Podręcznik PhishSpot

Przewodnik administratora

2026-06-02

Wprowadzenie

Witamy w PhishSpot, kompleksowej platformie do symulacji phishingu i szkoleń z zakresu świadomości bezpieczeństwa. Ten podręcznik obejmuje wszystkie funkcje dostępne dla administratorów konta. Został zaprojektowany dla użytkowników nietechnicznych i krok po kroku omawia każdą sekcję platformy. PhishSpot pozwala Twojej organizacji na przeprowadzanie realistycznych kampanii phishingowych, śledzenie reakcji pracowników, dostarczanie szkoleń ze świadomości bezpieczeństwa oraz mierzenie odporności Twojego zespołu na ataki socjotechniczne w czasie.

1.1 Czym jest PhishSpot?

PhishSpot to platforma SaaS, która pomaga organizacjom testować i ulepszać zdolność pracowników do rozpoznawania e-maili phishingowych. Jako administrator możesz tworzyć symulowane kampanie phishingowe, które naśladują rzeczywiste ataki, wysyłać je do swojego zespołu, a następnie śledzić, kto otworzył e-mail, kto kliknął link i kto podał poufne informacje na fałszywej stronie docelowej. Po kliknięciu pracownicy mogą zostać przekierowani na kurs szkoleniowy w celu poprawy ich świadomości.

1.2 Dla kogo jest ten podręcznik?

Ten podręcznik jest przeznaczony dla administratorów na poziomie konta. Jeśli masz rolę Administratora (Admin) w swoim zespole, masz pełny dostęp do wszystkich funkcji opisanych w tym przewodniku: zarządzania kampaniami, kontaktami, szablonami, domenami, kursami, członkami zespołu, raportami i ustawieniami konta.

1.3 Przegląd ról użytkowników

PhishSpot używa trzech ról użytkowników na każdym koncie. Twoja rola określa, co możesz zobaczyć i zrobić:

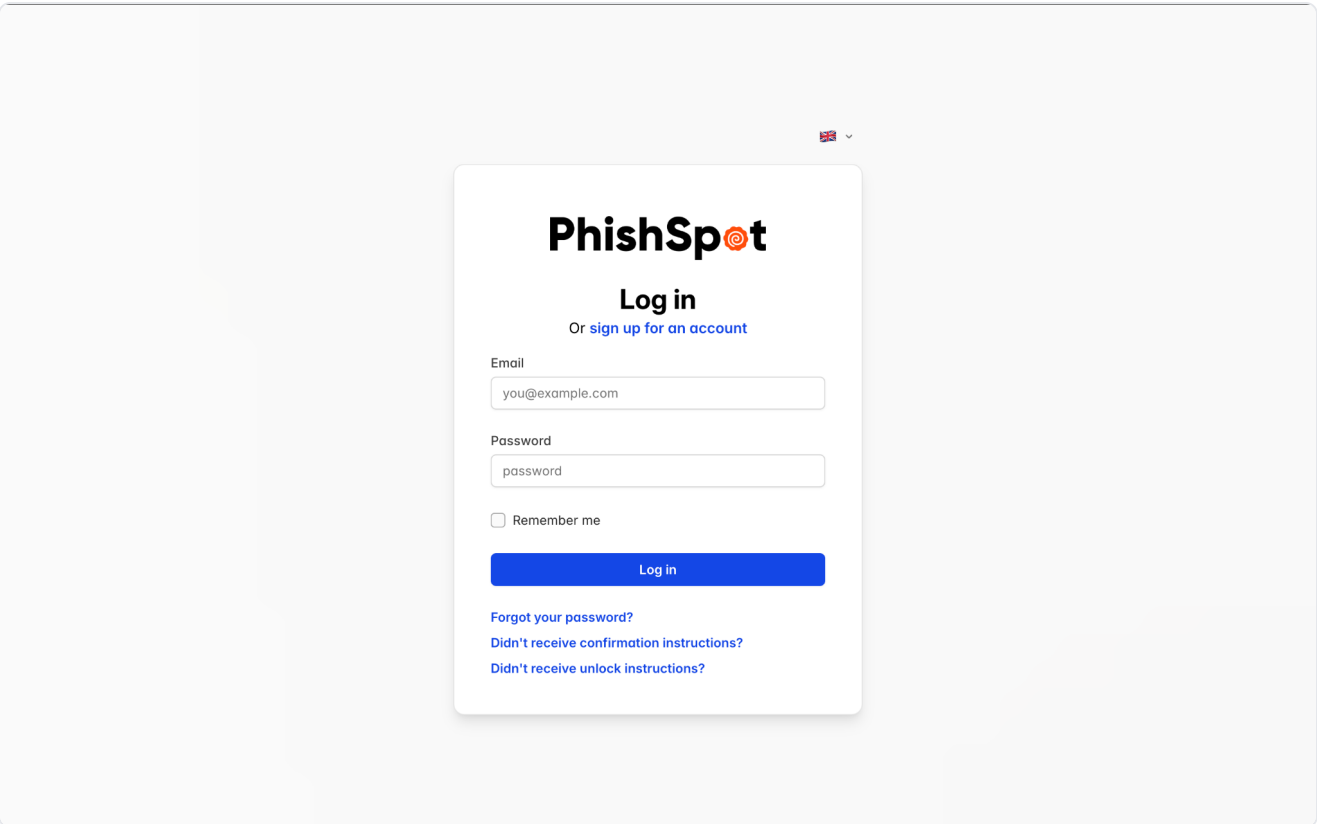
Rola	Poziom Dostępu	Kluczowe Uprawnienia
Admin	Pełny dostęp	Wszystko: kampanie, kontakty, szablony, zarządzanie zespołem, ustawienia konta, domeny, kursy, media, webhooki, raporty
Edytor	Dostęp do treści	Kampanie, kontakty, kursy, szablony, media, raporty. Nie może zarządzać członkami zespołu ani ustawieniami konta
Członek	Tylko do odczytu	Może przeglądać kampanie, kontakty i raporty, ale nie może niczego tworzyć ani modyfikować

Ten podręcznik skupia się wyłącznie na roli Administratora. Edytorzy i Członkowie zobaczą mniej elementów menu i przycisków akcji.

Rozpoczęcie Pracy

2.1 Logowanie

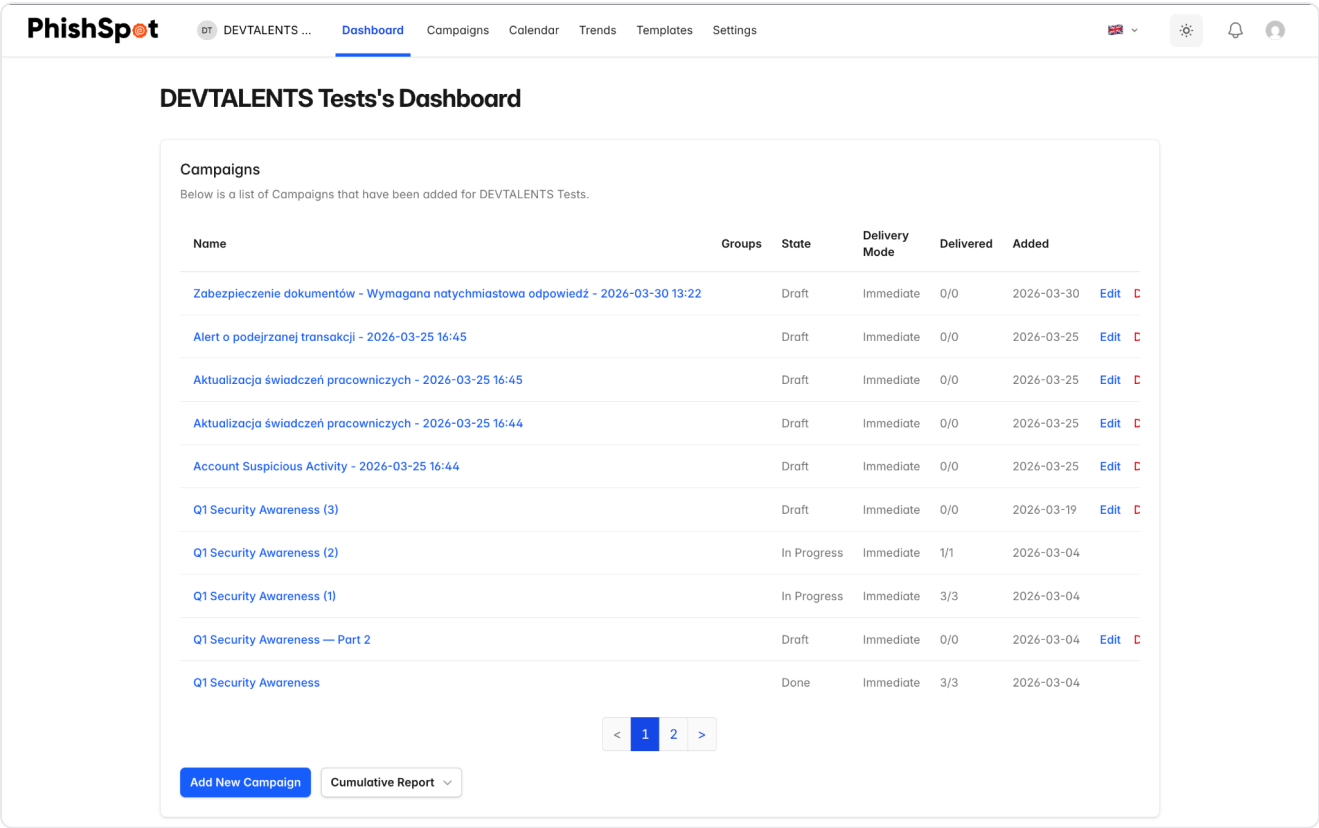
Przejdź do adresu URL platformy PhishSpot w swojej przeglądarce. Wprowadź swój adres e-mail i hasło na stronie logowania, a następnie kliknij przycisk Zaloguj się (Sign In). Jeśli Twoja organizacja włączyła uwierzytelnianie dwuskładnikowe (2FA), po wpisaniu hasła zostaniesz poproszony o wprowadzenie kodu weryfikacyjnego z aplikacji uwierzytelniającej.



2.2 Nawigacja po platformie

Po zalogowaniu zobaczysz główny pulpit nawigacyjny (Dashboard). Platforma wykorzystuje poziomy górny pasek nawigacyjny, który pojawia się na każdej stronie. Pasek nawigacyjny zawiera:

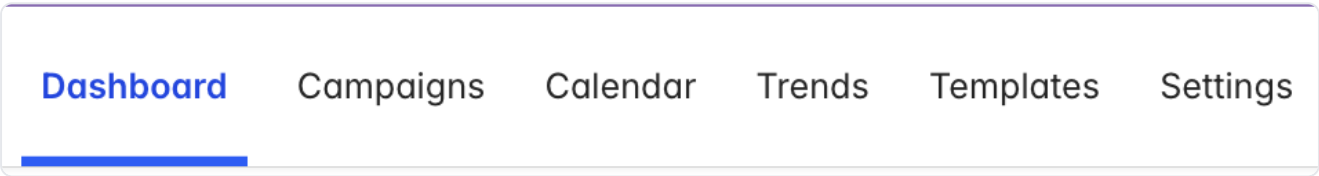
- **Lewa strona** — Logo PhishSpot (link do strony głównej) oraz przełącznik kont/zespołów (pokazuje nazwę Twojego obecnego zespołu).
- **Środek** — Główne linki nawigacyjne: Pulpit (Dashboard), Kampanie (Campaigns), Kalendarz (Calendar), Trendy (Trends), Szablony (Templates) i Ustawienia (Settings). Aktywna strona jest podświetlona niebieskim podkreśleniem.
- **Prawa strona** — Przełącznik języka (ikona flagi), przełącznik motywu (tryb jasny/ciemny), dzwonek powiadomień oraz awatar użytkownika/menu profilu.



2.3 Struktura Menu Nawigacyjnego

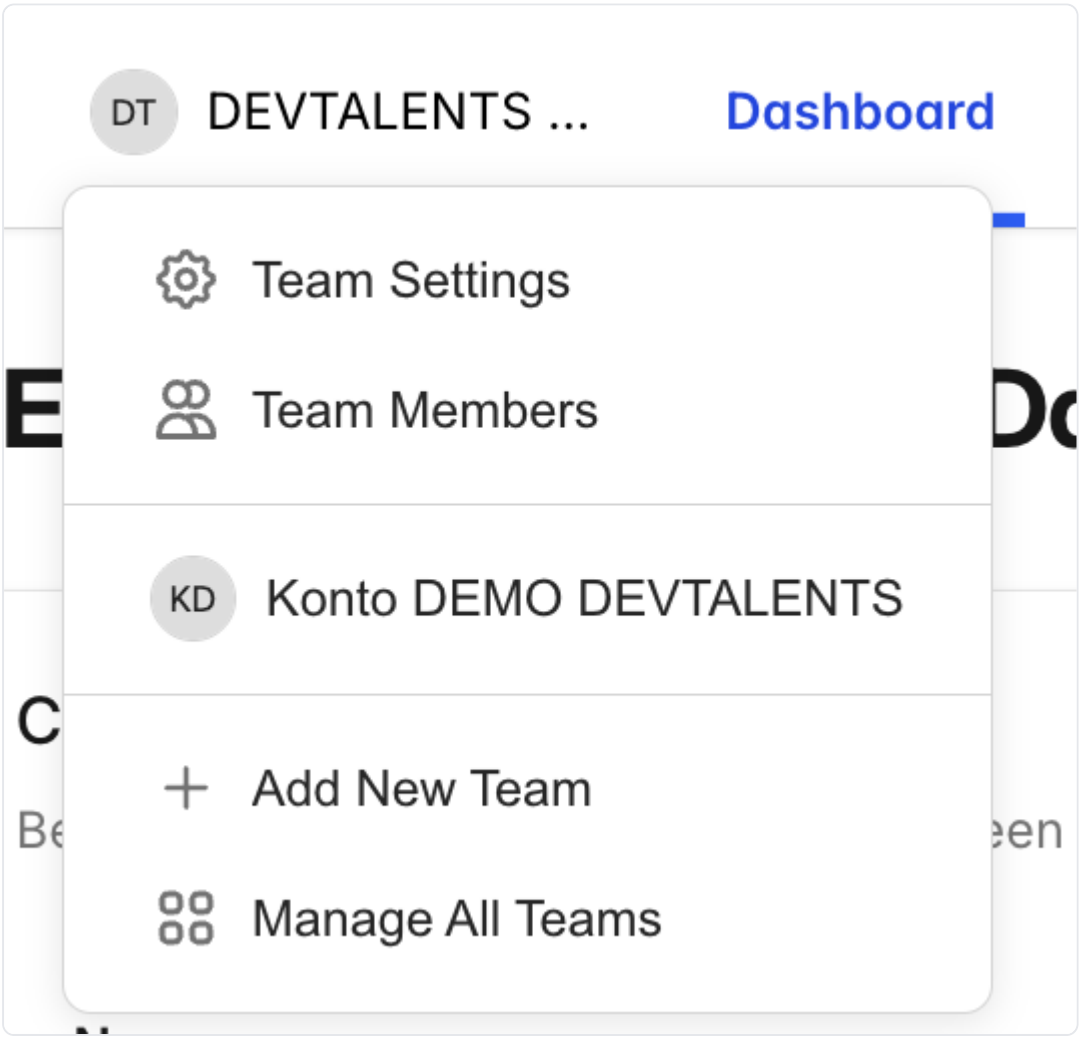
Górny pasek nawigacyjny zawiera następujące główne sekcje:

Pozycja Menu	Opis
Pulpit (Dashboard)	Przegląd Twojego konta z najnowszymi kampaniami i szybkimi statystykami
Kampanie (Campaigns)	Tworzenie, zarządzanie i monitorowanie kampanii symulujących phishing
Kalendarz Kampanii	Wizualny widok kalendarza zaplanowanych i przeszłych kampanii
Trendy (Trends)	Historyczne dane dotyczące trendów i analityka ze wszystkich kampanii
Szablony (Templates)	Przeglądanie wyselekcjonowanych szablonów phishingowych i zarządzanie własnymi szablonami
Ustawienia (Settings)	Rozwijana sekcja zawierająca: Kontakty, Grupy, Kursy, Media, Domeny, Domeny Platformy, Webhooki, Szczegóły Konta, Członkowie Zespołu



2.4 Przełączanie Kont

Jeśli należysz do wielu zespołów lub kont, możesz przełączać się między nimi za pomocą przełącznika kont na górze paska bocznego. Kliknij nazwę swojego obecnego konta, aby zobaczyć listę rozwijaną wszystkich kont, do których masz dostęp, a następnie wybierz to, na którym chcesz pracować.

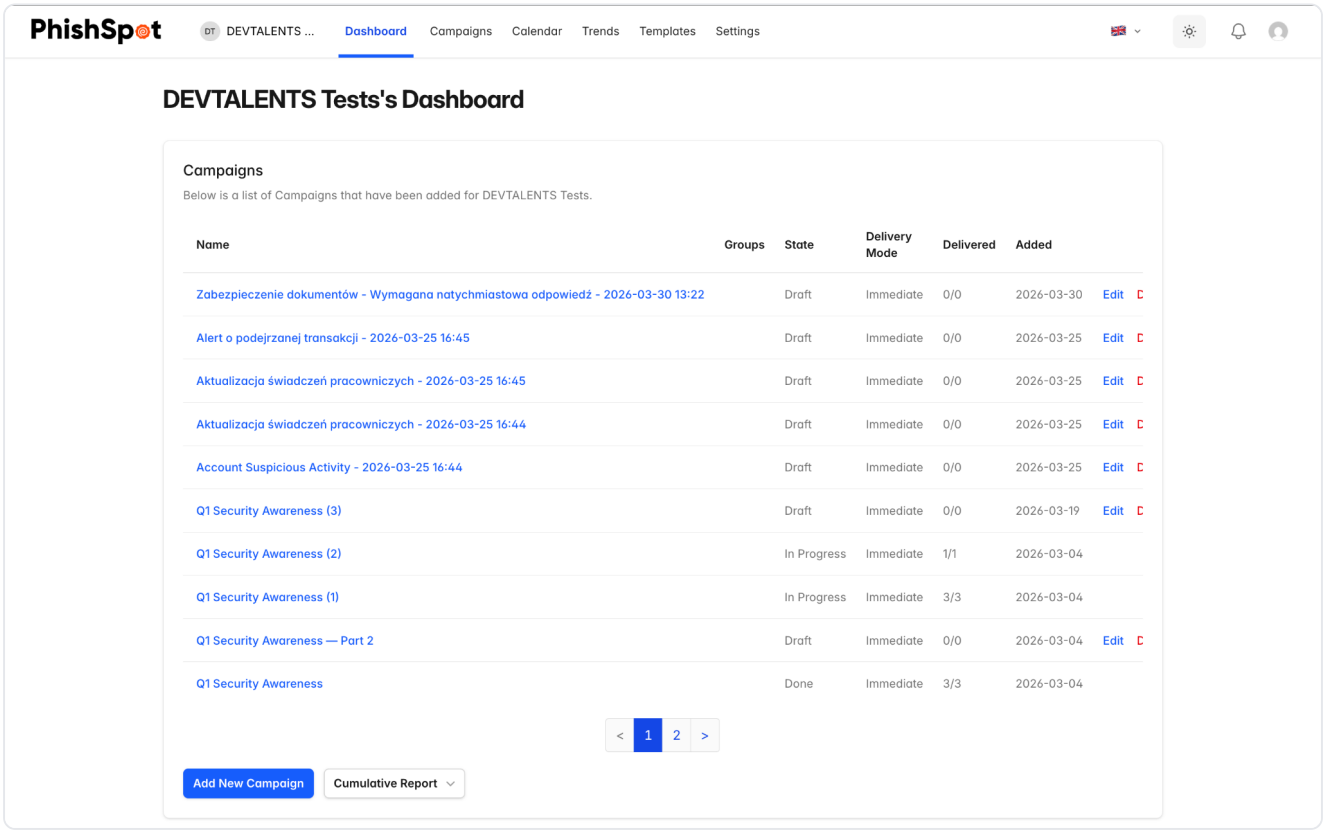


2.5 Powiadomienia

Dzwonek powiadomień w prawym górnym rogu pokazuje liczbę nieprzeczytanych powiadomień. Kliknij go, aby zobaczyć listę ostatnich zdarzeń, takich jak zakończenie kampanii, dołączenie nowych członków zespołu lub aktualizacje weryfikacji domeny. Każde powiadomienie jest linkiem do odpowiedniego elementu. Możesz oznaczyć wszystkie powiadomienia jako przeczytane za pomocą linku na górze panelu powiadomień.

Pulpit Nawigacyjny (Dashboard)

Pulpit nawigacyjny to Twój ekran główny po zalogowaniu. Zapewnia on ogólny przegląd aktywności na Twoim koncie.



3.1 Elementy pulpitu

Pulpit wyświetla:

- Podsumowanie Twoich ostatnich kampanii wraz z ich obecnym statusem (Szkic, Zaplanowane, Aktywne, Wstrzymane, Zakończone).
- Szybki dostęp do domen platformy przypisanych do Twojego konta.
- Przegląd Twojej biblioteki mediów.

Z poziomu pulpitu możesz szybko przejść do dowolnej kampanii klikając jej nazwę, lub utworzyć nową kampanię używając przycisku w sekcji kampanii.

Kampanie

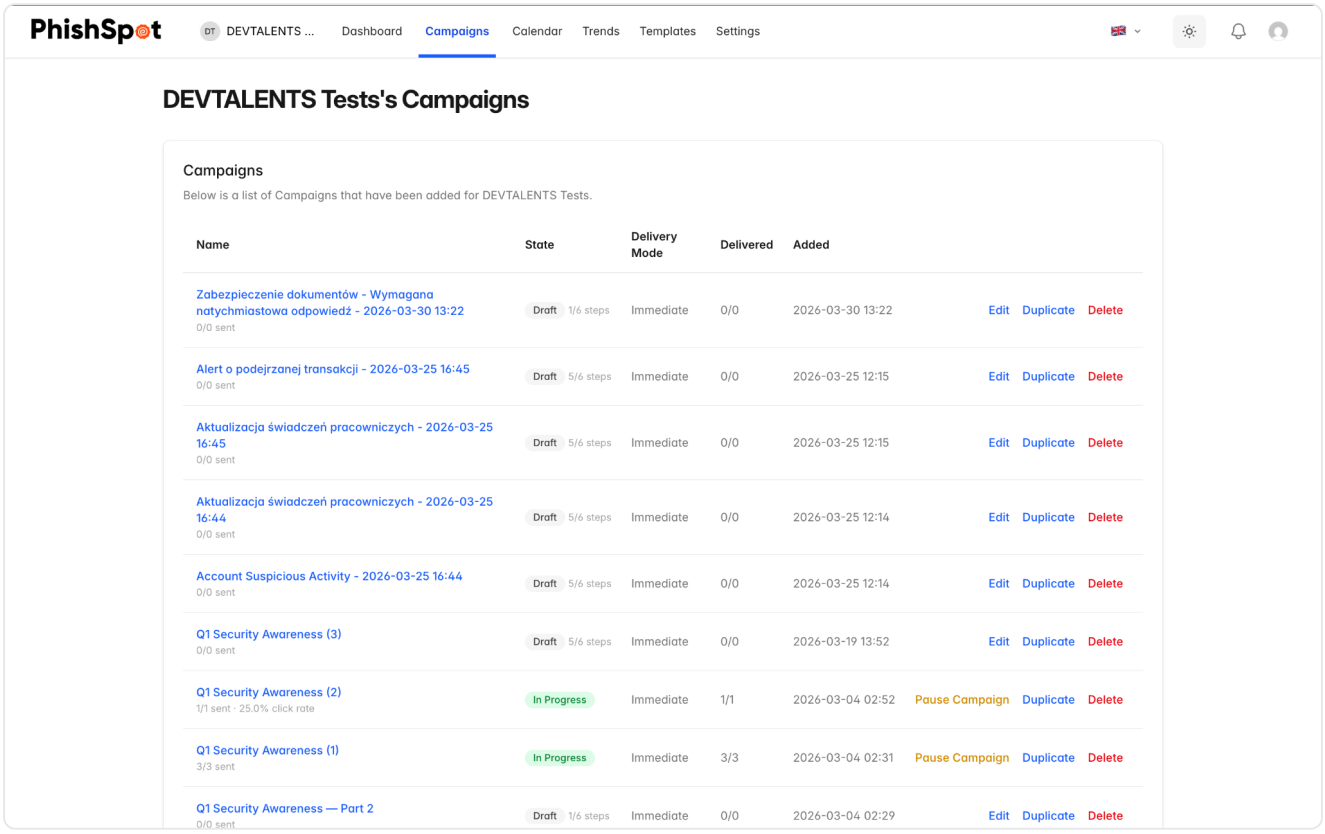
Kampanie stanowią rdzeń platformy PhishSpot. Kampania to symulowane ćwiczenie phishingowe, podczas którego wysyłasz spreprerowaną wiadomość e-mail do grupy kontaktów, udostępniasz fałszywą stronę docelową, aby przechwytywać interakcje, i opcjonalnie po kliknięciu przekierowujesz użytkowników na kurs szkoleniowy.

4.1 Lista Kampanii

Przejdź do zakładki Kampanie z paska bocznego, aby zobaczyć wszystkie kampanie na swoim koncie. Lista wyświetla:

Kolumna	Opis
Nazwa (Name)	Nazwa kampanii (klikalna, aby zobaczyć szczegóły)
Status (State)	Aktualny status: Szkic, Zaplanowana, Aktywna, Wstrzymana lub Zakończona
Tryb Dostawy	Sposób wysyłania e-maili: Natychmiastowy, Zaplanowany lub Rozłożony w czasie
Dostarczono	Liczba wysłanych e-maili w stosunku do wszystkich odbiorców
Utworzono	Kiedy kampania została utworzona
Akcje (Actions)	Przyciski Edytuj, Duplikuj i Usuń

Z tej strony możesz również wygenerować raport zbiorczy (Cumulative Report) w formacie PDF, który łączy dane z wielu kampanii.



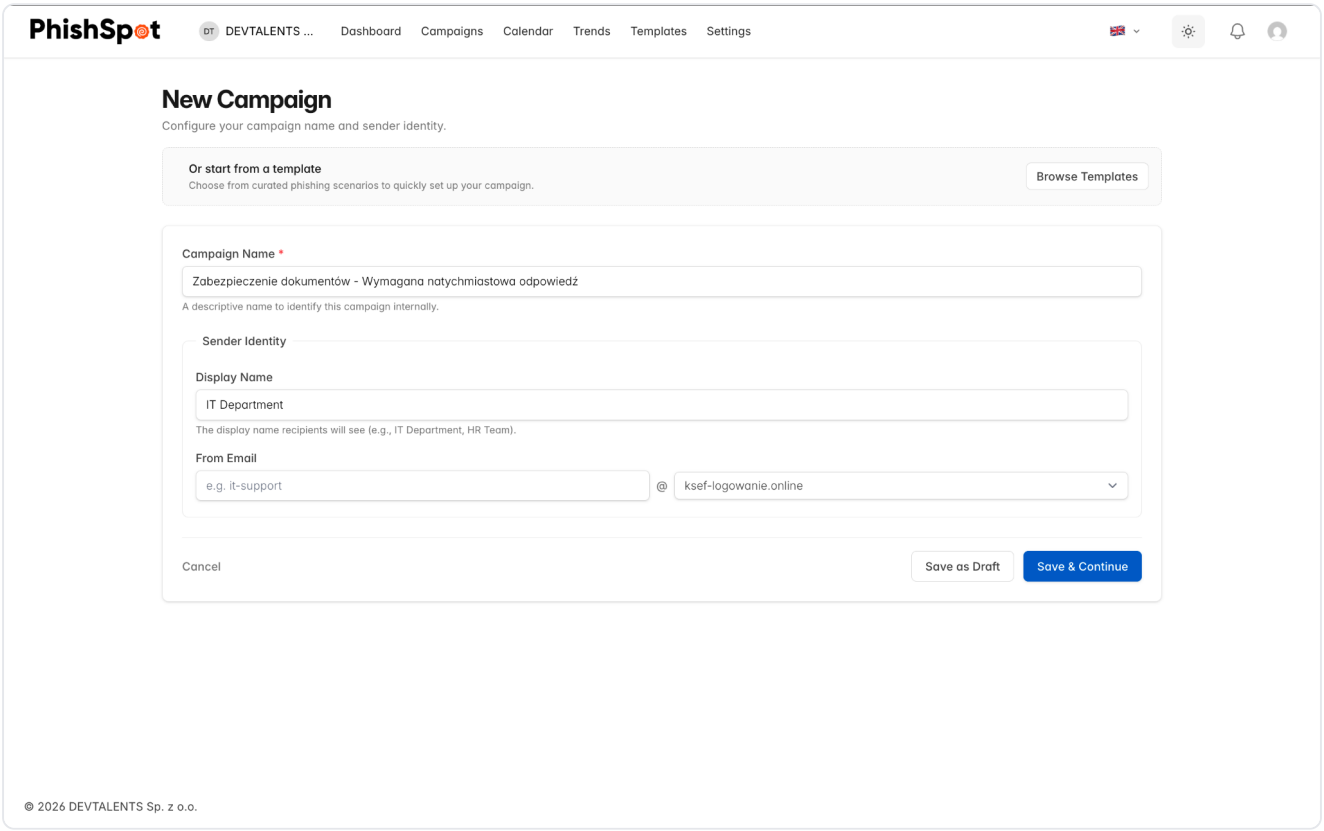
4.2 Tworzenie nowej kampanii

Kliknij przycisk Nowa Kampania (New Campaign), aby uruchomić kreator. Kreator przeprowadzi Cię przez sześć kroków:

Krok 1: Ustawienia (Settings)

Skonfiguruj podstawowe parametry kampanii:

- **Nazwa kampanii** — Nadaj kampanii opisową nazwę.
- **Tożsamość nadawcy** — Podaj nazwę wyświetlaną i adres e-mail nadawcy.
- **Nazwa wyświetlana** — Podaj nazwę wyświetlaną.
- **Adres e-mail nadawcy** — Podaj nazwę użytkownika e-mail i wybierz domenę.

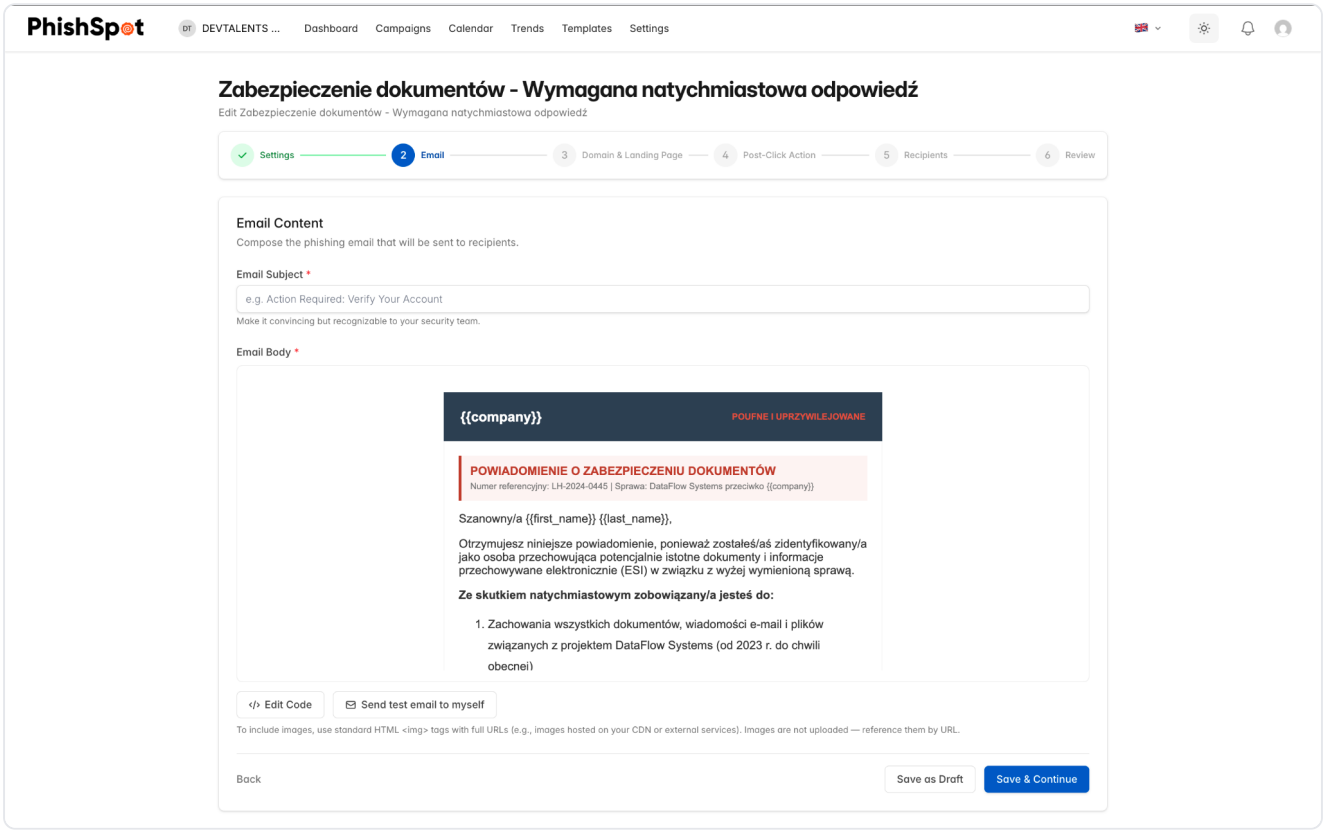


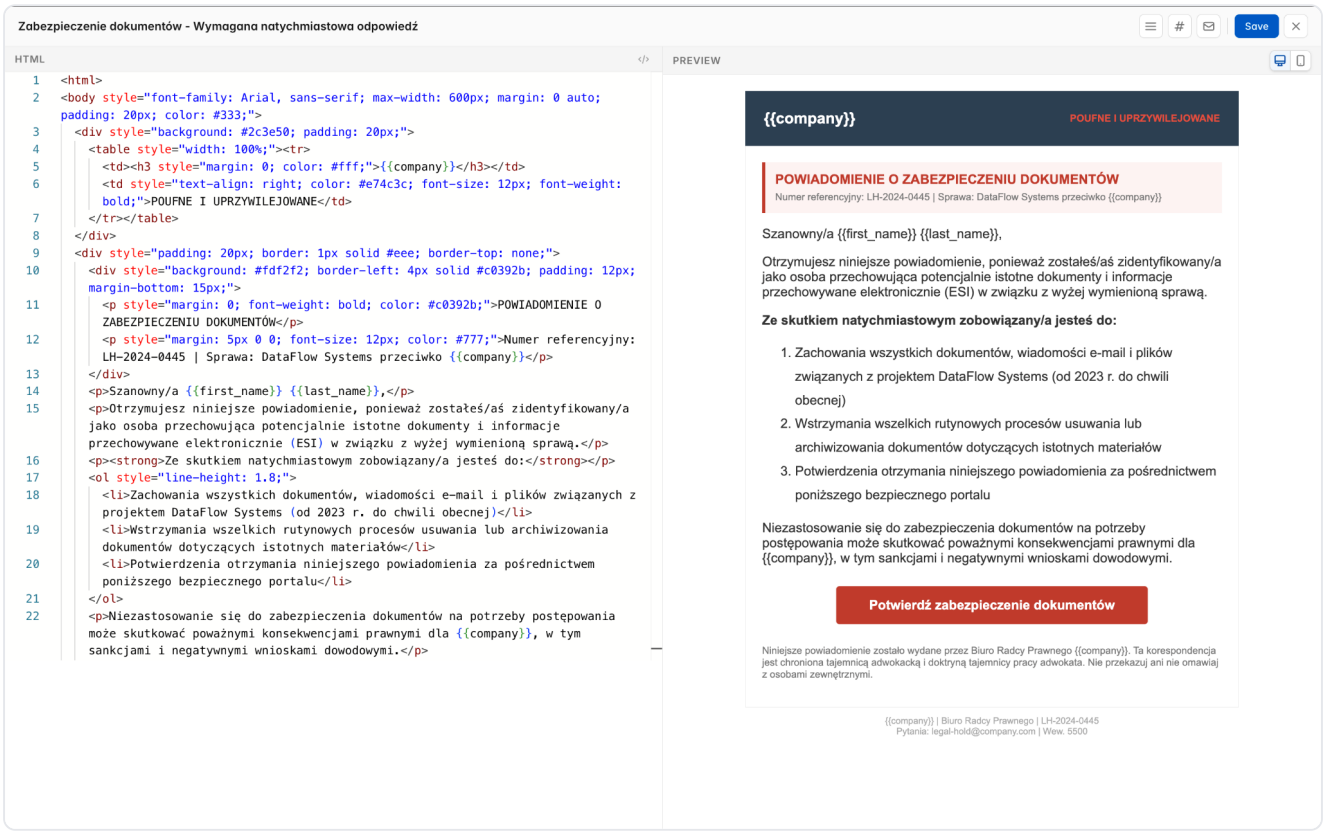
Krok 2: Treść E-maila (Email Content)

Zaprojektuj e-mail phishingowy, który otrzymają Twoje cele:

- **Temat E-maila** — Temat wiadomości phishingowej.
- **Treść E-maila** — Treść HTML wiadomości. Kliknij przycisk Edytuj Kod, aby otworzyć edytor kodu Monaco, gdzie możesz wpisać lub wkleić kod HTML.
- Edytor zapewnia podświetlanie składni i podgląd na żywo.
- Możesz używać zmiennych szablonu zarówno w temacie, jak i w treści, aby spersonalizować wiadomości. Popularne zmienne obejmują imię, nazwisko i adres e-mail odbiorcy.

> Zawsze wysyłaj do siebie e-mail testowy przed uruchomieniem kampanii, aby sprawdzić, czy formatowanie i linki działają poprawnie.



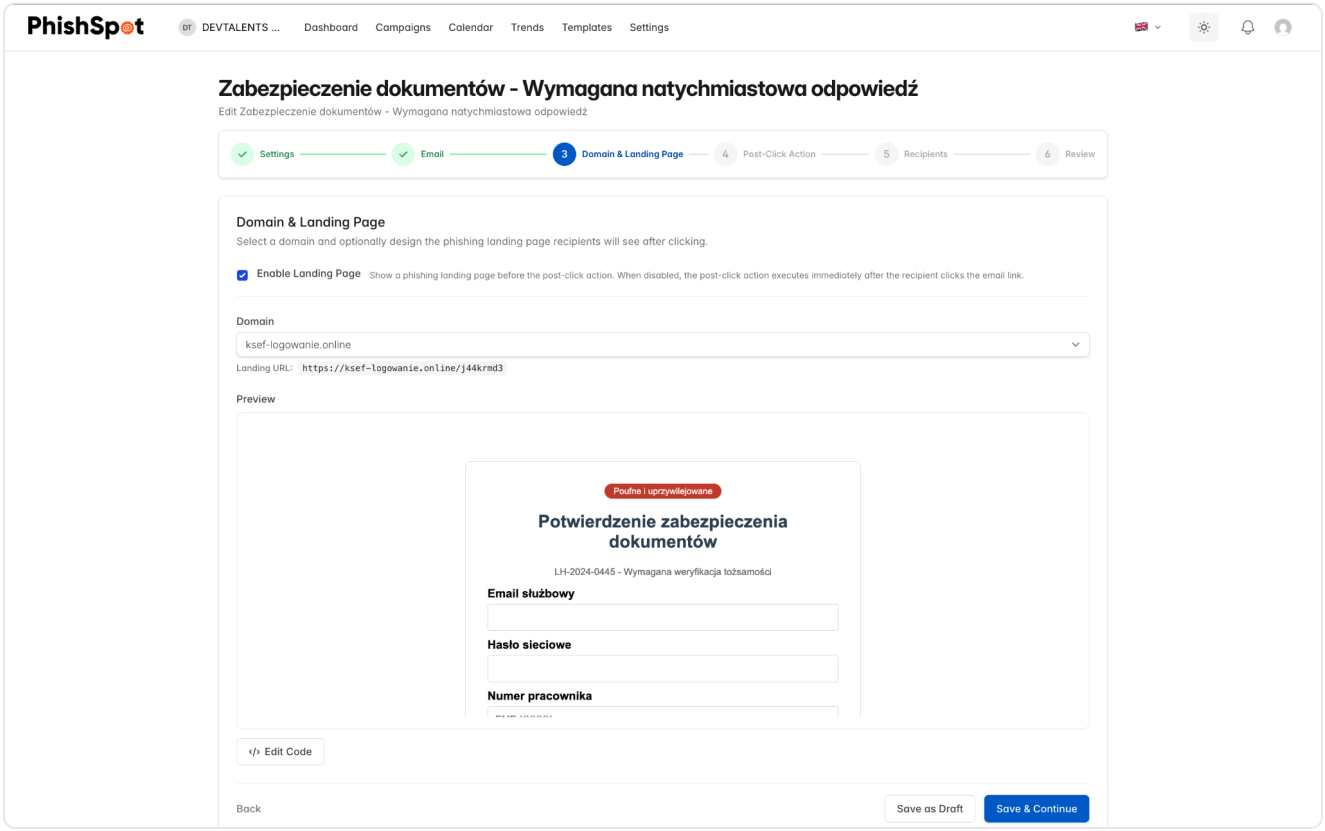


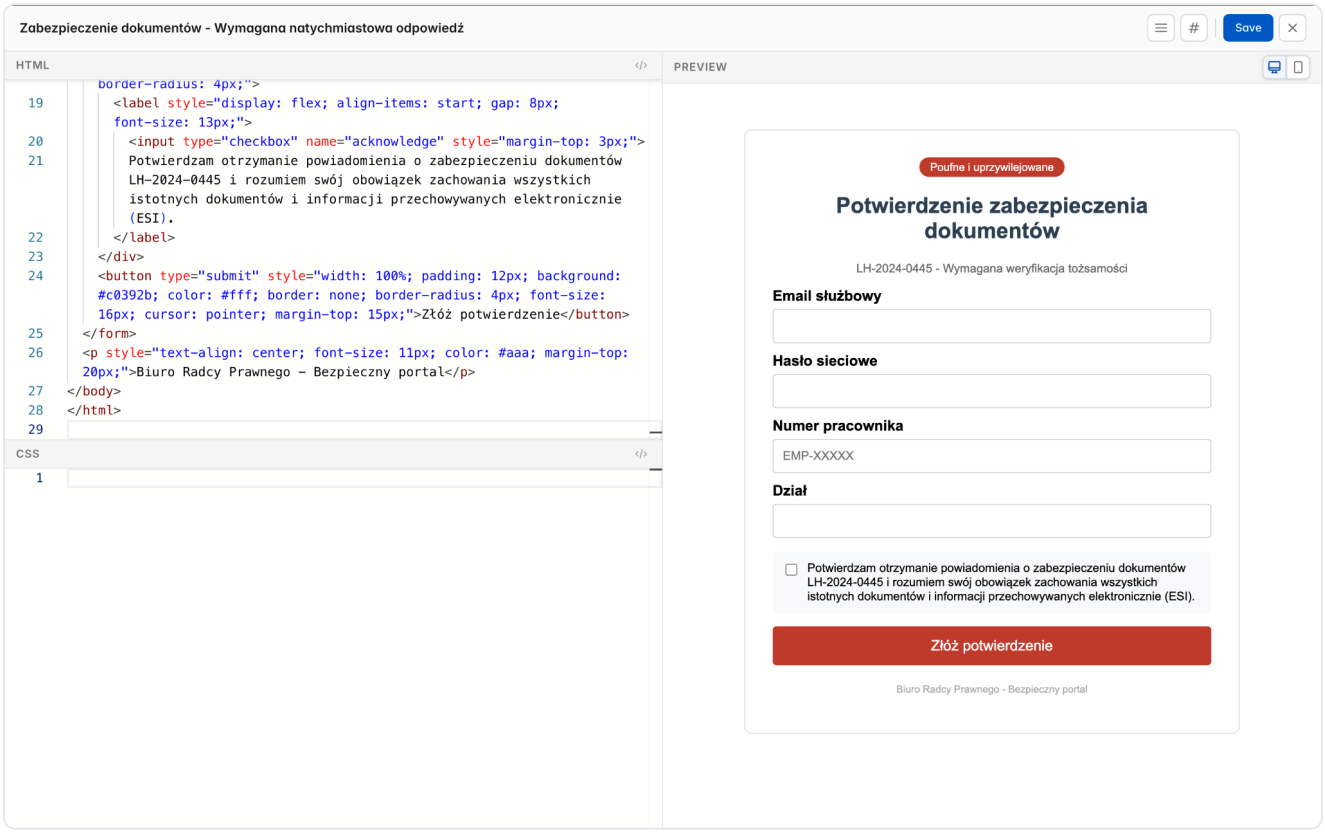
> Zawsze wyślij testowy e-mail do siebie przed uruchomieniem kampanii, aby sprawdzić, czy formatowanie i linki działają poprawnie.

Krok 3: Strona Docelowa (Landing Page)

Skonfiguruj fałszywą stronę docelową, którą zobaczą odbiorcy po kliknięciu linku:

- **Domena Platformy** — Wybierz domenę dla adresu URL swojej strony docelowej.
- **Treść Strony Docelowej** — Edytuj kod HTML strony docelowej za pomocą edytora wizualnego. To jest strona, która naśladuje autentyczny formularz logowania lub coś podobnego.
- **Włącz/Wyłącz Stronę Docelową** — Możesz wybrać śledzenie wyłącznie kliknięć, bez hostowania strony docelowej.

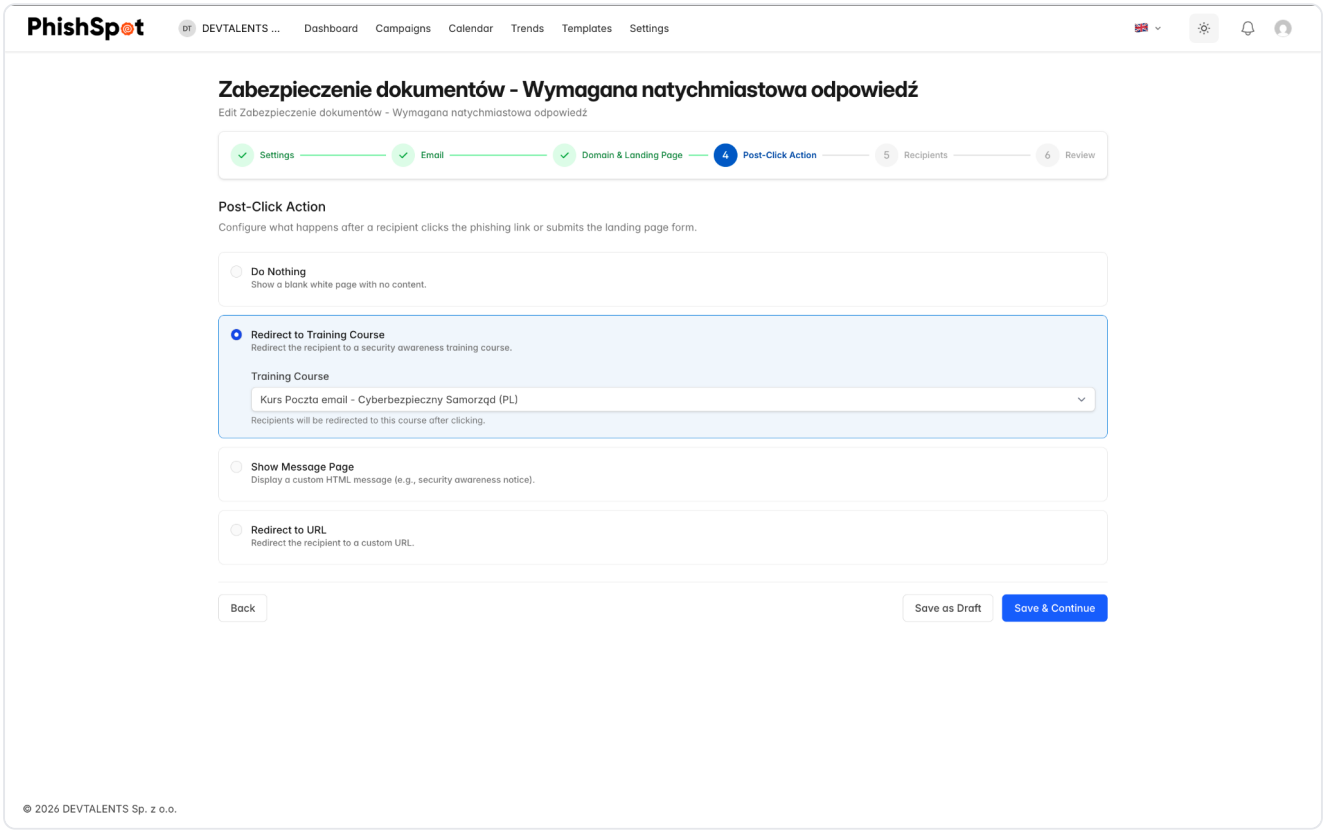




Krok 4: Akcja Po Kliknięciu (Post-Click Action)

Określ, co się stanie po wejściu przez odbiorcę w interakcję ze stroną docelową:

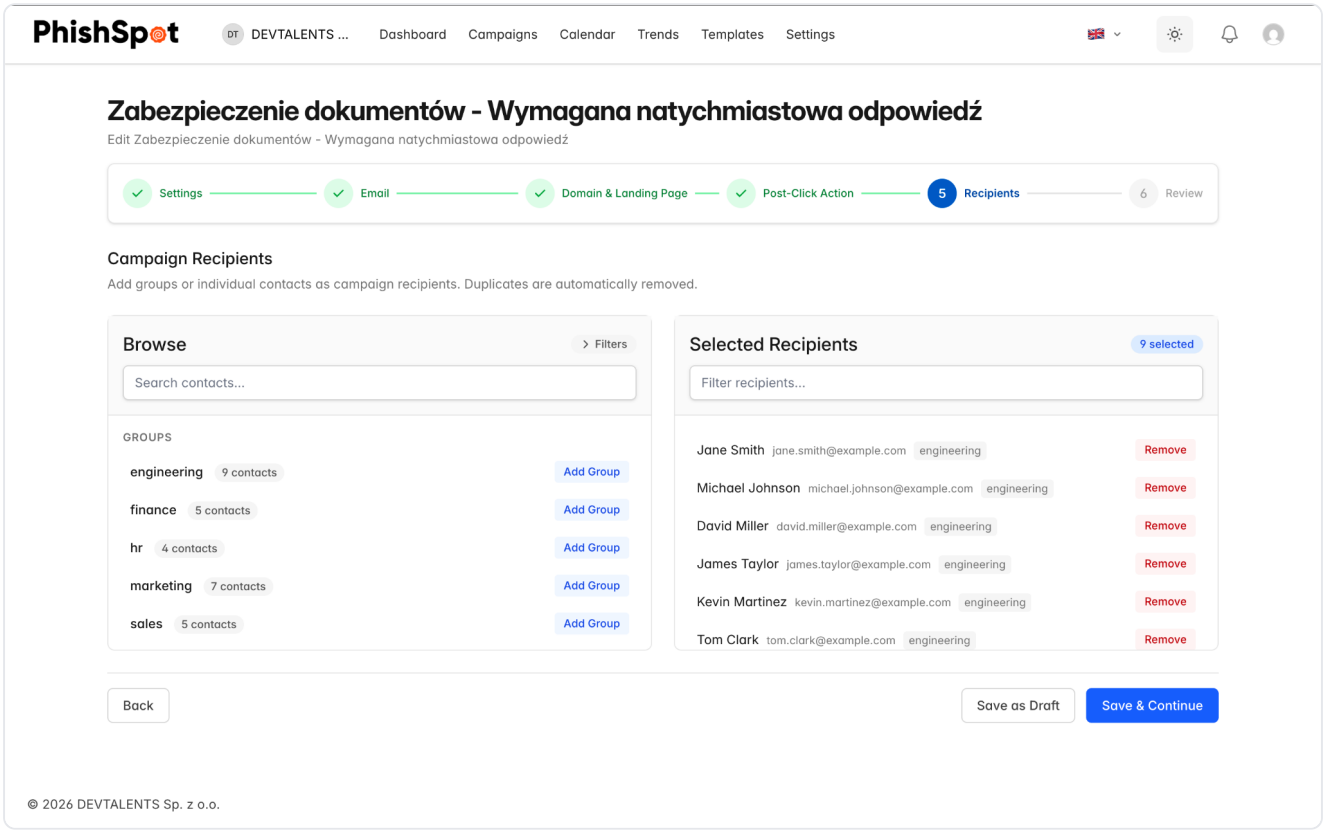
- **Kurs Szkoleniowy** — Przypisz kurs świadomości bezpieczeństwa, na który użytkownik zostanie przekierowany po kliknięciu lub przesłaniu danych.
- **Niestandardowy adres URL przekierowania** — Zamiast tego przekieruj użytkownika na określony adres URL.
- **Strona Świadomości** — Wyświetl wbudowaną wiadomość uświadamiającą, wyjaśniającą, że była to symulacja.



Krok 5: Odbiorcy (Recipients)

Wybierz, kto otrzyma e-maile z kampanii:

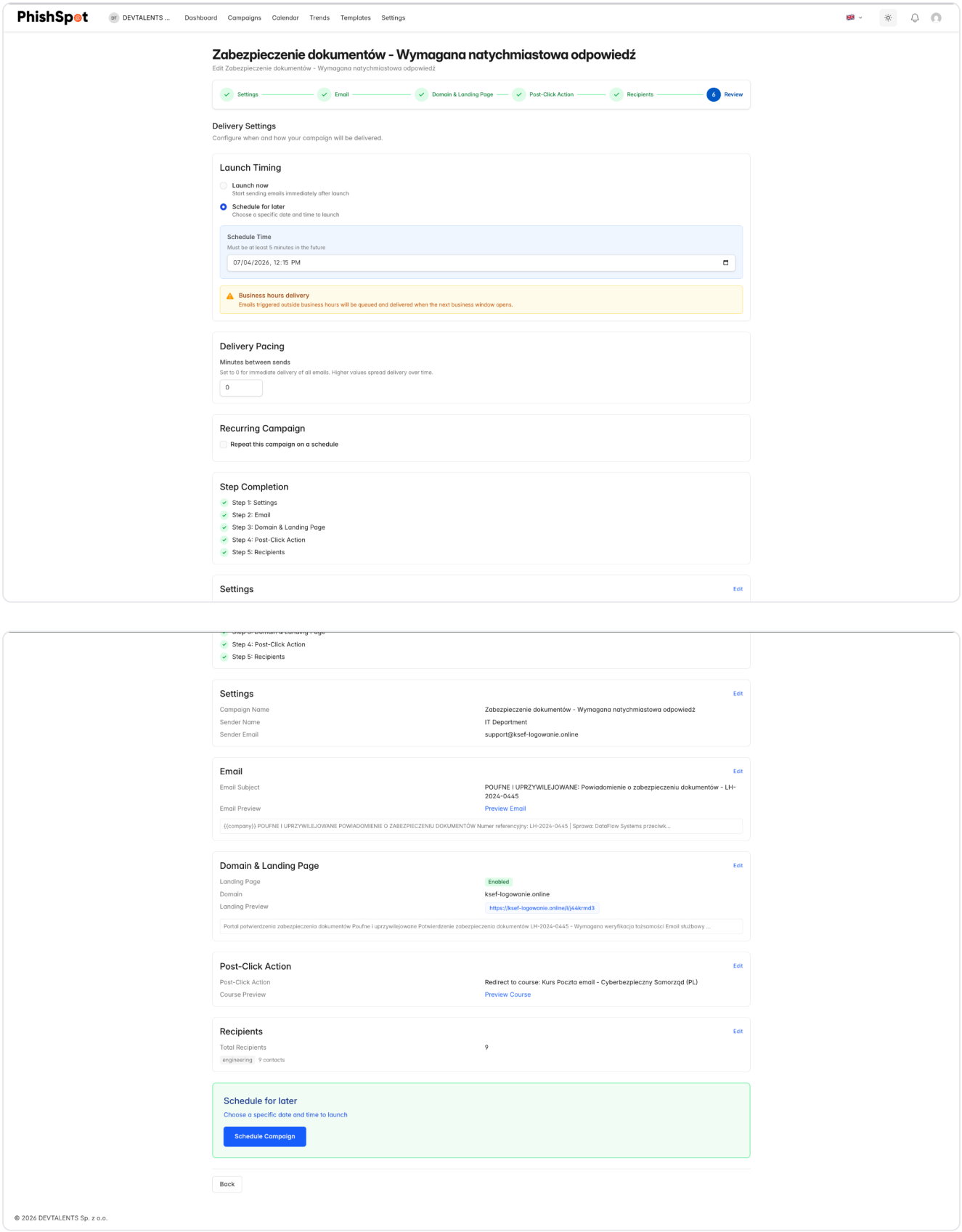
- Przeszukaj swoje kontakty i dodaj poszczególne osoby lub całe grupy.
- Przejrzyj wybraną listę odbiorców.
- W razie potrzeby usuń określone kontakty.
- Wyszukiwarka kontaktów obsługuje wyszukiwanie i filtrowanie według działu, stanowiska i lokalizacji.



Krok 6: Przegląd i Uruchomienie (Review & Launch)

Przejrzyj wszystkie ustawienia kampanii przed uruchomieniem:

- Podsumowanie treści e-maila, strony docelowej, odbiorców i ustawień dostawy.
- Ostateczne potwierdzenie przed rozpoczęciem kampanii.
- Opcja zapisania jako szkic i uruchomienia później.



4.3 Statusy Kampanii

Kampania przechodzi przez następujące statusy podczas swojego cyklu życia:

Status	Znaczenie	Dostępne akcje
Szkic (Draft)	Kampania jest konfigurowana i nie została wysłana	Edytuj, Uruchom, Zaplanuj, Usuń
Zaplanowana (Scheduled)	Kampania jest ustawiona na uruchomienie w przyszłej dacie/ czasie	Edytuj, Zmień Harmonogram, Anuluj Harmonogram, Usuń
Aktywna (Active)	Kampania aktualnie wysyła lub wysłała już e-maile	Wstrzymaj, Zatrzymaj, Wyświetl Pulpit
Wstrzymana (Paused)	Wysyłanie kampanii jest tymczasowo wstrzymane	Wznów (Uruchom), Zatrzymaj
Zakończona (Done)	Wszystkie e-maile zostały dostarczone, a śledzenie jest zakończone	Wyświetl Pulpit, Eksportuj Raporty, Duplikuj

4.4 Akcje Kampanii

Ze strony szczegółów kampanii masz dostęp do kilku akcji w zależności od jej aktualnego statusu:

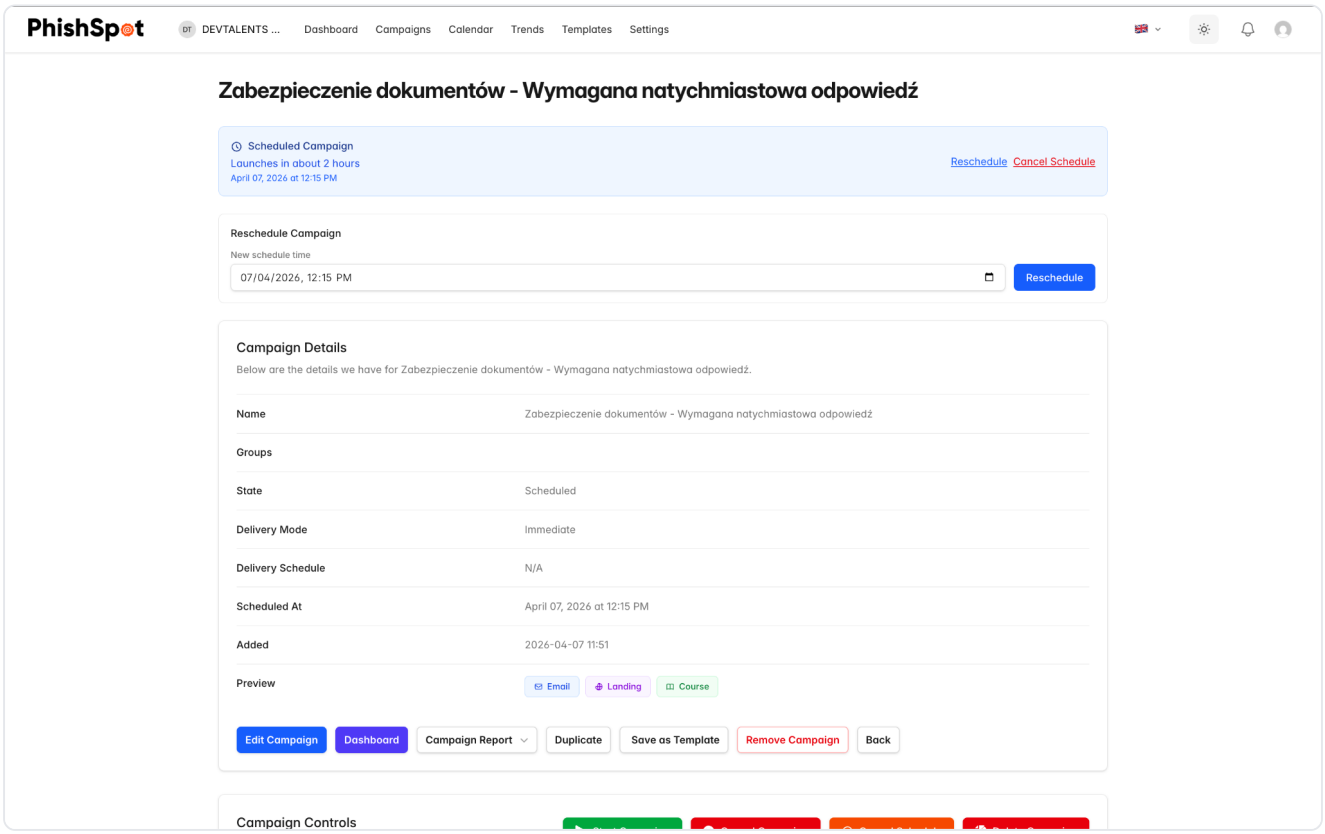
- **Uruchom (Start)** — Natychmiast rozpocznij wysyłanie kampanii.
- **Wstrzymaj (Pause)** — Tymczasowo wstrzymaj dostarczanie e-maili (można wznowić).
- **Zatrzymaj (Stop)** — Trwale zatrzymaj kampanię. Pozostałe, niewysłane e-maile nie zostaną dostarczone.
- **Zaplanuj / Zmień harmonogram** — Ustaw lub zmień przyszłą datę dostawy.
- **Duplikuj (Duplicate)** — Utwórz kopię kampanii jako nowy szkic.
- **Zapisz jako Szablon** — Zapisz aktualną treść wiadomości e-mail jako szablon phishingowy do ponownego użycia.
- **Wyślij E-mail Testowy** — Wyślij testową wersję e-maila do siebie, aby zweryfikować formatowanie.
- **Eksportuj Raport** — Pobierz wyniki kampanii w formacie PDF lub Excel.

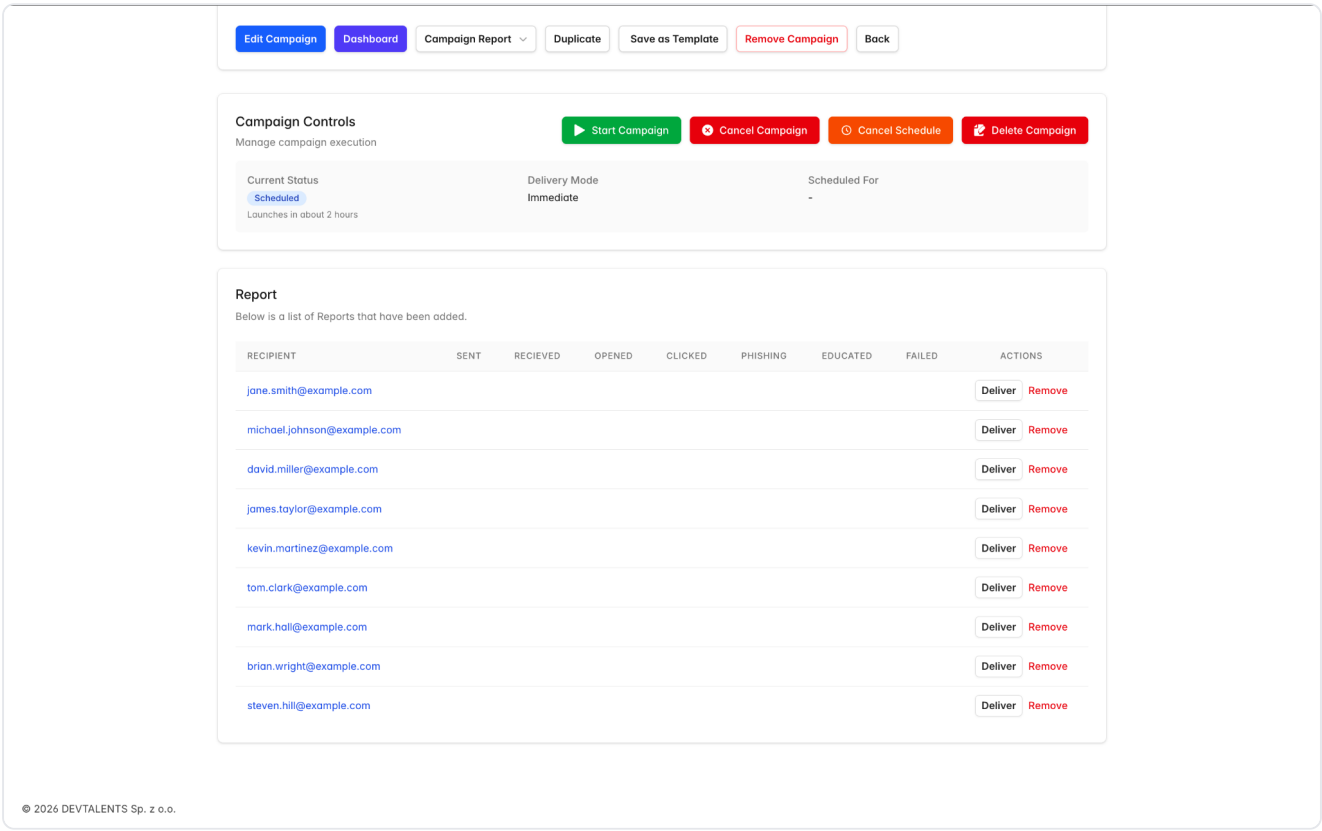
4.5 Pulpit Kampanii

Po aktywacji lub zakończeniu kampanii możesz uzyskać dostęp do jej pulpitu nawigacyjnego, aby uzyskać szczegółową analitykę. Pulpit kampanii zawiera:

- **Wykres lejka** — Wizualny lejek pokazujący status: Wysłane → Dostarczone → Otwarte → Kliknięte → Przesłane, z procentami konwersji na każdym etapie.
- **Podział na grupy** — Metryki wydajności w podziale na grupy kontaktów.

- **Podział na działy** — Metryki wydajności w podziale na działy.
- **Tabela odbiorców** — Lista każdego odbiorcy z jego indywidualnym statusem (wysłane, dostarczone, otwarte, kliknięte, przesłane).
- **Oś czasu odbiorcy** — Kliknij na dowolnego odbiorcę, aby otworzyć panel boczny pokazujący pełną oś czasu zdarzeń (kiedy e-mail został wysłany, otwarty, link kliknięty, strona odwiedzona, dane przesłane, kurs rozpoczęty/zakończony).
- **Eksport CSV** — Pobierz pełne dane odbiorców jako plik CSV do dalszej analizy.





4.6 Kampanie Cykliczne

PhishSpot obsługuje kampanie cykliczne, które automatycznie powtarzają się w określonych odstępach. Podczas konfigurowania zaplanowanej kampanii włącz checkbox **Powtarzaj** w kroku harmonogramu i ustaw dwie wartości:

- **Interwał** — liczba (np. `1`, `2`, `4`).
- **Jednostka** — `dni`, `tygodnie` lub `miesiące`.

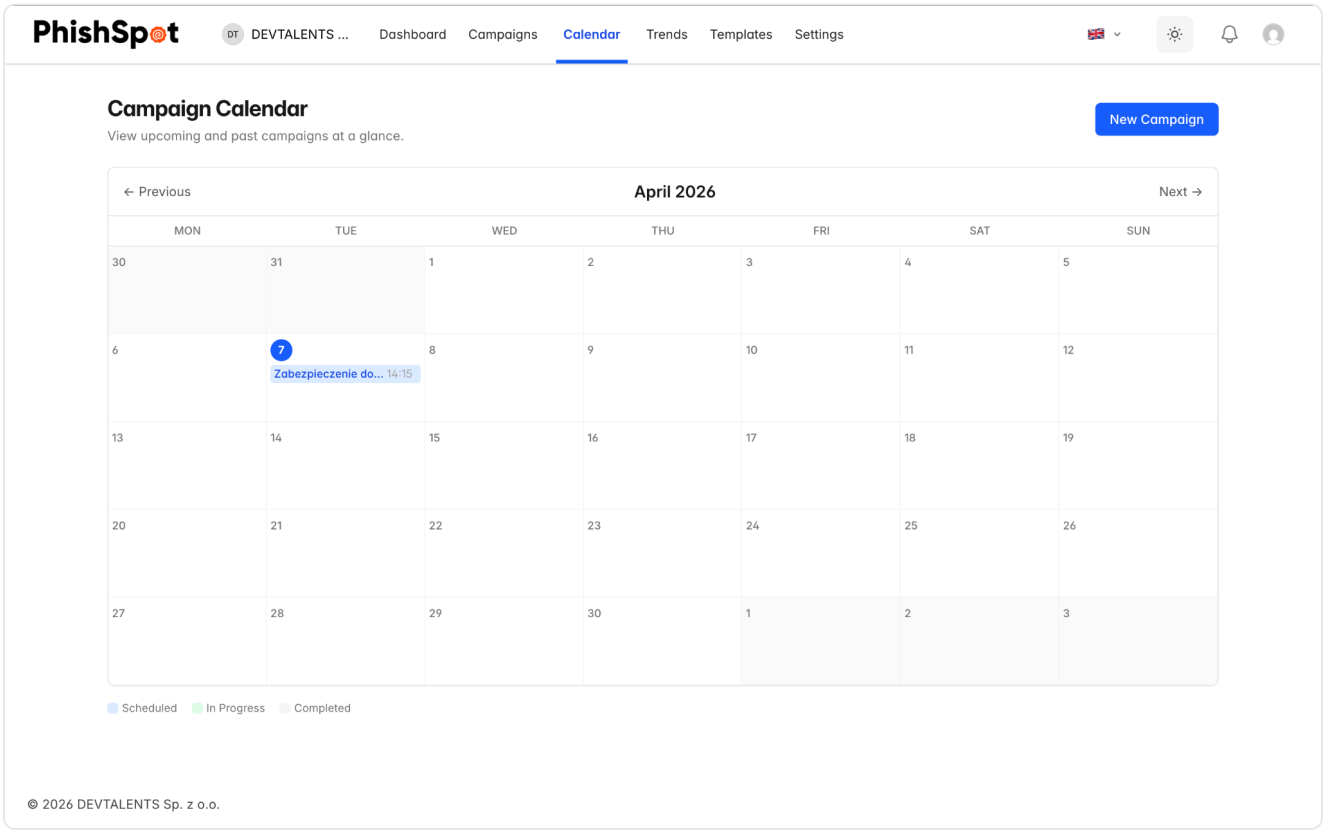
Czyli `1 tydzień` uruchamia kampanię co siedem dni; `2 miesiące` co dwa miesiące. Każde powtórzenie tworzy **kampanię podrzędną** połączoną z oryginalną nadrzędną — nadrzędna pozostaje kanonicznym wzorcem (jej treść, odbiorcy i finał po kliknięciu są zrzucane do każdego dziecka w momencie uruchomienia), a dzieci niosą własne raporty. Edycje nadrzędnej wpływają tylko na przyszłe powtórzenia; uruchomione dzieci zachowują konfigurację, z którą wystartowały.

Aby zatrzymać serię cykliczną, otwórz nadrzędną i ją anuluj — to powstrzymuje tworzenie kolejnych dzieci. Już uruchomione dzieci dalej idą niezależnie do końca.

> Jeśli Twoim celem jest ciągły program uświadamiający, a nie ściśle harmonogramowana wysyłka, rozważ **autopilot** zamiast tego — patrz Rozdział 23 Autopiloty. Autopiloty dostosowują dobór szablonów per odbiorca i automatycznie wciągają nowe kontakty — czego kampania cykliczna nie robi.

4.7 Kalendarz Kampanii

Kalendarz Kampanii udostępnia wizualny widok kalendarza dla wszystkich zaplanowanych i przeszłych kampanii. Możesz nawigować między miesiącami i klikać na dowolny wpis kampanii, aby przejść bezpośrednio na jej stronę szczegółów. Jest to przydatne do planowania programu phishingowego i unikania konfliktów w harmonogramie.



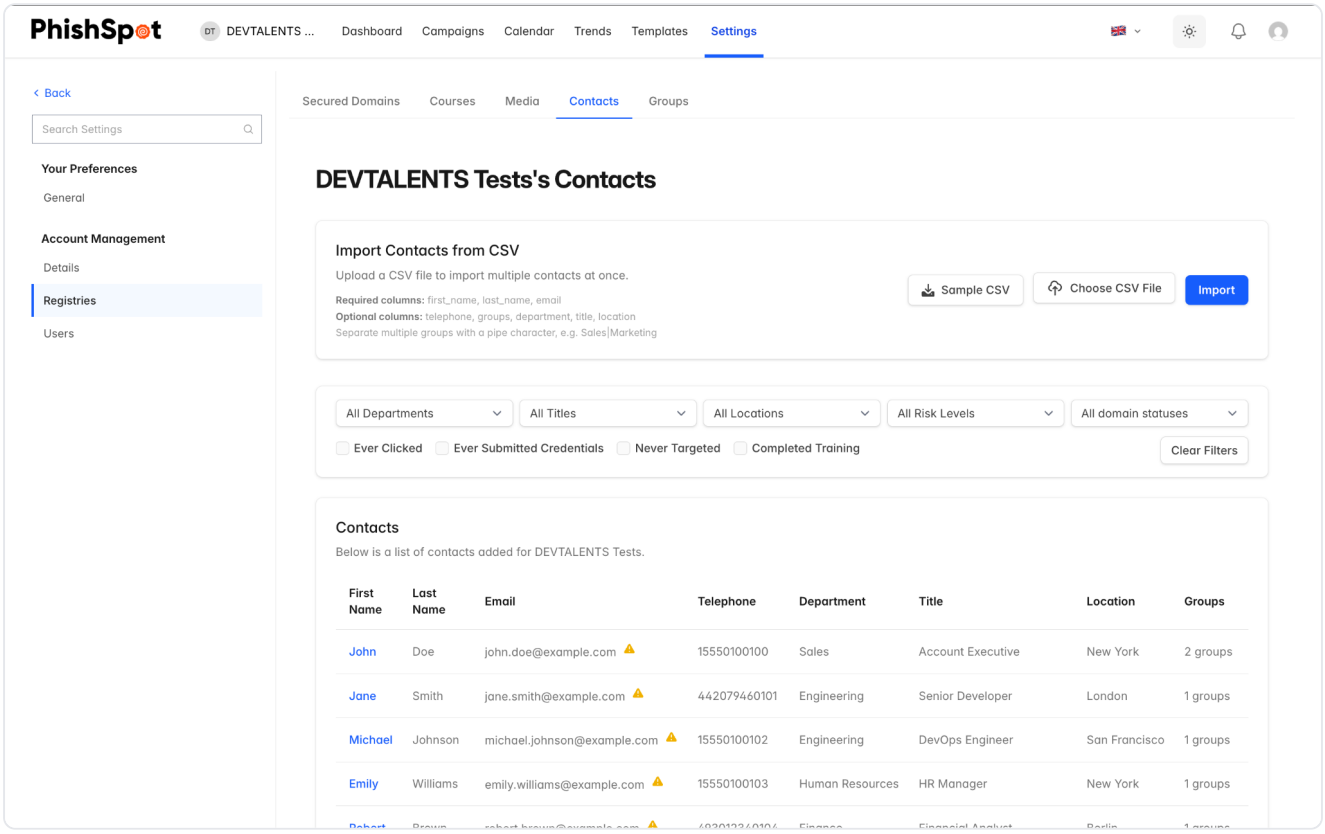
Kontakty

Kontakty to osoby w Twojej organizacji, które otrzymują e-maile symulujące phishing. Dokładne zarządzanie kontaktami jest kluczowe dla prowadzenia skutecznych kampanii.

5.1 Lista Kontaktów

Przejdź do Ustawienia → Kontakty na pasku bocznym. Lista kontaktów wyświetla wszystkie kontakty na Twoim koncie z następującymi kolumnami:

Kolumna	Opis
Imię	Imię kontaktu (klikalne, aby zobaczyć szczegóły)
Nazwisko	Nazwisko kontaktu
E-mail	Adres e-mail (z ikoną ostrzeżenia, jeśli domena nie jest zweryfikowana)
Telefon	Numer telefonu (opcjonalnie)
Dział (Department)	Dział, do którego należy kontakt
Stanowisko (Title)	Stanowisko pracy
Lokalizacja (Location)	Biuro lub lokalizacja
Grupy	Liczba grup, do których należy kontakt
Ocena Ryzyka	Ocena ryzyka oznaczona kolorami (zielony = niskie, żółty = średnie, pomarańczowy = wysokie, czerwony = krytyczne)
Wydajność (Performance)	Współczynnik klikalności: w ile kampanii kliknęli vs. w ilu byli celem
Utworzono	Kiedy kontakt został dodany



5.2 Filtrowanie Kontaktów

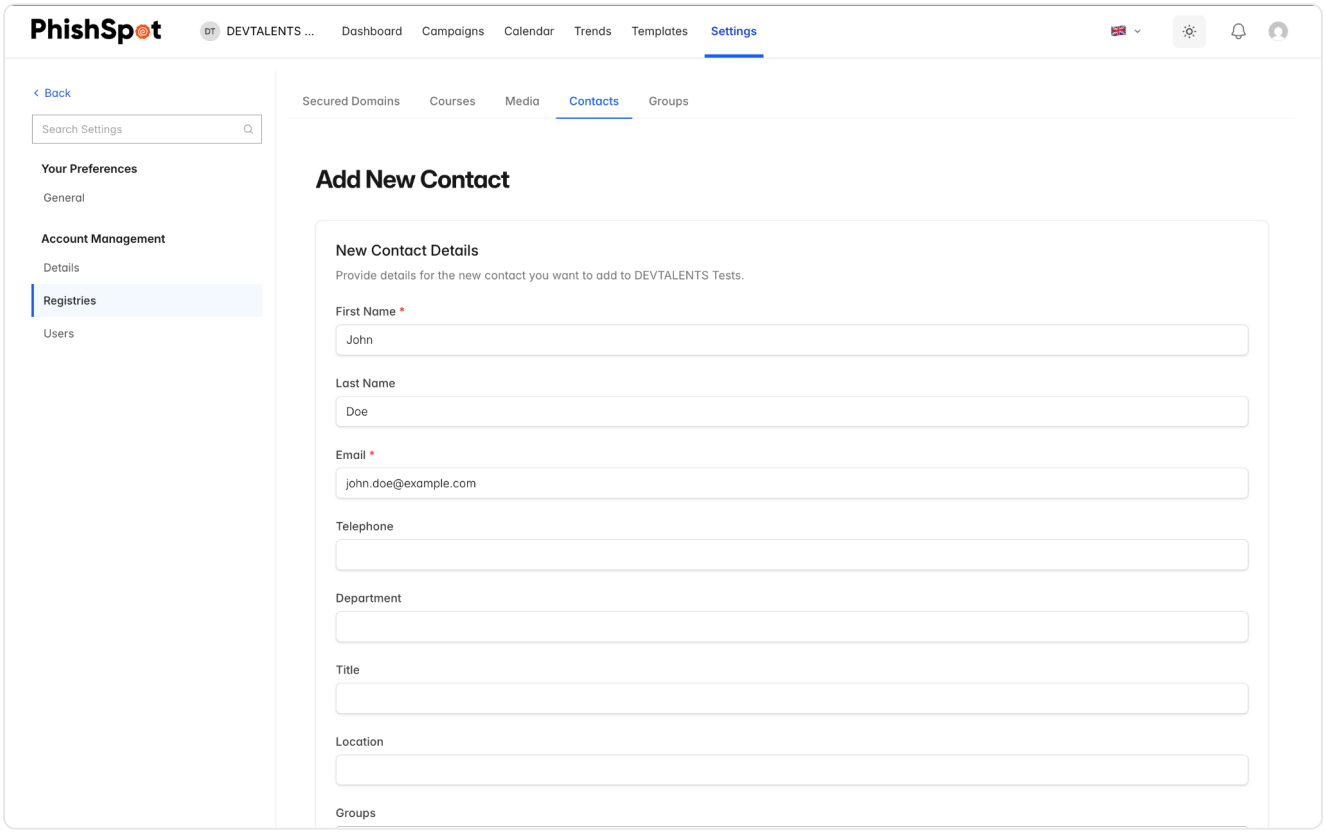
Lista kontaktów zawiera pasek filtrów na górze, który pozwala zawęzić listę według:

- Działu
- Stanowiska
- Lokalizacji
- Specjalnych filtrów statusu, takich jak: kiedykolwiek kliknął w link phishingowy, kiedykolwiek przesłał dane, nigdy nie był celem, lub ukończył szkolenie.

5.3 Dodawanie pojedynczego kontaktu

Kliknij przycisk Nowy Kontakt (New Contact), aby ręcznie dodać kontakt. Wypełnij następujące pola:

- **Imię i Nazwisko** — Wymagane.
- **E-mail** — Wymagane. Musi być prawidłowym adresem e-mail.
- **Telefon** — Opcjonalnie.
- **Dział, Stanowisko, Lokalizacja** — Pola opcjonalne do kategoryzacji i filtrowania.
- **Grupy** — Przypisz kontakt do jednej lub więcej grup.

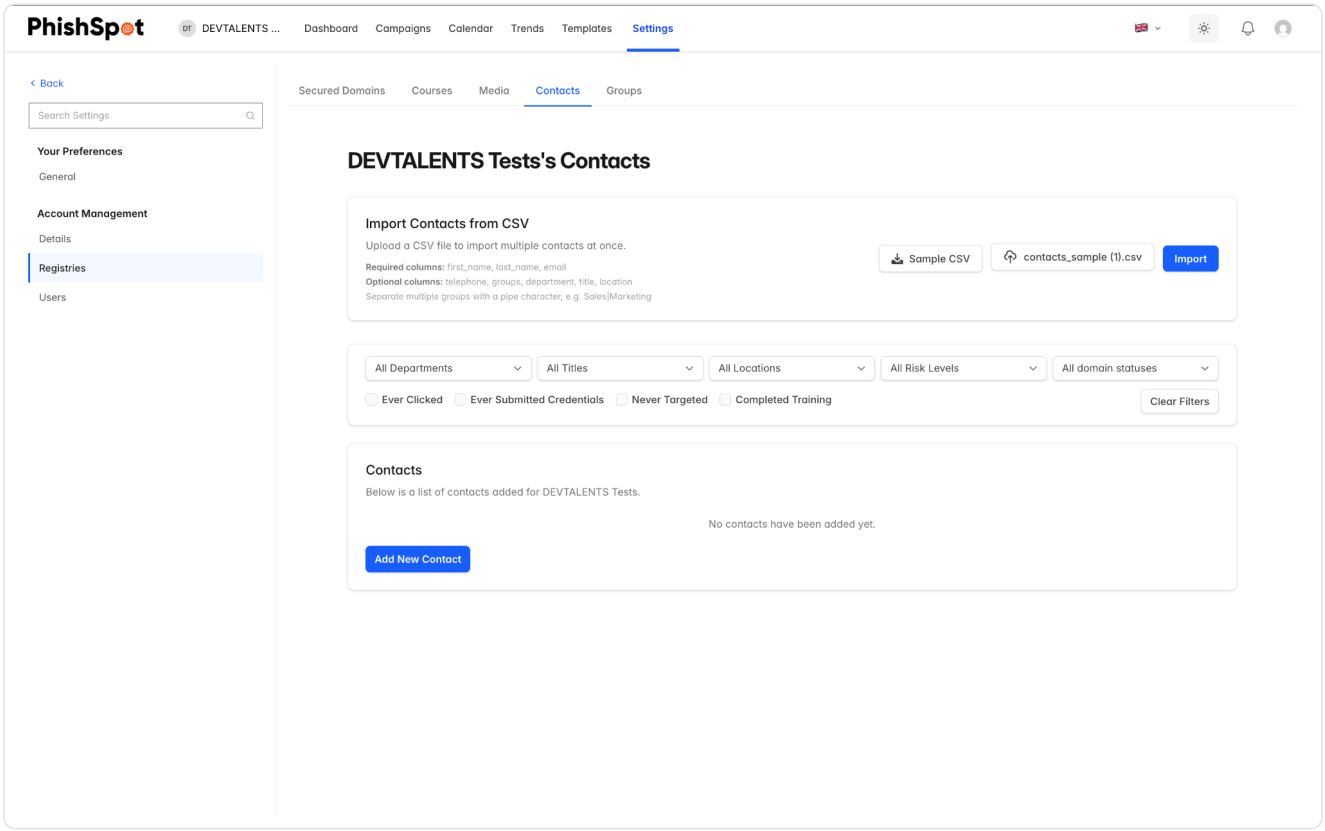


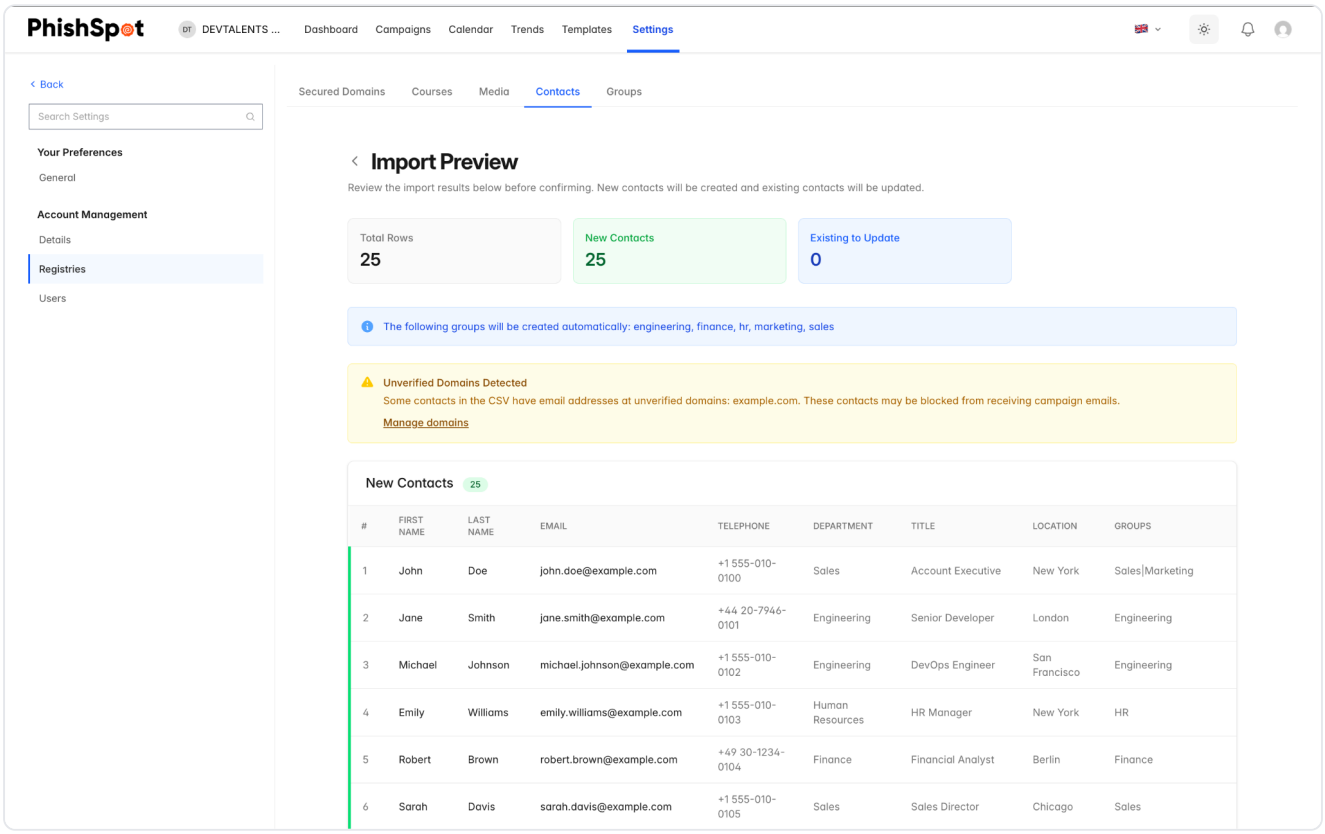
5.4 Import Kontaktów przez plik CSV

W przypadku importu masowego, PhishSpot obsługuje wgrywanie plików CSV. Proces ten składa się z trzech etapów:

1. **Wgraj plik CSV** — Kliknij przycisk Wybierz plik w sekcji importu i wybierz swój plik CSV. Możesz najpierw pobrać przykładowy plik CSV, aby zapoznać się z oczekiwanym formatem.
2. **Podgląd (Preview)** — Przejrzyj sparsowane dane przed importem. Podgląd pokazuje, które kolumny zostały wykryte oraz ewentualne znalezione błędy.
3. **Potwierdź (Confirm)** — Kliknij Potwierdź Import, aby utworzyć kontakty. Jeśli niektóre wiersze zawiodą, możesz pobrać plik CSV z błędnymi wierszami, aby je naprawić i zaimportować ponownie.

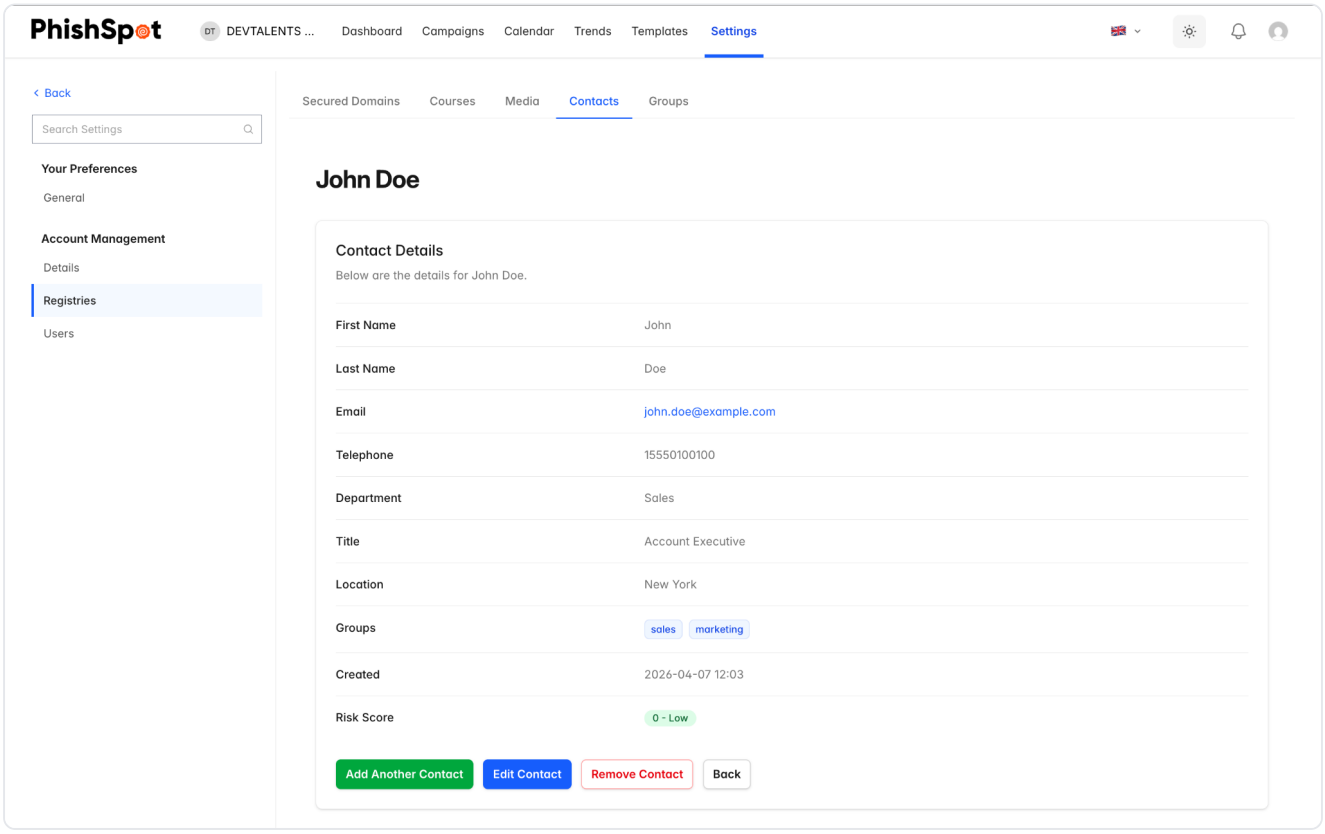
Wymagane kolumny w pliku CSV to: first_name, last_name, email. Opcjonalne kolumny to: telephone, groups (nazwy grup rozdzielone przecinkami), department, title, location.


PhishSpot
DEVTALENTS ...
Dashboard
Campaigns
Calendar
Trends
Templates
Settings
Back
Search Settings
Your Preferences
General
Account Management
Details
Registries
Users
Secured Domains
Courses
Media
Contacts
Groups
DEVTALENTS Tests's Contacts
Import Contacts from CSV
Upload a CSV file to import multiple contacts at once.
Required columns: first_name, last_name, email
Optional columns: telephone, groups, department, title, location
Separate multiple groups with a pipe character, e.g. Sales|Marketing
Sample CSV
contacts_sample (1).csv
Import
All Departments
All Titles
All Locations
All Risk Levels
All domain statuses
Ever Clicked
Ever Submitted Credentials
Never Targeted
Completed Training
Clear Filters
Contacts
Below is a list of contacts added for DEVTALENTS Tests.
No contacts have been added yet.
Add New Contact


PhishSpot
DEVTALENTS ...
Dashboard
Campaigns
Calendar
Trends
Templates
Settings
Back
Search Settings
Your Preferences
General
Account Management
Details
Registries
Users
Secured Domains
Courses
Media
Contacts
Groups
Import Preview
Review the import results below before confirming. New contacts will be created and existing contacts will be updated.
Total Rows
25
New Contacts
25
Existing to Update
0
The following groups will be created automatically: engineering, finance, hr, marketing, sales
Unverified Domains Detected
Some contacts in the CSV have email addresses at unverified domains: example.com. These contacts may be blocked from receiving campaign emails.
Manage domains
New Contacts 25
FIRST NAME LAST NAME EMAIL TELEPHONE DEPARTMENT TITLE LOCATION GROUPS
1 John Doe john.doe@example.com +1 555-010-0100 Sales Account Executive New York Sales|Marketing
2 Jane Smith jane.smith@example.com +44 20-7946-0101 Engineering Senior Developer London Engineering
3 Michael Johnson michael.johnson@example.com +1 555-010-0102 Engineering DevOps Engineer San Francisco Engineering
4 Emily Williams emily.williams@example.com +1 555-010-0103 Human Resources HR Manager New York HR
5 Robert Brown robert.brown@example.com +49 30-1234-0104 Finance Financial Analyst Berlin Finance
6 Sarah Davis sarah.davis@example.com +1 555-010-0105 Sales Sales Director Chicago Sales

5.5 Strona Szczegółów Kontaktu

Kliknij na imię i nazwisko dowolnego kontaktu, aby zobaczyć jego stronę szczegółów. Pokazuje ona pełne informacje profilowe, ocenę ryzyka, historię kampanii oraz wskaźniki wydajności pokazujące, jak dana osoba reagowała na przeszłe kampanie.



5.6 Operacje masowe

Każdy wiersz na liście kontaktów ma checkbox po lewej stronie. Zaznacz dwa lub więcej wierszy, a na dole strony pojawi się **pasek akcji masowych**, pokazując liczbę zaznaczonych i dostępne akcje. Dziś jedyna akcja masowa to **Usuń** — przydatna do oczyszczenia nieaktualnego importu, usunięcia działu, który opuścił firmę, albo przycięcia testowych kontaktów.

Przycisk **Usuń** na pasku prosi o potwierdzenie przed usunięciem; dialog potwierdzenia mówi dokładnie ile kontaktów zostanie usuniętych. Usunięte kontakty znikają z listy i z grup, do których należały; ich historia deliverables jest zachowywana na kampaniach, w których brali udział — raporty pozostają spójne.

> Kontakty zaimportowane z Entra AD (Rozdział 25) pojawią się ponownie przy następnej synchronizacji katalogu, jeśli nadal istnieją (albo nadal są włączone) w Entra. Masowe usuwanie jest najbardziej przydatne dla kontaktów **importowanych ręcznie**; w przypadku tych zarządzanych przez katalog — wyłącz je albo usuń w Entra, a następna synchronizacja odzwierciedli zmianę.

Grupy

Grupy pozwalają na organizowanie kontaktów w logiczne zbiory na potrzeby kampanii celowanych. Na przykład, możesz utworzyć grupy dla poszczególnych działów, lokalizacji biur lub poziomów ryzyka.

6.1 Lista Grup

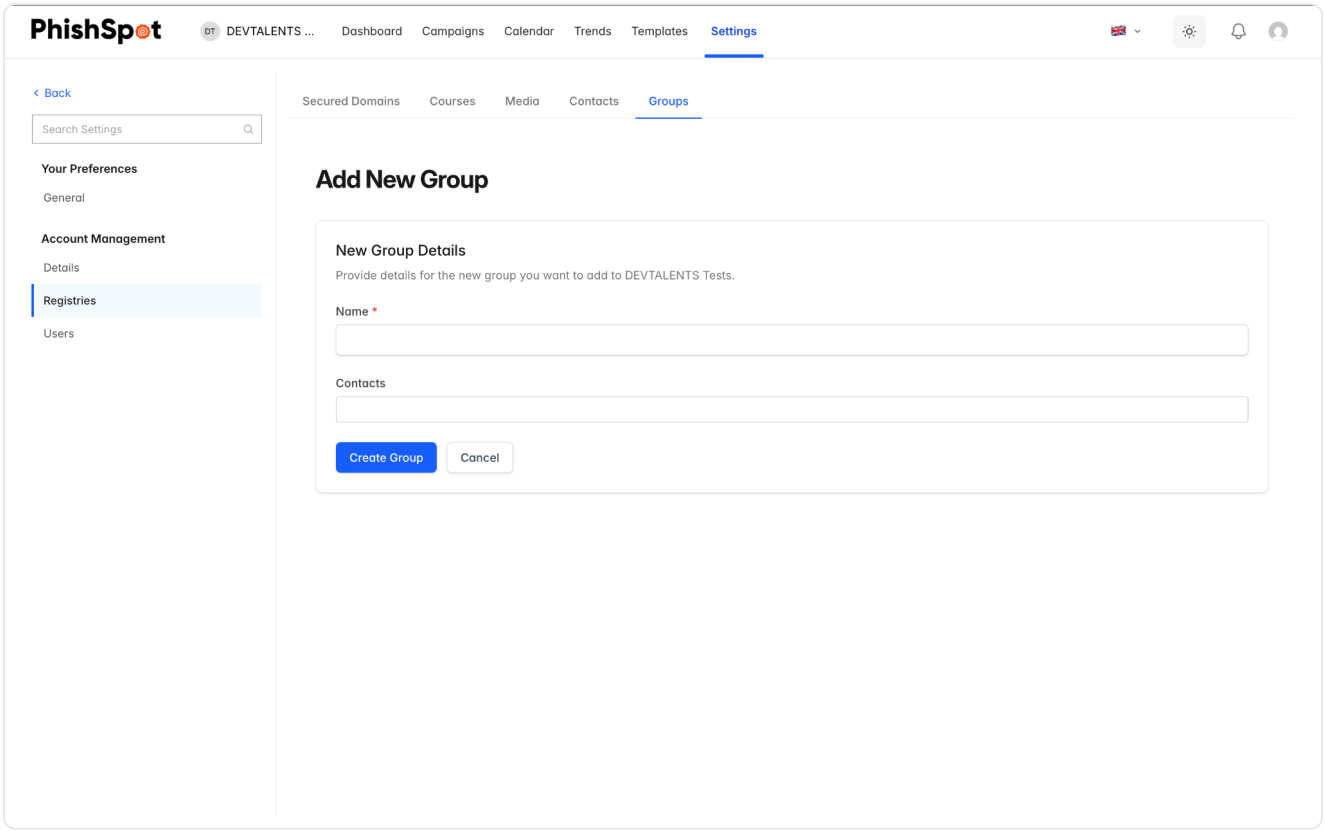
Przejdź do Ustawienia → Grupy. Lista wyświetla:

Kolumna	Opis
Nazwa	Nazwa grupy (klikalna, aby zobaczyć członków)
Kontakty	Liczba kontaktów w grupie
Kampanie	Liczba kampanii, w których użyto tej grupy
Utworzono	Kiedy grupa została utworzona
Akcje	Przyciski Edytuj i Usuń

> Grupy aktualnie używane w aktywnych kampaniach mogą być zablokowane i nie można ich edytować ani usunąć, dopóki kampania się nie zakończy.

6.2 Tworzenie Grupy

Kliknij Nowa Grupa (New Group) i wprowadź nazwę oraz opcjonalny opis. Możesz natychmiast przypisać kontakty do grupy korzystając z funkcji wyboru wielu kontaktów, lub dodać je później. Grupy mogą być również tworzone automatycznie podczas importu pliku CSV przez uwzględnienie nazw grup w kolumnie groups.


PhishSpot
DT DEVTALENTS ...
Dashboard
Campaigns
Calendar
Trends
Templates
Settings
Back
Search Settings
Your Preferences
General
Account Management
Details
Registries
Users
Secured Domains
Courses
Media
Contacts
Groups
Add New Group
New Group Details
Provide details for the new group you want to add to DEVTALENTS Tests.
Name *
Contacts
Create Group
Cancel

Szablony Phishingowe

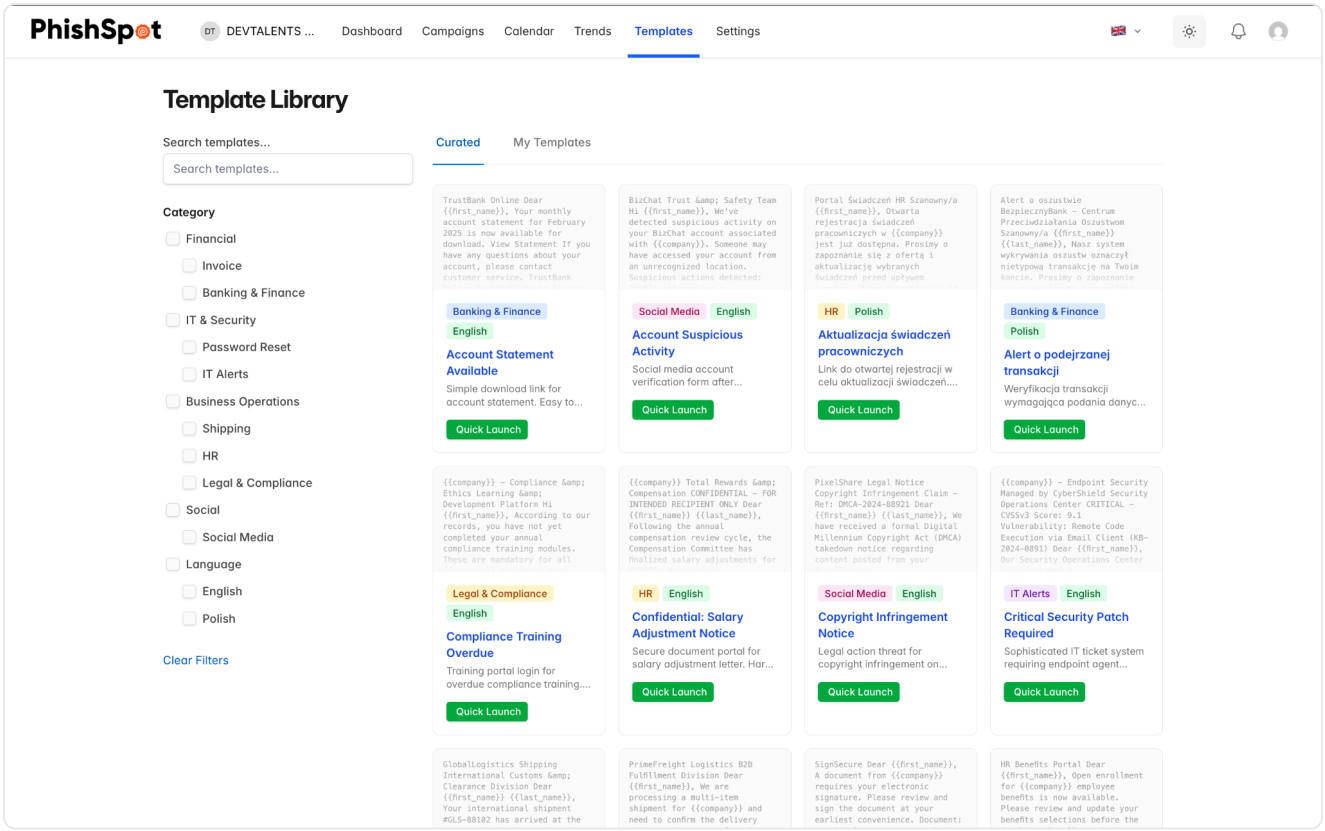
Szablony pozwalają zaoszczędzić czas, udostępniając gotowe projekty e-maili phishingowych, które można wdrożyć bezpośrednio w kampanii.

7.1 Biblioteka Szablonów

Przejdź do zakładki Szablony z paska bocznego. Biblioteka szablonów składa się z dwóch zakładek:

- **Wyselekcjonowane (Curated)** — Gotowe szablony dostarczane przez PhishSpot, uporządkowane według kategorii (np. kradzież poświadczeń, dostawa paczki, alerty IT, powiadomienia HR). Wyselekcjonowana biblioteka zawiera **48 szablonów: 24 po angielsku i 24 po polsku**, wszystkie tworzone lokalnie — polski zestaw pisze polskojęzyczny zespół, nie tłumaczy maszynowo, więc treść, nazwiska nadawców i preteksty brzmią naturalnie dla polskich odbiorców.
- **Moje Szablony (My Templates)** — Niestandardowe szablony, które utworzyłeś lub zapisałeś z poprzednich kampanii.

Lewy pasek boczny wyświetla drzewo kategorii, pozwalając na filtrowanie szablonów według typu. Szablony są wyświetlane w widoku siatki z miniaturami podglądu.



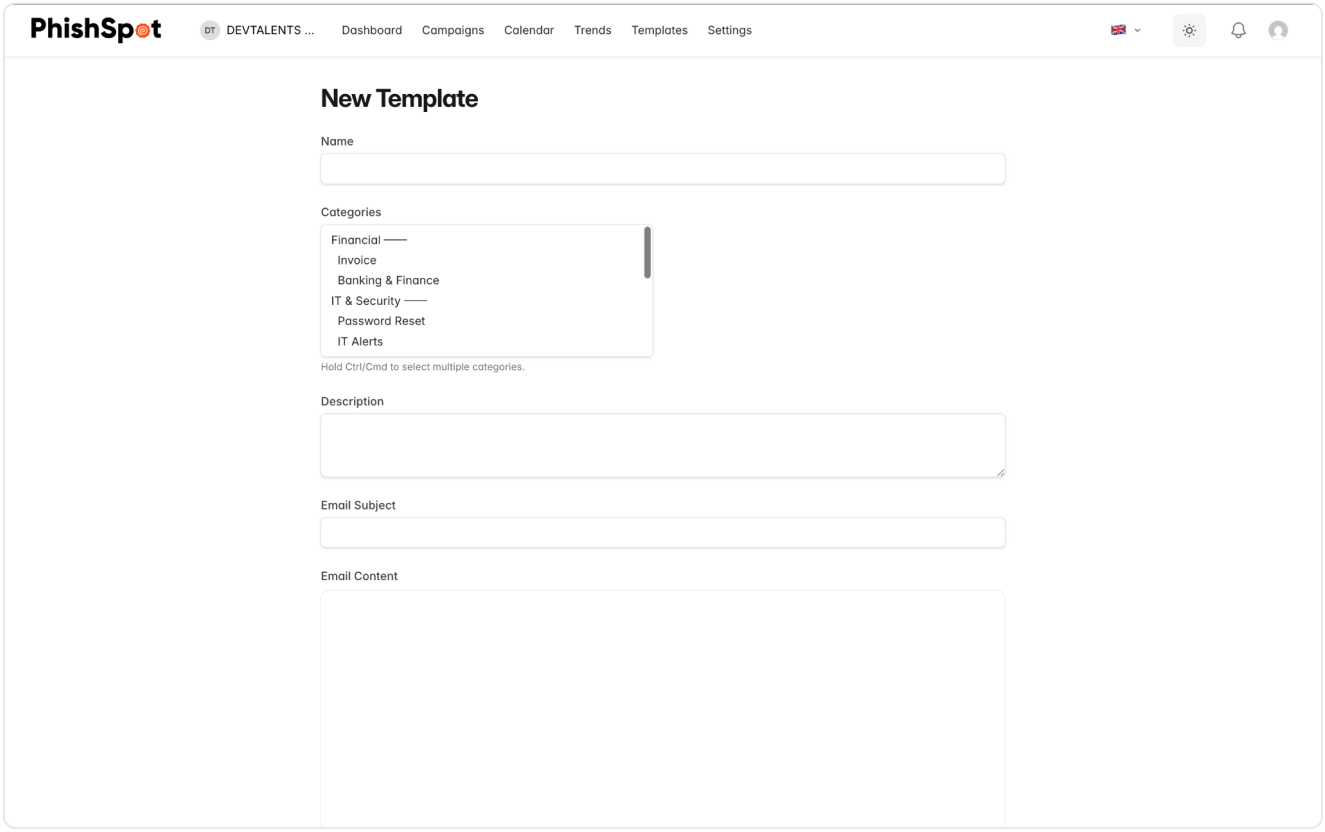
7.2 Używanie Szablonu

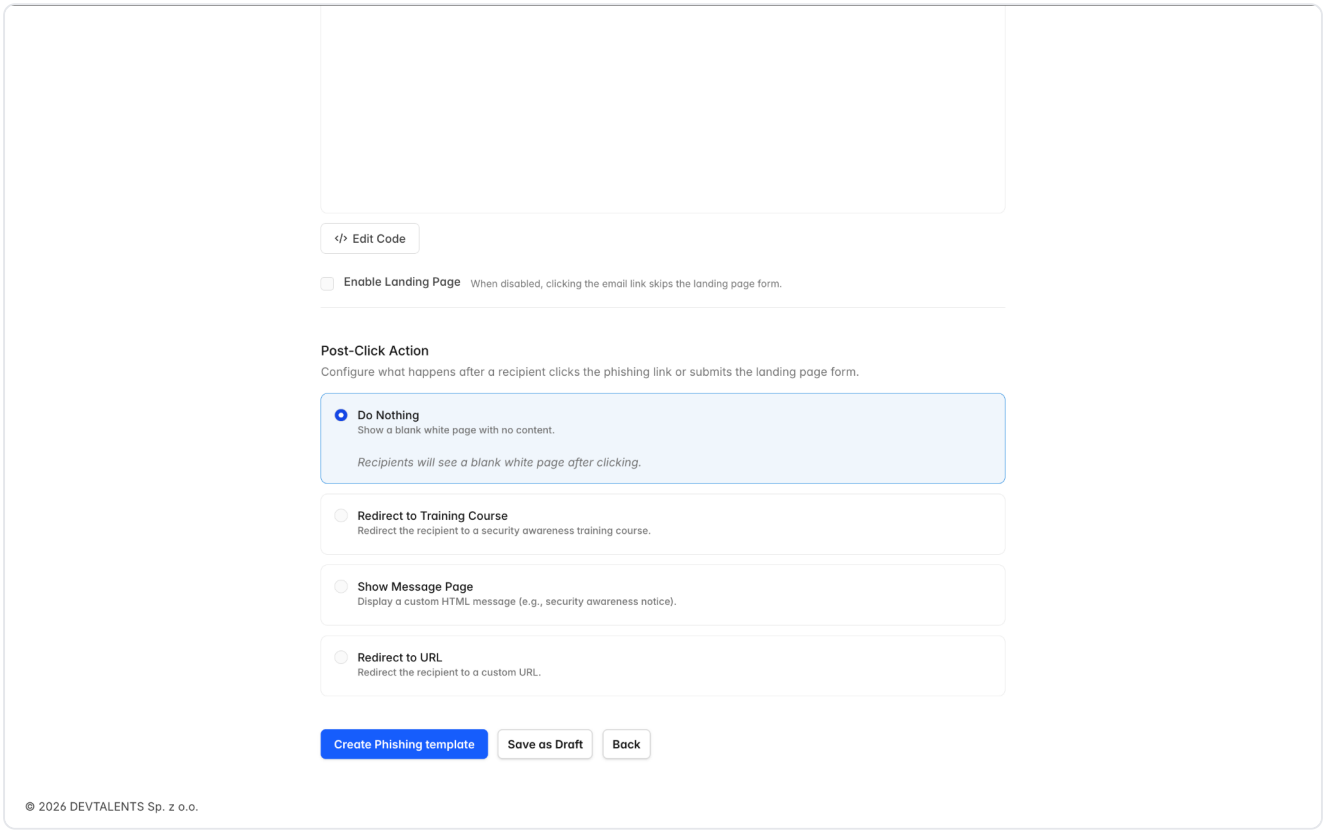
Istnieją dwa sposoby na użycie szablonu:

- **Wdróż (Deploy)** — Stosuje treść e-maila z szablonu do istniejącej kampanii będącej szkicem.
- **Szybkie uruchomienie (Quick Launch)** — Tworzy nową kampanię ze wstępnie wypełnioną treścią e-maila z szablonu, gotową do konfiguracji odbiorców i ustawień dostawy.

7.3 Tworzenie Własnych Szablonów

W zakładce Moje Szablony, kliknij Nowy Szablon (New Template), aby stworzyć własny. Możesz także zapisać e-mail z dowolnej kampanii jako szablon używając przycisku Zapisz jako Szablon na stronie szczegółów kampanii. Własne szablony wspierają ten sam edytor wiadomości i zmienne szablonu, co kampanie.




Edit Code
Enable Landing Page
When disabled, clicking the email link skips the landing page form.
Post-Click Action
Configure what happens after a recipient clicks the phishing link or submits the landing page form.
Do Nothing
Show a blank white page with no content.
Recipients will see a blank white page after clicking.
Redirect to Training Course
Redirect the recipient to a security awareness training course.
Show Message Page
Display a custom HTML message (e.g., security awareness notice).
Redirect to URL
Redirect the recipient to a custom URL.
Create Phishing template
Save as Draft
Back
© 2026 DEVTALENTS Sp. z o.o.

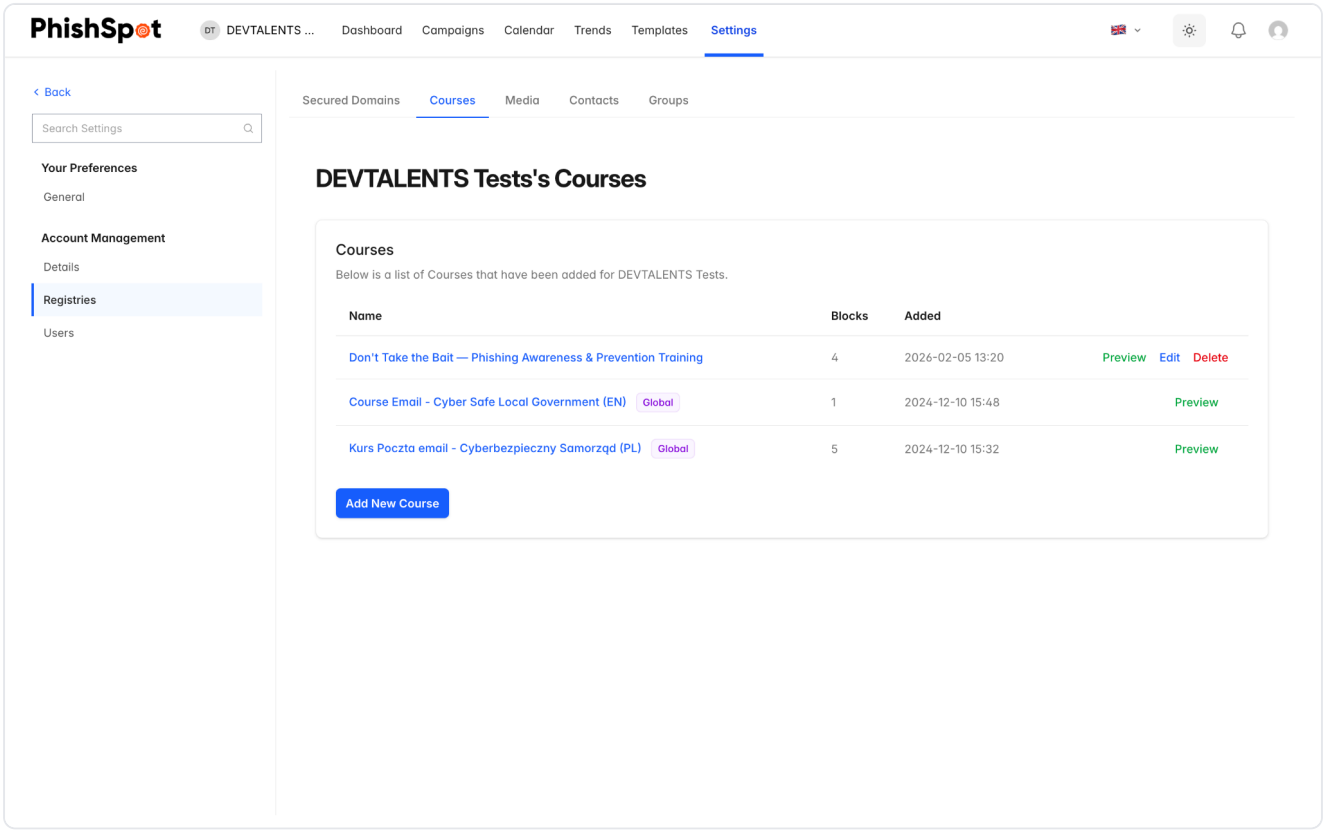
Kursy (Szkolenia ze świadomości bezpieczeństwa)

Kursy to moduły szkoleniowe, które wyświetlają się pracownikom po tym, jak dadzą się nabrać na symulację phishingu. Edukują one użytkowników o tym, jak rozpoznawać próby phishingu i poprawiają zachowania związane z bezpieczeństwem.

8.1 Lista Kursów

Przejdź do Ustawienia → Kursy. Lista prezentuje wszystkie dostępne kursy:

Kolumna	Opis
Nazwa	Tytuł kursu (z fioletową odznaką „Global”, jeśli jest to kurs dostarczany przez platformę)
Bloki	Liczba bloków z zawartością (lekcji, quizów) w kursie
Utworzono	Kiedy kurs został utworzony
Akcje	Przyciski Podgląd, Edytuj i Usuń



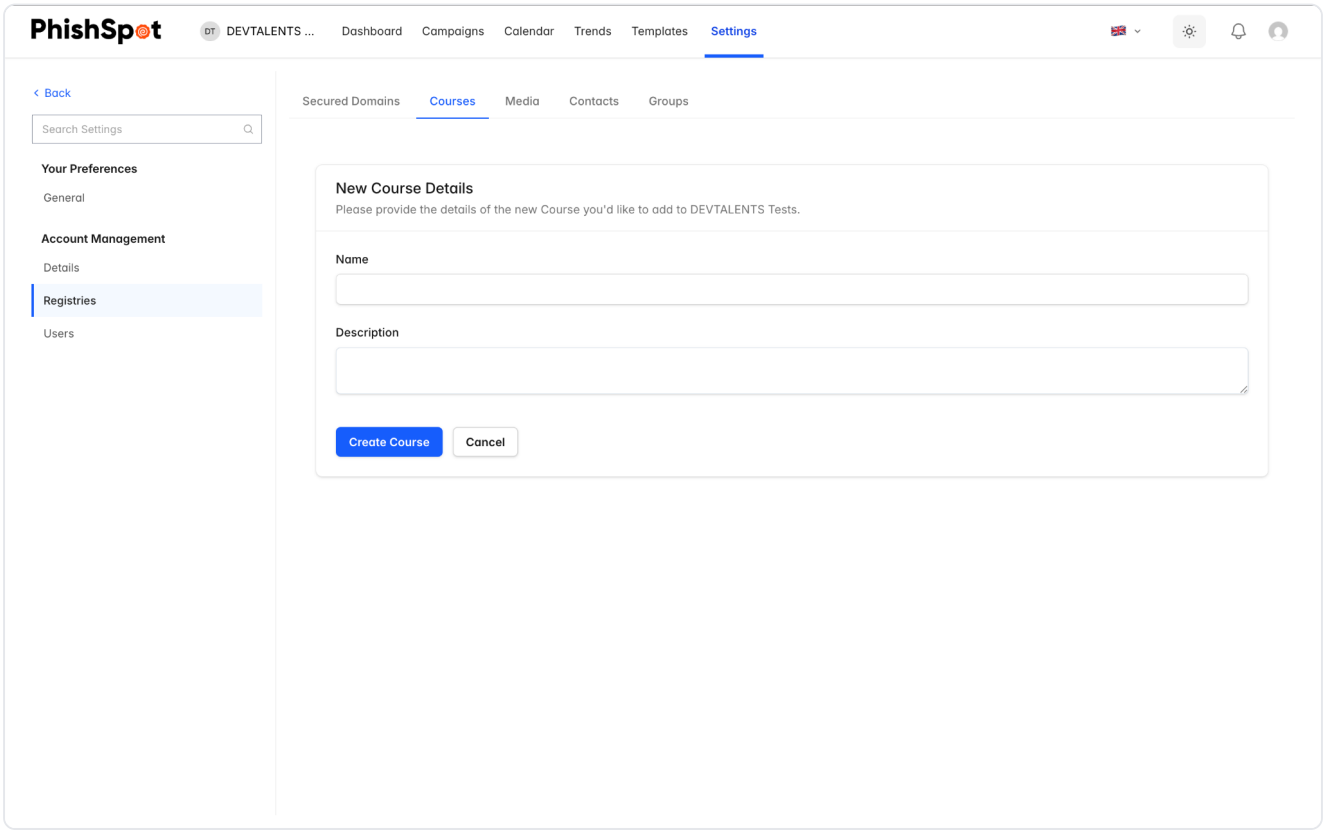
8.2 Tworzenie Kursu

Kliknij Nowy Kurs (New Course), aby utworzyć własne szkolenie. Kurs składa się z bloków, które stanowią poszczególne sekcje z treścią:

- **Bloki Lekcji** — Tekst, obrazy i treści edukacyjne na temat świadomości phishingu.

- **Bloki Quizów** — Interaktywne quizy testujące zrozumienie tematu przez użytkownika.

Bloki można układać w innej kolejności, przeciągając je na wybrane pozycje. Użyj przycisku Podgląd (Preview), aby zobaczyć, jak kurs będzie wyglądał dla użytkowników końcowych.



8.3 Przypisywanie Kursów do Kampanii

Kursy są przypisywane w trakcie tworzenia kampanii, w Kroku 4 (Akcja Po Kliknięciu). Po kliknięciu linku phishingowego lub przesłaniu danych na stronie docelowej, odbiorca jest przekierowywany do przydzielonego kursu. Postęp i status ukończenia szkolenia są śledzone na pulpicie nawigacyjnym kampanii.

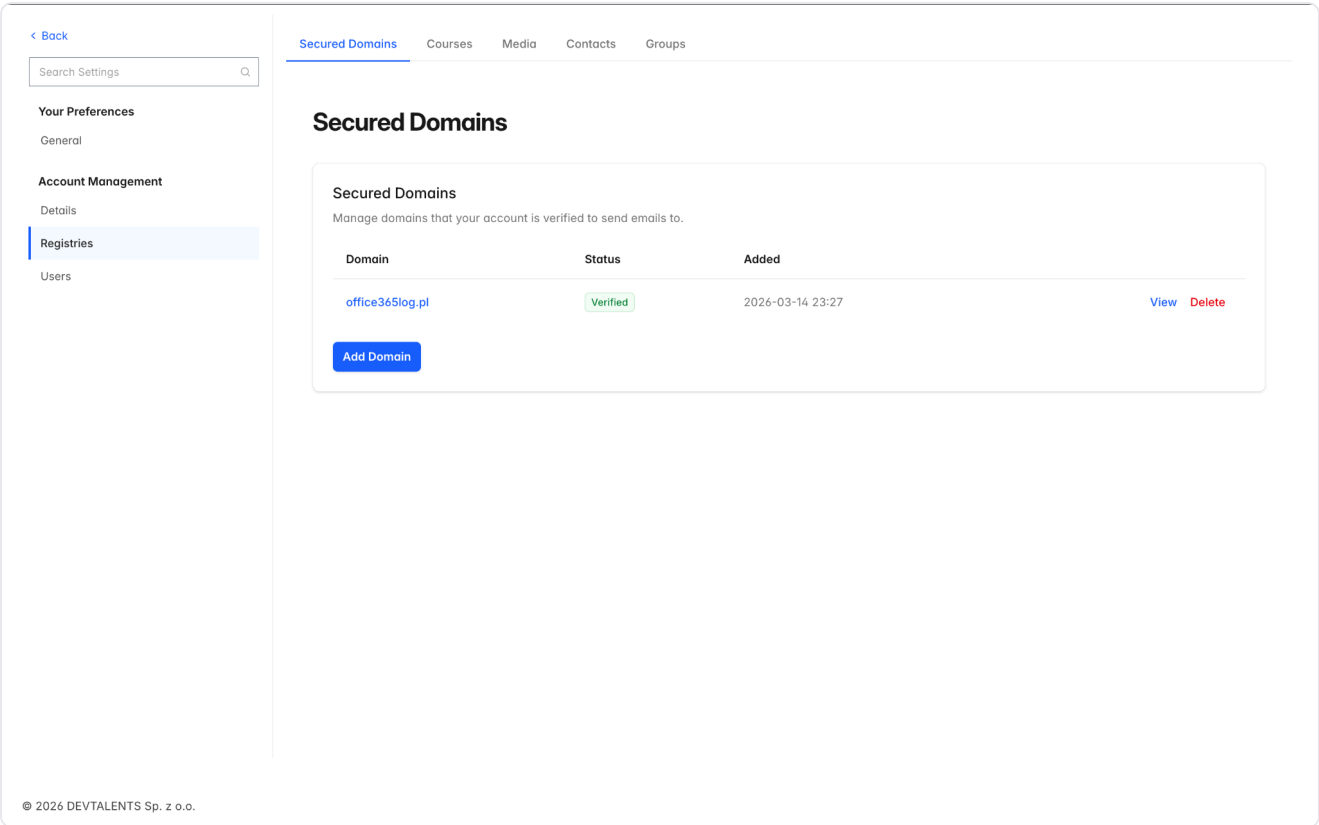
Domeny

PhishSpot wykorzystuje dwa rodzaje domen: Domeny Zabezpieczone (do wysyłania e-maili) oraz Domeny Platformy (do hostowania stron docelowych).

9.1 Zabezpieczone Domeny (Weryfikacja Nadawcy)

Zabezpieczone domeny weryfikują, że jesteś właścicielem domen e-mail, z których wysyłasz symulacje phishingu. Zapewnia to niezawodne dostarczanie wiadomości i chroni przed oznaczaniem ich jako spam. Przejdź do Ustawienia → Zabezpieczone Domeny (Secured Domains). Lista ukazuje każdą domenę z jej statusem weryfikacji:

Status	Znaczenie
Niezweryfikowana (Unverified)	Domena została dodana, ale weryfikacja nie została ukończona
Oczekująca (Pending)	Weryfikacja jest w toku (dodano rekordy DNS, oczekiwanie na propagację)
Zweryfikowana (Verified)	Prawo własności domeny potwierdzone — gotowa do użycia w kampaniach
Nieudana (Failed)	Próba weryfikacji nie powiodła się — sprawdź swoje rekordy DNS



Weryfikacja Domeny

Aby dodać i zweryfikować nową zabezpieczoną domenę:

1. Kliknij Nowa Domena (New Domain) i wpisz nazwę domeny (np. twojafirma.pl).
2. PhishSpot dostarczy rekordy DNS (CNAME lub TXT), które musisz dodać do ustawień DNS swojej domeny.
3. Po dodaniu rekordów DNS kliknij Weryfikuj DNS, aby sprawdzić, czy rekordy uległy propagacji.
4. Alternatywnie możesz zweryfikować ją przez e-mail — PhishSpot wysyła kod weryfikacyjny na standardowy adres administratora w domenie.

> Propagacja DNS może potrwać do 48 godzin. Jeśli weryfikacja się nie powiedzie, odczekaj i spróbuj ponownie.

9.2 Domeny Platformy (Adresy URL stron docelowych)

Domeny platformy to adresy URL używane dla Twoich phishingowych stron docelowych. Kiedy odbiorca kliknie link w wiadomości phishingowej, zostaje przeniesiony na stronę hostowaną w jednej z tych domen. Przejdź do Ustawienia → Domeny Platformy (Platform Domains). Lista wyświetla:

Kolumna	Opis
Nazwa	Wyświetlana nazwa domeny
Publiczna (Public)	Czy ta domena jest współdzielona przez wiele kont, czy jest prywatna dla Twojego
E-mail (Mail)	Czy domena może być również używana do wysyłania e-maili
Wygasa w dniu (Expires On)	Data wygaśnięcia (lub Nigdy, jeśli stała)
Kampanie	Liczba kampanii, które aktualnie używają tej domeny

> Domeny platformy są zazwyczaj konfigurowane przez zespół IT Twojej organizacji lub administratora platformy. Ty wybierasz spośród dostępnych domen podczas tworzenia kampanii.

9.3 Domeny własne (Bring Your Own Domain)

Domeny własne pozwalają wysyłać kampanie z domeny, którą **Ty** posiadasz, zarejestrowanej u dowolnego rejestratora. W przeciwieństwie do Domen Zabezpieczonych (które jedynie potwierdzają, że jesteś właścicielem adresu, na który wysyłasz) i Domen Platformy (zarządzanych przez administratora platformy), domena własna jest po skierowaniu w pełni zarządzana za Ciebie: kierujesz jej serwery nazw na nas, a my automatycznie tworzymy wszystkie rekordy DNS.

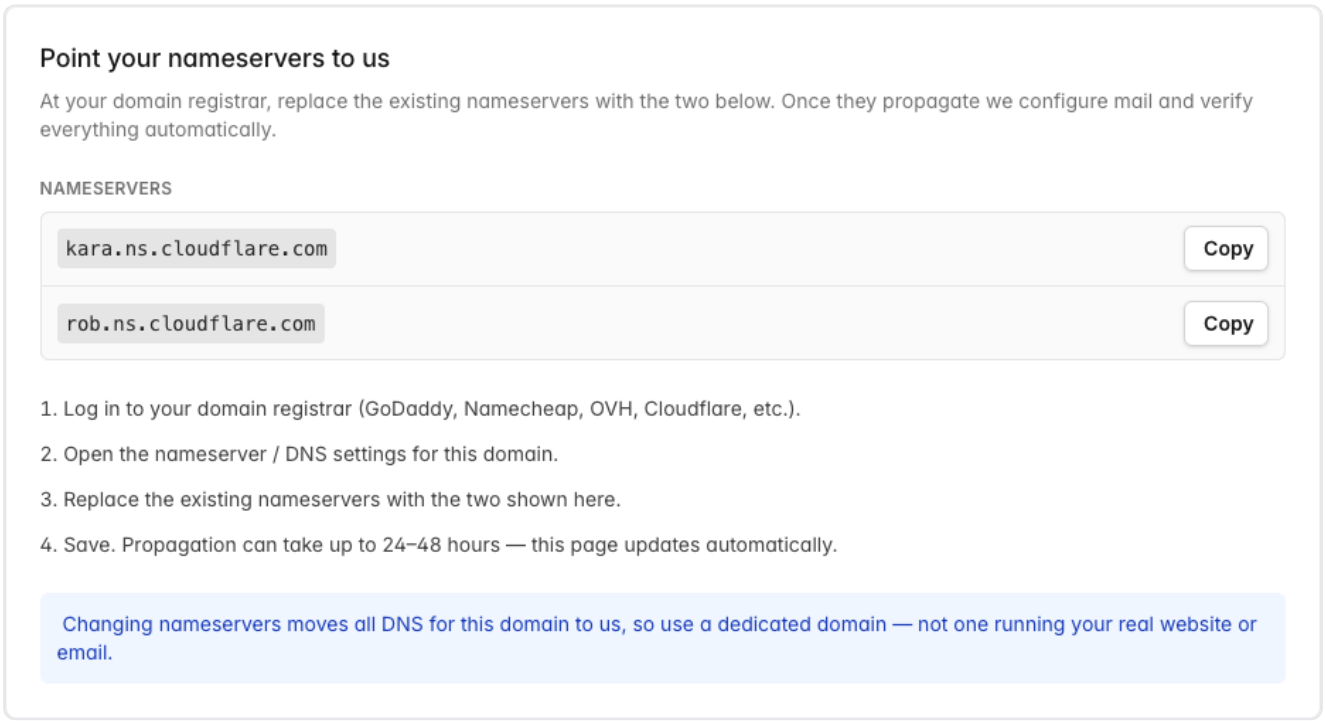
Przejdź do **Ustawienia** → **Domeny własne**.

Zakup dedykowanej domeny

Użyj **dedykowanej** domeny kupionej wyłącznie do symulacji — nie domeny, której używasz do prawdziwej strony lub poczty. Skierowanie serwerów nazw na nas przenosi do nas **całe** DNS tej domeny, więc istniejąca strona lub poczta przestałyby działać.

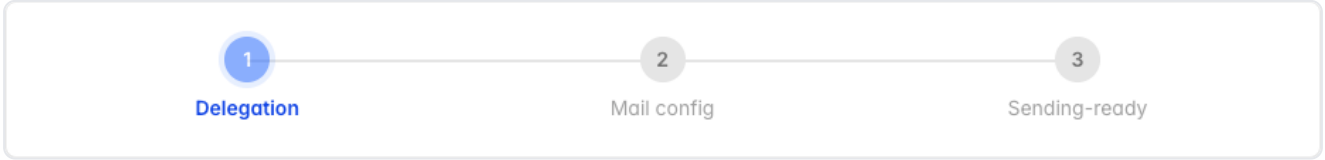
Pobranie serwerów nazw

1. Przejdź do **Ustawienia** → **Domeny własne** → **Dodaj domenę** i wpisz domenę, którą posiadasz.
2. Strona konfiguracji pokaże **dwa serwery nazw**, każdy z przyciskiem kopiowania.



Ustawienie serwerów nazw u rejestratora

1. Zaloguj się do rejestratora domeny (GoDaddy, Namecheap, OVH, Cloudflare itp.).
2. Otwórz ustawienia serwerów nazw / DNS dla domeny.
3. Zastąp istniejące serwery nazw dwoma pokazanymi na stronie konfiguracji.
4. Zapisz. Propagacja może potrwać do **24–48 godzin** — strona aktualizuje się samoczynnie.



Co weryfikujemy

Pasek postępu prowadzi przez trzy etapy — **Delegacja** → **Konfiguracja poczty** → **Gotowa do wysyłki**. W każdej chwili możesz też kliknąć **Sprawdź status teraz**. Znaczenie statusu:

Status	Znaczenie
Oczekiwanie na serwery nazw	Delegacja nie została jeszcze wykryta
Konfigurowanie poczty	Wykryto delegację; dodajemy i weryfikujemy rekordy wysyłki (SPF, DKIM, MX, Return-Path)
Gotowa do wysyłki	Zweryfikowana — domena pojawia się teraz na liście nadawców podczas tworzenia kampanii
Wymaga uwagi	Domena działała, ale później przestała; zablokowana dla nowych kampanii
Konfiguracja nieudana	Nie udało się ukończyć konfiguracji — sprawdź serwery nazw i spróbuj ponownie

Sprawna vs. zablokowana

Ponieważ domena własna nie jest pod naszą kontrolą, stale ją sprawdzamy. Jeśli rejestracja **wygaśnie**, **serwery nazw przestaną wskazywać** na nas, albo **rekordy pocztowe zostaną usunięte**, domena zostanie oznaczona jako **Wymaga uwagi** i zablokowana dla **nowych** kampanii. Kampanie już uruchomione na tej domenie nadal działają, a administratorzy konta otrzymują e-mail wyjaśniający, co naprawić.

> Odnawiaj domenę na czas. Wysyłamy e-mail do administratorów konta, gdy domena własna zbliża się do daty wygaśnięcia, aby nigdy nie wygasła w trakcie programu.

Rozwiązywanie problemów

- **Utknięcie na „Oczekiwanie na serwery nazw”** — upewnij się, że oba serwery nazw są ustawione dokładnie tak, jak pokazano u rejestratora; propagacja może potrwać do 48 godzin.
- **„Wymaga uwagi” po poprawnym działaniu** — otwórz domenę, aby zobaczyć konkretny powód (wygasła / zmienione serwery nazw / brak rekordów pocztowych), napraw go, a następnie kliknij **Sprawdź status teraz**.
- **Usuwanie domeny** — usunięcie domeny własnej kasuje jej konfigurację DNS i poczty. Nie można usunąć domeny z aktywną kampanią; najpierw je wstrzymaj lub zakończ.

Biblioteka Mediów

Biblioteka mediów przechowuje pliki (obrazy, dokumenty, załączniki), z których możesz korzystać w swoich kampaniach, kursach i na stronach docelowych. Przejdź do Ustawienia → Media lub znajdź ten element na Pulpicie nawigacyjnym. Biblioteka prezentuje tabelę z przesłanymi plikami z kolumnami dla Nazwy, Typu Zawartości (Content Type), kopiowalnego linku URL, daty utworzenia oraz przycisków akcji.

10.1 Wgrywanie Mediów

Kliknij Nowe Media (New Media), aby przesłać plik. Podaj opisową nazwę i wybierz plik z komputera. Po wgraniu do pliku przypisywany jest stały adres URL, który możesz skopiować i wkleić do szablonów e-mail lub kodu HTML strony docelowej.

Raporty i Analityka

PhishSpot udostępnia kilka sposobów analizy wyników kampanii i śledzenia poziomu bezpieczeństwa Twojej organizacji w czasie.

11.1 Raporty Kampanii

Każda kampania posiada swój własny pulpit nawigacyjny (patrz sekcja 4.5) ze szczegółowymi wykresami lejka, tabelami odbiorców oraz danymi w rozbiciu na grupy. Możesz eksportować indywidualne raporty z kampanii w dwóch formatach:

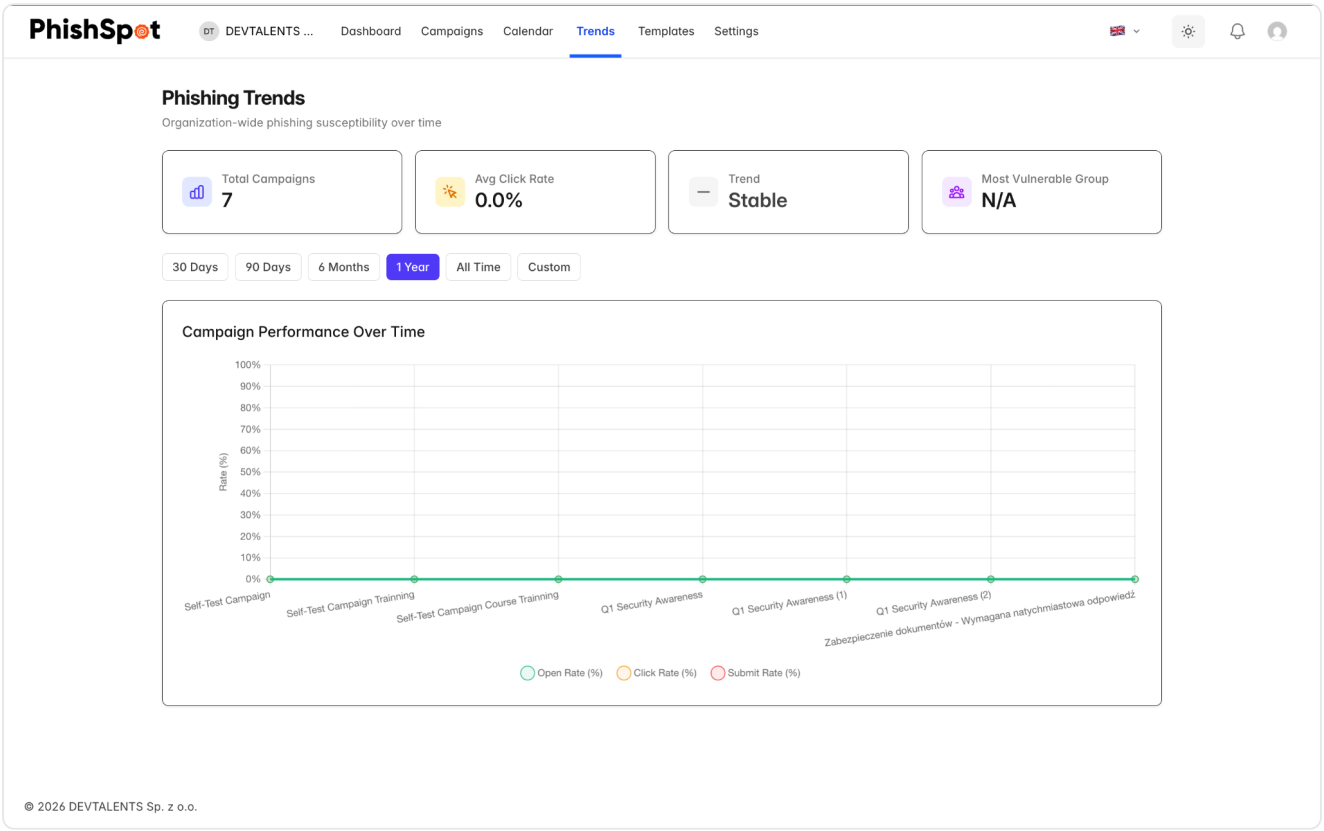
- **Raport PDF** — Sformatowany dokument idealny do przekazania zarządowi.
- **Raport Excel** — Arkusz kalkulacyjny z surowymi danymi do dogłębnej analizy.

11.2 Raporty Zbiorcze

Z poziomu strony z listą kampanii możesz generować raporty zbiorcze, które agregują dane ze wszystkich kampanii. Jest to użyteczne w przypadku kwartalnych lub rocznych przeglądów świadomości bezpieczeństwa.

11.3 Pulpit Trendów

Przejdź do Trendy na pasku bocznym, aby uzyskać dostęp do pulpitu trendów. Widok ten ukazuje historyczne dane wydajnościowe dla wszystkich Twoich kampanii, z opcją filtrowania zakresu dat: 30 dni, 90 dni, 6 miesięcy, 1 rok, cały okres lub niestandardowy zakres. Pulpit trendów pomaga odpowiedzieć na pytania takie jak: Czy z czasem pracownicy lepiej rozpoznają e-maile phishingowe? Które działy potrzebują dodatkowych szkoleń? Czy współczynnik klikalności maleje z każdą kolejną kampanią?



11.4 Oś Czasu Odbiorcy

Na każdym pulpicie kampanii, kliknięcie odbiorcy otwiera szczegółowy panel osi czasu, ukazujący każde śledzone zdarzenie dla danej osoby: kiedy e-mail został wysłany, otwarty, kiedy kliknięto w link, kiedy przeglądano stronę docelową, czy przesłano dane oraz czy kurs szkoleniowy został rozpoczęty, czy zakończony.

11.5 Podgląd maila, który dostał konkretny odbiorca

Każdy wiersz w tabeli **Odbiorcy** kampanii ma obok adresu email małą ikonę lupy na kopercie. Kliknij ją, aby otworzyć modal pokazujący dokładnie tego maila, którego ten kontakt otrzymał — z każdą zmienną szablonu (`{{first_name}}`, `{{company}}`, `{{position}}` …) podstawioną rzeczywistymi danymi tego kontaktu, z osadzonym faktycznym URL-em strony docelowej, z faktycznie użytym adresem From:. Nie generyczny podgląd: wyrenderowany mail dla tego konkretnego odbiorcy.

Modal ma na górze przełącznik **desktop / mobile** — przełączaj między nimi, żeby zobaczyć jak mail wyglądał na 1920-pikselowym Outlooku vs. renderingu iPhone Mail. Przydatne przy review kampanii ze stroną klienta („pokaż mi dokładnie, co Anna zobaczyła na telefonie") i przy dochodzeniach („czy link w tej konkretnej dostawie wskazywał na właściwą domenę?").

Ten sam podgląd jest też dostępny z widoku **deliverables** konkretnego kontaktu — otwórz stronę szczegółów kontaktu, a wiersze deliverables mają tę samą lupę. Dwie perspektywy na ten sam modal: per kampania (wszyscy odbiorcy jednej kampanii) i per kontakt (każda kampania, którą jedna osoba otrzymała).

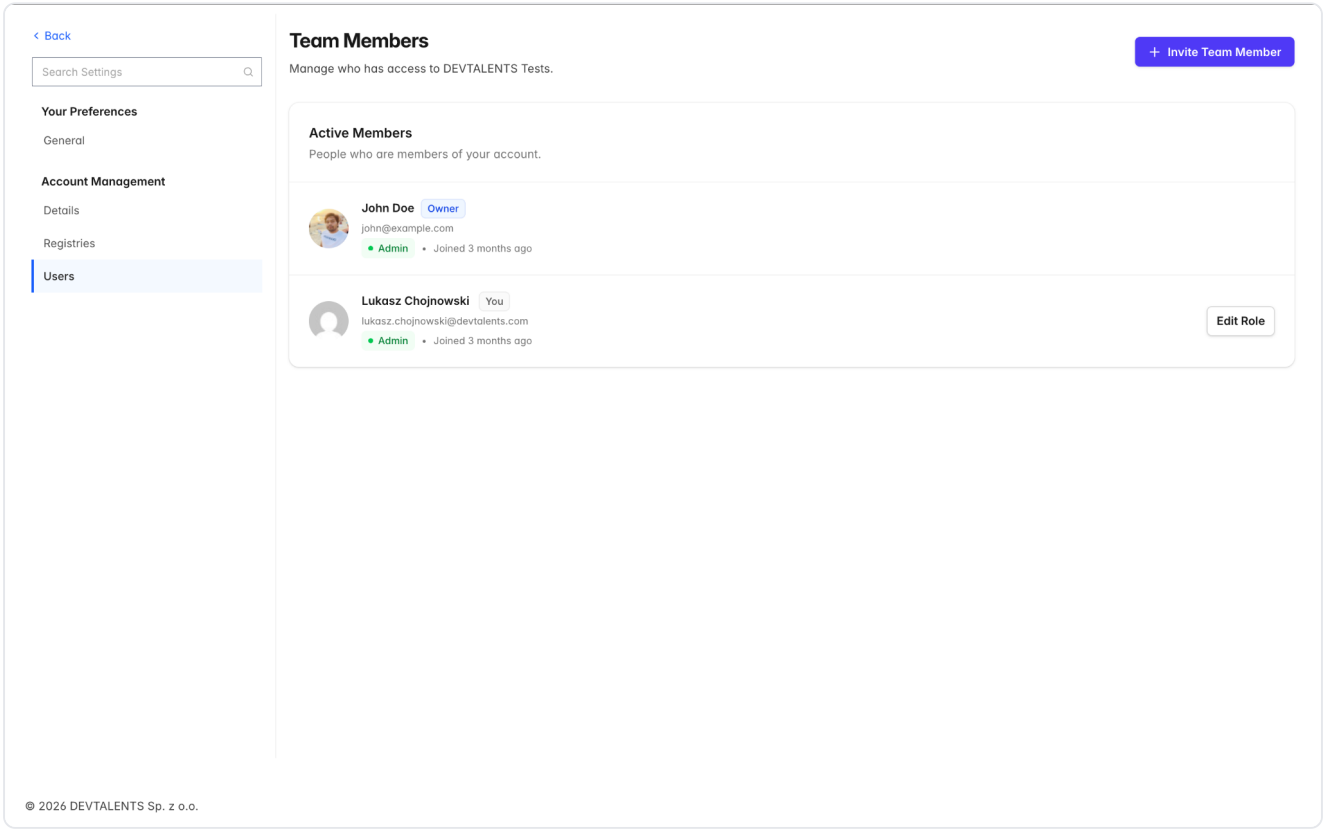
Zarządzanie Zespołem

Jako Administrator możesz zarządzać, kto ma dostęp do Twojego konta i co może na nim robić.

12.1 Przeglądanie Członków Zespołu

Przejdź do Ustawienia → Członkowie Zespołu. Ta strona posiada dwie sekcje:

- **Aktywni Członkowie** — Wszyscy użytkownicy aktualnie posiadający dostęp do Twojego konta, wraz z imieniem i nazwiskiem, adresem e-mail, rolą (Admin/Edytor/Członek) oraz datą dołączenia. Właściciel konta jest oznaczony odznaką Właściciel (Owner).
- **Oczekujące Zaproszenia** — Zaproszenia, które zostały wysłane, ale jeszcze ich nie zaakceptowano.

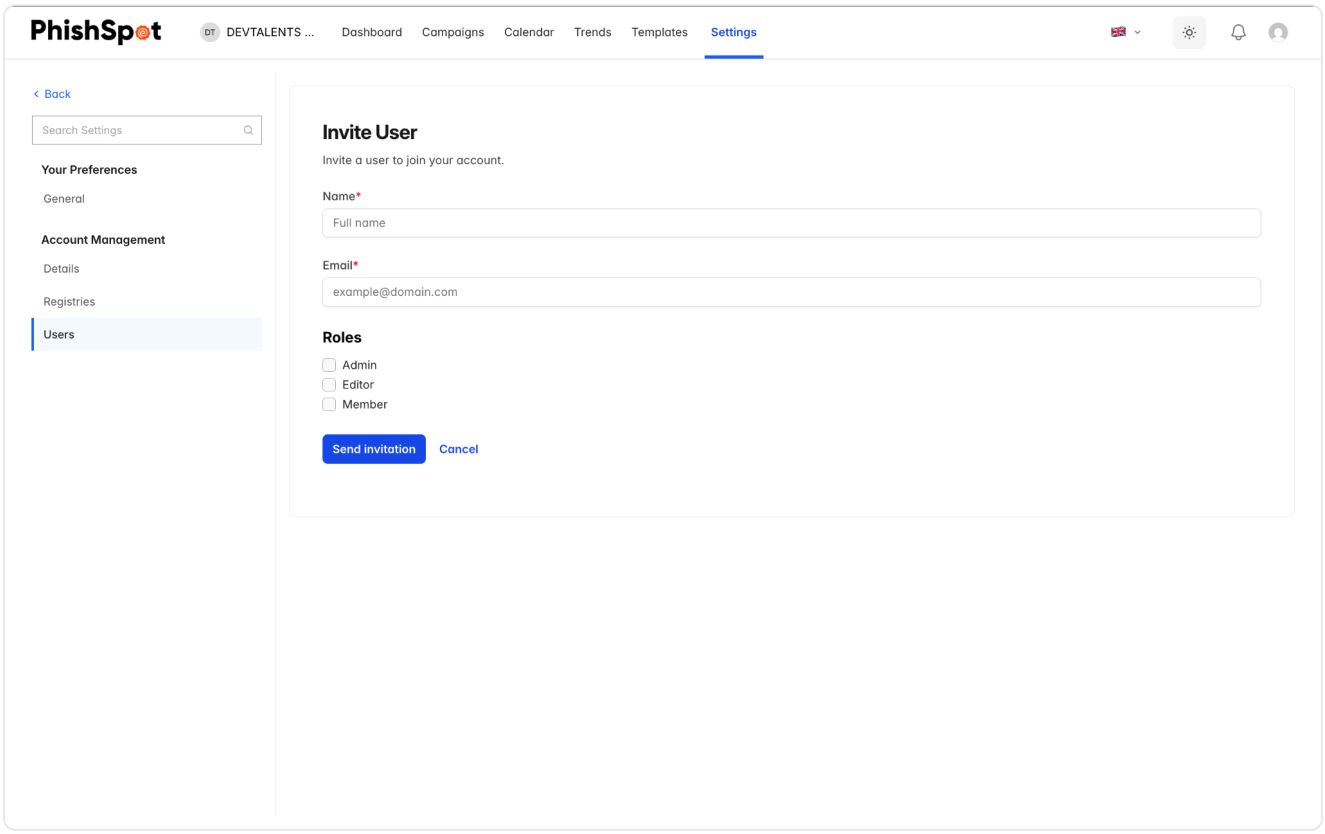


12.2 Zapraszanie Nowych Członków

Kliknij przycisk Zaproś Członka (Invite Member), aby dodać osobę do zespołu:

1. Wpisz adres e-mail tej osoby.
2. Wybierz rolę: Admin, Edytor lub Członek.
3. Kliknij Wyślij Zaproszenie (Send Invitation).

Zaproszona osoba otrzyma e-mail z linkiem do akceptacji zaproszenia. Jeśli posiada już konto PhishSpot, nowy zespół pojawi się w jej narzędziu do przełączania kont. Jeśli nie posiada konta, zostanie poproszona o jego utworzenie. Dla zaproszeń o statusie oczekującym możesz wysłać e-mail z zaproszeniem ponownie lub całkowicie je anulować.



12.3 Zmiana Ról

Aby zmienić rolę członka zespołu, kliknij przycisk Edytuj obok jego nazwiska. Wybierz nową rolę i zapisz. Pamiętaj:

- Tylko Administratorzy mogą zmieniać role innych członków.
- Rola właściciela konta nie może zostać zmieniona — zawsze posiada on uprawnienia Administratora.
- Nie możesz zmienić swojej własnej roli.

12.4 Usuwanie Członków

Aby usunąć członka zespołu, kliknij przycisk Usuń (Remove) obok jego nazwiska i potwierdź. Użytkownik straci dostęp do konta, ale jego historyczne dane (np. działania w logach kampanii) zostaną zachowane. Właściciel konta nie może zostać usunięty.

12.5 Przenoszenie Własności

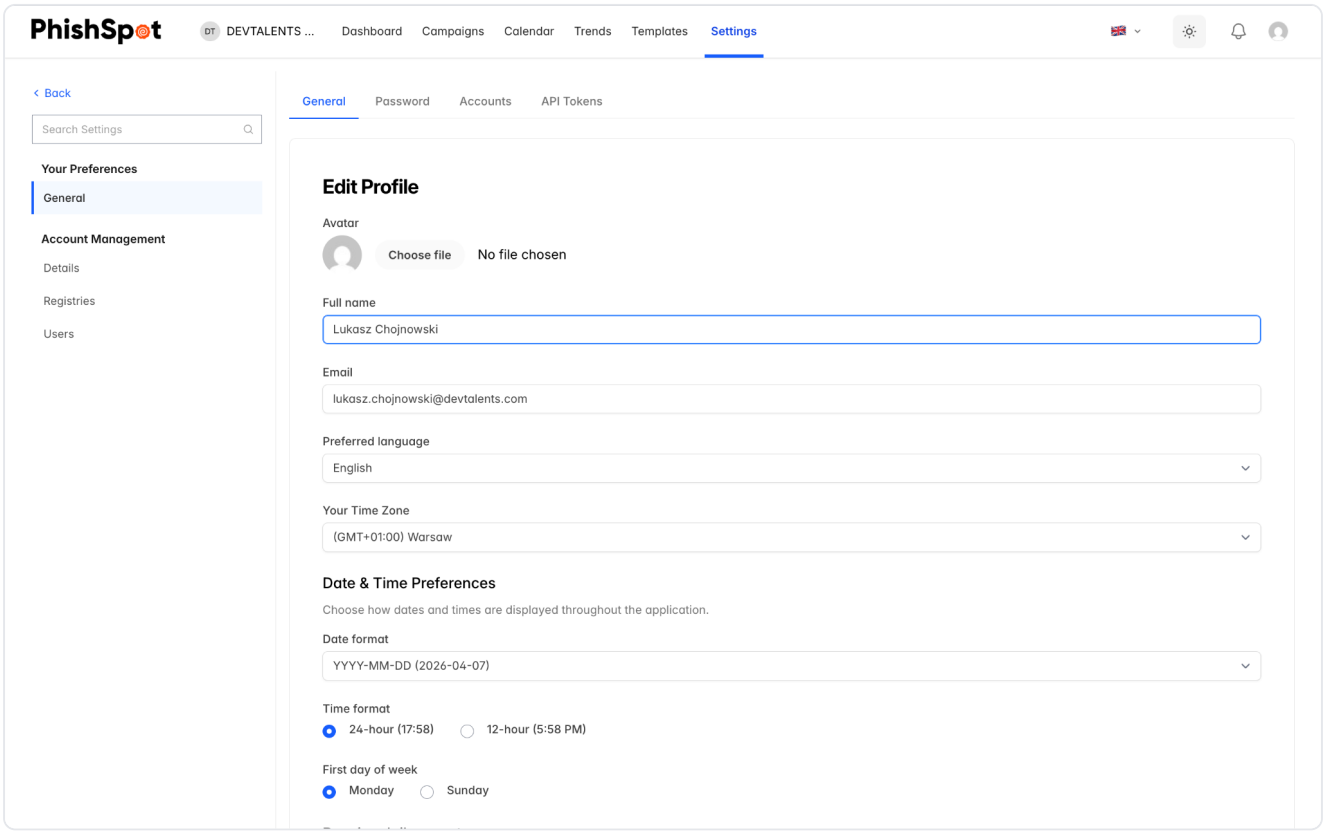
Jeśli jesteś właścicielem konta, możesz przekazać własność innemu Administratorowi w zespole. Przejdź do Ustawienia → Szczegóły Konta i użyj opcji Transferu Własności (Transfer Ownership). Docelowy użytkownik musi już posiadać rolę Administratora. Po transferze zostaje on nowym właścicielem, a Ty pozostajesz jako Administrator.

Ustawienia Konta

Przejdź do Ustawienia → Szczegóły Konta (Account Details), aby skonfigurować preferencje konta.

13.1 Podstawowe Informacje

- **Nazwa Konta** — Nazwa Twojej organizacji lub zespołu.
- **Strefa czasowa** — Domyślna strefa czasowa używana do planowania kampanii oraz dla znaczników czasu na raportach.
- **Język główny** — Język interfejsu (angielski lub polski).
- **Awatar** — Opcjonalny obraz konta/logo.



13.2 Godziny Pracy (Business Hours)

Włącz opcję godzin pracy, aby ograniczyć czas dostarczania wiadomości w ramach kampanii. Po włączeniu skonfiguruj:

- Które dni tygodnia wiadomości mogą być wysyłane (pola wyboru od poniedziałku do niedzieli).
- Godzina rozpoczęcia i godzina zakończenia dla okna dostawy.

E-maile zaplanowane na czas poza godzinami pracy zostaną zakolejkowane i dostarczone w następnym oknie czasowym.

13.3 Domyślna Strona Świadomości

Skonfiguruj domyślną stronę HTML pokazywaną użytkownikom po wejściu w interakcję z symulacją phishingu. Jest to komunikat uświadamiający/edukacyjny, który pojawia się, gdy do kampanii nie przydzielono konkretnego kursu. Możesz edytować kod HTML za pomocą wbudowanego edytora kodu oraz wyświetlać podgląd na żywo.

13.4 Usuwanie Konta

Na dole strony Szczegóły Konta znajduje się przycisk Usuń Zespół (Delete Team). Powoduje on trwałe usunięcie konta i wszystkich powiązanych danych, w tym kampanii, kontaktów, szablonów oraz wyników. Tej akcji nie można cofnąć. Jedynie właściciel konta posiada możliwość jego usunięcia.

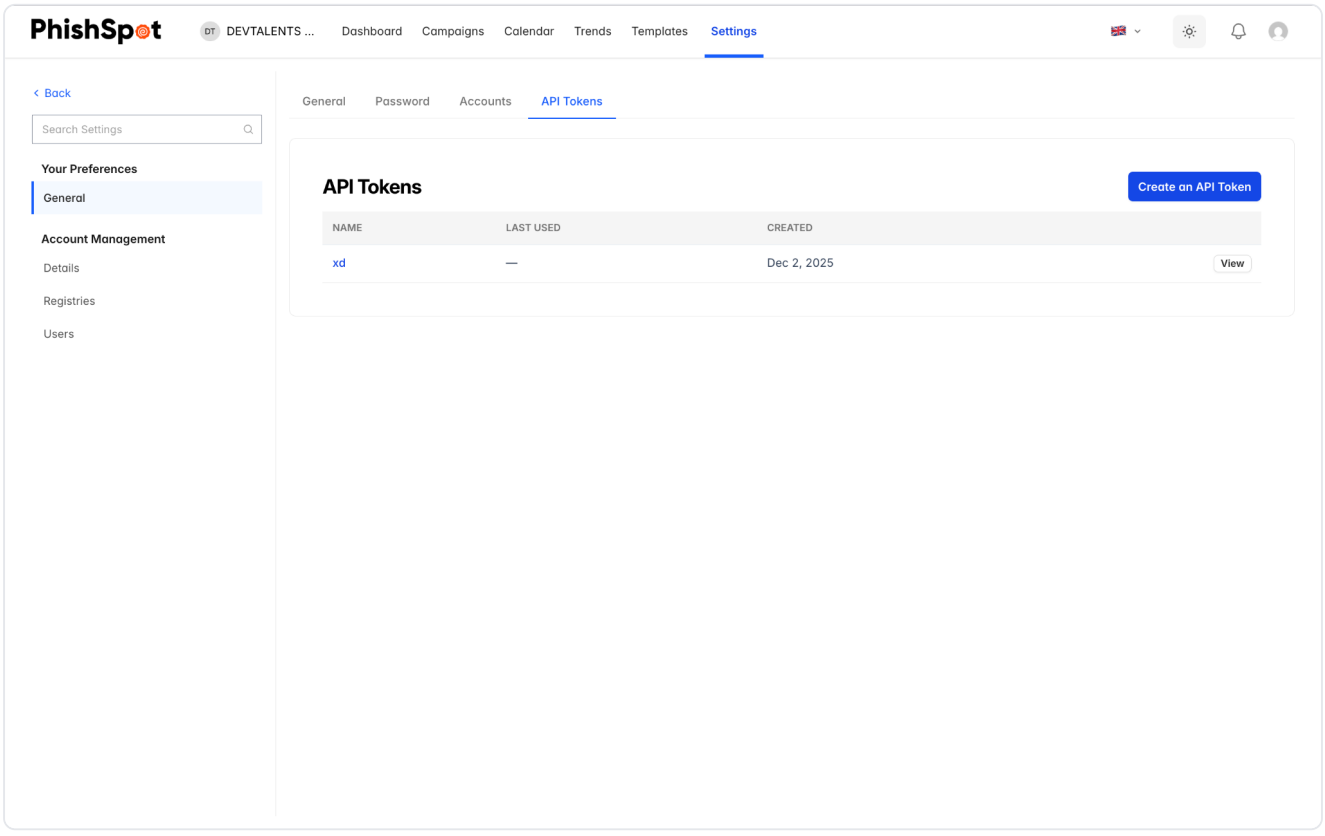
> Konta osobiste nie mogą zostać usunięte. Opcję usunięcia posiadają jedynie konta zespołowe/organizacyjne.

Tokeny API

PhishSpot udostępnia API typu REST dla dostępu programistycznego. Aby z niego skorzystać, potrzebujesz tokenu API.

14.1 Zarządzanie Tokenami

Przejdź do swojego profilu użytkownika i wybierz Tokeny API (API Tokens). Lista wykazuje wszystkie Twoje tokeny wraz z ich nazwą, datą ostatniego użycia i datą utworzenia. Kliknij Nowy Token (New Token), aby go utworzyć. Po utworzeniu wartość tokenu zostanie wyświetlona tylko raz — pamiętaj, aby od razu go skopiować, gdyż nie można go będzie podejrzeć w przyszłości.



> Tokeny API powiązane są z Twoim kontem użytkownika, a nie z konkretnym zespołem. Zapewnij im bezpieczeństwo i poddawaj je cyklicznej rotacji.

Profil Użytkownika i Preferencje

Uzyskaj dostęp do swoich ustawień osobistych poprzez kliknięcie swojego imienia lub awatara w prawym górnym rogu, a następnie wybranie opcji „profil”.

15.1 Ustawienia Profilu

- **Imię, Nazwisko i E-mail** — Zaktualizuj swoją wyświetlaną nazwę i adres e-mail.
- **Hasło** — Zmień swoje hasło logowania.
- **Uwierzytelnianie Dwuskładnikowe** — Aktywuj lub zarządzaj funkcją 2FA dla dodatkowego bezpieczeństwa.
- **Motyw** — Przełączaj pomiędzy trybem jasnym i ciemnym.

Typowe Przepływy Pracy

16.1 Przeprowadzenie Twojej Pierwszej Kampanii

Wykonaj poniższe kroki, aby wdrożyć swoją pierwszą symulację phishingu:

1. Dodaj swoje kontakty poprzez import pliku CSV (Ustawienia → Kontakty).
2. Utwórz przynajmniej jedną grupę i przypisz do niej swoje kontakty (Ustawienia → Grupy).
3. Zweryfikuj swoją domenę wysyłającą (Ustawienia → Zabezpieczone Domeny).
4. Przejrzyj bibliotekę szablonów i odnajdź odpowiedni szablon phishingowy (Szablony).
5. Kliknij opcję Szybkie Uruchomienie (Quick Launch) na szablonie lub utwórz nową kampanię ręcznie (Kampanie → Nowa Kampania).
6. Przejdź przez 6-krokowy kreator: skonfiguruj ustawienia, dopasuj wiadomość, przygotuj stronę docelową, wybierz akcję po kliknięciu, wskaż odbiorców i zweryfikuj podsumowanie.
7. Wyślij e-mail testowy do siebie i sprawdź, czy wszystko wygląda odpowiednio.
8. Rozpocznij lub zaplanuj kampanię.
9. Monitoruj wyniki na pulpicie kampanii.

16.2 Długoterminowy Program Phishingowy

W celu prowadzenia ciągłego programu budowania świadomości bezpieczeństwa:

- Planuj cykliczne kampanie, włączając ich automatyczne ponawianie w zadanym interwale.
- Korzystaj za każdym razem z innych szablonów w celu przetestowania różnorodnych wektorów ataku.
- Monitoruj Pulpit Trendów w celu śledzenia postępów w długim horyzoncie czasowym.
- Zogniskuj dodatkowe moduły szkoleniowe na działach lub grupach posiadających wyższy współczynnik klikalności (click rate).
- Eksportuj zbiorcze raporty na potrzeby kwartalnych analiz przez kierownictwo.
- Regularnie aktualizuj listę kontaktów w oparciu o zatrudnianie nowych i zwalnianie dotychczasowych pracowników.

16.3 Reagowanie na Użytkowników Wysokiego Ryzyka

Gdy platforma zidentyfikuje użytkowników charakteryzujących się wysokim współczynnikiem ryzyka (czerwone odznaki):

- Przejrzyj ich profil, aby zweryfikować kampanie, na które dali się nabrać.
- Sprawdź, czy pomyślnie ukończyli przydzielone kursy szkoleniowe.
- Rozważ włączenie ich do dedykowanej grupy celowej pod kątem specjalnie przygotowanych kampanii.
- Używaj filtrów kontaktów w celu znalezienia użytkowników wysokiego ryzyka z całej organizacji.

Zmienne szablonów

Pisząc treść e-maili lub tworząc strony docelowe, możesz korzystać ze zmiennych szablonu — tagów scalających — aby personalizować treść dla każdego odbiorcy. Zmienne są zastępowane rzeczywistymi wartościami danego odbiorcy podczas wysyłki e-maila lub wyświetlenia strony docelowej.

Otocz zmienną podwójnymi nawiasami klamrowymi: `{{first_name}}`. Dostępne zmienne różnią się między **e-mailem** (temat i treść) a **stroną docelową** (oraz wiadomością edukacyjną), ponieważ każde z nich renderowane jest w innym kontekście. Edytor to weryfikuje — nie zapiszesz e-maila odwołującego się do zmiennej dostępnej wyłącznie na stronie docelowej.

Zmienne w e-mailu (temat i treść)

Zmienna	Opis	Przykładowy wynik
`{{first_name}}`	Imię odbiorcy	Jan
`{{last_name}}`	Nazwisko odbiorcy	Kowalski
`{{full_name}}`	Imię i nazwisko odbiorcy	Jan Kowalski
`{{email}}`	Adres e-mail odbiorcy	jan.kowalski@firma.pl
`{{position}}`	Stanowisko odbiorcy	Starszy Analityk
`{{department}}`	Dział odbiorcy	Finanse
`{{company}}`	Nazwa Twojego konta (organizacji)	Acme Sp. z o.o.
`{{campaign_name}}`	Nazwa kampanii	Test faktur Q2
`{{landing_url}}`	Śledzony link odbiorcy	https://domena.pl/l/abc123?d=…

Zmienne na stronie docelowej i w wiadomości edukacyjnej

Zmienna	Opis
`{{first_name}}`, `{{last_name}}`, `{{full_name}}`, `{{email}}`	Jak wyżej
`{{company}}`	Nazwa Twojego konta (organizacji)
`{{landing_url}}`	Śledzony link odbiorcy
`{{elearning_url}}`	Link szkoleniowy odbiorcy (do użycia na stronie edukacyjnej)

> Nazwy zmiennych **nie rozróżniają wielkości liter** i tolerują otaczające spacje — `{{First_Name}}` oraz `{{ first_name }}` działają tak samo. Jeśli zmienna nie ma wartości dla danego odbiorcy, zostaje zastąpiona pustym tekstem. Nazwa zmiennej spoza powyższej listy pozostaje w treści **dosłownie**, więc uważaj na literówki i zawsze wysyłaj testowy e-mail.

Wskazówki, jak *skutecznie używać* tych zmiennych w kampanii, znajdziesz w Projektowanie skutecznych kampanii §30.1.

Rozwiązywanie problemów

18.1 E-maile nie są dostarczane

- Sprawdź, czy domena wysyłająca ma status „Zweryfikowana” (Ustawienia → Zabezpieczone Domeny).
- Sprawdź, czy adres nadawcy e-mail pasuje do zweryfikowanej domeny.
- Upewnij się, czy kampania jest w statusie „Aktywna” i nie została wstrzymana lub zablokowana.
- Jeżeli używasz trybu godzin pracy, zweryfikuj czy aktualny czas pokrywa się z właściwym oknem dostarczania wiadomości.

18.2 Strona Docelowa nie ładuje się

- Zweryfikuj w ustawieniach kampanii, czy platforma ma przypisaną prawidłową domenę.
- Zbadaj, czy strona docelowa została uaktywniona (przycisk w Kroku 3 w kreatorze).
- Upewnij się, że używana domena platformy nie wygasła.

18.3 Kontakty nie importują się

- Pobierz próbny plik CSV i zbadaj, czy zawartość dostarczanego przez Ciebie dokumentu zgadza się z pożądanym schematem wprowadzania danych.
- Skontroluj, czy kolumna „E-mail” posiada dopuszczalne wartości dla adresów pocztowych.
- Szukaj powtarzeń w adresach pocztowych — jeśli odnalezione zostaną podobne rekordy adresów, import użytkownika do platformy zostanie przerwany.
- Jeżeli pewne polecenia kończą się niepomyślnie, ściągnij plik z nieudanymi wynikami (CSV), żeby dociec sedna problemu poprzez wygenerowane powiadomienia o zakłóceniach działania skryptu.

18.4 Nie można edytować kampanii

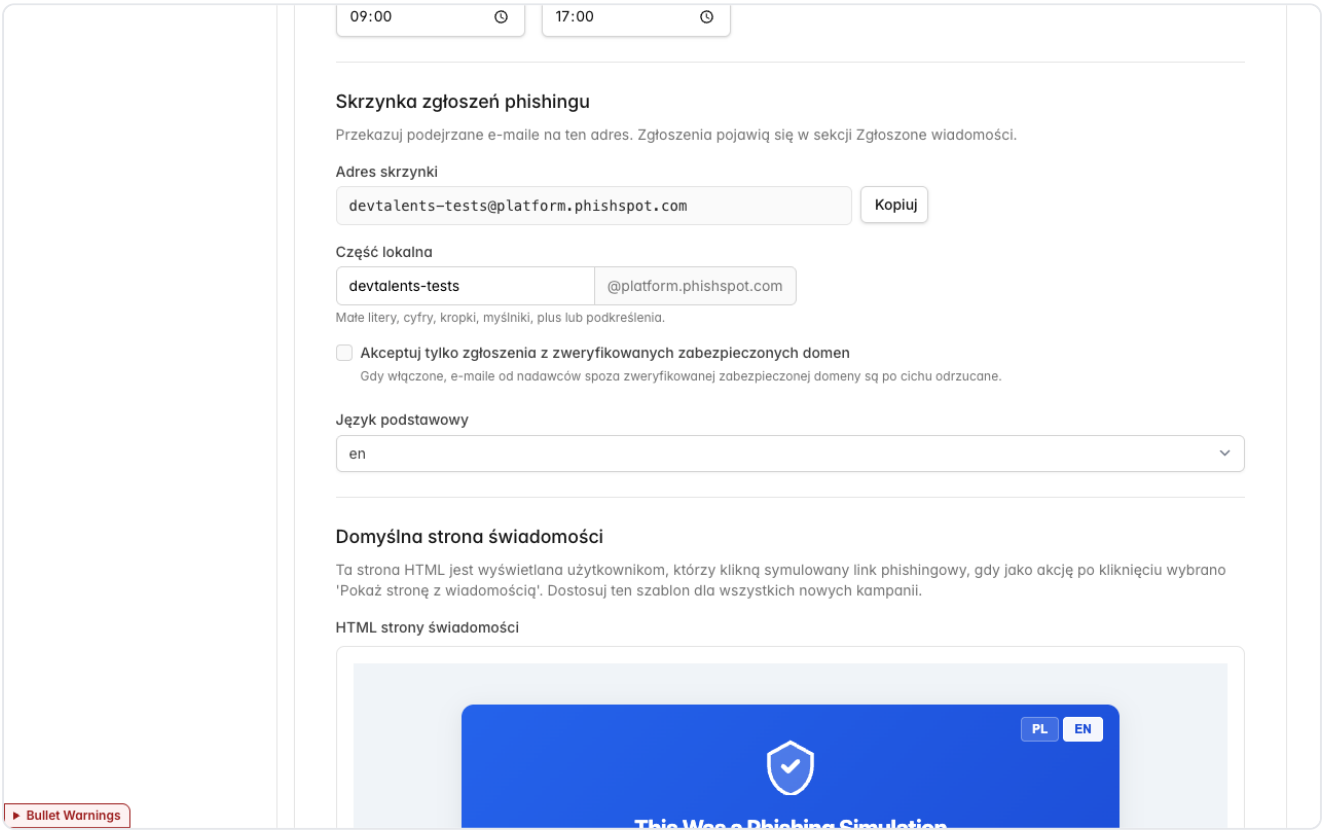
- Wyłącznie kampanie oznaczone jako „Szkic” lub „Zaplanowane” mogą być edytowane.
- Kampanie w stanie „Aktywne”, „Wstrzymane” oraz „Zakończone” są tylko do odczytu.
- Jeśli potrzebujesz zmodyfikować treść aktywnej kampanii, zduplikuj ją, dokonaj zmian i uruchom nową kopię.

Zgłoszone wiadomości

Zgłoszone wiadomości to skrzynka, do której Twoi pracownicy przekazują podejrzane e-maile, aby Twój zespół mógł je sprawdzić w PhishSpot. Każde konto otrzymuje własny unikalny adres. Zgłoszenia pojawiają się w dedykowanej sekcji w nawigacji głównej. Podgląd domyślnie blokuje potencjalnie niebezpieczne elementy — obrazy, style, linki i załączniki są wyłączone, dopóki sam ich nie włączysz.

19.1 Skrzynka zgłoszeń phishingu

Każde konto otrzymuje własny adres w postaci `<lokalna_część>@platform.phishspot.com`. Część lokalna jest uzupełniana automatycznie przy tworzeniu konta i można ją edytować w **Ustawienia** → **Szczegóły konta** → **Skrzynka zgłoszeń phishingu**.



- **Adres skrzynki** — pełny adres, na który pracownicy powinni przekazywać podejrzane e-maile. Przycisk **Kopiuj** wstawia adres do schowka, dzięki czemu możesz wkleić go w materiały onboardingowe, podpis mailowy lub bazę wiedzy helpdesku.
- **Część lokalna** — edytowalna nazwa użytkownika w adresie. Małe litery, cyfry, kropki, myślniki, plus lub podkreślenia.
- **Akceptuj tylko zgłoszenia z zweryfikowanych zabezpieczonych domen** — patrz 19.2.

19.2 Ograniczanie akceptowanych nadawców

Przełącznik **Akceptuj tylko zgłoszenia z zweryfikowanych zabezpieczonych domen** (domyślnie WŁ.) ogranicza krąg nadawców, którzy mogą złożyć zgłoszenie:

- **WŁ.** — akceptowane są wyłącznie e-maile, których domena nadawcy znajduje się wśród Twoich **zweryfikowanych Zabezpieczonych Domen**. Pozostałe są odrzucane bez powiadamiania nadawcy.
- **WYŁ.** — akceptowani są wszyscy nadawcy.

W produkcji zostaw WŁ. Wyłącz tymczasowo podczas pilotaży, gdy zgłaszający mogą pisać ze skrzynek, których jeszcze nie wciągnąłeś.

Gdy wiadomość jest odrzucana, nadawca nie jest powiadamiany — celowo, by ktoś sondujący Twoją skrzynkę nie otrzymał potwierdzenia.

19.3 Jak trafia zgłoszenie

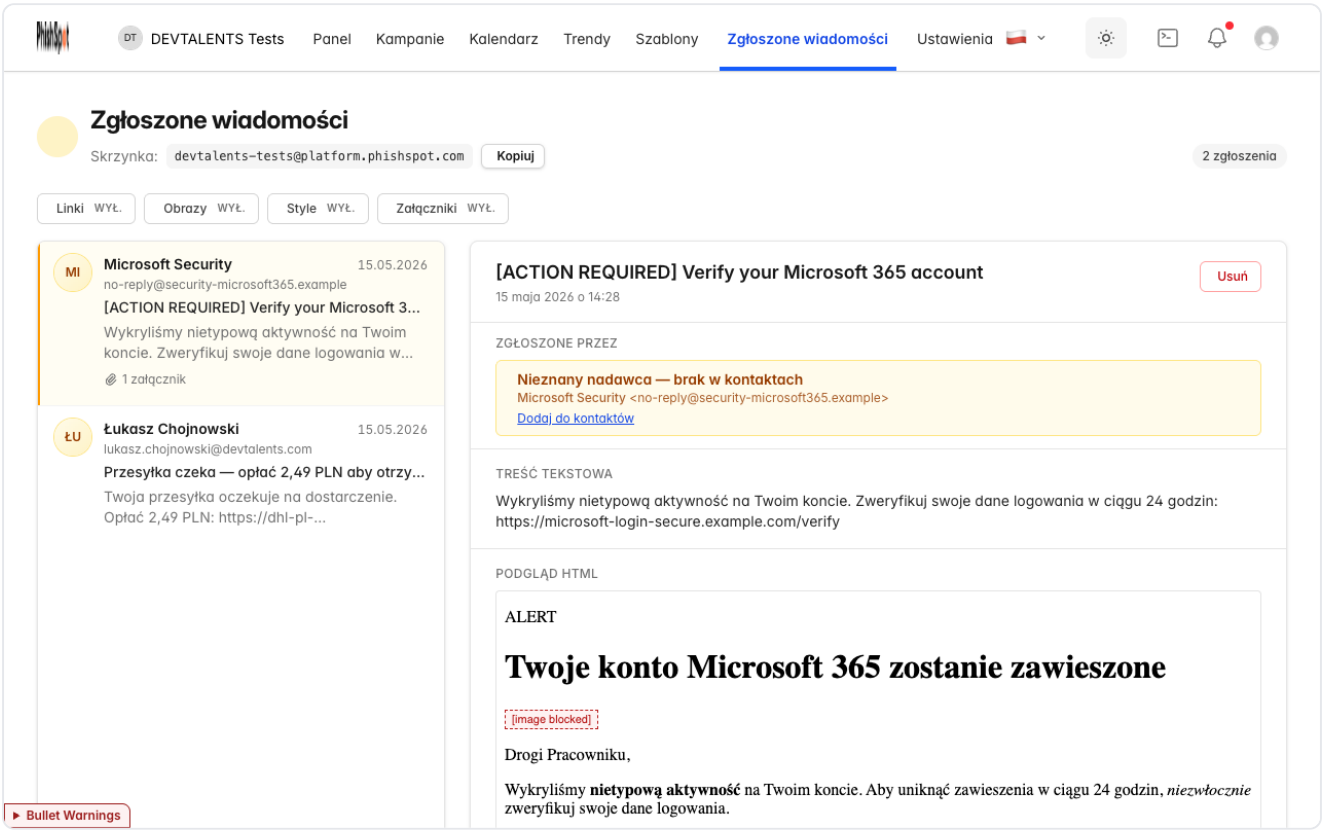
Przebieg dla Twojego zespołu:

1. Pracownik otrzymuje podejrzaną wiadomość.
2. Przekazuje ją na adres skrzynki Zgłoszonych wiadomości Twojego konta.
3. Zgłoszenie pojawia się w **Zgłoszone wiadomości** w nawigacji głównej, posortowane od najnowszych.

Propaguj adres skrzynki wśród pracowników podczas onboardingu, w bazie wiedzy helpdesku albo w stopce e-maila.

19.4 Strona Zgłoszone wiadomości

Otwórz **Zgłoszone wiadomości** z górnej nawigacji. Strona ma dwukolumnowy układ list/detal:



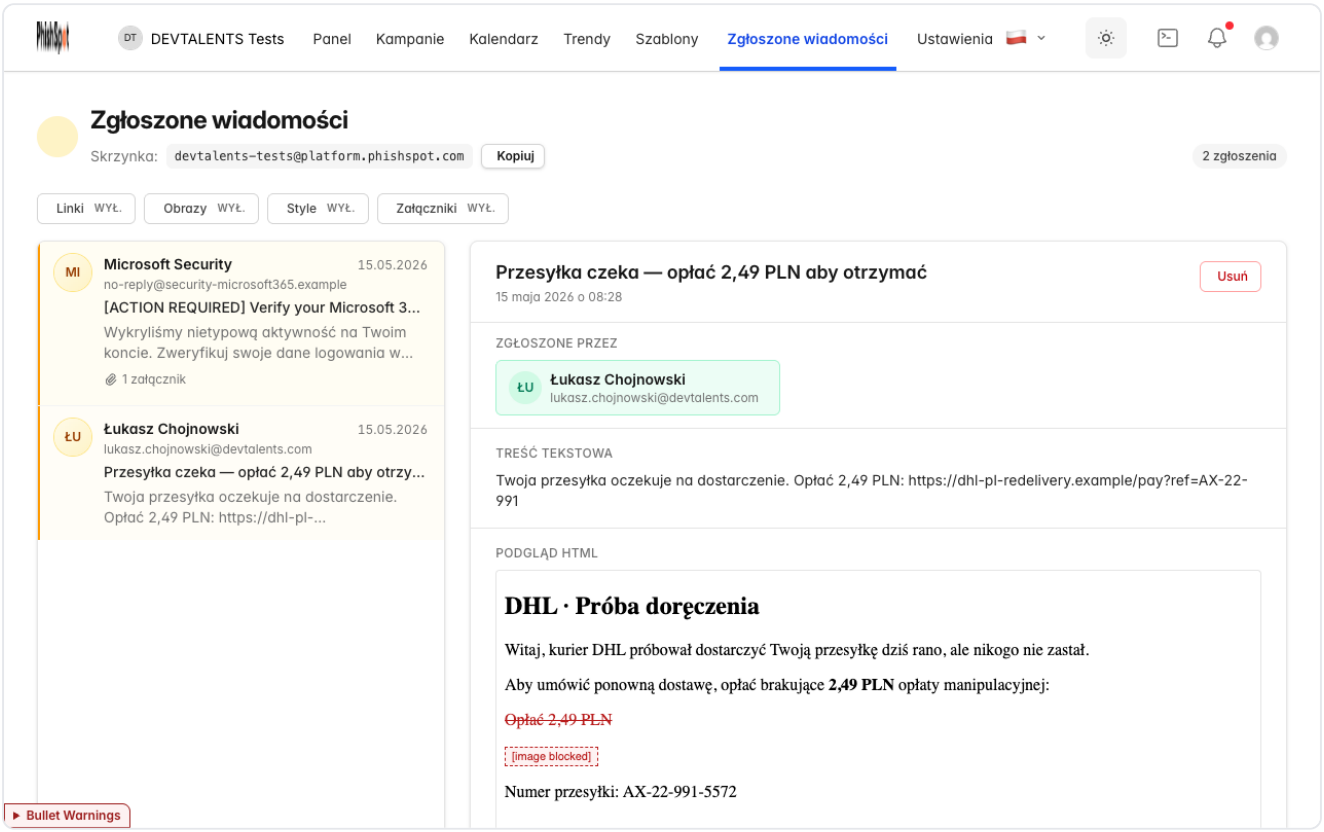
- **Lewa kolumna** — lista zgłoszeń, najnowsze na górze. Każdy element pokazuje imię (lub e-mail) zgłaszającego, temat i wycinek treści, liczbę załączników i datę otrzymania.
- **Prawa kolumna** — panel szczegółów wybranego zgłoszenia. Kliknij inny element po lewej, a prawy panel zmieni się natychmiast.
- **Licznik** — pigułka w prawym górnym rogu pokazuje liczbę zgłoszeń w koncie.
- **Skrzynka** — adres odbiorczy jest powtórzony pod tytułem wraz z przyciskiem **Kopiuj**.

19.5 Kto zgłosił

Tuż pod tematem każde zgłoszenie pokazuje panel **Zgłoszone przez**, który mówi Ci, czy nadawca jest znany w Twoim koncie.

Znany zgłaszający

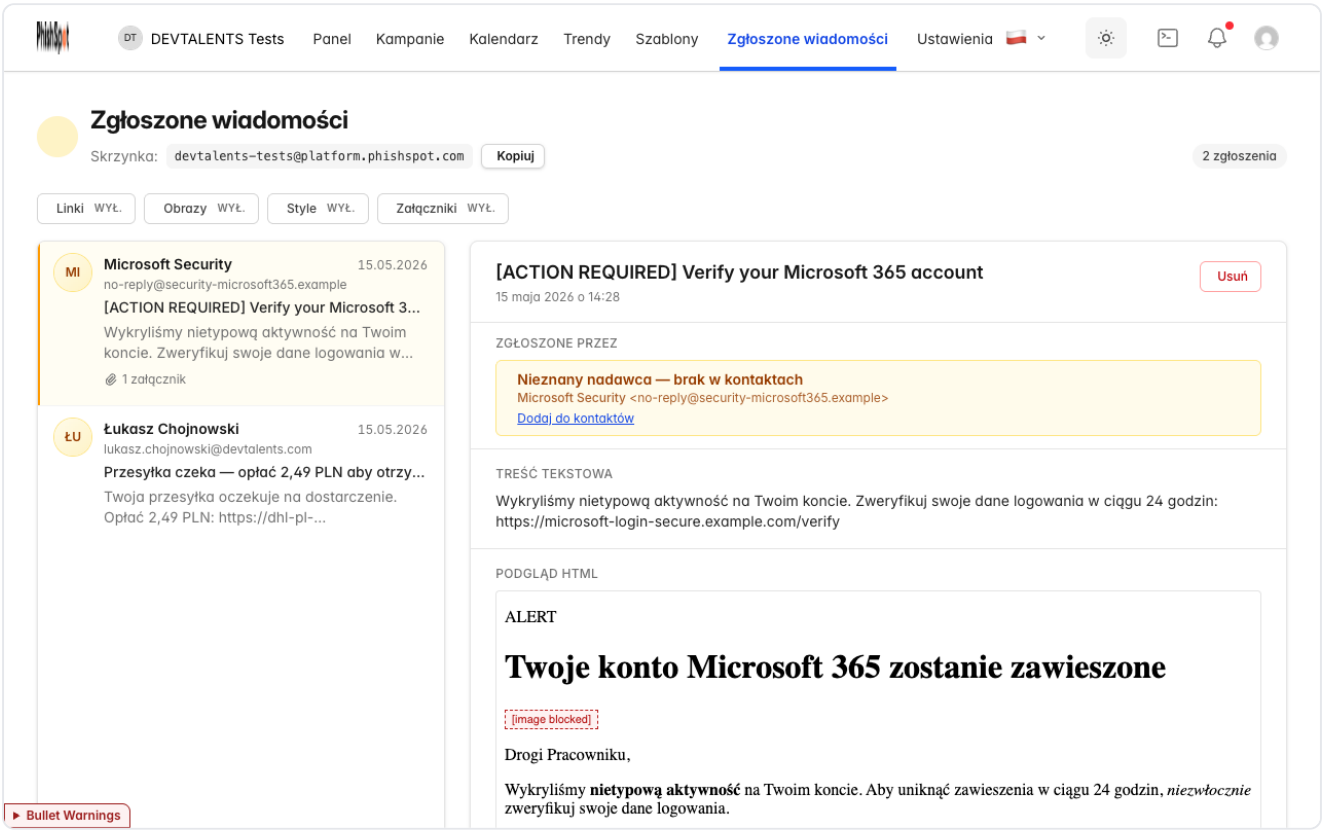
Jeśli e-mail nadawcy pasuje do **Kontaktu** w Twoim koncie, panel jest zielony i działa jak link do profilu tego kontaktu:



Kliknięcie panelu prowadzi prosto do kontaktu, gdzie możesz sprawdzić jego grupy, dotychczasowe wyniki kampanii i historię.

Nieznany zgłaszający

Jeśli żaden kontakt nie pasuje, panel jest bursztynowy i pokazuje dane nadawcy oraz szybki link dodawania:



Link **Dodaj do kontaktów** otwiera formularz nowego kontaktu z już wypełnionym e-mailem — wystarczy uzupełnić imię/nazwisko i zapisać.

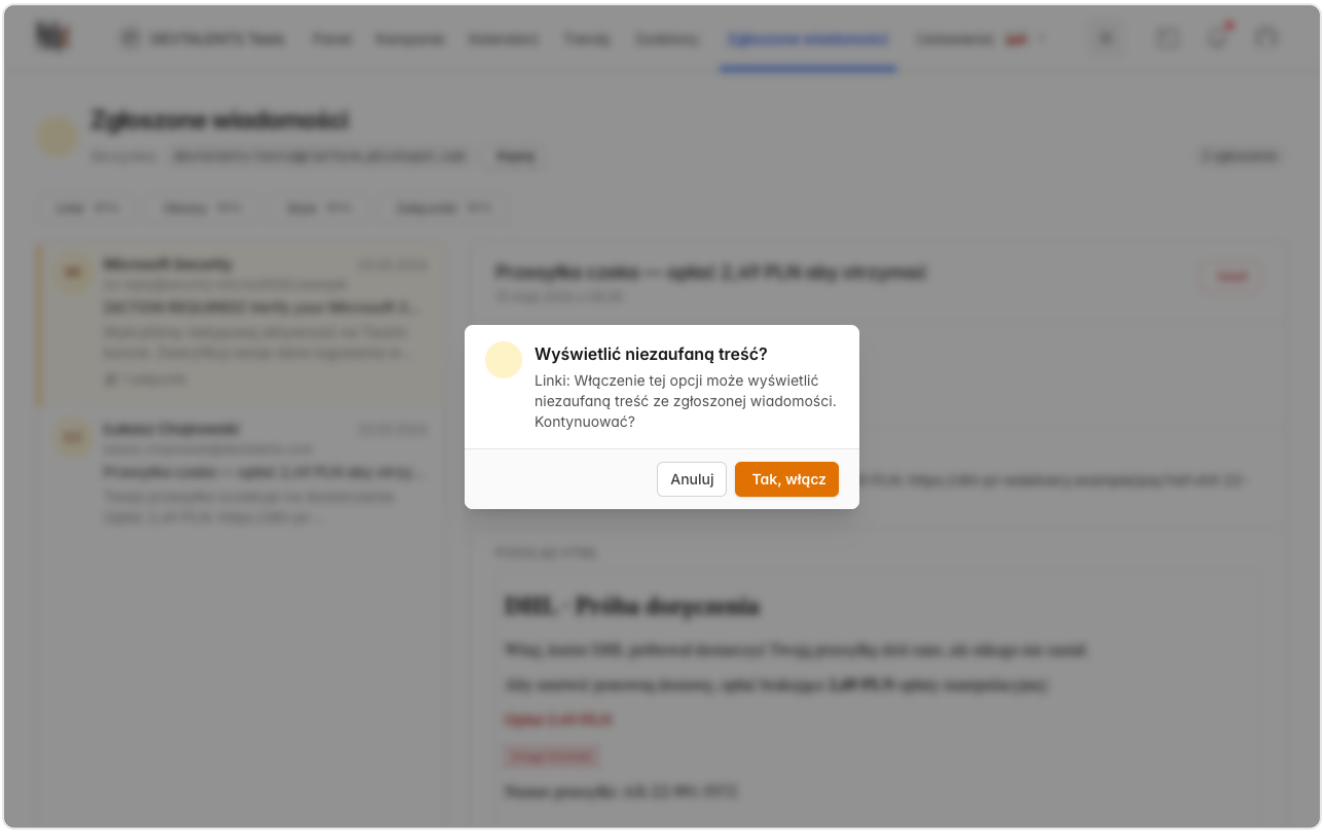
Zgłoszenie z adresu, którego nigdy nie wciągnąłeś, zasługuje na dodatkową analizę. Bursztynowe ostrzeżenie to pierwszy sygnał, że coś jest nie tak.

19.6 Bezpieczny podgląd

Wiadomości phishingowe są z definicji niezaufane. Widok szczegółów domyślnie wyłącza potencjalnie niebezpieczne części e-maila. Cztery przełączniki pozwalają stopniowo włączać kolejne elementy oryginalnej treści:

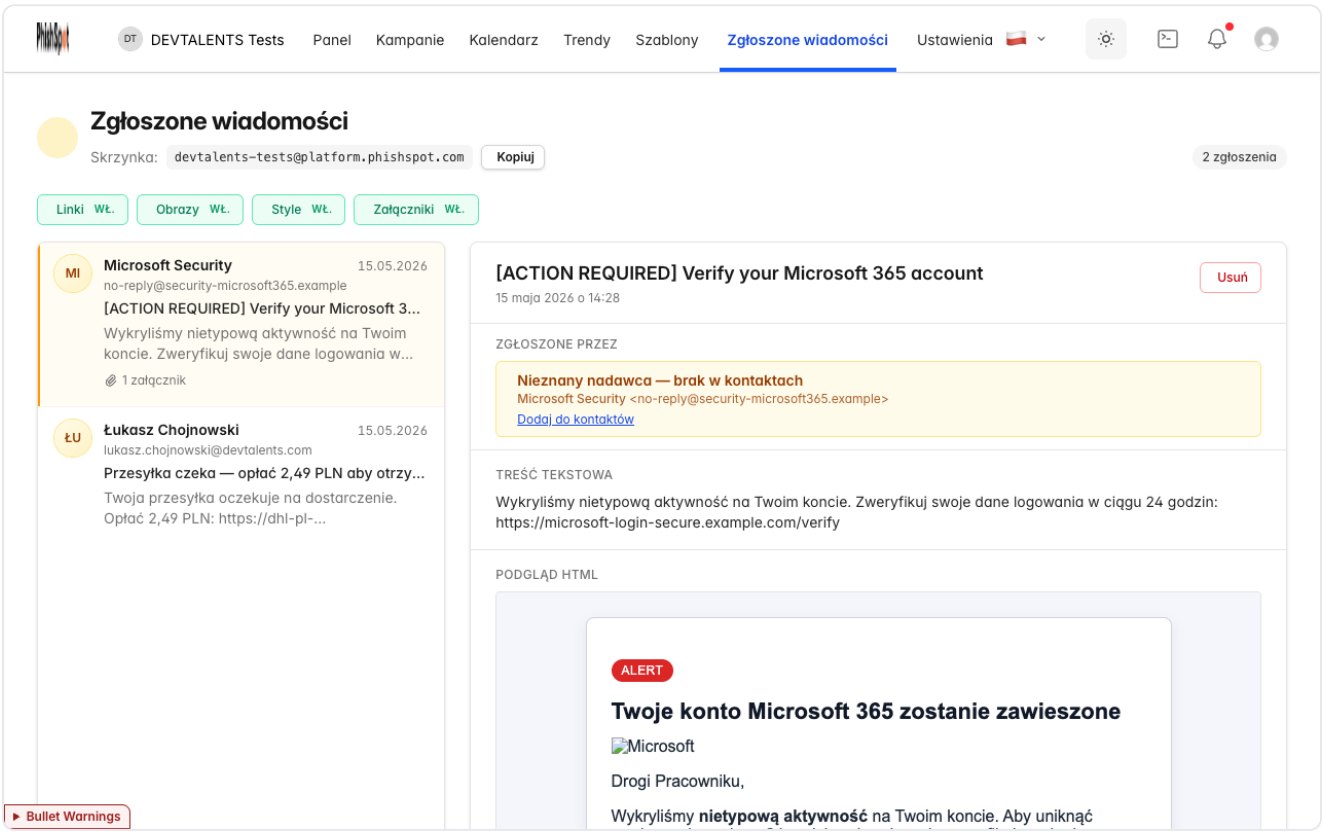
Przełącznik	Gdy WYŁ. (domyślnie)	Gdy WŁ.
Linki	Linki są pokazane jako czerwony przekreślony tekst. Po najechaniu w tooltipie widać adres docelowy. Nieklikalne.	Linki są klikalne i otwierają się w **nowej karcie przeglądarki** (nigdy w obrębie PhishSpot).
Obrazy	Każdy obraz jest zastąpiony placeholderem `[image blocked]`.	Obrazy ładują się z oryginalnych źródeł.
Style	Wszystkie style są usuwane — czysty tekst.	E-mail renderuje się z oryginalnym stylem.
Załączniki	Nazwy plików są wymienione, ale brak przycisków pobierania.	Każdy załącznik ma przycisk **Pobierz**.

Włączenie dowolnego przełącznika otwiera okno potwierdzenia:

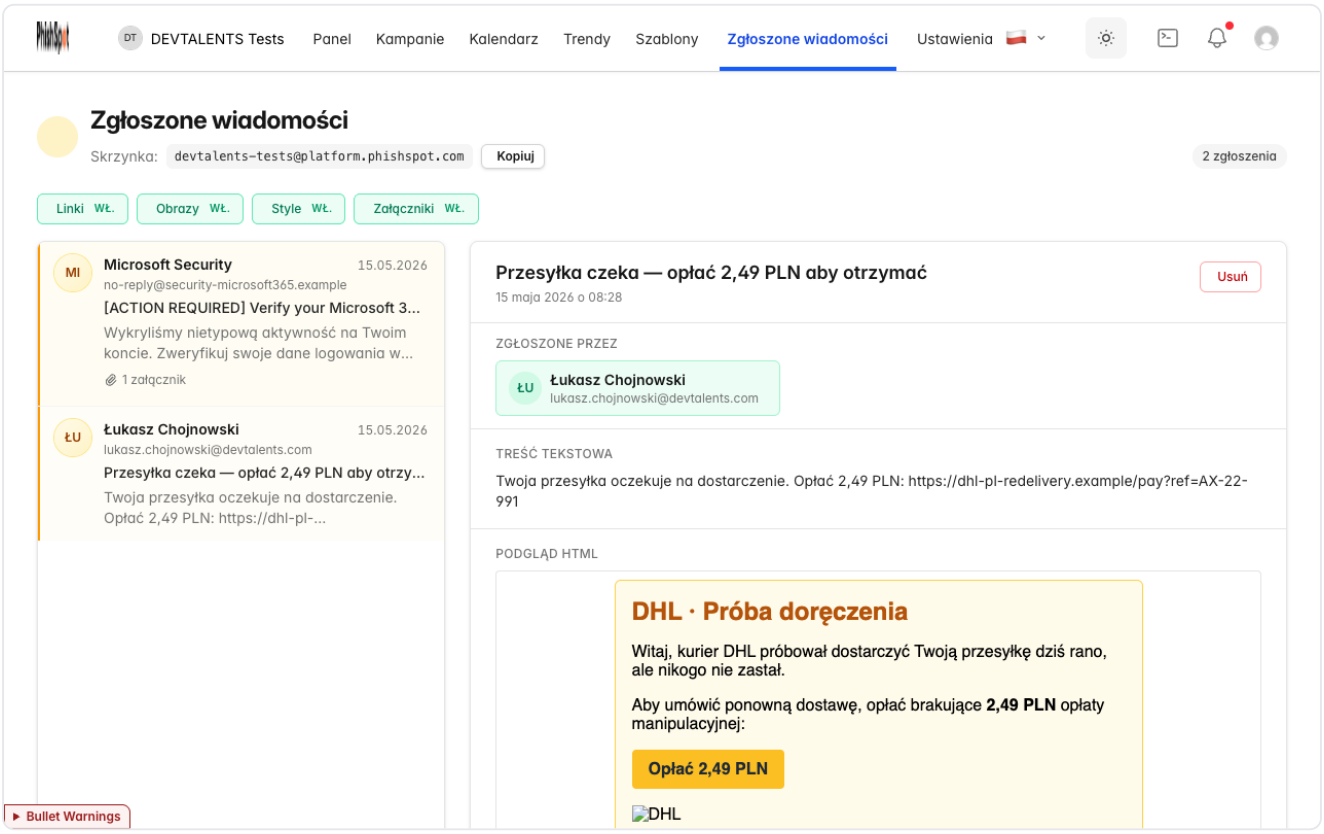


Wyłączenie nie wymaga potwierdzenia.

Po włączeniu Stylów i Obrazów e-mail renderuje się tak, jak zaprojektował go atakujący — przydatne przy analizie kampanii click-through:



Z włączonymi Linkami przyciski wewnątrz wiadomości stają się klikalne. Zawsze otwierają się w **nowej karcie przeglądarki**, więc możesz sprawdzić adres docelowy nie opuszczając PhishSpot:



> Przełączniki są **na poziomie konta**, nie pojedynczego zgłoszenia. Zmiana jednego wpływa na każde zgłoszenie w skrzynce. Domyślnie **wszystkie są WYŁ.** — nowe konta są bezpieczne od startu.

19.7 Usuwanie zgłoszenia

Przycisk **Usuń** w prawym górnym rogu panelu szczegółów usuwa zgłoszenie (po potwierdzeniu). Tylko **administratorzy** i **edytorzy** mogą usuwać; **członkowie** mogą wyłącznie podglądać.

Dodatek do Outlooka

Dodatek PhishSpot do Outlooka dodaje przycisk **Zgłoś phishing** do każdej otwieranej wiadomości. Jedno kliknięcie wysyła wiadomość (treść, nagłówki, załączniki) do listy zgłoszonych wiadomości w Twoim koncie PhishSpot. Bez przekierowywania na specjalny adres ani ręcznego kopiowania.

Ta strona jest przeznaczona dla użytkowników końcowych. Jeśli jesteś administratorem wdrażającym dodatek w całej organizacji, zobacz Dodatek do Outlooka: wdrożenie centralne.

20.1 Czego potrzebujesz

- Outlook w przeglądarce, Outlook dla Windows lub Mac, albo **nowy** Outlook dla Windows.
- Konto **Kontaktu** PhishSpot w Twojej organizacji (zespół IT może je utworzyć, jeśli go nie masz).
- Kilka minut na instalację i sparowanie dodatku.

Dodatek nie działa w Outlooku dla iOS / Android w wersji 1.

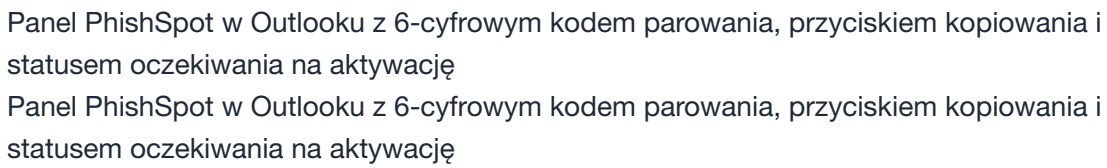
20.2 Instalacja dodatku

1. Pobierz paczkę sideload: phishspot-outlook-sideload-v1.1.0.zip.
2. Rozpakuj. Otrzymasz `manifest.xml`, folder z ikonami i `README.md` z instrukcjami dla każdej wersji Outlooka.
3. W Outlooku wybierz **Pobierz dodatki** → **Moje dodatki** → **Dodaj dodatek niestandardowy** → **Dodaj z pliku…** i wskaż `manifest.xml`.
4. Potwierdź instalację. Przycisk **Zgłoś phishing** pojawi się na wstążce.

Jeśli zespół IT wdrożył dodatek centralnie dla wszystkich, **pomiń instalację** — zobaczysz przycisk automatycznie.

20.3 Sparowanie dodatku (jednorazowo)

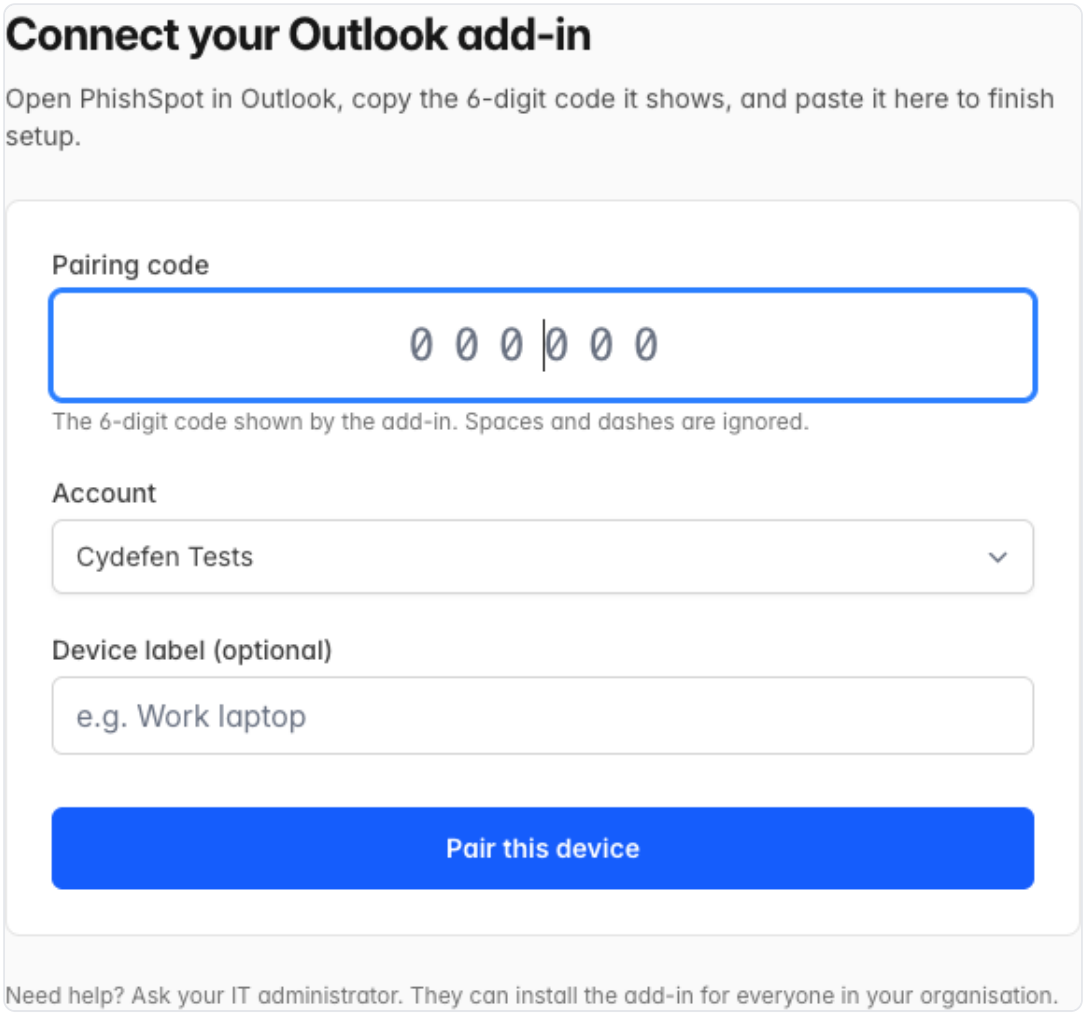
Przy pierwszym kliknięciu **Zgłoś phishing** dodatek pokaże 6-cyfrowy kod w panelu PhishSpot po prawej stronie Outlooka:



Panel PhishSpot w Outlooku z 6-cyfrowym kodem parowania, przyciskiem kopiowania i statusem oczekiwania na aktywację

Panel PhishSpot w Outlooku z 6-cyfrowym kodem parowania, przyciskiem kopiowania i statusem oczekiwania na aktywację

1. Otwórz `https://platform.phishspot.com/guest/activation/new` w przeglądarce (link **tutaj** w panelu zaprowadzi Cię bezpośrednio na tę stronę). Po zalogowaniu zobaczysz stronę **Connect your Outlook add-in**:



Strona Connect your Outlook add-in w przeglądarce, z polem na kod parowania, selektorem konta, opcjonalną etykietą urządzenia i przyciskiem Pair this device

2. Zaloguj się tym samym adresem e-mail, który zarejestrował zespół IT.
3. Wpisz lub wklej 6-cyfrowy kod pokazany w panelu.
4. Wybierz konto, z którym chcesz sparować (jeśli należysz do więcej niż jednego), opcjonalnie nazwij urządzenie i kliknij **Pair this device**.

Dodatek wykryje parowanie w ciągu kilku sekund i przejdzie do widoku normalnego — z dużym przyciskiem **Zgłoś podejrzaną wiadomość** i nazwą Twojej organizacji pod spodem:

> Panel PhishSpot w stanie sparowanym — duży przycisk zgłaszania, nazwa organizacji, znak wodny i ikony zmiany motywu/języka na dole
> Panel PhishSpot w stanie sparowanym — duży przycisk zgłaszania, nazwa organizacji, znak wodny i ikony zmiany motywu/języka na dole

Parowanie jest per-urządzenie — jeśli masz Outlook na dwóch komputerach, sparujesz każdy oddzielnie. Możesz nadać urządzeniu nazwę (np. “Laptop służbowy”), aby administrator mógł je rozróżnić w panelu tokenów API.

20.4 Zgłaszanie podejrzanej wiadomości

1. Otwórz wiadomość, którą podejrzewasz o phishing.
2. Kliknij **Zgłoś podejrzaną wiadomość** w panelu.
3. Panel pokaże krótko “Zgłaszanie…” w trakcie wysyłania.
4. Ekran z podziękowaniem potwierdzi wysłanie zgłoszenia:

   Panel PhishSpot pokazujący ekran z zielonym znaczkiem i podziękowaniem po pomyślnym zgłoszeniu
   Panel PhishSpot pokazujący ekran z zielonym znaczkiem i podziękowaniem po pomyślnym zgłoszeniu

Kliknij **Close**, aby zamknąć panel.

Zgłoszenie pojawi się na liście **Zgłoszone wiadomości** Twojej organizacji. Zespół bezpieczeństwa je przeanalizuje.

20.5 Co jest wysyłane

- Adres e-mail i nazwa nadawcy
- Temat oraz treść wiadomości (HTML + tekst)
- Pełne nagłówki internetowe
- Wszystkie załączniki
- Sygnatura czasowa i Internet Message ID (dla deduplikacji)

Token uwierzytelnienia ma uprawnienie wyłącznie do **reported_messages:create**. Dodatek nie może czytać, modyfikować ani wysyłać innej poczty.

20.6 Komunikat “Dostępna jest aktualizacja”

Przy każdym kliknięciu dodatek sprawdza wersję na serwerze. Dwa scenariusze:

- **Aktualizacja jest dostępna** — miękki baner; nadal możesz zgłaszać. Poproś IT o aktualizację, gdy będzie to dogodne.
- **Wymagana aktualizacja** — twarda blokada; przycisk znika do czasu aktualizacji. Rzadkie.

20.7 Odłączenie / wylogowanie

Na karcie sparowanej kliknij **Odłącz to urządzenie**. Token zostanie usunięty z Twojego Outlooka. Administrator może dodatkowo odebrać token w panelu **Tokeny API**.

Dodatek do Outlooka: wdrożenie centralne

Ta strona jest przeznaczona dla administratorów IT, którzy chcą, aby przycisk **Zgłoś phishing** pojawiał się automatycznie u każdego użytkownika w tenancie M365. Instrukcje dla użytkownika końcowego: Dodatek do Outlooka.

21.1 Co jest instalowane

Niewielki manifest XML (~5 KB). `SourceLocation` w manifeście wskazuje na `https://platform.phishspot.com/outlook/taskpane`, gdzie ładuje się aktualny pakiet UI. Efekt: **wdrażanie nowych funkcji nie wymaga ponownego dystrybuowania dodatku** — sam manifest zmienia się tylko wtedy, gdy zmieniają się etykiety, uprawnienia lub ikony.

21.2 Pobierz artefakt

Plik manifestu do bezpośredniego wgrania:

phishspot-outlook-manifest-v1.0.0.xml

Pełna paczka sideload (zip z ikonami + README):

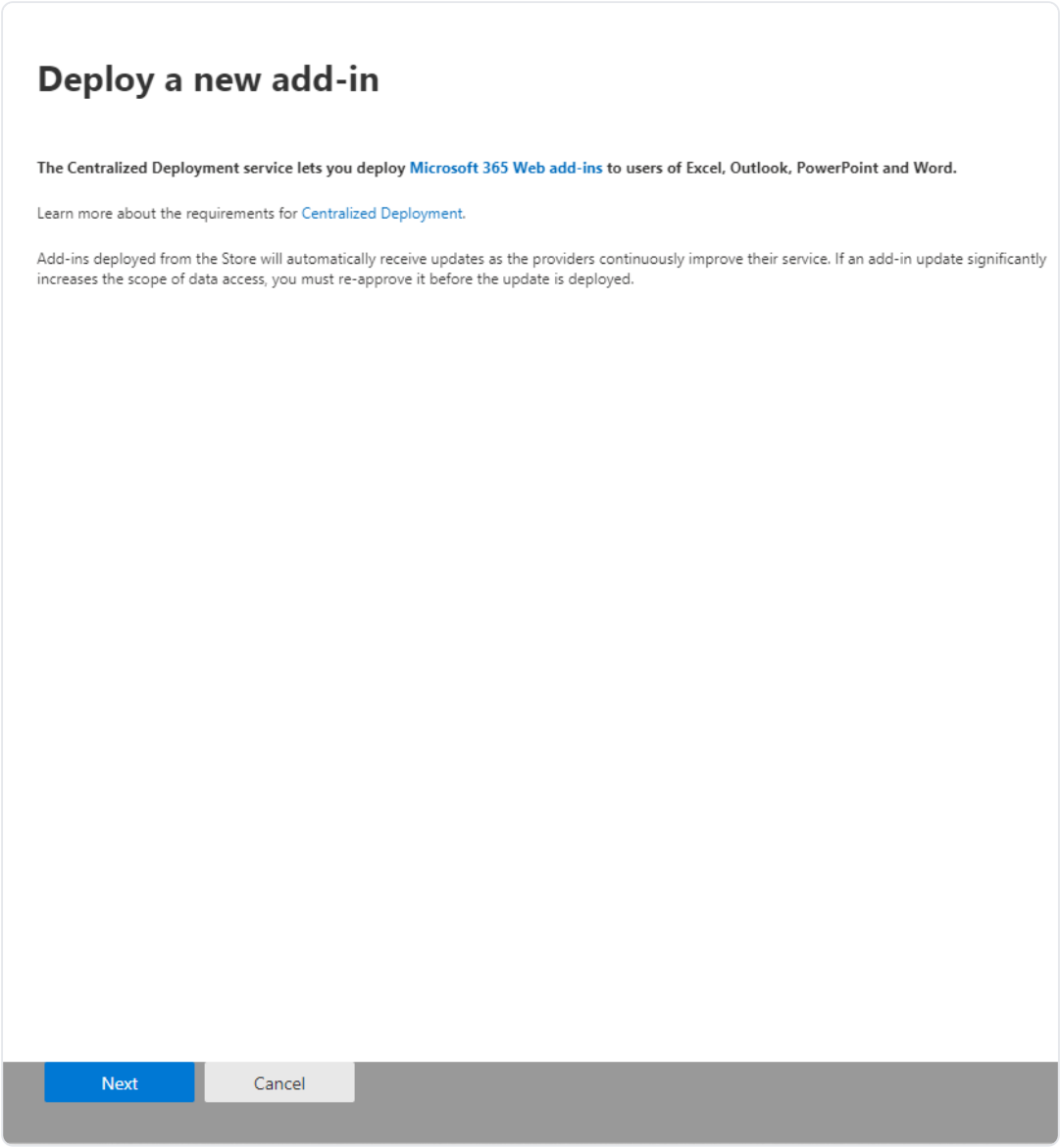
phishspot-outlook-sideload-v1.0.0.zip

21.3 Wdrożenie przez Microsoft 365 Admin Center

PhishSpot używa formatu **add-in only manifest**, więc wdrażaj go z portalu **Integrated apps** (ścieżka rekomendowana przez Microsoft). Klasyczny portal *Add-ins* w panelu administracyjnym też zadziała — oba obsługują ten format.

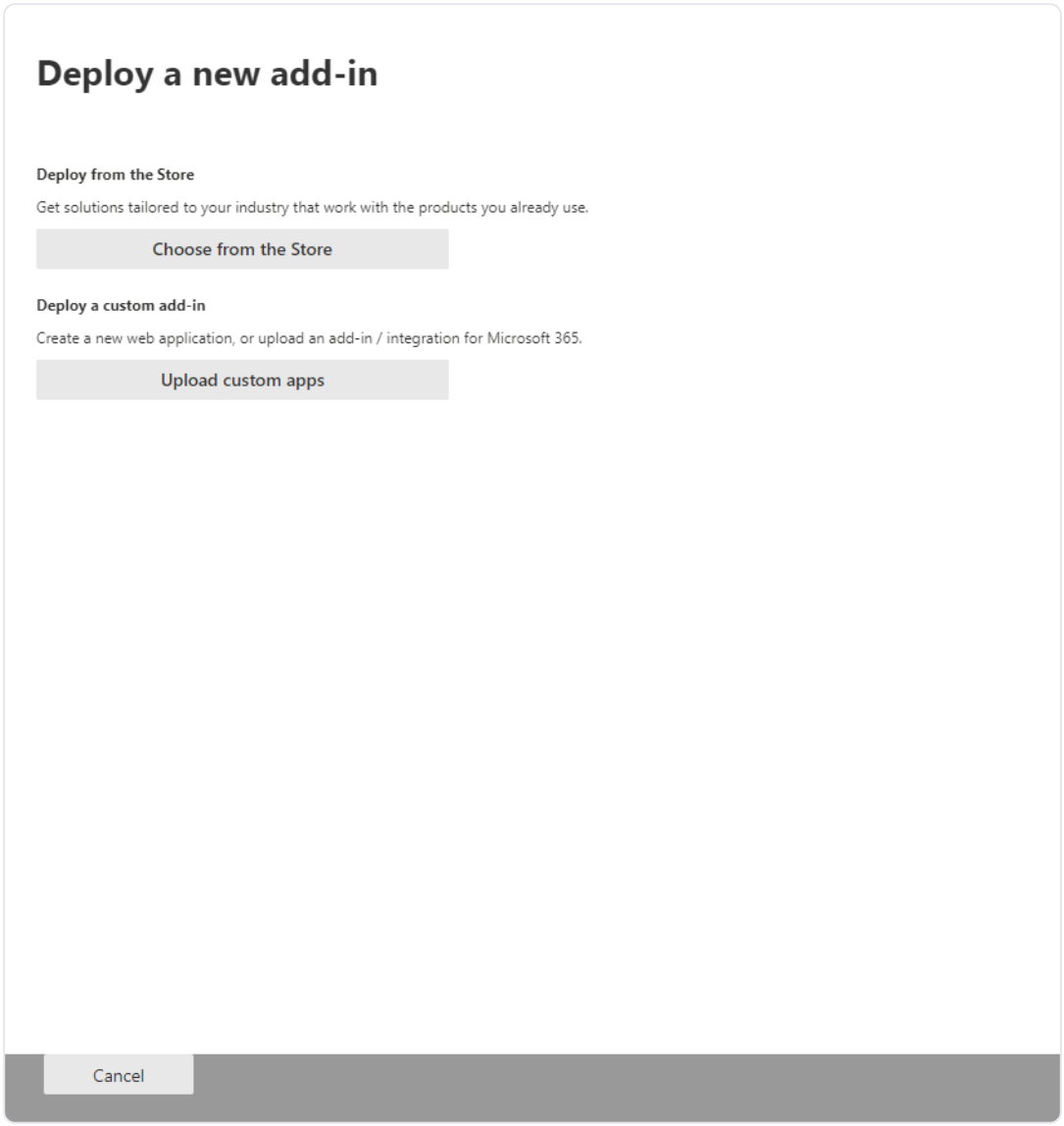
Przebieg krok po kroku

1. Zaloguj się do admin.microsoft.com jako Global Admin.
2. W menu po lewej rozwiń **… Show all**, a następnie wybierz **Settings** → **Integrated apps**.
3. Kliknij link **Add-ins** u góry strony Integrated apps, a potem **Deploy Add-in**.



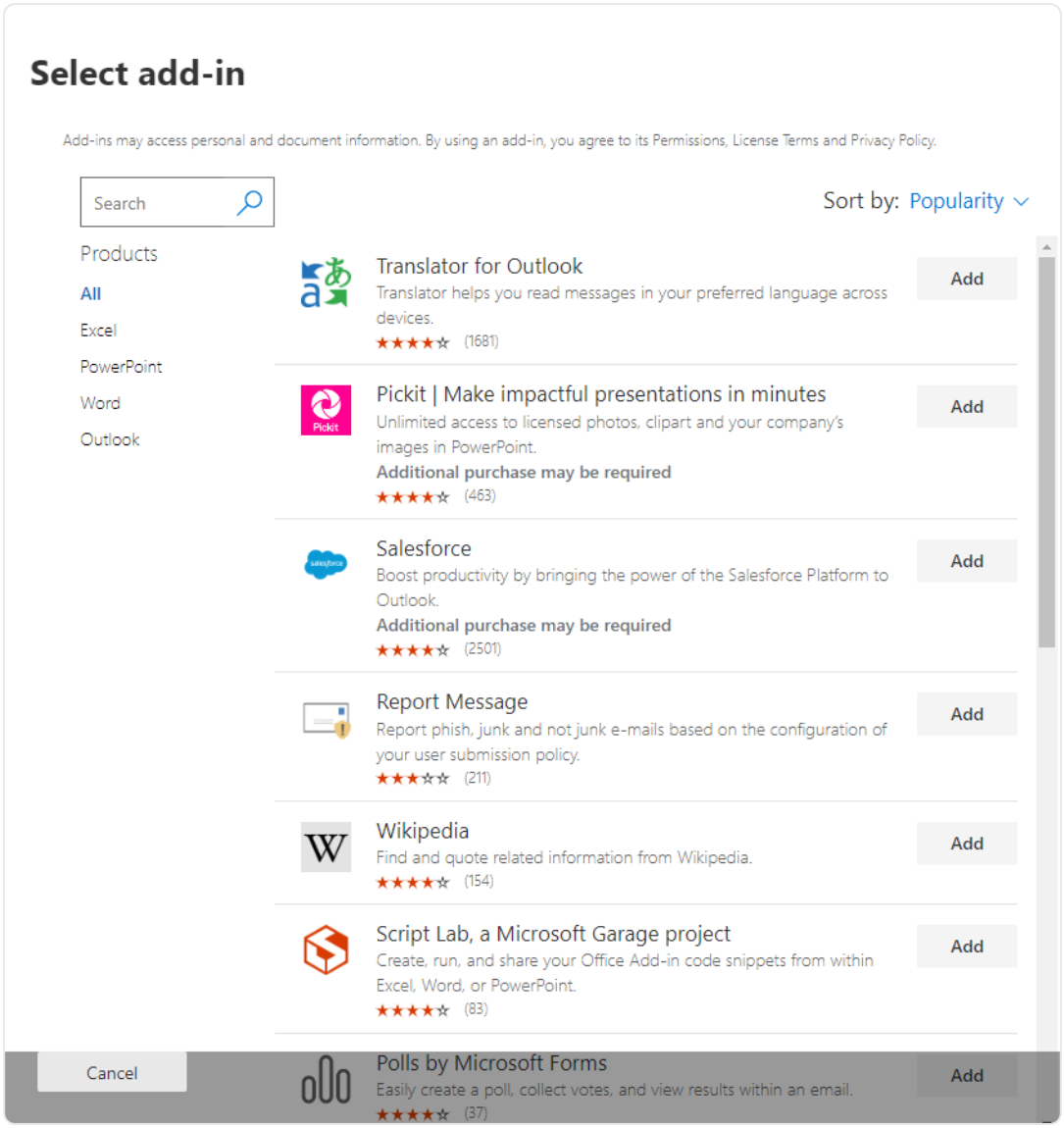
Microsoft 365 admin center z przyciskiem Deploy Add-in u góry strony Integrated apps

4. W wyborze źródła zaznacz **Upload custom apps** → **Upload manifest file (.xml) from device** i wskaż `phishspot-outlook-manifest-v1.0.0.xml`.



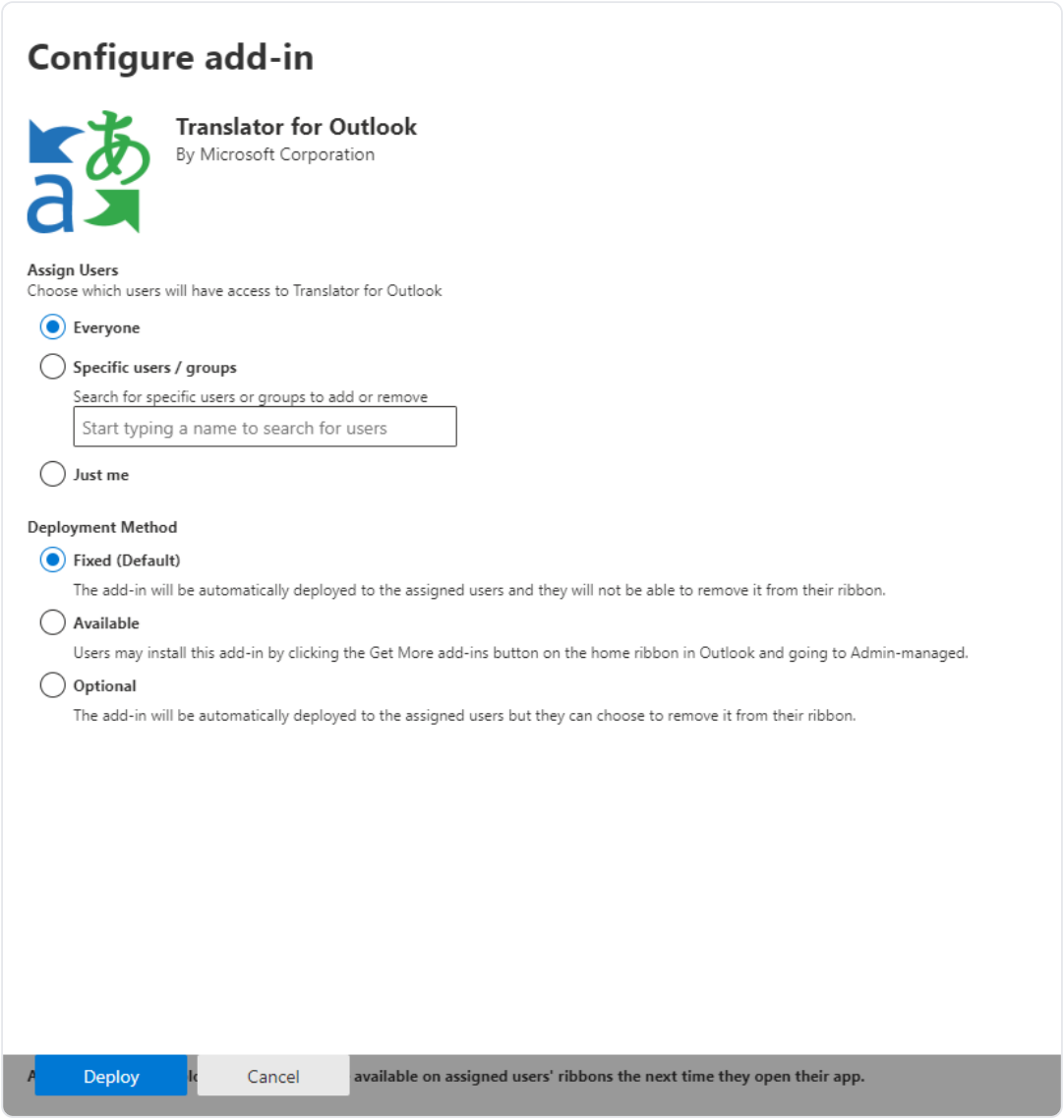
Kreator wdrożenia z wyborem źródła: Microsoft Marketplace albo upload własnego manifestu z pliku lub URL

(Kreator pokaże też dodatki z Microsoft Marketplace — to inna ścieżka, zignoruj. PhishSpot to dodatek typu LOB (line-of-business), instalowany z pliku manifestu.)



Kreator wdrożenia przeglądający dodatki z Microsoft Marketplace według kategorii

5. W kroku **Assign users** wybierz zakres i kliknij **Deploy**.



Krok kreatora z przypisaniem użytkowników/grup: opcje Everyone, Specific users/ groups, Just me

6. W następnym panelu przejrzyj uprawnienia — PhishSpot prosi tylko o zakres **ReadItem**. Nie może wysyłać poczty, modyfikować jej, ani czytać innych folderów niż aktualnie otwarta wiadomość. Uprawnienia są zadeklarowane w manifeście i nie zmieniają się przy aktualizacjach manifestu.

7. Potwierdź. Ostatni krok kreatora podpowiada, żeby **ogłosić wdrożenie** użytkownikom — zobacz *Wskazówki dla użytkowników* poniżej.

Zakres przypisania: wybieraj grupy, nie pojedynczych użytkowników

Zakres	Kiedy stosować
Everyone	“Używaj ostrożnie — tylko dla dodatków naprawdę uniwersalnych.” Zgłaszanie phishingu pasuje do wszystkich w większości organizacji, więc zwykle jest to dobry wybór.

Zakres	Kiedy stosować
Specific users / groups ⭐	**Zalecane.** Przypisanie do grupy oznacza, że nowi pracownicy automatycznie dostają dodatek, gdy zostaną dodani do grupy, a opuszczający — tracą go, gdy zostaną usunięci. Bez interwencji administratora. Przypisywanie do pojedynczych osób jest kruche — każda nowa osoba wymaga ręcznego dodania.
Just me	Idealne do testów. Po zweryfikowaniu, że przycisk działa w Twojej skrzynce, wróć do wdrożonego dodatku i kliknij **Change who has access to add-in**, aby poszerzyć rollout.

Czas propagacji

Microsoft dokumentuje, że **dodatki mogą pojawić się na wstążce po 24–72 godzinach** od wdrożenia, choć większość użytkowników widzi przycisk w ciągu 1–6 godzin. Użytkownicy mogą potrzebować zrestartować Outlooka (zamknąć wszystkie okna i otworzyć ponownie) zanim przycisk się pojawi. To normalne — nie eskaluj zbyt szybko.

21.4 Rekomendowana strategia rolloutu

Microsoft rekomenduje **wdrażanie falami**:

1. **Fala 1 — IT + interesariusze.** Wdróż dla zespołu IT i kilku interesariuszy biznesowych. Sprawdź, czy przycisk **Zgłoś phishing** pojawia się w ich Outlooku, czy parowanie działa od początku do końca, i czy testowo zgłoszona wiadomość trafia na listę **Zgłoszone wiadomości** w PhishSpot pod właściwym kontem. Rozwiąż tutaj wszelkie specyficzne dla tenanta niespodzianki (proxy / firewall / braki w prowizjonowaniu Kontaktów).
2. **Fala 2 — jeden lub dwa działy.** Rozszerz do jednego–dwóch działów. Oceń adopcję i obciążenie zespołu reagowania na incydenty. Dopracuj komunikację na podstawie wniosków z Fali 1.
3. **Fala 3 — pełny rollout.** Gdy Fala 2 wygląda zdrowo, przełącz przypisanie na grupę obejmującą całą organizację (lub **Everyone**) i ogłoś szeroko.

W tenancie do ~50 skrzynek można połączyć Fale 1 i 2 w jeden pilotaż. W tenancie powyżej kilku tysięcy skrzynek dodaj czwartą falę dzielącą Falę 3 wg regionu lub roli.

21.5 Wskazówki dla użytkowników

Microsoft wprost wskazuje to jako dobrą praktykę, a istotnie poprawia to liczbę zgłoszeń:

- **Wyślij e-mail do wszystkich w dniu uruchomienia dodatku.** Dodaj akapit wyjaśniający, do czego służy przycisk, screenshot wstążki i jedno zdanie o tym, czego *nie robić* (np. “w razie wątpliwości kliknij Zgłoś — fałszywe alarmy są w porządku; kliknięcie linku w wiadomości — już nie.”).

- **Linkuj do runbooka helpdesku.** Krótkie FAQ pokrywające: “Nie widzę jeszcze przycisku” (propagacja 24–72 h), “Pyta o 6-cyfrowy kod” (jednorazowe parowanie), “Dostałem podziękowanie — co dalej?” (SLA triażu zespołu bezpieczeństwa).
- **Onboarding nowych osób.** Dodaj do checklistry onboardingu IT krok potwierdzający, że użytkownik widzi przycisk i sparował swoje urządzenie.
- **Wzmocnij komunikację w Miesiącu Świadomości Cyberbezpieczeństwa.** Powtórz komunikaty w październiku — większość organizacji widzi wtedy skok zgłoszeń.

21.6 Zaprowiadź kontakty w PhishSpot

Dodatek paruje użytkownika z jednym **Kontaktem** PhishSpot. Upewnij się, że każdy użytkownik, który ma korzystać z dodatku, ma odpowiadający mu rekord Kontaktu, zanim spróbuje sparować — w przeciwnym razie pojawi się komunikat “Nie znaleziono konta”.

Możesz tworzyć kontakty:

- z importu CSV (zobacz Kontakty)
- przez synchronizację katalogu Microsoft Entra (Azure AD) — automatycznie
- ręcznie

21.7 Pierwsze parowanie — droga użytkownika

Każdy użytkownik paruje się raz na urządzenie. Droga:

1. Outlook → kliknij **Zgłoś phishing** w dowolnej otwartej wiadomości.
2. Panel pokazuje 6-cyfrowy kod.
3. Użytkownik otwiera `https://platform.phishspot.com/guest/activation/new`, loguje się i wkleja kod.
4. Panel automatycznie przełącza się w stan **Sparowano**.

Każde udane parowanie tworzy **token API** w PhishSpot z uprawnieniem `reported_messages:create` przypisanym do jednego konta. Listę i odwoływanie tokenów znajdziesz w **Ustawienia** → **Tokeny API**.

21.8 Aktualizacje przyrostowe

Nowe wersje pakietu JS pojawiają się co kilka tygodni. **Nie musisz ponownie wgrywać manifestu** — wskaźnik wersji na `https://platform.phishspot.com/api/v1/outlook/version` jest jedynym źródłem prawdy, a każdy Outlook pobiera nowy pakiet przy następnym uruchomieniu.

Gdy zmienia się sam manifest (nowe uprawnienie, nowy przycisk), w notatce o wydaniu znajdziesz adnotację “manifest update required” i nowy plik `phishspot-outlook-manifest-vX.Y.Z.xml`. Wgraj go w taki sam sposób — M365 Admin Center rozpoznaje go jako uaktualnienie istniejącej aplikacji (ten sam `Id` UUID). Aby wymusić aktualizację z poziomu panelu dodatku LOB, wybierz wdrożony dodatek i kliknij przycisk **Update Button** w prawym dolnym rogu panelu szczegółów; zmiana zostanie zastosowana przy następnym uruchomieniu Outlooka przez każdego użytkownika.

21.9 Aktualizacje a blokady

Bootstrap dodatku sprawdza wersję przy każdym otwarciu. Dwa scenariusze:

- `latest > zainstalowane` — miękki baner. Użytkownik nadal może zgłaszać.
- `min_supported > zainstalowane` — twarda blokada. Zgłaszanie wyłączone do czasu wgrania nowego manifestu.

`min_supported` podnosimy tylko wtedy, gdy stara wersja jest niekompatybilna z istotną zmianą bezpieczeństwa lub modelu danych. Rzadko — najwyżej raz lub dwa razy w roku.

21.10 Wyłączenie

Aby usunąć dodatek:

1. **M365 Admin Center** → **Integrated apps** → **PhishSpot Report Phishing** → **Remove**. Usunięcie z wszystkich skrzynek w ciągu kilku godzin.
2. **PhishSpot** → **Ustawienia** → **Tokeny API** — odwołaj wszystkie tokeny ze źródłem `outlook_addin`.

21.11 Rozwiązywanie problemów

Objaw	Prawdopodobna przyczyna	Rozwiązanie
Przycisk nie pojawia się nikomu	Trwa propagacja	Microsoft podaje, że 24–72 h to norma; zrestartuj Outlook, aby przyspieszyć
Przycisk jest, panel pusty	Brak dostępu do `platform.phishspot.com`	Sprawdź proxy / firewall
Parowanie zawsze mówi “brak konta”	Użytkownik nie ma rekordu Kontaktu	Utwórz Kontakt i spróbuj ponownie
Zgłoszenia 403	Token przypięty do innego konta	Odłącz i sparuj ponownie
Nowy Outlook na Windows utknął na starej wersji	Agresywne cache’owanie	`outlook.exe /resetnavpane` lub wyczyść folder Wef

21.12 Zgodność

- Zgłoszenia są przechowywane w Twoim koncie PhishSpot, zgodnie z ustawieniami rezydencji danych.
- Token nigdy nie opuszcza skrzynki użytkownika (przechowywany w `Office.roamingSettings`).
- Kod źródłowy dodatku znajduje się w tym samym repozytorium Git co platforma PhishSpot, w `plugins/office/`. Podlega temu samemu procesowi przeglądu kodu.

Whitelist filtra antyspamowego

Symulacje phishingu w PhishSpot wyglądają jak prawdziwe ataki — taki jest cel. Korporacyjne filtry antyspamowe (Microsoft 365, Google Workspace, Mimecast, Proofpoint, on-prem Postfix/SpamAssassin) rutynowo je blokują, chyba że są jawnie wpuszczone na białą listę. Ten rozdział opisuje, jak dać administratorowi serwera pocztowego jeden URL, który wpina się w filtr — i sprawia, że lista pozostaje aktualna automatycznie.

22.1 Po co whitelist?

SPF, DKIM i DMARC mówią serwerom odbierającym: “ten mail naprawdę pochodzi z domeny, z której się podaje”. Prawdziwy phishing często to spełnia — dlatego phishing jest skuteczny. Te same testy przechodzą również **nasze** symulacje, ale nowoczesne filtry antyspamowe używają znacznie więcej niż SPF/DKIM: analizują wzorce treści, reputację linków, historię zachowań nadawcy i kilkadziesiąt innych sygnałów. Wiele z tych sygnałów (słusznie!) zakwalifikuje symulację phishingu jako podejrzaną.

Właściwe rozwiązanie polega na tym, żeby filtr odbiorcy **omijał** skanowanie spamu dla ruchu pochodzącego z PhishSpot. Wymaga to, żeby admin powiedział swojemu filtrowi:

- z jakich **adresów IP** wysyłamy,
- jakich **domen nadawcy** używamy, oraz
- (opcjonalnie) jakie konkretne **adresy nadawcy** pojawiają się w polu From:.

PhishSpot generuje tę listę per account i udostępnia ją pod stałym URL-em. Skonfiguruj filtr żeby pobierał ją cyklicznie (albo reagował na nasz webhook gdy się zmieni) i gotowe.

22.2 Twój URL whitelisty

Otwórz **Ustawienia konta** → **Integracje** → **Whitelist filtra antyspamowego**. Zobaczysz panel z:

- Twoim **unikalnym URL-em** zawierającym 64-znakowy token sekretny,
- **Selektorem formatu** (txt / json / csv / md / Microsoft 365 / Google Workspace / Mimecast / Proofpoint / Postfix / SpamAssassin),
- **Plakietką statusu** pokazującą, kiedy URL był ostatnio pobierany i z jakiego IP,
- **Przyciskiem rotacji**, który unieważnia bieżący URL,
- **Przełącznikiem wyłączania**, który zwraca 410 Gone do czasu ponownego włączenia,
- **Podglądem na żywo** tego, co jest aktualnie dozwolone,
- **Historią pobrań** ostatnich 50 odsłon.

URL to jedna linia, którą wklejasz do filtra antyspamowego lub do małego skryptu odświeżającego. Nie ma żadnego API tokena, żadnego nagłówka Authorization — sekret jest w ścieżce, a HTTPS szyfruje go w trakcie przesyłania. Ograniczamy każdy token do 60 zapytań na minutę, logujemy każde pobranie (IP + UA) w historii i działamy wyłącznie po HTTPS.

> Traktuj URL jak hasło. Każdy, kto go ma, może odczytać pełną listę IP-ek i domen nadawczych dla Twojego konta. Jeśli podejrzewasz wyciek — **wygeneruj nowy** w panelu; stary działa jeszcze 24 godziny, żeby filtr antyspamowy zdążył się przełączyć.

22.3 Wybór odpowiedniego formatu

Format	Kiedy używać
`txt`	Czysty tekst. Domyślny. Łatwy do grepowania i pipe'owania do skryptów.
`json`	Ustrukturyzowany payload. Najlepszy do integracji niestandardowych.
`csv`	Generyczny CSV — dobry fallback.
`md`	Markdown czytelny dla człowieka — do dokumentacji i przeglądu.
`microsoft365`	Snippet PowerShell + komendy Tenant Allow/Block List dla Exchange Online.
`google-workspace`	CSV w formacie importu Google Admin email allowlist.
`mimecast`	CSV w kształcie polityki Mimecast Permitted Senders.
`proofpoint`	CSV w kształcie Proofpoint PPS Safelist.
`postfix`	Snippet `access` table dla on-prem Postfix.
`spamassassin`	Linie `whitelist_from` dla `local.cf`.

Schemat URL: `https://platform.phishspot.com/api/v1/integrations/spam/<TOKEN>/<format>` — jeśli pominiesz format, dostaniesz czysty tekst.

22.4 Instrukcje konfiguracji per dostawca

22.4.1 Microsoft 365 / Exchange Online

1. W panelu PhishSpot wybierz **Microsoft 365 (PowerShell)** i skopiuj URL.
2. Zapisz do `phishspot-whitelist.ps1` na stacji roboczej z zainstalowanym Exchange Online PowerShell.
3. Uruchom `Connect-ExchangeOnline` (potrzebne uprawnienia Exchange Administrator).
4. Wykonaj skrypt. Robi dwie rzeczy:
   - Dodaje każdą domenę i adres nadawcy do **Tenant Allow/Block List** przez `New-TenantAllowBlockListItems`,
   - Łączy IP-ki bramki z **Hosted Connection Filter Policy** przez `Set-HostedConnectionFilterPolicy`.
5. Opcjonalnie utwórz **regułę Mail Flow** z "skip spam filtering" dla nadawców pasujących do `@<twoja-domena-phishspot>`. Ponawiaj pobieranie URL co tydzień, żeby lista pozostała aktualna.

22.4.2 Google Workspace

1. Wybierz format **Google Workspace (CSV)** i pobierz plik.
2. W Google Admin Console przejdź do **Aplikacje** → **Google Workspace** → **Gmail** → **Spam, phishing i złośliwe oprogramowanie**.
3. Otwórz **Email allowlist** dla swojej OU najwyższego poziomu i wklej wpisy IP z CSV (jeden na linię).
4. Otwórz **Inbound gateway** (też w ustawieniach spam) i dodaj te same IP. To sprawia, że Gmail omija scoring spam dla tych połączeń.
5. Aby zezwalać po domenie zamiast po IP, dodaj wpisy domen z CSV do listy **Approved senders** (ta sama sekcja).

22.4.3 Mimecast

1. Wybierz **Mimecast (CSV)** w panelu.
2. W Mimecast Administration przejdź do **Gateway** → **Policies** → **Permitted Senders**.
3. Kliknij **Import** i załaduj CSV. Mimecast pobiera IP-ki nadawcy z kolumny `Sender IP`, a nadawców/domeny z kolumny `Sender`.
4. Zaplanuj zadanie `curl` (`curl -fSL '<URL>' > whitelist.csv` potem re-import) albo użyj Mimecast API do automatyzacji.

22.4.4 Proofpoint Protection Server (PPS)

1. Wybierz **Proofpoint PPS (CSV)**.
2. Załaduj przez **System** → **User Management** → **Safelists** → **Import** w UI PPS, albo przepchnij przez PPS REST API (`/api/v1/safelist/import`).
3. PPS traktuje wpisy nadawcy, domeny i IP inaczej — kolumna `type` w CSV mówi PPS-owi, na którą listę dany wiersz wrzucić.

22.4.5 Postfix (on-prem)

1. Wybierz **Postfix access table**.
2. Zapisz do `/etc/postfix/phishspot_whitelist`, potem uruchom `postmap /etc/postfix/phishspot_whitelist` żeby skompilować tabelę.
3. Odwołaj się w `main.cf`:

```
smtpd_sender_restrictions =
  check_sender_access hash:/etc/postfix/phishspot_whitelist,
  ...
```

4. Uruchom `postfix reload`.
5. Dla obejścia po IP, skopiuj IP-ki do osobnego pliku CIDR i dodaj `check_client_access cidr:/etc/postfix/phishspot_ips` do `smtpd_client_restrictions`.

22.4.6 SpamAssassin

1. Wybierz **SpamAssassin local.cf**.
2. Doklej snippet do `/etc/spamassassin/local.cf`.
3. Sprawdź `spamassassin -D --lint`.
4. Zrestartuj `spamd`.
5. Snippet używa `whitelist_from *@<domena>` i `trusted_networks <ipsy>` — to drugie podnosi score zaufania dla relayowanej poczty.

22.5 Auto-refresh przez webhook

Whitelist zmienia się, gdy (Ty lub PhishSpot) dodaje domenę nadawczą, gdy kampania używa nowego adresu From:, albo gdy nasz infra-team rotuje IP-ki bramki. Aby utrzymać stronę klienta zawsze aktualną:

1. W **Ustawienia konta** → **Webhooki** → **Endpointy** dodaj nowy endpoint wskazujący na URL po Twojej stronie.
2. Zasubskrybuj event type `spam_whitelist.updated`.
3. Gdy lista się zmieni, POST-ujemy do tego URL podpisany payload (HMAC-SHA256 w `X-Webhook-Signature` używając signing secret endpointu). Payload zawiera nowy snapshot digest i pełny zestaw URL-i whitelisty w różnych formatach.
4. Twój handler weryfikuje podpis, a potem uruchamia import specyficzny dla platformy (job PowerShell powyżej, wywołanie Google Admin API, Mimecast / Proofpoint API, etc.).

Powtarzamy nieudane dostarczenia 5 razy z exponential backoff. Po 5 kolejnych porażkach mailujemy adminów konta, żeby integracja nie zgniła po cichu.

22.6 Powiadomienia o stałości

Śledzimy, kiedy każdy URL był ostatnio pobrany. Jeśli minie 24 godziny bez udanego pobrania — czyli filtr antyspamowy przestał pobierać listę — wysyłamy mail do **każdego admina** w koncie. Najczęstsze przyczyny:

- Cron / scheduled task pobierający URL przestał działać.
- Firewall blokuje teraz wychodzący HTTPS do `platform.phishspot.com`.
- URL został wygenerowany ponownie, a stary wygasł, zanim ktokolwiek zaktualizował filtr.
- Integracja została przypadkowo usunięta z filtra antyspamowego.

Aby uciszyć ostrzeżenie, wywołaj ręcznie pobranie po Twojej stronie (wystarczy jeden `curl` — resetujemy licznik przy każdym udanym zapytaniu).

22.7 Najlepsze praktyki

- **Zaplanuj pobieranie** przynajmniej raz dziennie, najlepiej co godzinę. Endpoint jest tani.
- **Weryfikuj snapshot digest** (nagłówek `X-PhishSpot-Snapshot-Digest`) — jeśli zgadza się z tym, co już masz, pomiń re-import żeby uniknąć szumu w downstream systemie.

- **Rotuj kwartalnie**. Nawet bez wycieku regularna rotacja ogranicza blast radius, gdyby skrypt kiedyś zalogował URL.
- **Monitoruj też po swojej stronie**. Alarmuj, jeśli cron job nie zadziałał poprawnie przez N godzin. Nie polegaj wyłącznie na naszym mailu stale-warning.
- **Używaj webhooka oprócz crona**, nie zamiast. Cron to safety net; webhook to szybka ścieżka.
- **Przetestuj bypass** funkcją "Wyślij testowy email" w PhishSpot przed pełnym uruchomieniem. Jeśli test nie trafia do skrzynki odbiorcy — bypass nie działa.

22.8 FAQ i rozwiązywanie problemów

"Nasze symulacje phishingu nadal trafiają do spamu." Sprawdź, czy filtr antyspamowy faktycznie pobiera URL: zajrzyj do historii pobrań w panelu PhishSpot — czy IP i timestamp zgadzają się z egress IP i harmonogramem pobierania Twojego filtra? Jeśli tak, sprawdź, czy reguła bypass jest na odpowiedniej polityce (filtry często mają osobne polityki inbound vs. transport). Jeśli nie, URL nie dociera do filtra.

"Format CSV, którego oczekuje mój filtr, jest inny." Użyj zwykłego formatu `csv` jako szablonu i przetransformuj po stronie serwera. Format `json` jest najbardziej elastycznym źródłem — łatwy do zmapowania do dowolnego docelowego schematu z `jq` lub 20-linijkowym skryptem.

"Mój webhook nie otrzymuje dostarczeń." Sprawdź URL endpointu w **Webhooki** → **Endpointy** — upewnij się, że jest HTTPS, publicznie osiągalny i nie jest za ścianą uwierzytelniania. Otwórz stronę szczegółów endpointu w PhishSpot, żeby zobaczyć log dostarczeń z kodami odpowiedzi i body. Sprawdź, czy obsługa podpisu HMAC po Twojej stronie pasuje do `OpenSSL::HMAC.hexdigest("SHA256", signing_secret, raw_body)`.

"Co jeśli zmienicie IP-ki bramki?" Dostaniesz event `spam_whitelist.updated` w momencie, gdy dokonamy zmiany, a odpowiedź URL zawiera nowe IP natychmiast. Jeśli Twój filtr ma świeże pobranie w oknie zmiany — w ogóle tego nie zauważysz.

"Czy mogę mieć wiele URL-i dla różnych filtrów?" Nie w MVP — jest jeden aktywny URL per account. Jeśli potrzebujesz osobnych URL-i (np. dla phased rollout), skorzystaj z przepływu rotacji: zrotuj, zaczekaj 24h, zrotuj ponownie. Każda rotacja daje świeży URL z 24-godzinnym grace period.

Autopiloty

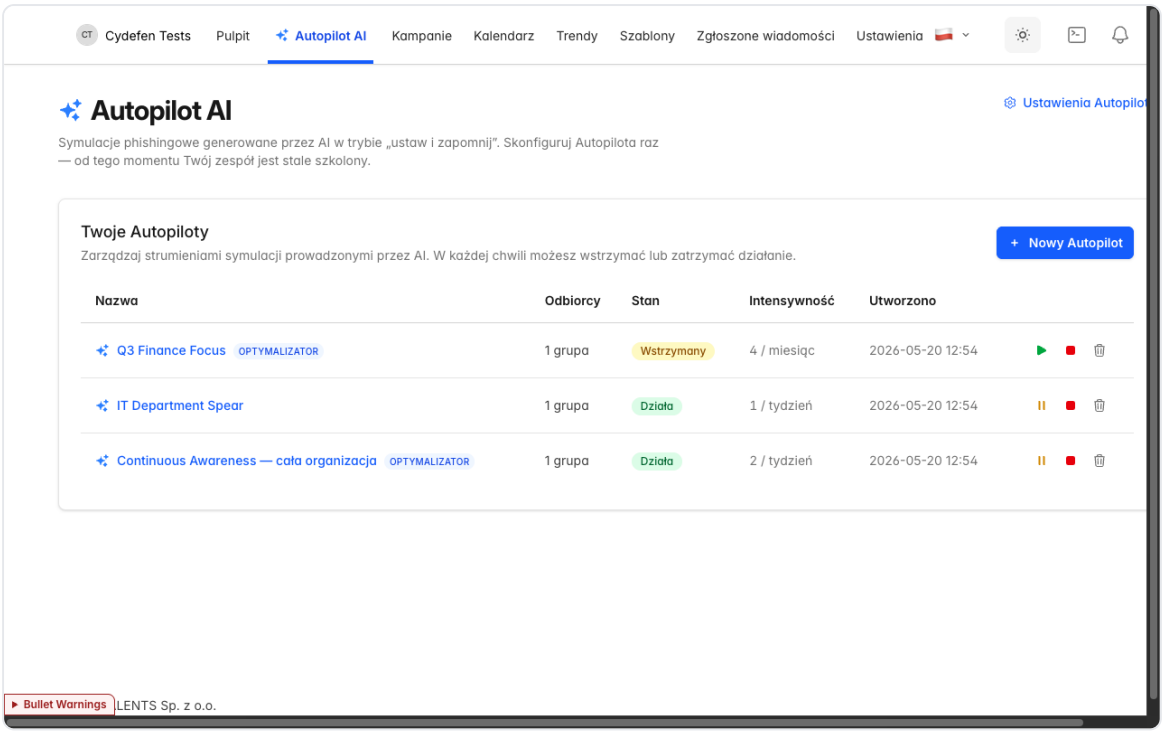
Kampania to jednorazowa wysyłka. **Autopilot** to konfiguracja, która tworzy kampanie automatycznie, w wybranym przez Ciebie rytmie, tak długo jak ma działać. Definiujesz grupę docelową, intensywność (jak często), finał po kliknięciu i kontekst targetowania (język, kraj, branża) — a PhishSpot odpala kolejne symulacje wobec pasujących kontaktów aż do momentu, w którym autopilot wstrzymasz lub zatrzymasz.

Model brzmi: „ustaw raz, niech pracuje". Jeśli nowy kontakt dołącza do jednej z grup autopilotu (albo przyjdzie przez synchronizację katalogu), zostanie wciągnięty w kolejną iterację. Jeśli zmienisz finał albo kurs w trakcie działania, kolejna uruchomiona kampania użyje już nowych ustawień.

23.1 Czym autopilot jest — a czym nie

Autopilot to **nie** pojedyncza, długo trwająca kampania. To przepis. Za każdym razem gdy autopilot się odpala, tworzy świeży rekord `Campaign`, dobiera szablon phishingowy dopasowany do języka i branży, robi snapshot odbiorców z wybranych grup i wysyła. Raporty z tych kampanii znajdziesz w **Raportach i analityce** tak samo jak z kampanii ręcznych.

Używaj autopilotów, gdy chcesz prowadzić ciągły, mało absorbujący program uświadamiający. Używaj jednorazowych kampanii (Rozdział 4), gdy potrzebujesz pełnej kontroli nad czasem, treścią i odbiorcami konkretnej wysyłki.



Lista autopilotów z trzema skonfigurowanymi autopilotami

23.2 Tworzenie autopilotu

Otwórz **Autopiloty** w lewym pasku bocznym i kliknij **Nowy autopilot**. Formularz ma dwie widoczne sekcje:

23.2.1 Nazwa i odbiorcy

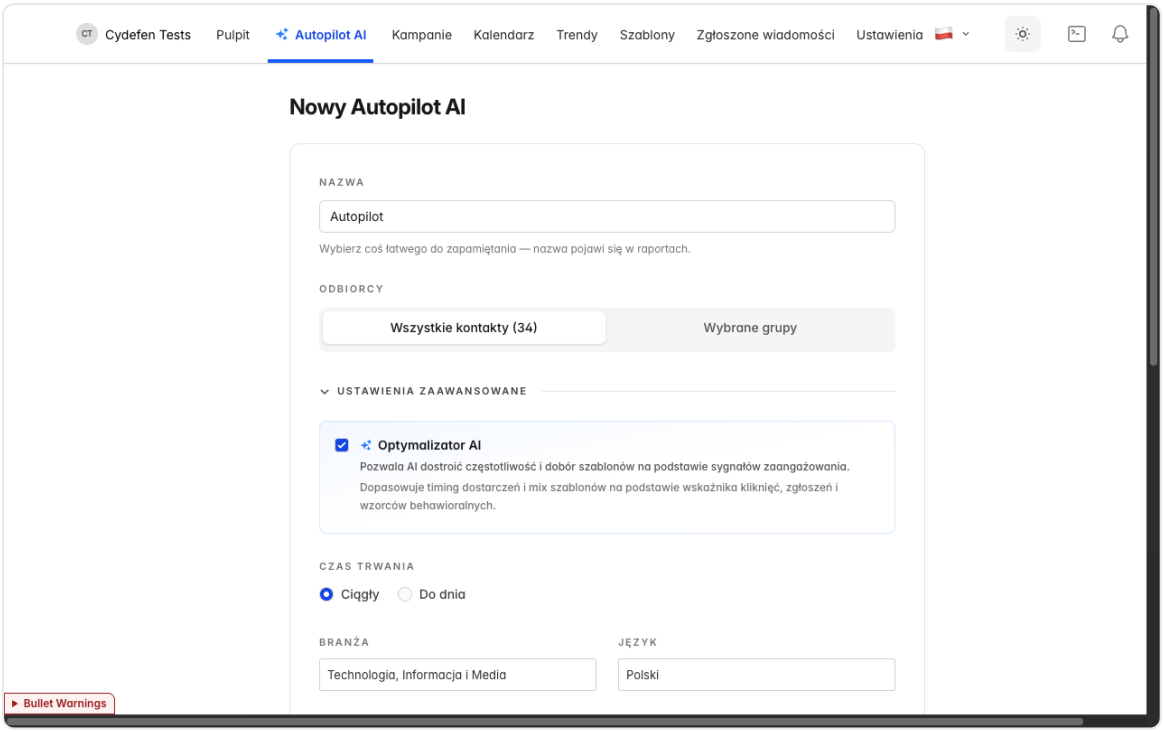
- **Nazwa** — to, co zobaczysz na liście autopilotów. Maks. 80 znaków. Przykłady z typowej konfiguracji: „Continuous Awareness — cała organizacja", „IT Department Spear", „Q3 Finance Focus".
- **Odbiorcy** — wybierz **Wszystkie kontakty**, aby objąć każdy kontakt na koncie, lub **Wybrane grupy**, aby zawęzić autopilot do jednej lub kilku grup. W momencie odpalenia autopilotu odbiorcy są próbkowani z grup „na żywo" — więc grupy, które rosną w czasie, rozszerzają zasięg autopilotu.

23.2.2 Ustawienia zaawansowane

Sekcja jest domyślnie rozwinięta podczas edycji istniejącego autopilotu. Zawiera:

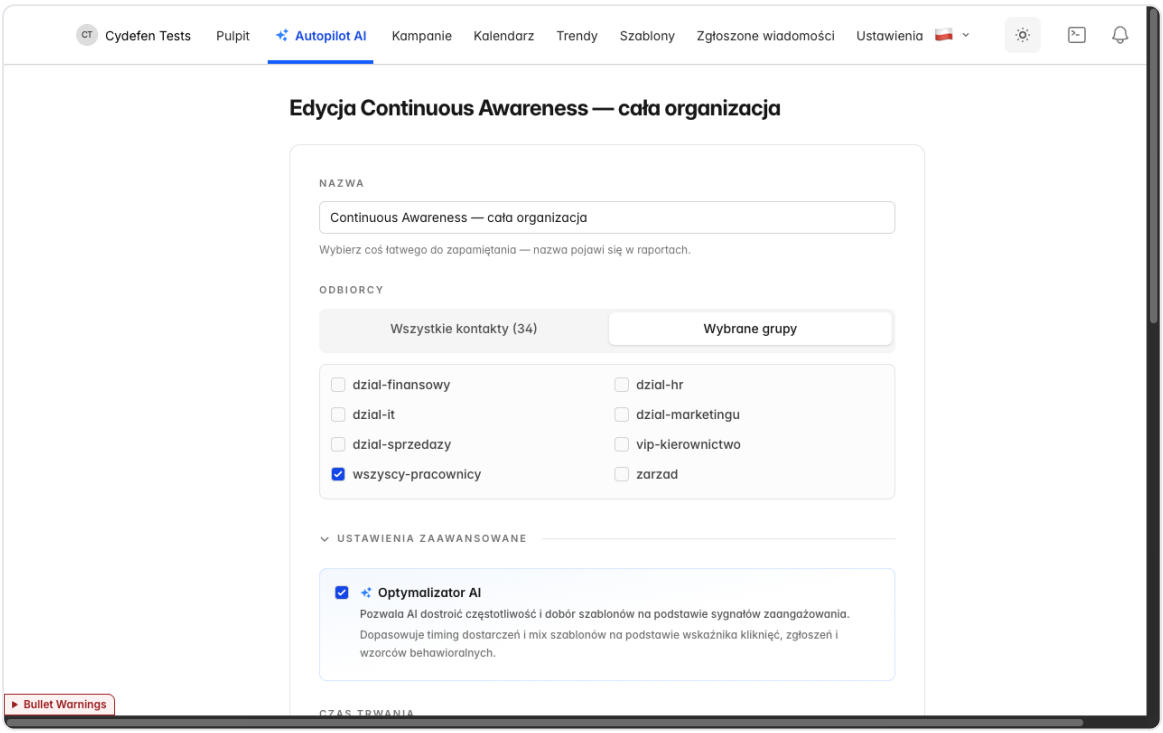
- **Optymalizator AI** — gdy włączony, PhishSpot dostraja, które szablony trafiają do których osób, na bazie wcześniejszych interakcji. Nowe autopiloty mają tę opcję domyślnie WŁ.
- **Czas trwania** — **Ciągły** (działa do momentu zatrzymania) albo **Do** (zatrzymuje się automatycznie w wybranym dniu).
- **Branża** — branża docelowej organizacji (taksonomia NAICS + LinkedIn). Używana do biasowania wyboru szablonów w stronę motywów wiarygodnych dla danej wertykali. Zostaw puste, aby dziedziczyć z ustawień autopilotów (§23.6).
- **Język** — język, w jakim będą tworzone treści symulacji. Zostaw puste, aby dziedziczyć.
- **Domyślny finał (po kliknięciu)** — co pokazać odbiorcy po kliknięciu w symulowany link phishingowy:
  - **Nic nie rób** — brak strony docelowej; kliknięcie zostaje tylko zalogowane.
  - **Przekieruj na kurs szkoleniowy** — otwiera wybrany przez Ciebie kurs.
  - **Pokaż stronę uświadamiającą (zalecane)** — renderuje stronę „to była symulacja phishingu".
  - **Przekieruj na URL** — wysyła użytkownika pod zewnętrzny adres.
- **Automatycznie dołączaj nowych członków grup i kontakty** — gdy włączone, kontakty dodane do grup autopilotu po starcie zostaną włączone w kolejnej iteracji. Domyślnie WŁ.
- **Intensywność kampanii** — patrz §23.3.

Zapisz, autopilot zostaje utworzony w stanie **Wersja robocza**. Kliknij **Uruchom** by ruszyć.



Formularz nowego autopilotu z rozwiniętą sekcją Ustawienia zaawansowane

Poniższy zrzut pokazuje istniejący autopilot w trybie edycji — widać każde ustawienie zaawansowane: Optymalizator AI, czas trwania, branżę, język, finał, auto-dołączanie nowych członków, intensywność.



Edycja działającego autopilotu — pełny panel ustawień

23.3 Intensywność i dzienny limit

Intensywność to dwie wartości: **liczba** i **okres** — `2 na tydzień`, `1 na miesiąc`, `4 na rok` itd. Okresy: **dzień**, **tydzień**, **miesiąc**, **rok**.

PhishSpot wymusza twardy sufit: **żaden pojedynczy kontakt nie zostanie zaadresowany przez autopilot więcej niż dwa razy dziennie**, niezależnie od ustawienia intensywności. Pole intensywności w formularzu odrzuca wartości, które łamią ten limit:

- `1/dzień` i `2/dzień` są dozwolone.
- `3/dzień` i więcej zostają odrzucone — formularz pokazuje błąd.
- Wartości tygodniowe/miesięczne/roczne są wewnętrznie przeliczane na stawkę dzienną (`PERIOD_DAILY_RATE` odpowiednio `1`, `7`, `30`, `365`) i sprawdzane wobec tego samego limitu.

Limit jest per autopilot. Jeśli kontakt znajduje się w kilku autopilotach, każdy z nich pilnuje swojego limitu niezależnie — miej to na uwadze przy równoległych programach na nakładających się grupach.

23.4 Stany cyklu życia

Każdy autopilot jest dokładnie w jednym stanie:

Stan	Znaczenie	Edytowalny?
Wersja robocza	Utworzony, ale jeszcze nie uruchomiony. Żadnych kampanii.	Tak
Działa	Aktywny. Kampanie odpalają się zgodnie z rytmem.	Tak
Wstrzymany	Czasowo zatrzymany. Brak nowych kampanii do wznowienia.	Tak
Zatrzymany	Trwale zakończony. **Tylko do odczytu.** Aby zacząć od nowa, usuń autopilot.	Nie

Przejścia są jawnymi przyciskami w wierszu autopilotu:

- **Uruchom** — `Wersja robocza` lub `Wstrzymany` → `Działa`.
- **Wstrzymaj** — `Działa` → `Wstrzymany`.
- **Zatrzymaj** — dowolny stan → `Zatrzymany`. Nieodwracalne; aby ponownie modyfikować, trzeba usunąć i utworzyć od nowa.

Zatrzymany autopilot to nagrobek — zachowuje historię (które kampanie odpalił i kiedy), ale żadnego pola nie da się już zmienić. Intencja: dać audytowalny ślad zakończonych programów, nie zaśmiecając listy aktywnych.

23.5 Optymalizator AI

Gdy włączony, Optymalizator AI dostosowuje, które szablony autopilot dobiera dla każdego odbiorcy, na podstawie wcześniejszego zachowania: osoby, które konsekwentnie dają się nabrać na motyw fakturowy, dostają więcej takich (i szkolenia idącego za nimi); osoby, które ich nigdy nie klikają, dostają trudniejsze, mniej oczywiste warianty. Optymalizator jest domyślnie WŁ dla nowych autopilotów i można go przełączać per autopilot w sekcji **Ustawienia zaawansowane**.

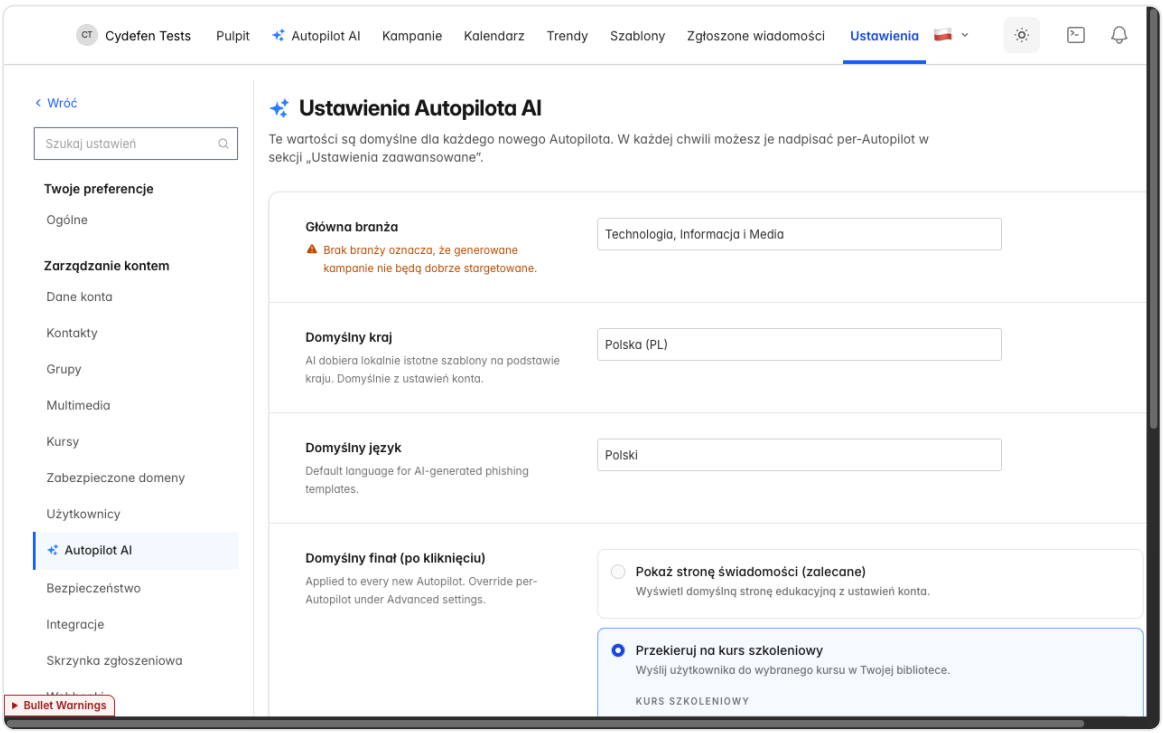
Logika adaptacyjna optymalizatora jest dostarczana etapami. Toggle i scoring per szablon są aktywne już dziś; pełna warstwa wyboru (multi-armed bandit) wchodzi w trakcie wdrożenia i jest objęta subskrypcją SaaS — gdy się włączy, nie wymaga dodatkowej konfiguracji.

23.6 Ustawienia domyślne

Kliknij **ikonę koła zębatego → Ustawienia autopilotów** na liście autopilotów, aby otworzyć ustawienia na poziomie konta. Pola tu wprowadzone pre-wypełniają formularz nowego autopilotu, żebyś nie musiał ich powtarzać:

- **Główna branża** — branża Twojej organizacji. Szablony używają jej automatycznie.
- **Domyślny kraj** — używany do biasowania wyboru szablonów (nazwiska nadawców, marki, które są podszywane).
- **Domyślny język** — język treści symulacji.
- **Domyślny finał (po kliknięciu)** — te same cztery opcje co w formularzu autopilotu, używane jako wartość początkowa.
- **Domyślna intensywność kampanii** — liczba + okres używane jako wartość początkowa.

Zmiana ustawień **nie modyfikuje wstecznie** istniejących autopilotów — wpływa tylko na domyślne wartości przyszłych. Pola per autopilot nadpisują te ustawienia, gdy są wypełnione.



Ustawienia autopilotów — domyślne wartości na poziomie konta

23.7 Przykłady z życia

Poniżej trzy konfiguracje autopilotów z działającego setupu — pokazują typowe scenariusze.

Continuous Awareness — cała organizacja

Bazowy program dla wszystkich na koncie.

- Odbiorcy: grupa „Wszyscy pracownicy” (wszyscy pracownicy zsynchronizowani z Entra AD).
- Intensywność: 2/tydzień. Z dziennym limitem to nadal nie więcej niż 2 maile na dobę per kontakt — ale rozłożone przez tydzień.
- Optymalizator AI: WŁ.
- Język: pl. Branża: Technology, Information and Media.
- Finał: Przekierowanie na kurs „Świadomość phishingowa 101”.
- Auto-dołączanie nowych członków: WŁ — zmiany z sync katalogu wpadają od razu.

IT Department Spear

Trudniejsze symulacje wycelowane w zespół IT — grupę najbardziej narażoną na realne ataki.

- Odbiorcy: tylko grupa „Dział IT”.
- Intensywność: 1/tydzień — niższa niż w programie ogólnym, bo używane szablony są trudniejsze, a kohorta mała.
- Optymalizator AI: WYŁ — admin chce deterministycznego, ręcznie kontrolowanego doboru na czas początkowej kalibracji.
- Finał: Przekierowanie na URL — wewnętrzna strona wiki bezpieczeństwa.

Q3 Finance Focus (wstrzymany)

Program z ramą czasową dla działu finansowego.

- Odbiorcy: „Dział Finansowy”.
- Intensywność: 4/miesiąc.
- Stan: Wstrzymany — utrzymywany między kwartałami; wznawiany na początku kolejnego.

Każdy z nich tworzy się raz i zostawia w spokoju. Raportowanie per autopilot widać pod pasującymi kampaniami w Raportach i analityce.

23.8 Odnośniki

- Domyślne wartości na poziomie konta: zobacz §23.6 wyżej.
- Kontakty i grupy, które autopiloty obsługują: Rozdział 5 Kontakty i Rozdział 6 Grupy.
- Synchronizacja katalogu, która automatycznie zwiększa zasięg: Rozdział 25 Synchronizacja katalogu.
- Raportowanie kampanii z autopilotów: Rozdział 11 Raporty i analityka.
- Kurs używany jako finał po kliknięciu: Rozdział 8 Kursy.

Logowanie przez Microsoft 365

PhishSpot integruje się z Microsoft 365 (Entra ID) do logowania użytkowników końcowych. Pracownicy zaimportowani z Twojego katalogu logują się swoim firmowym kontem Microsoft — bez osobnego hasła, bez osobnej tożsamości do wprowadzania. Przy pierwszym logowaniu PhishSpot łączy zalogowanego użytkownika z istniejącym rekordem kontaktu z Entry i wyświetla mu osobisty panel szkoleniowy pod `/guest/dashboard`.

Ten rozdział opisuje przepływ logowania widziany przez pracownika, osobisty portal, do którego po zalogowaniu trafia, oraz selektor dwóch ról pokazywany adminom, którzy są jednocześnie użytkownikami końcowymi.

24.1 Po co Microsoft 365 SSO?

Trzy powody:

- **Brak dodatkowego hasła do zapomnienia.** Pracownicy używają tego samego konta Entra, którego używają już w Outlooku, Teams, SharePoint i reszcie Microsoft 365. Nic nowego do zapamiętania.
- **Automatyczny onboarding.** Gdy synchronizacja katalogu Entra (Rozdział 25) zaimportuje pracownika, jego pierwsze logowanie przez Microsoft od razu zamienia kontakt w pełne konto użytkownika — bez ingerencji admina.
- **Dziedziczony poziom zabezpieczeń.** Conditional Access, MFA, zgodność urządzeń — każda polityka Entra obowiązuje. PhishSpot nie wymusza własnego MFA na ścieżce SSO, bo Microsoft robi to wcześniej w przepływie.

24.2 Konfiguracja po stronie admina

Aplikacja OAuth na poziomie platformy jest już zarejestrowana w tenancie PhishSpot. Aby włączyć logowanie pracowników z Twojego tenanta, wystarczy nadać zgodę administracyjną dla aplikacji PhishSpot i (opcjonalnie) podpiąć synchronizację katalogu:

1. Otwórz **Ustawienia konta** → **Integracje** → **Microsoft 365**.
2. Kliknij **Połącz Microsoft 365**. Zostaniesz przekierowany do ekranu zgody administratora Microsoft.
3. Nadaj żądane uprawnienia (`User.Read.All`, `Group.Read.All`, `Directory.Read.All` dla synchronizacji; `openid`, `profile`, `email` dla logowania).
4. Microsoft przekieruje Cię z powrotem. PhishSpot zapisze Twój tenant ID i tokenem aplikacji ograniczony do tego tenanta.
5. (Opcjonalnie, ale zalecane) skonfiguruj harmonogram synchronizacji — patrz Rozdział 25 §25.3.

Po nadaniu zgody każdy użytkownik w Twoim tenancie, którego email pasuje do zaimportowanego kontaktu na koncie, może się zalogować. Użytkownicy, którzy nie pasują do żadnego kontaktu (albo

których tenant ID nie odpowiada żadnej skonfigurowanej integracji), trafiają na uprzejmą stronę „brak dostępu” — nie tworzą kont „na żywo”.

24.3 Przepływ logowania użytkownika końcowego

Co widzi pracownik:

1. Otwiera `https://platform.phishspot.com/users/sign_in`.
2. Pod formularzem email/hasło, oddzielony „LUB”, widzi przycisk **Kontynuuj z Microsoft** (z logo Microsoft). Kliknięcie przekierowuje na ekran logowania Microsoft.
3. Microsoft uwierzytelnia użytkownika — z MFA, jeśli Twój tenant tego wymaga. Użytkownik nadaje aplikacji PhishSpot uprawnienia przy pierwszym logowaniu (jednorazowa zgoda per użytkownik, chyba że nadałeś zgodę admina w jego imieniu — wtedy ekran zgody w ogóle się nie pojawia).
4. Microsoft przekierowuje z powrotem do PhishSpot. W tle:
    - Jeśli istnieje User o tym samym emailu, jest używany.
    - Jeśli nie, tworzony jest nowy User z tym emailem, oznaczony jako zweryfikowany.
    - PhishSpot zapisuje **tenant ID** Entra dla szybkich wyszukiwań.
    - Każdy niezlinkowany Contact pasujący po emailu zostaje dowiązany do tego usera — staje się „Twój kontakt, Twój user”.
5. Użytkownik ląduje na `/guest/dashboard`. Żadnego hasła nie ustawiał. Żaden email z zaproszeniem nie został wysłany. Jest w środku.

Pierwsze logowanie zamyka się w jednym round-tripie; kolejne są jeszcze szybsze — Microsoft pamięta zgodę, a krok dopinania jest no-op po pierwszym razie.

24.4 Panel użytkownika końcowego

`/guest/dashboard` to portal skierowany do pracownika. Pokazuje wszystko, czym pracownik powinien się osobiście zająć — i nic więcej. Pracownik nie widzi wyników innych osób, listy kampanii, ustawień konta ani żadnych stron adminowych.

Panel ma trzy sekcje:

24.4.1 Twoje szkolenia

Lista szkoleń, które pracownik ma do zrobienia — zwykle jedno na każdą kampanię phishingową, w którą pracownik kliknął i która ma przypisany kurs jako finał po kliknięciu. Każdy wiersz pokazuje:

- Nazwę kursu (np. „Świadomość phishingowa 101”).
- Status: nierozpoczęty / w toku (z % postępu) / ukończony.
- Przycisk otwierający odtwarzacz kursu w tym samym oknie.

Szkolenia są wyprowadzane z rekordów `Deliverable` — gdy kontakt dotrze do stanu `clicked` lub dalej na kampanii z przypisanym kursem, pojawia się tu zadanie.

24.4.2 Historia maili

Ostatnie 50 maili z symulacji phishingowych, z którymi użytkownik miał kontakt. Dla każdego:

- Nazwa kampanii (firmowa etykieta, nie adres nadawcy symulacji).
- Jakie akcje użytkownik wykonał (otworzył / kliknął / wysłał formularz / zgłosił).
- Znacznik czasu.

To osobista wersja tego, co admini widzą w dashboardzie kampanii. Krótka z premedytacją — długie retencje to sprawa admina, nie pracownika.

24.4.3 Zgłoszone maile

Jeśli użytkownik zgłosił phishing przez dodatek do Outlooka (Rozdział 20), każde zgłoszenie pojawia się tu z tematem, nadawcą i czasem zgłoszenia. Sekcja pokazuje też **adres skrzynki zgłoszeń per konto** — przydatny dla użytkowników na urządzeniach bez dodatku Outlook, którzy mogą ręcznie forwardować podejrzanego maila.

24.5 Selektor podwójnej roli

Niektórzy użytkownicy są jednocześnie adminami i pracownikami: menedżer bezpieczeństwa, który prowadzi kampanie phishingowe, sam jest też celem phishingu. PhishSpot rozwiązuje to jawnym selektorem.

Gdy użytkownik z `account_user` (rola admina na co najmniej jednym koncie) ORAZ `contact_membership` (rekord kontaktu na co najmniej jednym koncie) loguje się, resolver kieruje go na `/guest/role` zamiast prosto na dashboard. Selektor pokazuje dwa duże przyciski-karty:

- 🛡️ **Panel admina** — otwiera adminowy UI scoped per konto (`/accounts/:account_id`).
- 🎓 **Portal szkoleniowy** — otwiera `/guest/dashboard`.

Użytkownik wybiera raz na sesję. Selektor jest też dostępny z menu użytkownika — admin może przełączyć kontekst w trakcie pracy.

Użytkownik z samym `account_user` (czysty admin) pomija selektor i ląduje od razu w panelu adminowym. Użytkownik z samym `contact_membership` (czysty pracownik) pomija selektor i ląduje na `/guest/dashboard`. Selektor pojawia się tylko gdy oba warunki są spełnione.

24.6 Model bezpieczeństwa

PhishSpot deleguje uwierzytelnianie do Microsoft dla sesji SSO. To znaczy:

- **MFA jest wymuszane przed PhishSpot.** Jeśli Twój tenant wymaga MFA, każde logowanie do PhishSpot przez SSO przez nie przechodzi. Jeśli nie wymagasz MFA, PhishSpot nie nakłada go „po cichu” na ścieżce SSO.
- **Conditional Access działa.** Polityki tenanta (zgodność urządzenia, restrykcje geograficzne, ochrona aplikacji) obejmują logowanie do PhishSpot tak samo jak każdą inną aplikację Entra.

- **Zawężanie do tenanta (opcjonalne).** PhishSpot można skonfigurować tak, żeby odrzucał logowania z Entra tenant ID nie pasującego do żadnego skonfigurowanego `AccountOauthIntegration` na platformie. Zalecane dla tenantów, które nie chcą żeby przypadkowi użytkownicy Microsoft próbowali się logować.
- **Lokalne 2FA dla kont bez SSO.** Admini, którzy nie logują się przez Microsoft (np. konta serwisowe), mogą włączyć TOTP-owe 2FA — patrz Rozdział 15 Profil użytkownika.

24.7 Rozwiązywanie problemów

Przycisk Microsoft zabiera mnie na „brak dostępu". Albo żaden Contact nie pasuje do mojego emaila na żadnym koncie, albo tenant ID nie jest rozpoznany. Poproś admina o potwierdzenie: (1) synchronizacja katalogu działała i Twoje konto zostało zaimportowane; (2) integracja jest połączona ze zgodą administracyjną (Rozdział 25 §25.2).

Kliknąłem Kontynuuj z Microsoft, ale Microsoft nigdy nie poprosił mnie o zgodę. Zgoda administratora jest już nadana w Twoim tenancie — to oczekiwane i szybsze.

Jestem adminem i ciągle ląduję na selektorze ról. To jest oczekiwane: jesteś jednocześnie adminem i kontaktem na tym samym koncie. Wybierz rolę; wybór trwa do końca bieżącej sesji.

Spodziewałem się zobaczyć wyniki innych pracowników. Nie zobaczysz — Panel pokazuje tylko Twoje dane. Zbiorcze dashboardy są tylko dla adminów i są pod adminowym UI konta.

24.8 Odnośniki

- Synchronizacja katalogu, która tworzy kontakty z Entra: Rozdział 25 Synchronizacja katalogu.
- Dodatek Outlook karmiący sekcję „Zgłoszone maile": Rozdział 20 Dodatek do Outlooka.
- Raporty kampanii, których admini używają do monitorowania tego, co pracownicy widzą w portalu: Rozdział 11 Raporty i analityka.
- Lokalne TOTP-owe 2FA dla kont bez SSO: Rozdział 15 Profil użytkownika.

Synchronizacja katalogu Entra AD

Gdy firma prowadzi symulacje phishingu wobec 50, 500 albo 5 000 pracowników, ręczne utrzymywanie listy kontaktów na bieżąco nie jest realne. PhishSpot łączy się z Microsoft Entra ID (dawniej Azure AD) i pobiera użytkowników oraz grupy bezpośrednio z Twojego katalogu. Nowi pracownicy się pojawiają, odchodzący zostają wyłączeni, członkostwo w grupach odpowiada aktualnej strukturze — bez ręcznej edycji arkusza.

Ten rozdział opisuje konfigurację integracji, harmonogram synchronizacji, co i jak jest importowane, ręczne synchronizacje oraz log historii, do którego zaglądasz gdy coś wygląda nie tak.

> Zanim podłączysz Entra ID, przeczytaj Rozdział 28 — Entra ID: ryzyka i kompromisy. Dla większości organizacji PhishSpot zaleca ręczny import z CSV zamiast synchronizacji katalogu. Ten rozdział jest referencją techniczną dla sytuacji, w której i tak zdecydowałeś się podłączyć.

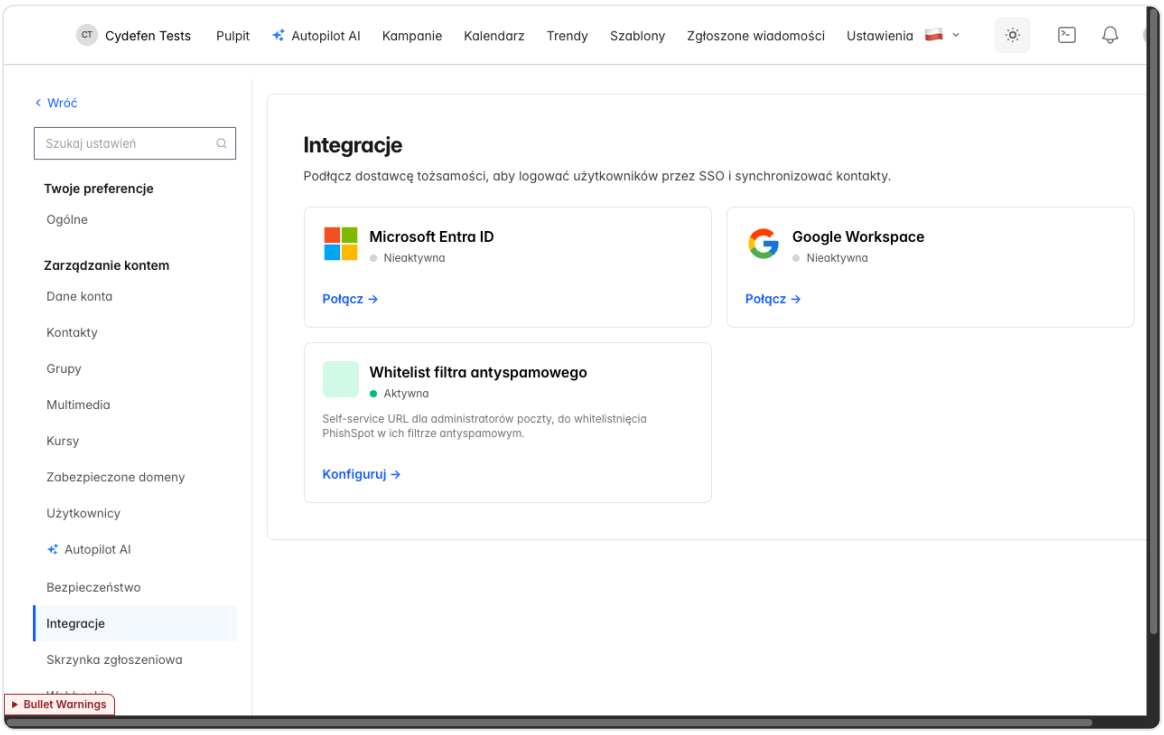
25.1 Po co synchronizacja katalogu?

Alternatywa to import z CSV (Rozdział 5 Kontakty opisuje ścieżki ręczne). Są w porządku dla proof-of-concept albo jednorazowych pilotaży, ale w produkcji szybko się dezaktualizują. Synchronizacja katalogu daje:

- **Autorytatywne źródło.** Twój IT już utrzymuje Entrę. PhishSpot dziedziczy tę pracę — brak równoległej listy do utrzymania.
- **Automatyczny onboarding.** Nowy pracownik, którego konto Entra zostało założone dziś, pokaże się w PhishSpot rano (albo szybciej, w zależności od harmonogramu) i od razu staje się prawidłowym celem dla kampanii autopilotów.
- **Eleganckie obsłużenie odchodzących.** Gdy IT wyłącza konto w Entra, pasujący Contact w PhishSpot zostaje oznaczony `disabled` — pozostaje w bazie do raportów historycznych, ale autopiloty przestają go obsługiwać.
- **Grupy nadążają.** Członkostwo w „Engineering”, „Finance”, „Zarząd” — cokolwiek zdefiniowano w Entra — zostaje odbite w grupach PhishSpot, więc odbiorcy autopilotów automatycznie podążają za strukturą organizacji.

Jeśli chcesz też, żeby użytkownicy logowali się do swojego portalu szkoleniowego przez Microsoft, ta sama integracja obsługuje ten przepływ — patrz Rozdział 24 Logowanie przez Microsoft 365.

25.2 Połączenie z Entra



Lista integracji — karta Microsoft Entra ID obok Google Workspace i Whitelist filtra antyspamowego

1. Otwórz **Ustawienia konta** → **Integracje**. Zobaczysz siatkę kart integracji. Znajdź kartę **Microsoft Entra ID**; pokazuje szary punkt statusu („nieaktywna") dopóki nie zostanie połączona.
2. Kliknij **Połącz z Microsoft**. PhishSpot poprosi o **tenant ID** Entra (GUID, np. `1f3a8d2e-...`). Znajdziesz go w centrum administracyjnym Entra w sekcji „Właściwości".
3. Zatwierdź. PhishSpot generuje token state podpisany HMAC i przekierowuje Cię na ekran zgody administracyjnej Microsoft pod `login.microsoftonline.com/<tenant>/v2.0/adminconsent`. **Musisz być zalogowany jako Global Administrator** w docelowym tenancie — zgoda administracyjna nadaje aplikacji enterprise PhishSpot uprawnienia odczytu katalogu w imieniu wszystkich użytkowników.
4. Ekran zgody pokazuje żądane uprawnienia:
   - `User.Read.All` — odczyt profili użytkowników (do listy kontaktów).
   - `Group.Read.All` — odczyt definicji grup.
   - `Directory.Read.All` — odczyt członkostwa w grupach.
   - `openid` / `profile` / `email` — potrzebne dla przepływu logowania SSO.
5. Nadaj. Microsoft przekierowuje z powrotem do callbacku PhishSpot z `admin_consent=True&tenant=<ID>&state=<HMAC>`. PhishSpot weryfikuje HMAC, zapisuje token aplikacji ograniczony do tenanta i zmienia status integracji na **aktywna**.

Połączone. Karta Microsoft pokazuje zielony punkt statusu, tenant ID monospace i znacznik czasu zgody.

25.3 Harmonogram synchronizacji

Kliknij **Zarządzaj** na aktywnej karcie Microsoft, aby otworzyć ustawienia integracji. Dwa checkboxy i jeden dropdown:

- **Synchronizuj użytkowników do kontaktów** — domyślnie WŁ. Pobiera każdego użytkownika Entra (z wyłączeniem gości i kont wyłączonych) i upsertuje jako rekord `Contact` w PhishSpot.
- **Synchronizuj grupy** — domyślnie WŁ. Pobiera każdą grupę Entra (security i Microsoft 365 groups) i upsertuje jako `Group`. Członkostwa są uzgadniane w tym samym przebiegu.
- **Harmonogram** — jedno z:
  - **Wyłączony** — brak automatycznej synchronizacji. Możesz nadal odpalać ją ręcznie (§25.5).
  - **Co godzinę** — uruchamia się co godzinę o pełnej.
  - **Codziennie** — uruchamia się raz dziennie o 02:00 UTC. **Domyślny dla tenantów produkcyjnych.**
  - **Co tydzień** — uruchamia się raz w tygodniu, w poniedziałki o 02:00 UTC.

Zapisz ustawienia. Scheduler platformy (`ScheduledDirectorySyncsJob`) rozsyła w każdym interwale, kolejkując jeden `DirectorySyncJob` per aktywna integracja pasująca do harmonogramu.

Pierwsza synchronizacja po świeżym połączeniu jest zwykle największa — importuje wszystko. Kolejne dotykają tylko tego, co się zmieniło (kilka zmodyfikowanych użytkowników, jedna utworzona grupa, jedno usunięte członkostwo), więc są szybkie — zwykle poniżej minuty nawet dla tysięcy użytkowników.

25.4 Co jest importowane

Dla każdego **użytkownika** Entra importer tworzy lub aktualizuje `Contact` kluczowany po Entra Object ID (`oid`). Mapowanie:

Pole Contact w PhishSpot	Źródło Entra
`email`	`userPrincipalName` (fallback do `mail`)
`first_name`, `last_name`	`givenName`, `surname`
`title`	`jobTitle`
`department`	`department`
`location`	`officeLocation` (fallback do city + country)
`telephone`	`mobilePhone` (fallback do `businessPhones`)
`external_id`	`id` (OID Entry)
`external_state`	`active` jeśli `accountEnabled=true`, inaczej `disabled`
`source`	zawsze `:entra`
`synced_at`	znacznik czasu synchronizacji

Dla każdej **grupy** Entra importer tworzy `Group` kluczowany po OID grupy:

Pole Group w PhishSpot	Źródło Entra
`name`	sluggowany `displayName` (np. „Dział IT” → `dzial-it`)
`display_name`	`displayName` (zachowuje wielkość liter i polskie znaki)
`external_id`	`id` grupy
`source`	`:entra`

Członkostwo jest uzgadniane per synchronizacja: PhishSpot listuje aktualnych członków każdej grupy Entra, usuwa lokalne rekordy `ContactGroup` dla kontaktów, których już nie ma w grupie Entra, i tworzy nowe dla dodanych.

Ważne: Kontakty, których konto Entra zostało **usunięte** (a nie tylko wyłączone), nie znikają z PhishSpot — są oznaczane `external_state: disabled`, żeby raporty historyczne pozostały spójne. Aby całkowicie wyczyścić kontakt, usuń go ręcznie z UI PhishSpot.

25.5 Ręczna synchronizacja („Synchronizuj teraz”)

Strona zarządzania integracją ma przycisk **Synchronizuj teraz**. Kliknij go aby natychmiast zakolejkować `DirectorySyncJob`, niezależnie od harmonogramu. Używaj do:

- **Początkowego połączenia** — większość adminów klika Synchronizuj teraz raz, zaraz po nadaniu zgody, żeby pierwszy import nie czekał na jutrzejszy cron o 02:00 UTC.
- **Push onboardingowy** — gdy IT oznaczy w Entra 20 nowych pracowników, chcesz mieć ich w PhishSpot przed następnym zaplanowanym przebiegiem.
- **Troubleshooting** — żeby spróbować ponownie po przejściowym błędzie Microsoft Graph widocznym w logu aktywności.

Ręczna synchronizacja zapisuje wpis `DirectorySyncLog` z `trigger: manual` — przydatne do odróżniania świadomych akcji admina od przebiegów z crona przy audytowaniu.

25.6 Historia synchronizacji

Pod ustawieniami tabela aktywności pokazuje ostatnie 50 przebiegów synchronizacji. Kolumny:

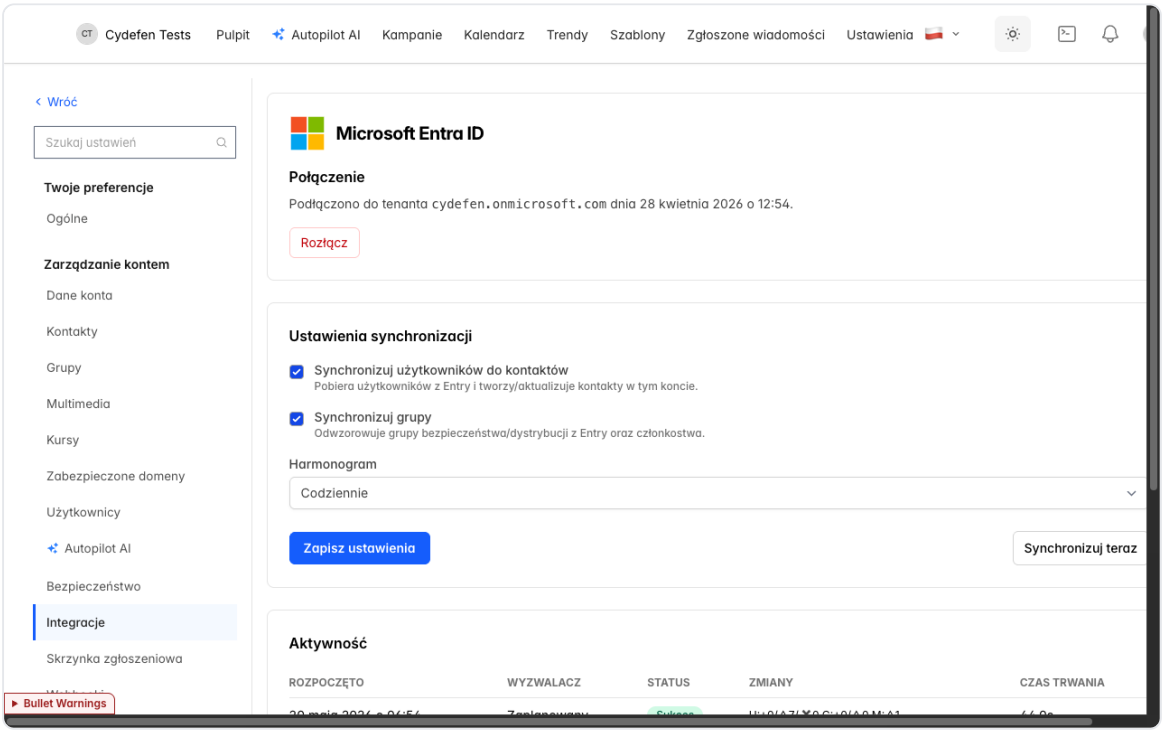
Kolumna	Co pokazuje
Rozpoczęto	Kiedy przebieg się zaczął
Wyzwalacz	`Ręczny` (admin kliknął Synchronizuj teraz), `Zaplanowany` (cron), lub `Callback OAuth` (auto-sync zaraz po nadaniu zgody)
Status	`W trakcie`, `Sukces`, `Błąd`, lub `Częściowy` (kolorowy badge)
Zmiany	Użytkownicy utworzeni / zaktualizowani / wyłączeni, grupy utworzone / zaktualizowane, zmiany członkostwa

Kolumna	Co pokazuje
Czas trwania	Wall-clock czas przebiegu

Typowa tabela aktywności dla małej organizacji wygląda tak (rzeczywisty przykład z działającego setupu):

Rozpoczęto	Wyzwalacz	Status	Zmiany	Czas trwania
6 godzin temu	Zaplanowany	Sukces	0c · 7u · 0d / 0c · 0u / 1m	22 s
2 dni temu	Zaplanowany	Sukces	1c · 2u · 1d / 0c · 0u / 2m	19 s
7 dni temu	Ręczny	Sukces	0c · 4u · 0d / 0c · 0u / 0m	14 s
8 dni temu	Zaplanowany	Błąd	—	1 s
10 dni temu	Zaplanowany	Sukces	1c · 3u · 0d / 0c · 0u / 1m	16 s

Nieudane przebiegi rozwijają się, pokazując komunikat błędu Microsoft Graph — większość to przejściowe odpowiedzi rate-limit (HTTP 429), które kolejny zaplanowany przebieg czysto absorbuje.



Strona zarządzania integracją Entra — ustawienia synchronizacji + historia aktywności

25.7 Rozwiązywanie problemów

Przycisk Połącz zabiera mnie na ekran „odmowa zgody”. Zalogowałeś się jako użytkownik bez uprawnień admin w tenancie. Wyloguj się ze wszystkich kont Microsoft, zaloguj się od nowa jako Global Administrator i spróbuj jeszcze raz.

Synchronizacja przechodzi, ale nie pojawiają się kontakty. Otwórz log aktywności. Jeśli status to **Sukces** i wszystkie zmiany są zerowe, Twój tenant Entra nie ma użytkowników pasujących do filtra (goście i konta wyłączone są pomijane). Sprawdź w Entra, że oczekiwani użytkownicy mają `accountEnabled=true`.

„Tenant mismatch" na callbacku. Tenant ID Entra, który wprowadziłeś, nie pasuje do tenanta, którego admin nadał zgodę. Rozłącz i połącz ponownie z poprawnym tenant ID.

Częściowe synchronizacje. Jeśli synchronizacja kończy się statusem **Częściowy**, część upsertów się udała, a część nie — zwykle dlatego, że jeden rekord użytkownika złamał constraint unikalności (np. dwóch użytkowników Entra ma ten sam email). Sprawdź wpis w logu aktywności; komunikat błędu zawiera dotknięte adresy.

Harmonogram jest „Wyłączony", a spodziewałem się Codziennie. Harmonogram domyślnie pokazuje ostatnio zapisaną wartość — nie ma platformowego defaultu. Nowe połączenia są tworzone z `Wyłączony`, żebyś mógł przejrzeć ustawienia zanim automatyzacja ruszy.

25.8 Odnośniki

- Logowanie SSO Microsoft używające tej samej integracji: Rozdział 24 Logowanie przez Microsoft 365.
- Lista kontaktów, do której trafiają zaimportowane kontakty: Rozdział 5 Kontakty.
- Funkcja Grup odzwierciedlająca grupy Entra: Rozdział 6 Grupy.
- Autopiloty, które automatycznie włączają nowo zsynchronizowane kontakty przez flagę **Auto-dołączaj nowych członków**: Rozdział 23 Autopiloty.
- Webhooks mogące powiadamiać systemy zewnętrzne, gdy kontakty albo grupy się zmieniają: Rozdział 26 Webhooks.

Webhooks

REST API PhishSpot (Rozdział 27) pozwala pobierać dane na żądanie. Webhooks odwracają kierunek: zamiast Ty pollujesz nas, my wywołujemy POST do Twojego URL-a w momencie, gdy coś się dzieje. Wpięty w SIEM webhook zamienia zdarzenie `opened` kampanii w alert bezpieczeństwa parę sekund po kliknięciu użytkownika. Wpięty w LMS — aktualizuje rekord uczącego się bez nocnej synchronizacji.

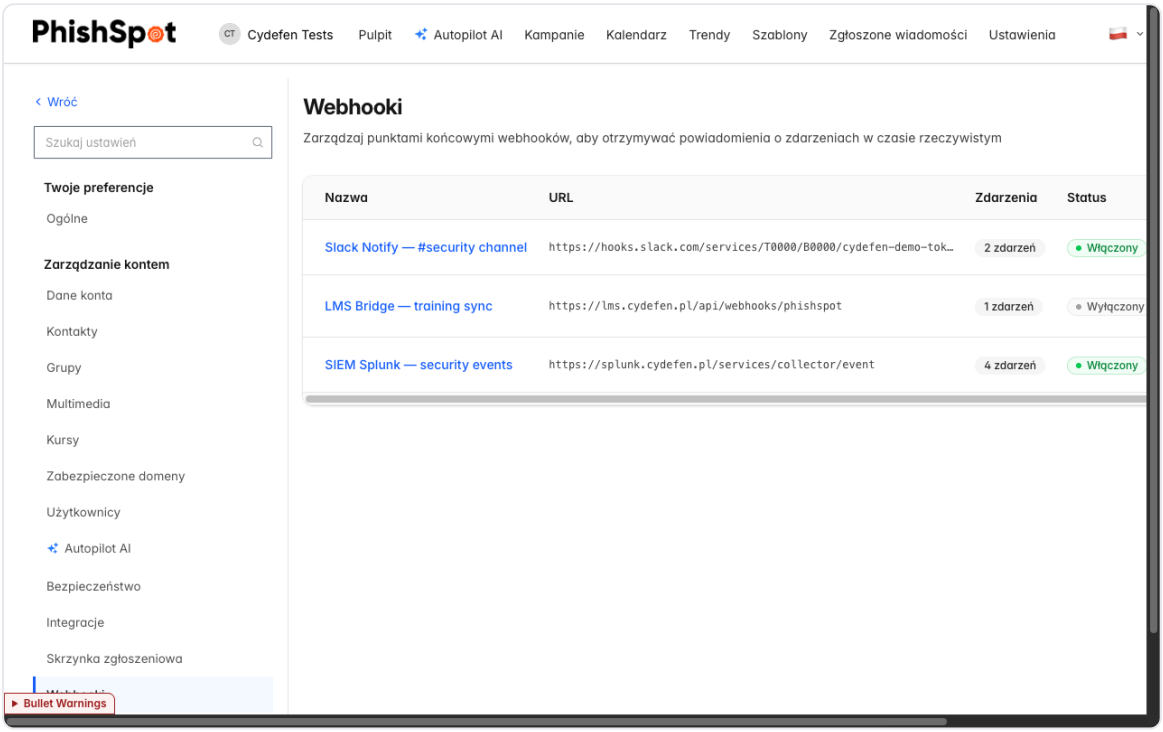
Ten rozdział opisuje dostępne zdarzenia, jak zarejestrować endpoint, co przychodzi na kablu i jak działają retry oraz podpisywanie.

26.1 Webhooks vs polling

Polling to pytanie „jest coś nowego?” w pętli — i ignorowanie odpowiedzi większość czasu. Marnuje wywołania API, ma wbudowane opóźnienie (dowiadujesz się o zdarzeniach przy następnym pollu, nie w momencie ich wystąpienia), źle się skaluje (dłuższe polly tracą zdarzenia, krótsze obciążają API).

Webhooks odwracają to. Rejestrujesz URL raz; my dostarczamy każde zdarzenie pod ten adres dokładnie wtedy, gdy wystąpi. Te same dane, niższe opóźnienie, mniej requestów. Minus: musisz mieć osiągalny endpoint HTTPS, żeby odbierać dostawy — ale dla celu integracji (SIEM, SOAR, LMS, bot, narzędzie wewnętrzne) to zwykle trywialne.

26.2 Tworzenie endpointu



Lista webhooków pokazująca trzy skonfigurowane endpointy

1. Otwórz **Ustawienia konta** → **Webhooks**. Strona endpoints listuje istniejące webhooki z kolumnami **Nazwa**, **URL**, **Zdarzenia** (liczba subskrybowanych typów), **Status** (Włączony / Wyłączony), **Dostawy** (łącznie + liczba nieudanych) i **Akcje**.
2. Kliknij **Nowy webhook**. Formularz ma cztery pola:
   - **Nazwa** — przyjazna etykieta. Przykłady z działającego setupu: „SIEM Splunk — security events", „LMS Bridge — training sync", „Slack Notify — #security channel".
   - **URL webhooka** — gdzie POST-ujemy dostawy. Musi być HTTPS. Platforma odrzuca URL-e wskazujące na localhost, link-local (169.254/16) i każdy zakres prywatny RFC1918 (10/8, 172.16/12, 192.168/16). Blokuje też `*.phishspot.com`. Cel: webhook nie może być nadużyty do sondowania sieci wewnętrznej.
   - **Subskrybuj zdarzenia** — checkboxy dla każdego typu (patrz §26.3). Zaznacz co najmniej jedno.
   - **Włącz endpoint webhooka** — przełącznik. Wyłączony oznacza, że trzymamy rekord, ale nic nie wysyłamy.
3. Zapisz. PhishSpot generuje **klucz podpisu** (64-znakowy hex z `SecureRandom.hex(32)`) i wyświetla go w całości na stronie szczegółów endpointu, z przyciskiem kopiowania. Zapisz go w bezpiecznym miejscu; nigdzie indziej go nie pokazujemy ponownie.

Endpoint jest aktywny natychmiast. Każde subskrybowane zdarzenie, które wystąpi od teraz, zostanie wysłane POST-em pod Twój URL.

26.3 Dostępne typy zdarzeń

Dziewięć typów zdarzeń jest dostępnych dziś, pogrupowanych po subiekcie:

Typ zdarzenia	Kiedy się odpala
`campaign.created`	Powstaje nowa kampania (ręcznie albo z iteracji autopilotu).
`campaign.updated`	Zmienia się stan kampanii, odbiorcy albo treść.
`campaign.deleted`	Kampania zostaje usunięta.
`contact.created`	Dodano kontakt (CSV, ręcznie albo synchronizacja katalogu).
`contact.updated`	Zmienia się email, dział, stanowisko, członkostwo w grupie albo external state.
`contact.deleted`	Kontakt zostaje usunięty z konta.
`deliverable.created`	Wysyłka kampanii produkuje rekord deliverable (jeden per odbiorca).
`deliverable.updated`	Stan odbiorcy się zmienia (sent → opened → clicked → submitted → educated, albo bounced).
`spam_whitelist.updated`	Lista IP / domen nadawcy dla konta się zmienia — patrz Rozdział 22 §22.5.

Endpoint może subskrybować dowolną kombinację. Typowy SIEM subskrybuje `contact.*` i `deliverable.*`, żeby widzieć kogo atakujemy i jak reagują. Typowy bridge do LMS subskrybuje tylko `deliverable.updated`, bo interesuje go jedynie postęp w szkoleniach.

26.4 Dostawa: payload + podpis

Każda dostawa to HTTP POST z ciałem JSON. Ciało to **zdarzenie** — ten sam rekord, który możesz pobrać przez API. Kształt:

```
{
  "id": "550e8400-e29b-41d4-a716-446655440000",
  "type": "contact.created",
  "created_at": "2026-05-20T14:22:33.000Z",
  "api_version": 1,
  "data": {
    "id": 42,
    "email": "anna.kowalska@cydefen.pl"
  }
}
```

- `id` — UUID identyfikujący to zdarzenie; klucz idempotentności. Powtórki tego samego zdarzenia używają tego samego `id`.
- `type` — nazwa typu zdarzenia (jeden z dziewięciu w §26.3).
- `created_at` — ISO-8601 UTC, kiedy zdarzenie wystąpiło.
- `api_version` — wersja schematu jako integer. `1` dla powyższego formatu. Przyszłe zmiany łamiące kształt podniosą tę wartość, a my powiadomimy z wyprzedzeniem.
- `data` — pola specyficzne dla subiektu. Na razie `data` zawiera `id` subiektu i kluczowe atrybuty identyfikujące; pełen rekord pobierzesz z REST API używając `id`.

Podpisywanie. Każdy POST niesie nagłówek `X-Webhook-Signature` zawierający HMAC-SHA256 ciała JSON, wyliczone z kluczem podpisu endpointu. Weryfikacja po Twojej stronie:

```ruby
expected = OpenSSL::HMAC.hexdigest("SHA256", signing_secret, request.raw_post)
signature = request.headers["X-Webhook-Signature"]
ActiveSupport::SecurityUtils.secure_compare(expected, signature) or render status: 401
```

```python
import hmac, hashlib
expected = hmac.new(secret.encode(), request.body, hashlib.sha256).hexdigest()
if not hmac.compare_digest(expected, request.headers["X-Webhook-Signature"]):
    abort(401)
```

Akceptuj tylko POST-y podpisane sekretem — nigdy nie ufaj niepodpisanemu requestowi, który twierdzi, że jest z PhishSpot.

26.5 Retry

Jeśli Twój endpoint odpowie czymś innym niż HTTP `2xx`, dostawa trafia do kolejki retry. Retry idzie według ustalonego harmonogramu:

Próba	Opóźnienie od poprzedniej
1	(natychmiast)
2	+15 sekund
3	+1 minuta
4	+5 minut
5	+15 minut
6	+1 godzina

Po **5 retry** (łącznie 6 prób) dostawa jest oznaczana **Failed** i już nie retrowana. Licznik `consecutive_failures` endpointu rośnie przy każdej całkowicie nieudanej dostawie. Po przekroczeniu 5 kolejnych niepowodzeń admini konta dostają mail jeden raz (z 7-dniowym cooldownem, żeby nie spamować, gdy endpoint jest źle skonfigurowany od dawna). Sam endpoint zostaje włączony — nie wyłączamy go automatycznie, bo większość awarii jest przejściowa i samonaprawiające się dostawy powinny móc się udać.

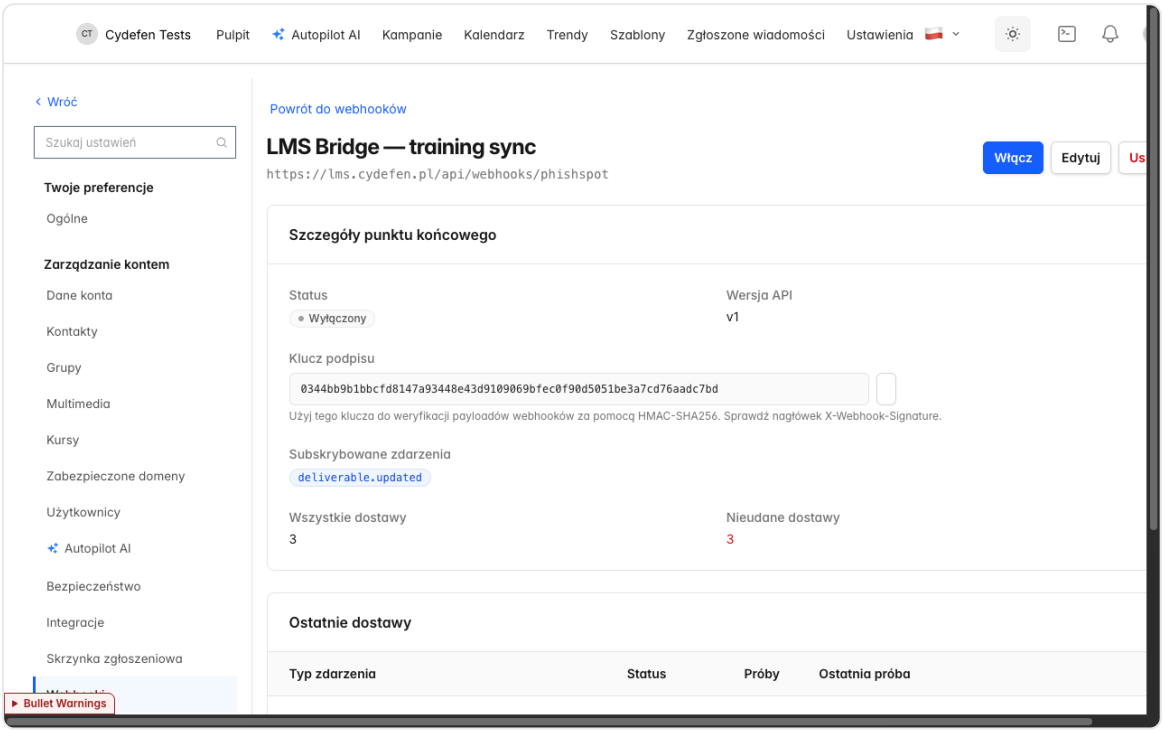
Jeśli chcesz ręcznie ponowić jedną nieudaną dostawę po naprawie po swojej stronie, otwórz stronę szczegółów dostawy (§26.6) i kliknij **Ponów**. To tworzy świeżą dostawę dla tego samego zdarzenia, z wyzerowanymi licznikami prób.

26.6 Historia dostaw

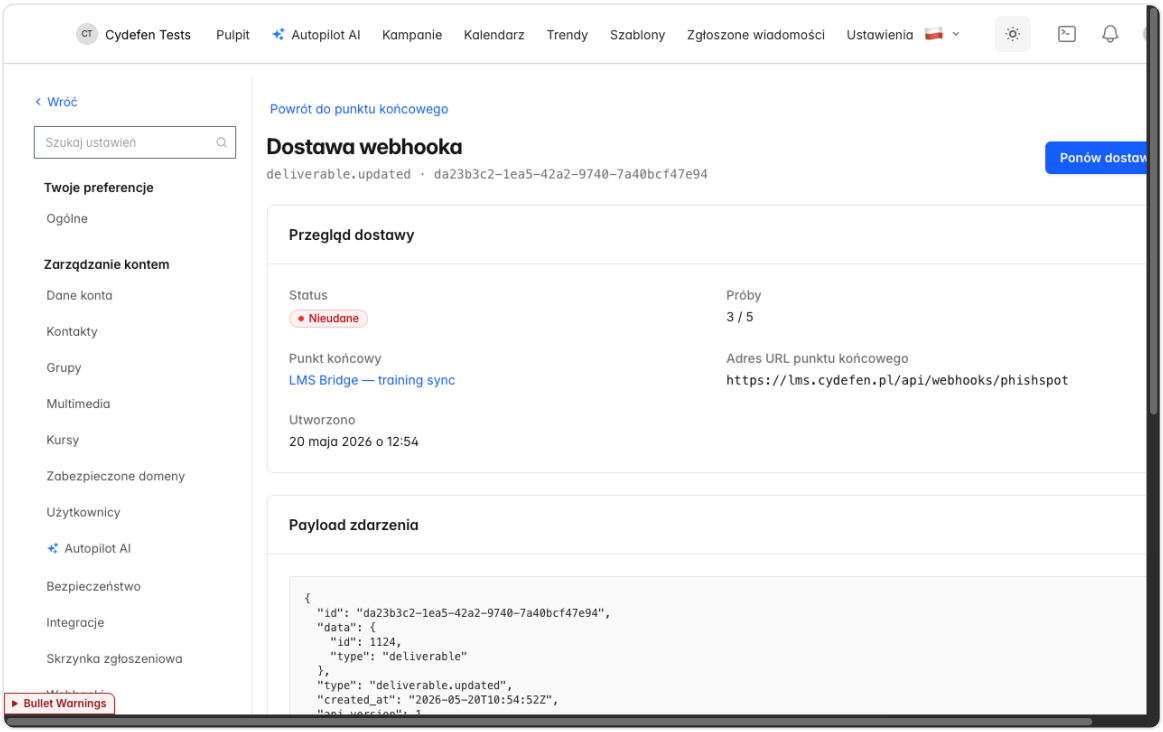
Strona szczegółów endpointu (kliknij dowolną nazwę endpointu na liście) pokazuje wszystko, co wiemy o tym endpoincie:

- **Szczegóły endpointu** — nazwa, URL, wersja API, klucz podpisu (z przyciskiem kopiowania), subskrybowane zdarzenia.
- **Status** — przełącznik Włączony / Wyłączony.
- **Ostatnie dostawy** — tabela ostatnich 50 dostaw z kolumnami:
  - **Typ zdarzenia** (np. `contact.created`)
  - **Status** — Oczekuje / Dostarcza / Dostarczone / Nieudane
  - **Próby** — aktualna liczba prób / max (np. `1 / 5`, `5 / 5`)
  - **Ostatnia próba** — znacznik czasu
  - **Akcje** — Zobacz szczegóły, Ponów dostawę

Kliknij Zobacz szczegóły na dowolnym wierszu dostawy, aby otworzyć stronę szczegółów. Pokazuje pełny payload (sformatowany JSON), docelowy URL i log per-próba: numer próby, kod HTTP, czas odpowiedzi w ms i ciało odpowiedzi (albo komunikat błędu, jeśli request nie doszedł). To Twoja główna powierzchnia debugowania, gdy integracja się psuje.



Szczegóły endpointu webhook — klucz podpisu, subskrybowane zdarzenia, ostatnie dostawy z licznikami prób



Szczegóły dostawy webhooka — payload zdarzenia + log per-próba HTTP

26.7 Wskazówki operacyjne

- **Potwierdzaj szybko.** Twój handler powinien przyjąć dostawę (zwrócić 2xx) i przetwarzać asynchronicznie. My się poddajemy wolnym responderom — a wolni responderzy kaskadują się w retry, które kaskadują się w maile o „consecutive failures".

- **Obsłuż duplikaty.** Problemy sieciowe mogą sprawić, że to samo zdarzenie dotrze dwa razy. Deduplikuj po polu `id` — jest stabilne między retry.
- **Weryfikuj podpis.** Nie działaj na webhooku, którego podpis się nie zgadza. POST chroniony sekretem to jedyne uwierzytelnienie; bez niego integrację może odtworzyć każdy, kto zgadnie URL.
- **Spodziewaj się szczytów.** Kampania z 1000 odbiorców produkuje 1000 zdarzeń `deliverable.created` w krótkim oknie. Upewnij się, że Twój handler się skaluje.
- **Rotuj sekret jeśli wycieknie.** Usuń i utwórz endpoint na nowo — UI nie oferuje dziś rotacji „w miejscu".

26.8 Odnośniki

- REST API do pobierania tych samych danych na żądanie: Rozdział 27 Referencja REST API.
- Integracja auto-odświeżania whitelisty używająca tego samego pipeline'u dostaw: Rozdział 22 Whitelist filtra antyspamowego.
- Kontakty, do których odnoszą się zdarzenia `contact.*`: Rozdział 5 Kontakty.
- Kampanie, do których odnoszą się zdarzenia `campaign.*`: Rozdział 4 Kampanie.
- Zdarzenia synchronizacji katalogu, które generują większość ruchu `contact.*` w produkcji: Rozdział 25 Synchronizacja katalogu.

Dokumentacja REST API

PhishSpot udostępnia REST API w formacie JSON pod adresem `https://platform.phishspot.com/api/v1`. Obejmuje ono praktycznie wszystko, co można zrobić w aplikacji administracyjnej: budować, planować i analizować kampanie, zarządzać odbiorcami/grupami/szablonami/kursami/mediami/domenami/autopilotami oraz przesyłać wyniki do własnych narzędzi.

Ten rozdział dokumentuje szczegółowo każdy punkt końcowy — parametry, treści żądań, pola odpowiedzi i kody statusu — abyś mógł zintegrować się bez czytania kodu źródłowego. Model zdarzeń oparty na powiadomieniach push opisano w Rozdziale 26 Webhooki; interfejs AI w języku naturalnym oferujący te same możliwości opisano w Rozdziale 29 Serwer MCP.

:::tip[Jak czytać ten rozdział] §27.1 i §27.2 opisują uwierzytelnianie, formaty identyfikatorów, stronicowanie oraz **odpowiedzi błędów wspólne dla wszystkich punktów końcowych** — sekcje poszczególnych punktów końcowych poniżej wymieniają tylko ich *dodatkowe* kody statusu. Każdy punkt końcowy zawiera swoje parametry (path / query / body), gotowy do uruchomienia przykład `curl`, pola odpowiedzi oraz przykładową odpowiedź. :::

27.1 Uwierzytelnianie

Każde uwierzytelnione żądanie musi przesyłać token API jako nagłówek bearer:

```
Authorization: Bearer <token>
```

Token można uzyskać na jeden z dwóch sposobów:

Z interfejsu administracyjnego (zalecane). Ustawienia konta → Tokeny API → Nowy token (zobacz Rozdział 14). Skopiuj wartość — jest ona wyświetlana tylko raz. Przechowuj ją w menedżerze sekretów.

Z API. Wyślij metodą POST `email` + `password` (oraz `otp_attempt`, jeśli włączone jest uwierzytelnianie dwuskładnikowe) na adres `/auth`:

```
curl -X POST https://platform.phishspot.com/api/v1/auth \
  -H 'Content-Type: application/json' \
  -d '{"email":"admin@example.com","password":"secret"}'
```

```
{ "token": "abc123…", "user": { "id": 2, "email": "admin@example.com" } }
```

Pole	Typ	Opis
`email`	string	**Wymagane.** Adres e-mail użytkownika.
`password`	string	**Wymagane.** Hasło użytkownika.
`otp_attempt`	string	Wymagane tylko wtedy, gdy użytkownik ma włączone uwierzytelnianie dwuskładnikowe.

Token należy do pojedynczego użytkownika i dziedziczy jego przynależności do kont. Traktuj go jak hasło. Wszystkie poniższe przykłady zakładają, że `$TOKEN` zawiera prawidłowy token.

27.2 Konwencje

- **Bazowy URL:** `https://platform.phishspot.com/api/v1`. Wszystkie poniższe ścieżki są względne wobec niego.
- **Typ treści:** wysyłaj `Content-Type: application/json`; treści żądań i odpowiedzi są w formacie JSON.
- **Czasy:** ISO-8601 (`2026-05-20T14:22:33.000Z`), UTC, o ile nie zaznaczono inaczej. Wartość wejściowa kampanii `scheduled_at` jest interpretowana w **strefie czasowej konta**.
- **Identyfikatory w ścieżkach:** wszędzie tam, gdzie ścieżka przyjmuje `:id`, możesz przekazać **albo** całkowity klucz główny (`/campaigns/42`), **albo** prefiksowany identyfikator rekordu (`/campaigns/camp_0u1k…`). Odpowiedzi zawsze udostępniają całkowite `id`; niektóre udostępniają również prefiksowany identyfikator.
- **`account_id`:** trasy zagnieżdżone przyjmują `account_id` w ścieżce; akceptuje on całkowity identyfikator lub prefiksowany identyfikator `acct_…`. Swój znajdziesz przez `GET /accounts`.
- **Zakres konta:** token może działać tylko na kontach, do których należy jego użytkownik. Żądanie rekordu z innego konta zwraca **404** — API nigdy nie potwierdza, że dane innego najemcy istnieją.
- **Role:** punkty końcowe odczytu wymagają dowolnej roli (w tym `member`). Punkty końcowe zapisu (`POST` / `PATCH` / `PUT` / `DELETE` oraz akcje zmieniające stan) wymagają roli **admin** lub **editor**; token z rolą `member` otrzymuje `403`. Akcje administracyjne zespołu/rozliczeń oraz domen platformy wymagają roli **admin**.
- **Stronicowanie:** punkty końcowe obsługujące stronicowanie przyjmują `?page=N` (liczone od 1), a czasem `?per_page=M` lub `?limit=M`; wartości domyślne są podane przy każdym punkcie końcowym. Listy bez stronicowania zwracają pełny uporządkowany zbiór.

Wspólne odpowiedzi błędów

O ile punkt końcowy nie stanowi inaczej, dotyczą one każdego wywołania (poniżej powtarzane są tylko kody specyficzne dla danego punktu końcowego):

Kod	Treść	Kiedy
`401 Unauthorized`	*(puste)*	Brak lub nieprawidłowy token `Authorization`.
`403 Forbidden`	`{"error":"You are not authorized to perform this action"}`	Token prawidłowy, ale rola użytkownika jest niewystarczająca dla tej akcji.
`404 Not Found`	`{"error":"Resource not found"}`	Brak takiego rekordu **lub** rekord należy do konta, do którego token nie ma dostępu.
`422 Unprocessable Content`	`{"errors":{"field":["message"]}}` *(lub* `{"errors":["message"]}` *dla punktów końcowych akcji)*	Walidacja nie powiodła się; sprawdź `errors`.

Kod	Treść	Kiedy
`429 Too Many Requests`	*(różne)*	Przekroczono limit żądań; zobacz §27.17. Nagłówek `Retry-After` wskazuje, kiedy ponowić próbę.

27.3 Tożsamość i konta

`GET /me`

Zwraca użytkownika stojącego za tokenem.

Parametry: brak (tylko token bearer).

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/me
```

Odpowiedź `200 OK`

Pole	Typ	Opis
`id`	integer	Identyfikator użytkownika.
`email`	string	Adres e-mail użytkownika.
`name`	string	Nazwa wyświetlana.
`locale`	string	Ustawienia językowe interfejsu (`en` / `pl`).
`accounts`	array	Konta, na których token może działać (zobacz `GET /accounts`).

`GET /accounts`

Wyświetla wszystkie konta, do których użytkownik tokenu ma dostęp. Użyj tego, aby znaleźć `account_id` dla tras zagnieżdżonych.

Parametry: brak.

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts
```

Odpowiedź `200 OK` — tablica obiektów:

Pole	Typ	Opis
`id`	integer	Identyfikator konta (używany w ścieżkach zagnieżdżonych).
`prefix_id`	string	Prefiksowany identyfikator (`acct_…`).
`name`	string	Nazwa konta.

Pole	Typ	Opis
`locale`	string	Domyślne ustawienia językowe konta.

```
[{ "id": 11, "name": "Cydefen Tests", "locale": "pl", "prefix_id": "acct_3kf…" }]
```

27.4 Kampanie

Zarządzaj kampaniami symulacji phishingu: twórz i edytuj wersje robocze, prowadź kampanię przez jej cykl życia (start, pauza, zatrzymanie, anulowanie), zaplanuj przyszłą wysyłkę, duplikuj oraz odczytuj wyniki, postęp odbiorców, odpowiedzi i oś czasu zdarzeń dla pojedynczego kontaktu.

Autoryzacja jest egzekwowana per konto: kampania jest dostępna tylko wtedy, gdy należy do jednego z kont, których członkiem jest użytkownik tokenu (bearer) — każda rola w ramach członkostwa może odczytywać i zapisywać; nie ma akcji kampanii dostępnych wyłącznie dla administratorów. Punkty końcowe zmieniające stan dodatkowo wymagają, aby kampania znajdowała się w zgodnym stanie (np. zapauzować można tylko kampanię w stanie in_progress), w przeciwnym razie zwracają `403`.

> `POST /campaigns/:id/start` oraz `POST /campaigns/:id/schedule` wysyłają **prawdziwe wiadomości phishingowe** do odbiorców kampanii (natychmiast lub o zaplanowanej godzinie). Nie są to przebiegi próbne. Traktuj je jako destrukcyjne, nieodwracalne wysyłki.

Obiekt kampanii zwracany przez `show`, `create`, `update` oraz wszystkie punkty końcowe zmieniające stan jest identyczny i opisany jednokrotnie w sekcji `GET /campaigns/:id`.

`GET /accounts/:account_id/campaigns`

Wyświetla listę wszystkich kampanii na koncie, od najnowszych. Użyj go, aby wyliczyć kampanie przed przejściem do szczegółów jednej z nich. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokenu.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/campaigns
```

Odpowiedź `200 OK` — tablica JSON obiektów kampanii (lista pól dla pojedynczego obiektu znajduje się w `GET /campaigns/:id`), uporządkowana malejąco według `created_at`.

```
[
  {
    "id": 42,
    "account_id": 11,
    "name": "Q2 Invoice Lure",
    "state": "in_progress",
    "delivery_mode": "immediate",
    "delivery_schedule": null,
    "created_at": "2026-05-01T09:00:00.000Z",
    "updated_at": "2026-05-02T14:12:00.000Z",
    "email_subject": "Your April invoice is ready",
    "email_content": "<p>Hello {{first_name}}…</p>",
    "landing_html": "<form>…</form>",
    "domain": "officelogin.in",
    "course_id": 7,
    "groups": [{ "id": 3, "name": "Finance" }],
    "statistics": {
      "total_contacts": 120,
      "total_deliverables": 120,
      "completion_percentage": 100.0
    },
    "can_start": false,
    "can_pause": true,
    "can_cancel": true
  }
]
```


Kody statusu

Kod	Kiedy
200	Kampanie wyświetlone (pusta tablica, jeśli konto nie ma żadnych).
403	Użytkownik tokenu nie jest uprawniony do wyświetlenia konta.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.

`POST /accounts/:account_id/campaigns`

Tworzy nową roboczą kampanię na koncie. Wszystkie pola treści są opcjonalne przy tworzeniu — wymagane jest tylko `name` — dzięki czemu możesz utworzyć pustą wersję roboczą i uzupełnić ją za pomocą `PATCH`. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Wszystkie parametry treści żądania są opakowane w obiekt `campaign`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
campaign[name]	body	string	tak	Nazwa kampanii. Musi być unikalna w obrębie konta (bez uwzględniania wielkości liter).
campaign[delivery_mode]	body	string	nie	Jedna z wartości `immediate` , `scheduled` , `staggered` . Domyślnie `immediate` .
campaign[delivery_schedule]	body	string	nie	Dowolny ciąg harmonogramu używany wyłącznie, gdy `delivery_mode` to `scheduled` (data i czas ISO8601 lub 5-polowy cron). Zamiast tego preferuj punkt końcowy `/schedule` .
campaign[email_subject]	body	string	nie	Temat wiadomości. Może zawierać znaczniki scalania wiadomości (np. `{{first_name}}`); nieznane znaczniki nie przejdą walidacji.
campaign[email_content]	body	string	nie	Treść HTML wiadomości. Musi być poprawnym HTML i używać wyłącznie dozwolonych znaczników scalania wiadomości.
campaign[landing_html]	body	string	nie	HTML strony docelowej. Musi być poprawnym HTML i używać wyłącznie dozwolonych znaczników scalania strony docelowej.
campaign[landing_css]	body	string	nie	CSS strony docelowej. Musi być poprawnym CSS.
campaign[landing_page_enabled]	body	boolean	nie	Czy strona docelowa jest serwowana. Domyślnie `false` .
campaign[platform_domain_id]	body	integer	nie	Identyfikator domeny `PlatformDomain` (domeny atakującego) używanej do wysyłki i strony docelowej. Wymagany, zanim kampania może wystartować.

Nazwa	Gdzie	Typ	Wymagane	Opis
campaign[course_id]	body	integer	nie	Identyfikator kursu e-learningowego, do którego przekierowywane są ofiary (używany, gdy `end_action_type` to `redirect_to_course`).
campaign[from_email]	body	string	nie	Adres e-mail nadawcy. Wymagany, zanim kampania może wystartować.
campaign[from_name]	body	string	nie	Wyświetlana nazwa nadawcy.
campaign[end_action_type]	body	string	nie	Co dzieje się po działaniu ofiary. Jedna z wartości `nothing`, `redirect_to_course`, `message_page`, `redirect_to_url`. Domyślnie `message_page`.
campaign[end_action_url]	body	string	nie	Zewnętrzny adres URL do przekierowania. Wymagany (i musi być `http` / `https`, nie może zapętlać się z powrotem do domeny platformy), gdy `end_action_type` to `redirect_to_url`.
campaign[end_action_html]	body	string	nie	Niestandardowa strona z komunikatem HTML. Wymagana, gdy `end_action_type` to `message_page` (uzupełniana automatycznie wartością domyślną, jeśli pominięta).
campaign[group_ids]	body	array of integer	nie	Identyfikatory grup kontaktów, na które jest kierowana kampania.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{
        "campaign": {
          "name": "Q2 Invoice Lure",
          "delivery_mode": "immediate",
          "email_subject": "Your April invoice is ready",
          "email_content": "<p>Hello {{first_name}}…</p>",
          "from_email": "billing@officelogin.in",
          "from_name": "Accounts Payable",
          "platform_domain_id": 5,
          "end_action_type": "redirect_to_course",
          "course_id": 7,
          "group_ids": [3]
        }
      }' \
  https://platform.phishspot.com/api/v1/accounts/11/campaigns
```

Odpowiedź `201 Created` — nowo utworzony obiekt kampanii (taki sam kształt jak `GET /campaigns/:id`).

Kody statusu

Kod	Kiedy
201	Kampania utworzona.
400	Obiekt `campaign` brakuje w treści żądania (`ParameterMissing`).
403	Użytkownik tokenu nie jest uprawniony do tworzenia kampanii na koncie.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.
422	Walidacja nie powiodła się — np. puste/zduplikowane `name`, nieprawidłowa wartość enum `delivery_mode` / `end_action_type`, niepoprawny HTML/CSS, niedozwolony znacznik scalania lub brakujące `end_action_url` / `end_action_html` dla wybranego `end_action_type`. Treść: `{ "errors": { "<field>": ["…"] } }`.

`GET /campaigns/:id`

Pobiera pojedynczą kampanię po identyfikatorze (płytka trasa, nie zagnieżdżona pod kontem). Użyj go, aby odczytać pełną treść kampanii oraz flagi akcji informujące, które przejścia są obecnie dozwolone. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita). Musi należeć do konta, którego członkiem jest użytkownik tokenu.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42
```

Odpowiedź `200 OK` — obiekt kampanii.

Pole	Typ	Opis
id	integer	Identyfikator kampanii.
account_id	integer	Identyfikator konta właściciela.
name	string	Nazwa kampanii.
state	string	Stan cyklu życia: `draft`, `in_progress`, `paused`, `cancelled`, `done` lub `scheduled`.
delivery_mode	string	`immediate`, `scheduled` lub `staggered`.
delivery_schedule	string | null	Surowy ciąg harmonogramu dostarczania (znaczący tylko dla trybu `scheduled`).
created_at	string	Znacznik czasu ISO8601.
updated_at	string	Znacznik czasu ISO8601.
email_subject	string | null	Temat wiadomości.
email_content	string | null	Treść HTML wiadomości.
landing_html	string | null	HTML strony docelowej.
domain	string | null	Nazwa powiązanej domeny `PlatformDomain` (np. `officelogin.in`) lub null, jeśli żadna nie jest ustawiona.
course_id	integer | null	Identyfikator powiązanego kursu lub null.
groups	array	Grupy docelowe, każda w postaci `{ "id": integer, "name": string }`.
statistics	object	**Obecne tylko wtedy, gdy** `state` to `in_progress`, `paused` lub `done`. Obiekt z `total_contacts` (integer), `total_deliverables` (integer), `completion_percentage` (float).
can_start	boolean	Czy `start` / `schedule` jest teraz dozwolone (true dla `draft` / `scheduled`).
can_pause	boolean	Czy `pause` jest teraz dozwolone (true tylko gdy `in_progress`).

Pole	Typ	Opis
can_cancel	boolean	Czy `cancel` jest teraz dozwolone (true dla `in_progress` / `paused` / `scheduled`).


```
{
  "id": 42,
  "account_id": 11,
  "name": "Q2 Invoice Lure",
  "state": "draft",
  "delivery_mode": "immediate",
  "delivery_schedule": null,
  "created_at": "2026-05-01T09:00:00.000Z",
  "updated_at": "2026-05-01T09:00:00.000Z",
  "email_subject": "Your April invoice is ready",
  "email_content": "<p>Hello {{first_name}}…</p>",
  "landing_html": "<form>…</form>",
  "domain": "officelogin.in",
  "course_id": 7,
  "groups": [{ "id": 3, "name": "Finance" }],
  "can_start": true,
  "can_pause": false,
  "can_cancel": false
}
```


Kody statusu

Kod	Kiedy
200	Kampania zwrócona.
404	Brak kampanii o tym identyfikatorze na jakimkolwiek koncie, do którego należy użytkownik tokenu (obejmuje próby dostępu między kontami).

`PATCH /campaigns/:id`

Aktualizuje istniejącą kampanię. Edycja jest dozwolona tylko wtedy, gdy kampania znajduje się w stanie `draft` lub `scheduled` (polityka autoryzacji odrzuca edycję uruchomionych/zakończonych kampanii). **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Parametry treści żądania są opakowane w obiekt `campaign`; obowiązują te same dozwolone klucze co przy `POST` (wszystkie opcjonalne przy aktualizacji — wyślij tylko te pola, które chcesz zmienić).

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Nazwa	Gdzie	Typ	Wymagane	Opis
campaign[...]	body	—	nie	Dowolny podzbiór kluczy wymienionych w `POST /accounts/:account_id/campaigns` (`name`, `delivery_mode`, `delivery_schedule`, `email_subject`, `email_content`, `landing_html`, `landing_css`, `landing_page_enabled`, `platform_domain_id`, `course_id`, `from_email`, `from_name`, `end_action_type`, `end_action_url`, `end_action_html`, `group_ids[]`).

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "campaign": { "email_subject": "Action required: invoice overdue" } }' \
  https://platform.phishspot.com/api/v1/campaigns/42
```

Odpowiedź `200 OK` — zaktualizowany obiekt kampanii (taki sam kształt jak `GET /campaigns/:id`).

Kody statusu

Kod	Kiedy
200	Kampania zaktualizowana.
400	Obiekt `campaign` brakuje w treści żądania (`ParameterMissing`).
403	Kampania nie jest w stanie `draft` / `scheduled` (edycja zablokowana) lub użytkownik nie jest uprawniony.
404	Kampania nie została znaleziona na kontach użytkownika.
422	Walidacja nie powiodła się (te same walidacje co przy `POST`). Treść: `{ "errors": { … } }`.

`DELETE /campaigns/:id`

Trwale usuwa kampanię i jej rekordy zależne (odbiorców, przesyłki, zdarzenia, odpowiedzi). Dozwolone w dowolnym stanie. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42
```

Odpowiedź `204 No Content` — pusta treść.

Kody statusu

Kod	Kiedy
204	Kampania usunięta.
403	Użytkownik nie jest uprawniony do usunięcia kampanii.
404	Kampania nie została znaleziona na kontach użytkownika.

`POST /campaigns/:id/start`

> Uruchamia kampanię **i wysyła prawdziwe wiadomości phishingowe** do wszystkich odbiorców docelowych (partiami w trybie `immediate` lub zgodnie z harmonogramem dostarczania w pozostałych trybach). Jest to nieodwracalne — po uruchomieniu wiadomości zostają wysłane.

Przenosi kampanię w stanie `draft` lub `scheduled` do `in_progress` i kolejkuje zadania wysyłki. Przed wysłaniem serwer wykonuje kontrolę wstępną gotowości i odrzuca żądanie, jeśli kampania jest niekompletna. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/start
```

Odpowiedź `200 OK` — obiekt kampanii z `state: "in_progress"`.

Kody statusu

Kod	Kiedy
200	Kampania uruchomiona; wysyłki zakolejkowane.

Kod	Kiedy
403	Kampania nie jest w stanie umożliwiającym uruchomienie (`draft` / `paused` / `scheduled`).
404	Kampania nie została znaleziona na kontach użytkownika.
422	Kontrola wstępna gotowości nie powiodła się. Treść: `{ "errors": ["…", "…"] }` (płaska tablica czytelnych dla człowieka komunikatów). Przyczyny obejmują: brakujący temat wiadomości, brakującą treść wiadomości, brakujący adres e-mail nadawcy, brak ustawionej domeny platformy, nieaktywną lub zablokowaną do wysyłki domenę platformy, brak odbiorców docelowych oraz braki w akcji końcowej (brakujący kurs dla `redirect_to_course`, brakujący URL dla `redirect_to_url`, brakujący HTML dla `message_page`).

`POST /campaigns/:id/stop`

Oznacza trwającą kampanię jako `done` (zakończoną). Użyj go, aby wcześniej zakończyć działającą kampanię; oczekujące wysyłki nie są ponownie kolejkowane. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/stop
```

Odpowiedź `200 OK` — obiekt kampanii z `state: "done"`.

Kody statusu

Kod	Kiedy
200	Kampania oznaczona jako zakończona.
403	Kampania nie jest w stanie `in_progress`.
404	Kampania nie została znaleziona na kontach użytkownika.
422	Przejście stanu odrzucone przez model. Treść: `{ "errors": { … } }`.

`POST /campaigns/:id/pause`

Pauzuje trwającą kampanię (stan → `paused`), wstrzymując dalsze zaplanowane wysyłki. Wznów, wywołując ponownie `start`. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/pause
```

Odpowiedź `200 OK` — obiekt kampanii z `state: "paused"`.

Kody statusu

Kod	Kiedy
200	Kampania zapauzowana.
403	Kampania nie jest w stanie `in_progress`.
404	Kampania nie została znaleziona na kontach użytkownika.
422	Przejście stanu odrzucone przez model. Treść: `{ "errors": { … } }`.

`POST /campaigns/:id/cancel`

Anuluje kampanię (stan → `cancelled`). Dozwolone ze stanu `in_progress`, `paused` lub `scheduled` (nie ze stanu `draft` ani z już zakończonych kampanii). **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/cancel
```

Odpowiedź `200 OK` — obiekt kampanii z `state: "cancelled"`.

Kody statusu

Kod	Kiedy
200	Kampania anulowana.
403	Kampania nie jest w stanie umożliwiającym anulowanie (`in_progress` / `paused` / `scheduled`).
404	Kampania nie została znaleziona na kontach użytkownika.
422	Przejście stanu odrzucone przez model. Treść: `{ "errors": { … } }`.

`POST /campaigns/:id/duplicate`

Klonuje kampanię do nowej wersji `draft` (z nazwą z numerowanym sufiksem, np. `"Q2 Invoice Lure (1)"`), kopiując treść, grupy docelowe i odbiorców, ale resetując stan, harmonogram i migawkę. Użyj go, aby ponownie uruchomić lub rozgałęzić kampanię. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita) kampanii źródłowej.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/duplicate
```

Odpowiedź `201 Created` — nowy obiekt roboczej kampanii (taki sam kształt jak `GET /campaigns/:id`), z nowym `id` i `state: "draft"`.

Kody statusu

Kod	Kiedy
201	Duplikat utworzony.
403	Użytkownik nie jest uprawniony.
404	Kampania źródłowa nie została znaleziona na kontach użytkownika.
422	Zapisanie duplikatu nie powiodło się (walidacja). Treść: `{ "errors": { … } }`.

`POST /campaigns/:id/schedule`

> Planuje kampanię tak, aby **wysłała prawdziwe wiadomości phishingowe** o podanej przyszłej godzinie. Gdy nadejdzie zaplanowany czas, wiadomości zostaną wysłane automatycznie.

Planuje roboczą kampanię (`draft`) na przyszłą wysyłkę (stan → `scheduled`). Wykonuje tę samą kontrolę wstępną gotowości co `start` , a dodatkowo sprawdza poprawność czasu. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).
scheduled_at	body	string	tak	Docelowy czas wysyłki jako lokalna data i czas (w strefie czasowej konta), bez przesunięcia — np. `2026-06-10T09:00` (wartość produkowana przez pole `datetime-local`). Jest interpretowany w strefie czasowej konta (z fallbackiem do UTC, jeśli konto jej nie ma) i konwertowany na UTC po stronie serwera. Musi przypadać w przyszłości i co najmniej 5 minut od teraz. **Nie** jest opakowany w obiekt `campaign` — wysyłany jako klucz najwyższego poziomu w treści żądania.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "scheduled_at": "2026-06-10T09:00" }' \
  https://platform.phishspot.com/api/v1/campaigns/42/schedule
```

Odpowiedź `200 OK` — obiekt kampanii z `state: "scheduled"` .

Kody statusu

Kod	Kiedy
200	Kampania zaplanowana.
403	Kampania nie jest w stanie umożliwiającym uruchomienie (musi być `draft`).
404	Kampania nie została znaleziona na kontach użytkownika.
422	Planowanie nie powiodło się. Treść: `{ "errors": ["…"] }` (płaska tablica). Przyczyny: puste `scheduled_at` , niemożliwa do sparsowania data i czas, czas w przeszłości, czas mniej niż 5 minut od teraz lub niepowodzenie kontroli wstępnej gotowości do startu (te same kontrole treści/nadawcy/domeny/odbiorcy/akcji końcowej co przy `start`).

`POST /campaigns/:id/cancel_schedule`

Anuluje oczekujący harmonogram, przywracając kampanię do stanu `draft` i usuwając jej zakolejkowane zadanie wysyłki. Ważne tylko dla kampanii w stanie `scheduled`. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/cancel_schedule
```

Odpowiedź `200 OK` — obiekt kampanii (stan przywrócony do `draft`).

Kody statusu

Kod	Kiedy
200	Harmonogram anulowany.
403	Użytkownik nie jest uprawniony (polityka wymaga stanu `scheduled`).
404	Kampania nie została znaleziona na kontach użytkownika.
422	Kampania nie jest obecnie w stanie `scheduled`. Treść: `{ "error": "Campaign is not scheduled (state: <state>); nothing to cancel." }` (zwróć uwagę na klucz `error` w liczbie pojedynczej w tym przypadku).

`GET /campaigns/:id/results`

Zwraca zagregowane statystyki kampanii: ogólny lejek zaangażowania oraz zestawienia per grupa i per dział. Użyj go do renderowania pulpitów i raportów. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/campaigns/42/results
```

Odpowiedź `200 OK` — obiekt statystyk.

Pole	Typ	Opis
campaign_id	integer	Identyfikator kampanii.
name	string	Nazwa kampanii.
funnel	object	Ogólny lejek zaangażowania (liczby + współczynniki). Zobacz podpola poniżej.
groups	array	Zestawienie per grupa. Pusta tablica, jeśli kampania nie jest kierowana na żadne grupy. Zobacz podpola poniżej.
departments	array	Zestawienie per dział (kontakty pogrupowane według ich `department`). Puste, jeśli brak działów. Te same podpola liczbowe co wpis grupy, z `name`, ale bez `id`.

Podpola `funnel`:

Pole	Typ	Opis
sent	integer	Liczba unikalnych kontaktów, do których wiadomość została pomyślnie wysłana.
opened	integer	Liczba unikalnych kontaktów, które otworzyły wiadomość.
clicked	integer	Liczba unikalnych kontaktów, które kliknęły.
submitted	integer	Liczba unikalnych kontaktów, które przesłały dane na stronie docelowej.
trained	integer	Przesyłki, które osiągnęły stan `educated` (ukończone szkolenie).
replied	integer	Liczba unikalnych kontaktów, które odpowiedziały na wiadomość phishingową (sygnał z bocznego kanału, niewchodzący w skład lejka kliknięć/przesłań).
open_rate	float	`opened / sent` jako wartość procentowa (1 miejsce po przecinku).
click_rate	float	`clicked / sent` w procentach.
submit_rate	float	`submitted / sent` w procentach.
train_rate	float	`trained / sent` w procentach.
reply_rate	float	`replied / sent` w procentach.

Każdy wpis `groups[]`: `name` (string), `id` (integer), `total_contacts` (integer), `sent`, `opened`, `clicked`, `submitted`, `trained` (integers) oraz `open_rate`, `click_rate`, `submit_rate`, `train_rate` (floats).

```
{
  "campaign_id": 42,
  "name": "Q2 Invoice Lure",
  "funnel": {
    "sent": 120,
    "opened": 84,
    "clicked": 37,
    "submitted": 12,
    "trained": 9,
    "replied": 3,
    "open_rate": 70.0,
    "click_rate": 30.8,
    "submit_rate": 10.0,
    "train_rate": 7.5,
    "reply_rate": 2.5
  },
  "groups": [
    {
      "name": "Finance",
      "id": 3,
      "total_contacts": 60,
      "sent": 60,
      "opened": 45,
      "clicked": 22,
      "submitted": 8,
      "trained": 6,
      "open_rate": 75.0,
      "click_rate": 36.7,
      "submit_rate": 13.3,
      "train_rate": 10.0
    }
  ],
  "departments": [
    {
      "name": "Accounting",
      "total_contacts": 40,
      "sent": 40,
      "opened": 30,
      "clicked": 15,
      "submitted": 5,
      "trained": 4,
      "open_rate": 75.0,
      "click_rate": 37.5,
      "submit_rate": 12.5,
      "train_rate": 10.0
    }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Statystyki zwrócone.
404	Kampania nie została znaleziona na kontach użytkownika.

`GET /campaigns/:id/recipients`

Zwraca stronicowaną, filtrowalną listę odbiorców kampanii wraz z ich etapem dostarczenia, statusem szkolenia i flagą odpowiedzi dla pojedynczego kontaktu. Odbiorcy są uporządkowani według nazwiska kontaktu, a następnie imienia. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).
page	query	integer	nie	Numer strony liczony od 1; wartości poniżej 1 są przycinane do 1. Domyślnie 1. Rozmiar strony jest ustalony na 25.
stage	query	string	nie	Filtruj według etapu lejka: `sent` , `opened` , `clicked` , `submitted` lub `trained` . `all` (lub pominięcie) zwraca wszystkich. Filtry są kumulatywne względem etapu (np. `opened` obejmuje tych, którzy później kliknęli/przesłali/zostali przeszkoleni).
replied	query	boolean	nie	Gdy prawdziwe (`true` / `1`), ogranicza do kontaktów, które odpowiedziały na wiadomość.
group_id	query	integer	nie	Ogranicza do kontaktów w tej grupie (musi należeć do konta kampanii).
department	query	string	nie	Ogranicza do kontaktów, których `department` dokładnie odpowiada tej wartości.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/campaigns/42/recipients?stage=clicked&page=1"
```

Odpowiedź `200 OK` — stronicowani odbiorcy.

Pole	Typ	Opis
campaign_id	integer	Identyfikator kampanii.

Pole	Typ	Opis
page	integer	Bieżący numer strony.
per_page	integer	Rozmiar strony (zawsze 25).
total	integer	Łączna liczba odbiorców pasujących do filtrów (na wszystkich stronach).
recipients	array	Wiersze odbiorców (zobacz podpola).

Każdy wpis `recipients[]`:

Pole	Typ	Opis
id	integer	Identyfikator kontaktu.
contact_id	integer	Identyfikator kontaktu (ta sama wartość co `id`).
email	string	Adres e-mail kontaktu.
full_name	string	Pełna nazwa kontaktu.
status	string	Stan dostarczenia: `pending`, `sent`, `delivered`, `bounced`, `opened`, `clicked`, `submitted` lub `educated`.
stage	string	Ta sama wartość co `status` (alias).
training_status	string	`not_started`, `in_progress` lub `completed`.
replied	boolean	Czy kontakt odpowiedział na wiadomość phishingową.


```
{
  "campaign_id": 42,
  "page": 1,
  "per_page": 25,
  "total": 37,
  "recipients": [
    {
      "id": 901,
      "contact_id": 901,
      "email": "jane.doe@victimco.com",
      "full_name": "Jane Doe",
      "status": "clicked",
      "stage": "clicked",
      "training_status": "in_progress",
      "replied": false
    }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Odbiorcy zwróceni.
404	Kampania nie została znaleziona na kontach użytkownika lub wyszukiwanie `group_id` / `department` odwołuje się do rekordu spoza konta kampanii.

`GET /campaigns/:id/replies`

Zwraca stronicowaną listę przychodzących odpowiedzi, które odbiorcy odesłali na wiadomość phishingową, od najnowszych. Użyj go, aby uwidocznić zaangażowane cele i przejrzeć treść odpowiedzi. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).
page	query	integer	nie	Numer strony liczony od 1; przycinany do minimum 1. Domyślnie 1. Rozmiar strony jest ustalony na 25.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/campaigns/42/replies?page=1"
```

Odpowiedź `200 OK` — stronicowane odpowiedzi.

Pole	Typ	Opis
campaign_id	integer	Identyfikator kampanii.
page	integer	Bieżący numer strony.
per_page	integer	Rozmiar strony (zawsze 25).
total	integer	Łączna liczba odpowiedzi dla kampanii.
replies	array	Wiersze odpowiedzi (zobacz podpola).

Każdy wpis `replies[]`:

Pole	Typ	Opis
id	integer	Identyfikator odpowiedzi.
from_email	string	Adres e-mail nadawcy (odbiorcy).
received_at	string	Znacznik czasu ISO8601 momentu otrzymania odpowiedzi.

Pole	Typ	Opis
subject	string	Temat odpowiedzi.
excerpt	string	Tekstowy fragment treści odpowiedzi (skrócony).
attachments_count	integer	Liczba załączników w odpowiedzi.


```
{
  "campaign_id": 42,
  "page": 1,
  "per_page": 25,
  "total": 3,
  "replies": [
    {
      "id": 5501,
      "from_email": "jane.doe@victimco.com",
      "received_at": "2026-05-02T11:24:00Z",
      "subject": "Re: Your April invoice is ready",
      "excerpt": "Is this really from accounting? I don't recognize…",
      "attachments_count": 0
    }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Odpowiedzi zwrócone.
404	Kampania nie została znaleziona na kontach użytkownika.

`GET /campaigns/:id/timeline`

Zwraca chronologiczną oś czasu zdarzeń dla pojedynczego kontaktu w ramach kampanii (sent → opened → clicked → submitted → szkolenie itd.). Użyj go, aby zbadać pełną historię interakcji jednej ofiary. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator kampanii (`camp_…` lub liczba całkowita).
contact_id	query	integer	tak	Identyfikator kontaktu, którego oś czasu należy zwrócić. Musi należeć do konta kampanii.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/campaigns/42/timeline?contact_id=901"
```

Odpowiedź `200 OK` — lista zdarzeń kontaktu, uporządkowana od najstarszych.

Pole	Typ	Opis
campaign_id	integer	Identyfikator kampanii.
contact_id	integer	Identyfikator kontaktu.
events	array	Zdarzenia dla tego kontaktu (zobacz podpola).

Każdy wpis `events[]`:

Pole	Typ	Opis
genre	string	Typ zdarzenia: `sent`, `delivered`, `bounced`, `opened`, `clicked`, `submitted_data`, `started_training`, `completed_training`, `failed_quiz`, `passed_quiz` lub `replied`.
created_at	string	Znacznik czasu ISO8601 zdarzenia.
metadata	object | null	Dowolne metadane zdarzenia (np. user agent, IP, szczegóły quizu), w zapisanej postaci.

```
{
  "campaign_id": 42,
  "contact_id": 901,
  "events": [
    { "genre": "sent", "created_at": "2026-05-01T09:05:00Z", "metadata": {} },
    { "genre": "opened", "created_at": "2026-05-01T09:41:00Z", "metadata": { "ua":
        "Mozilla/5.0" } },
    { "genre": "clicked", "created_at": "2026-05-01T09:42:00Z", "metadata": { "ip":
        "203.0.113.7" } }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Oś czasu zwrócona.
404	Kampania nie została znaleziona na kontach użytkownika lub `contact_id` nie odwołuje się do kontaktu na koncie kampanii (brakujący/nieprawidłowy `contact_id` powoduje błąd nieznalezienia).

27.5 Szablony phishingowe

Biblioteka szablonów phishingowych to katalog gotowych scenariuszy phishingowych (e-mail + strona docelowa + akcja po kliknięciu), które konto może wdrożyć w rzeczywistej kampanii. Szablony występują w dwóch wariantach: **kuratorowane** (dostarczane przez platformę, współdzielone z każdym kontem, tylko do odczytu) oraz **niestandardowe** (utworzone przez konto, widoczne wyłącznie dla tego konta). Szablony są zorganizowane w drzewo kategorii (do trzech poziomów zagnieżdżenia). Wdrożenie szablonu tworzy nową roboczą kampanię wstępnie wypełnioną treścią szablonu — nigdy nie wysyła żadnego e-maila.

`GET /accounts/:account_id/phishing_templates`

Zwraca listę szablonów widocznych dla konta, stronicowaną po 12 na stronę. Użyj parametru `tab`, aby przełączać się między współdzieloną biblioteką kuratorowaną a własnymi szablonami niestandardowymi konta, oraz `category` / `search`, aby zawęzić wyniki. Zwraca tylko metadane (bez bloków HTML) — wywołaj punkt końcowy show, aby uzyskać pełną treść. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokenu.
tab	query	string	nie	Która biblioteka ma zostać wyświetlona. `custom` zwraca własne szablony tego konta; każda inna wartość (lub jej pominięcie) zwraca współdzieloną bibliotekę `curated`. Domyślnie: curated.
category	query	string lub tablica	nie	Jeden lub więcej identyfikatorów kategorii (identyfikatory z prefiksem `tcat_…` lub liczby całkowite) do filtrowania. Dopasowuje szablony przypisane do danej kategorii **lub dowolnego z jej potomków**. Wiele wartości przekaż jako powtórzone parametry `category[]`. Nierozpoznane identyfikatory są ignorowane.
search	query	string	nie	Dopasowanie podciągu (bez rozróżniania wielkości liter) względem `name` i `description` szablonu.
page	query	integer	nie	Numer strony liczony od 1. Wartości poniżej 1 są zaokrąglane do 1. Domyślnie: 1. Rozmiar strony jest ustalony na 12.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/phishing_templates?
        tab=curated&category=tcat_abc123&search=invoice&page=1"
```

Odpowiedź `200 OK` — koperta stronicowania plus tablica `templates` z metadanymi szablonów.

Pole	Typ	Opis
tab	string	Rozwiązana zakładka: `"curated"` lub `"custom"`.
page	integer	Bieżący numer strony.
per_page	integer	Rozmiar strony (zawsze 12).
total	integer	Łączna liczba szablonów pasujących do filtrów (na wszystkich stronach).
templates	array	Tablica obiektów szablonów (zobacz pola poniżej).
templates[].id	integer	Surowy numeryczny identyfikator szablonu.
templates[].name	string	Nazwa szablonu.
templates[].description	string | null	Opis w dowolnej formie tekstowej.
templates[].curated	boolean	`true` dla szablonów dostarczanych przez platformę, `false` dla należących do konta.
templates[].draft	boolean	`true`, jeśli szablon jest nieopublikowaną wersją roboczą (brak wymaganej treści). Wersji roboczych nie można wdrażać.
templates[].email_subject	string | null	Temat phishingowej wiadomości e-mail.
templates[].landing_page_enabled	boolean	Czy szablon zawiera hostowaną stronę docelową.
templates[].created_at	string (ISO 8601)	Znacznik czasu utworzenia.
templates[].updated_at	string (ISO 8601)	Znacznik czasu ostatniej aktualizacji.
templates[].template_id	string	Identyfikator z prefiksem (`tmpl_…`). Użyj go w ścieżkach show/deploy.
templates[].categories	array	Kategorie, do których przypisany jest ten szablon.
templates[].categories[].id	integer	Surowy numeryczny identyfikator kategorii.
templates[].categories[].category_id	string	Identyfikator kategorii z prefiksem (`tcat_…`).
templates[].categories[].name	string	Zlokalizowana nazwa kategorii (bieżąca lokalizacja żądania, z odwołaniem do angielskiego).

```
{
  "tab": "curated",
  "page": 1,
  "per_page": 12,
  "total": 37,
  "templates": [
    {
      "id": 84,
      "name": "Unpaid Invoice Reminder",
      "description": "Spoofed accounts-payable invoice with a credential-harvesting
        login page.",
      "curated": true,
      "draft": false,
      "email_subject": "Action required: invoice #44021 is overdue",
      "landing_page_enabled": true,
      "created_at": "2026-01-14T09:12:00.000Z",
      "updated_at": "2026-03-02T16:40:11.000Z",
      "template_id": "tmpl_8x2k9q",
      "categories": [
        { "id": 5, "category_id": "tcat_abc123", "name": "Finance" }
      ]
    }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Szablony wyświetlone (tablica może być pusta).
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu. Treść: `{"error":"Account not found"}`.

`GET /accounts/:account_id/phishing_template_categories`

Zwraca pełne drzewo kategorii (korzenie z zagnieżdżonymi elementami podrzędnymi, do trzech poziomów) na potrzeby interfejsu filtrowania biblioteki szablonów. Przydatne do zbudowania selektora kategorii przed wywołaniem listy szablonów z parametrem `category=`. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokenu.

(Kategorie są globalne, a nie ograniczone do konta — `account_id` jedynie kontroluje dostęp. Brak innych parametrów.)

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/phishing_template_categories
```

Odpowiedź `200 OK` — tablica `categories` kategorii głównych, z których każda rekurencyjnie osadza swoje elementy podrzędne.

Pole	Typ	Opis
categories	array	Kategorie główne, uporządkowane według `position`.
categories[].id	integer	Surowy numeryczny identyfikator kategorii.
categories[].category_id	string	Identyfikator kategorii z prefiksem (`tcat_…`).
categories[].name	string	Zlokalizowana nazwa kategorii (lokalizacja żądania, z odwołaniem do angielskiego).
categories[].slug	string	Slug bezpieczny dla adresów URL (unikalny, wyprowadzony z angielskiej nazwy).
categories[].depth	integer	Głębokość drzewa: `0` dla korzeni, `1` dla elementów podrzędnych, `2` dla wnuków.
categories[].is_leaf	boolean	`true`, gdy kategoria nie ma elementów podrzędnych.
categories[].children	array	Zagnieżdżone kategorie podrzędne o tym samym kształcie (pusta tablica dla liści).

```
{
  "categories": [
    {
      "id": 1,
      "category_id": "tcat_root01",
      "name": "Finance",
      "slug": "finance",
      "depth": 0,
      "is_leaf": false,
      "children": [
        {
          "id": 5,
          "category_id": "tcat_abc123",
          "name": "Invoices",
          "slug": "invoices",
          "depth": 1,
          "is_leaf": true,
          "children": []
        }
      ]
    }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Zwrócono drzewo kategorii (może być pustą tablicą).
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu. Treść: `{"error":"Account not found"}`.

`GET /phishing_templates/:id`

Zwraca pojedynczy szablon z jego **pełną treścią** — treścią wiadomości e-mail, kodem HTML/CSS strony docelowej oraz konfiguracją akcji po kliknięciu (akcji końcowej). Użyj tego, aby wyrenderować podgląd lub sprawdzić, co wdrożenie skopiuje do kampanii. Ta ścieżka jest płytka (bez `account_id` w ścieżce); użytkownik tokenu musi mieć możliwość zobaczenia szablonu (własne szablony niestandardowe oraz wszystkie kuratorowane). **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator szablonu (`tmpl_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/phishing_templates/tmpl_8x2k9q
```

Odpowiedź `200 OK` — pełny obiekt szablonu.

Pole	Typ	Opis
id	integer	Surowy numeryczny identyfikator szablonu.
name	string	Nazwa szablonu.
description	string | null	Opis w dowolnej formie tekstowej.
curated	boolean	`true` dla szablonów dostarczanych przez platformę, `false` dla należących do konta.
draft	boolean	`true`, jeśli nieopublikowany. Wersji roboczych nie można wdrażać.
email_subject	string | null	Temat phishingowej wiadomości e-mail (może zawierać merge tagi).
email_content	string | null	Pełna treść HTML phishingowej wiadomości e-mail.
landing_html	string | null	Kod HTML strony docelowej.

Pole	Typ	Opis
landing_css	string | null	Kod CSS strony docelowej.
landing_page_enabled	boolean	Czy dołączona jest hostowana strona docelowa.
end_action_type	string	Co dzieje się po przesłaniu strony docelowej przez ofiarę. Jedna z wartości `nothing`, `redirect_to_course`, `message_page`, `redirect_to_url`.
end_action_url	string | null	Docelowy adres URL, gdy `end_action_type` ma wartość `redirect_to_url` (musi być http/https).
end_action_html	string | null	Kod HTML wyświetlany, gdy `end_action_type` ma wartość `message_page` (np. strona uświadamiająca).
created_at	string (ISO 8601)	Znacznik czasu utworzenia.
updated_at	string (ISO 8601)	Znacznik czasu ostatniej aktualizacji.
template_id	string	Identyfikator z prefiksem (`tmpl_…`).
course_id	integer | null	Identyfikator powiązanego kursu e-learningowego (używany, gdy `end_action_type` ma wartość `redirect_to_course`).
publishable	boolean	`true`, gdy obecne są wszystkie wymagane pola (nazwa, temat, treść e-maila, HTML strony docelowej).
categories	array	Przypisane kategorie: każda z `id` (liczba całkowita), `category_id` (`tcat_…`) oraz `name`.

```
{
  "id": 84,
  "name": "Unpaid Invoice Reminder",
  "description": "Spoofed accounts-payable invoice with a credential-harvesting login
      page.",
  "curated": true,
  "draft": false,
  "email_subject": "Action required: invoice #44021 is overdue",
  "email_content": "<html><body><p>Dear {{first_name}}, your invoice is overdue…</p></
      body></html>",
  "landing_html": "<form action=\"#\">…</form>",
  "landing_css": "body { font-family: sans-serif; }",
  "landing_page_enabled": true,
  "end_action_type": "message_page",
  "end_action_url": null,
  "end_action_html": "<h1>You've been phished by a simulation.</h1>",
  "created_at": "2026-01-14T09:12:00.000Z",
  "updated_at": "2026-03-02T16:40:11.000Z",
  "template_id": "tmpl_8x2k9q",
  "course_id": null,
  "publishable": true,
  "categories": [
    { "id": 5, "category_id": "tcat_abc123", "name": "Finance" }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Zwrócono szablon.
403	Szablon nie jest widoczny dla użytkownika tokenu (niestandardowy szablon innego konta). Treść: `{"error":"You are not authorized to perform this action"}`.
404	Żaden szablon nie pasuje do `id`. Treść: `{"error":"Resource not found"}`.

`POST /phishing_templates/:id/deploy`

Tworzy nową **roboczą kampanię** na koncie docelowym, wstępnie wypełnioną treścią szablonu (temat/treść e-maila, HTML/CSS strony docelowej, akcja końcowa, kurs). Ta ścieżka jest płytka, więc wdrażające konto jest przekazywane w treści żądania jako `account_id`. Przy `quick_launch=true` dodatkowo dodaje **wszystkich** odbiorców z kontaktów konta jako odbiorców i przenosi kampanię do kroku przeglądu. **Ten punkt końcowy nigdy nie wysyła żadnego e-maila** — kampanię uruchamia człowiek z interfejsu PhishSpot. Wersji roboczych nie można wdrażać. **Uwierzytelnianie:** Bearer; **rola:** dowolny członek konta docelowego.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator szablonu do wdrożenia (`tmpl_…` lub liczba całkowita). Nie może być szablonem roboczym.
account_id	body	string	tak	Konto, na którym ma zostać utworzona kampania (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokenu.
quick_launch	body	boolean	nie	Gdy wartość jest prawdziwa (`true` , `"1"` itp.), masowo dodaje każdy kontakt konta jako odbiorcę i oznacza kroki kreatora 1–5 jako ukończone, dzięki czemu kampania trafia do kroku przeglądu. Wymaga aktywnej domeny wysyłkowej i co najmniej jednego kontaktu. Domyślnie: `false` .

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "account_id": "acct_4f8a2c", "quick_launch": true }' \
  https://platform.phishspot.com/api/v1/phishing_templates/tmpl_8x2k9q/deploy
```

Odpowiedź `201 Created` — nowo utworzona kampania (taki sam kształt jak punkt końcowy show kampanii). Świeżo wdrożona kampania jest w stanie `draft` , więc blok `statistics` jest pomijany (pojawia się dopiero, gdy kampania jest w toku, wstrzymana lub zakończona).

Pole	Typ	Opis
id	integer	Surowy numeryczny identyfikator kampanii.
account_id	integer	Identyfikator konta będącego właścicielem.
name	string	Automatycznie wygenerowana nazwa: `"<Template name> – YYYY-MM-DD HH:MM:SS"` (z numerycznym sufiksem w razie kolizji).
state	string	Stan cyklu życia — `draft` natychmiast po wdrożeniu. Jedna z wartości `draft` , `in_progress` , `paused` , `cancelled` , `done` , `scheduled` .
delivery_mode	string | null	`immediate` , `scheduled` lub `staggered` (nie ustawiane przy wdrożeniu).
delivery_schedule	object | null	Konfiguracja harmonogramu dostarczania (nie ustawiana przy wdrożeniu).
created_at	string (ISO 8601)	Znacznik czasu utworzenia.
updated_at	string (ISO 8601)	Znacznik czasu ostatniej aktualizacji.
email_subject	string | null	Skopiowane z szablonu.

Pole	Typ	Opis
email_content	string | null	Skopiowane z szablonu.
landing_html	string | null	Skopiowane z szablonu.
domain	string | null	Nazwa domeny platformy wysyłkowej/docelowej (automatycznie wybrana spośród dostępnych domen konta, może być null).
course_id	integer | null	Identyfikator powiązanego kursu (kurs szablonu lub domyślny kurs konta).
groups	array	Grupy kontaktów w kampanii — puste tuż po wdrożeniu. Każda: `id`, `name`.
can_start	boolean	Czy kampania może przejść do uruchomienia.
can_pause	boolean	Czy kampania może zostać wstrzymana.
can_cancel	boolean	Czy kampania może zostać anulowana.


```
{
  "id": 512,
  "account_id": 11,
  "name": "Unpaid Invoice Reminder – 2026-06-02 14:30:07",
  "state": "draft",
  "delivery_mode": null,
  "delivery_schedule": null,
  "created_at": "2026-06-02T14:30:07.000Z",
  "updated_at": "2026-06-02T14:30:07.000Z",
  "email_subject": "Action required: invoice #44021 is overdue",
  "email_content": "<html><body><p>Dear {{first_name}}…</p></body></html>",
  "landing_html": "<form action=\"#\">…</form>",
  "domain": "officelogin.in",
  "course_id": null,
  "groups": [],
  "can_start": false,
  "can_pause": false,
  "can_cancel": false
}
```


Kody statusu

Kod	Kiedy
201	Kampania utworzona z szablonu.
403	Szablon jest wersją roboczą (wersji roboczych nie można wdrażać) lub nie jest widoczny dla użytkownika tokenu. Treść: `{"error":"You are not authorized to perform this action"}`.

Kod	Kiedy
404	Żaden szablon nie pasuje do `id`, **lub** `account_id` w treści żądania nie jest kontem, do którego należy użytkownik tokenu. Treść: `{"error":"Resource not found"}` (szablon) / `{"error":"Account not found"}` (konto).
422	`quick_launch=true`, ale konto nie ma aktywnej domeny wysyłkowej (`"Quick launch needs an active sending domain for this account."`) lub nie ma kontaktów (`"Quick launch needs at least one contact in the account."`). Treść: `{"error":"<message>"}`.

27.6 Odbiorcy i grupy

Odbiorcy to pracownicy, których obierasz za cel symulacji phishingowych; grupy to nazwane zbiory służące do zawężania kampanii. Oba zasoby są ograniczone do konta: akcje kolekcji są zagnieżdżone pod `/accounts/:account_id/…`, natomiast odczyty/zapisy na pojedynczym rekordzie korzystają z płytkich ścieżek `/contacts/:id` i `/groups/:id`. Członkostwo w koncie jest wymagane dla każdego punktu końcowego — wszystkie sprawdzenia uprawnień przechodzą dla dowolnego członka konta (zarówno odczyt, jak i zapis), więc nie ma tu rozróżnienia admin/edytor. Jedynym ograniczeniem zapisu jest to, że grupa biorąca udział w aktywnej kampanii (`in_progress` lub `paused`) jest **zablokowana** i nie można jej zaktualizować, usunąć ani zmienić jej członkostwa.

`GET /accounts/:account_id/contacts`

Zwraca listę wszystkich odbiorców w koncie, posortowanych według nazwiska, a następnie imienia, z grupami każdego odbiorcy umieszczonymi w treści. Użyj go do stronicowania lub synchronizacji listy. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/contacts
```

Odpowiedź `200 OK` — tablica JSON obiektów odbiorców (zobacz pola odbiorcy poniżej).

Pole	Typ	Opis
id	integer	Klucz główny odbiorcy.

Pole	Typ	Opis
account_id	integer	Identyfikator konta będącego właścicielem.
first_name	string	Imię.
last_name	string|null	Nazwisko.
email	string	Adres e-mail (unikalny w obrębie konta).
telephone	string|null	Numer telefonu.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
full_name	string	Wygodne: `"first_name last_name"` po przycięciu.
groups	array	Grupy, do których należy ten odbiorca; każda `{ id, name }`.
groups[].id	integer	Identyfikator grupy.
groups[].name	string	Nazwa grupy (znormalizowana, snake_case dla grup ręcznych).


```
[
  {
    "id": 501,
    "account_id": 11,
    "first_name": "Ada",
    "last_name": "Kowalska",
    "email": "ada.kowalska@example.com",
    "telephone": "+48 600 123 456",
    "created_at": "2026-05-01T09:30:00.000Z",
    "updated_at": "2026-05-12T14:02:11.000Z",
    "full_name": "Ada Kowalska",
    "groups": [
      { "id": 90, "name": "finance" }
    ]
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono odbiorców (być może pustą tablicę).
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.

`POST /accounts/:account_id/contacts`

Tworzy pojedynczego odbiorcę w koncie. Do masowego ładowania użyj zamiast tego punktu końcowego importu. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Parametry treści żądania są opakowane w obiekt `contact`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
first_name	body	string	tak	Imię (maks. 255). Wymagane przez model.
email	body	string	tak	Adres e-mail. Musi odpowiadać standardowemu formatowi e-mail i być unikalny w obrębie konta (bez rozróżniania wielkości liter). Maks. 255.
last_name	body	string	nie	Nazwisko (maks. 255).
telephone	body	string	nie	Numer telefonu (maks. 50). Musi odpowiadać formatom typu `+CC (NNN) NNN-NNNN`; dozwolona wartość pusta.
group_ids	body	array	nie	Tablica identyfikatorów grup, do których odbiorca ma zostać dołączony przy tworzeniu.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "contact": { "first_name": "Ada", "last_name": "Kowalska", "email":
        "ada.kowalska@example.com", "telephone": "+48 600 123 456", "group_ids":
        [90] } }' \
  https://platform.phishspot.com/api/v1/accounts/11/contacts
```

Odpowiedź `201 Created` — utworzony odbiorca, z tymi samymi polami co punkt końcowy listy powyżej.

```
{
  "id": 501,
  "account_id": 11,
  "first_name": "Ada",
  "last_name": "Kowalska",
  "email": "ada.kowalska@example.com",
  "telephone": "+48 600 123 456",
  "created_at": "2026-05-01T09:30:00.000Z",
  "updated_at": "2026-05-01T09:30:00.000Z",
  "full_name": "Ada Kowalska",
  "groups": [
    { "id": 90, "name": "finance" }
  ]
}
```


Kody statusu

Kod	Kiedy
201	Odbiorca utworzony.
400	W treści brakuje klucza najwyższego poziomu `contact`.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.
422	Walidacja nie powiodła się (np. brak `first_name`, brakujący/nieprawidłowy `email` lub zduplikowany adres e-mail w obrębie konta). Treść to `{ "errors": { … } }`.

`POST /accounts/:account_id/contacts/import`

Masowo importuje odbiorców do konta z pliku CSV. Istniejący odbiorcy (dopasowani po adresie e-mail) są aktualizowani niepustymi wartościami; nowi są tworzeni; grupy nazwane w danych są tworzone, a powiązania są ustanawiane. Podaj **albo** surowy tekst CSV w `csv`, **albo** tablicę JSON w `contacts` — tablica jest konwertowana na CSV po stronie serwera przy użyciu kanonicznej kolejności nagłówków. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Kanoniczna kolejność nagłówków CSV to: `first_name`, `last_name`, `email`, `telephone`, `groups`, `department`, `title`, `location`. W kolumnie `groups` wiele grup rozdziela się znakiem `|` (pionowa kreska). Przy korzystaniu z formy JSON `contacts` pole `groups` każdego wiersza może być tablicą (np. `["finance","exec"]`), która jest automatycznie łączona znakiem `|`.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Nazwa	Gdzie	Typ	Wymagane	Opis
csv	body	string	warunkowo	Surowy tekst CSV z kanonicznym wierszem nagłówka. Wymagane, jeśli pominięto `contacts`. Ma pierwszeństwo, jeśli podano oba.
contacts	body	array	warunkowo	Tablica obiektów wierszy z kluczami zgodnymi z kanonicznymi nagłówkami. Wymagane, jeśli pominięto `csv`. Pole `groups` każdego wiersza może być ciągiem znaków lub tablicą nazw grup.

> Musisz podać dokładnie jedno z `csv` lub `contacts`. Jeśli oba są puste/nieobecne, żądanie kończy się niepowodzeniem z kodem `422`.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "contacts": [
        { "first_name": "Ada", "last_name": "Kowalska", "email":
        "ada.kowalska@example.com", "telephone": "+48600123456", "groups": ["finance"],
        "department": "Finance", "title": "Analyst", "location": "Warsaw" },
        { "first_name": "Jan", "email": "jan.nowak@example.com", "groups": ["finance",
        "exec"] }
      ] }' \
  https://platform.phishspot.com/api/v1/accounts/11/contacts/import
```

Odpowiedź `200 OK` — podsumowanie sposobu przetworzenia wierszy.

Pole	Typ	Opis
created	integer	Liczba wstawionych nowych odbiorców.
updated	integer	Liczba istniejących odbiorców (dopasowanych po adresie e-mail) zaktualizowanych nowymi niepustymi wartościami.
failed	integer	Liczba wierszy odrzuconych jako nieprawidłowe. (Do konta dołączany jest możliwy do pobrania raport CSV z nieudanymi wierszami.)

```
{
  "created": 1,
  "updated": 1,
  "failed": 0
}
```

Kody statusu

Kod	Kiedy
200	Import wykonany; zwraca podsumowanie `{created, updated, failed}`.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.
422	Nie podano ani `csv`, ani `contacts`. Treść to `{ "error": "Provide either csv or contacts." }`.

`GET /contacts/:id`

Pobiera pojedynczego odbiorcę po identyfikatorze, ograniczonego do kont użytkownika tokenu. Użyj go do odczytania jednego odbiorcy bez wyświetlania całego konta. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator odbiorcy (`cont_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i identyfikatorem ścieżki.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/contacts/cont_abc123
```

Odpowiedź `200 OK` — odbiorca, z tymi samymi polami co punkt końcowy listy.

```
{
  "id": 501,
  "account_id": 11,
  "first_name": "Ada",
  "last_name": "Kowalska",
  "email": "ada.kowalska@example.com",
  "telephone": "+48 600 123 456",
  "created_at": "2026-05-01T09:30:00.000Z",
  "updated_at": "2026-05-12T14:02:11.000Z",
  "full_name": "Ada Kowalska",
  "groups": [
    { "id": 90, "name": "finance" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Odbiorca znaleziony.
404	Brak odbiorcy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

`PATCH /contacts/:id`

Aktualizuje pojedynczego odbiorcę. Wyślij tylko te pola, które chcesz zmienić, opakowane w obiekt `contact`. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Parametry treści żądania są opakowane w obiekt `contact`.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator odbiorcy (`cont_…` lub liczba całkowita).
first_name	body	string	nie	Imię (maks. 255). Nie można wyczyścić do wartości pustej — jest wymagane.
last_name	body	string	nie	Nazwisko (maks. 255).
email	body	string	nie	Adres e-mail. Musi pozostać prawidłowy i unikalny w obrębie konta (bez rozróżniania wielkości liter). Maks. 255.
telephone	body	string	nie	Numer telefonu (maks. 50, walidowany formatowo; dozwolona wartość pusta).
group_ids	body	array	nie	Zastępuje członkostwo grupowe odbiorcy dokładnie tym zestawem identyfikatorów grup.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "contact": { "title": "Senior Analyst", "group_ids": [90, 91] } }' \
  https://platform.phishspot.com/api/v1/contacts/cont_abc123
```

> `title`, `department` i `location` istnieją w modelu, ale **nie** znajdują się wśród dozwolonych parametrów API, więc są ignorowane przy tworzeniu/aktualizacji za pośrednictwem tego punktu końcowego — ustaw je zamiast tego przez import CSV. Powyższy przykład pokazuje `group_ids`, które jest honorowane; `title` zostałoby po cichu odrzucone.

Odpowiedź `200 OK` — zaktualizowany odbiorca, z tymi samymi polami co punkt końcowy listy.

```
{
  "id": 501,
  "account_id": 11,
  "first_name": "Ada",
  "last_name": "Kowalska",
  "email": "ada.kowalska@example.com",
  "telephone": "+48 600 123 456",
  "created_at": "2026-05-01T09:30:00.000Z",
  "updated_at": "2026-05-20T08:15:00.000Z",
  "full_name": "Ada Kowalska",
  "groups": [
    { "id": 90, "name": "finance" },
    { "id": 91, "name": "exec" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Odbiorca zaktualizowany.
400	W treści brakuje klucza najwyższego poziomu `contact`.
404	Brak odbiorcy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.
422	Walidacja nie powiodła się (pusty `first_name`, nieprawidłowy/zduplikowany `email`, błędny format `telephone`). Treść to `{ "errors": { … } }`.

`DELETE /contacts/:id`

Trwale usuwa odbiorcę oraz jego członkostwa w grupach, dostarczalne elementy, zdarzenia i wyniki. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator odbiorcy (`cont_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i identyfikatorem ścieżki.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/contacts/cont_abc123
```

Odpowiedź `204 No Content` — pusta treść.

Kody statusu

Kod	Kiedy
204	Odbiorca usunięty.
404	Brak odbiorcy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

`GET /accounts/:account_id/groups`

Zwraca listę wszystkich grup w koncie, posortowanych według nazwy, z odbiorcami każdej grupy umieszczonymi w treści. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Odpowiedź `200 OK` — tablica JSON obiektów grup (zobacz pola grupy poniżej).

Pole	Typ	Opis
id	integer	Klucz główny grupy.
account_id	integer	Identyfikator konta będącego właścicielem.
name	string	Nazwa grupy. Dla grup ręcznych jest ona normalizowana do snake_case (spacje → podkreślenia, znaki niealfanumeryczne usuwane, małe litery).
contact_count	integer	Zbuforowana liczba odbiorców w grupie.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
contacts	array	Członkowie grupy.
contacts[].id	integer	Identyfikator odbiorcy.
contacts[].email	string	Adres e-mail odbiorcy.
contacts[].first_name	string	Imię odbiorcy.
contacts[].last_name	string|null	Nazwisko odbiorcy.
contacts[].full_name	string	`"first_name last_name"` po przycięciu.

```
[
  {
    "id": 90,
    "account_id": 11,
    "name": "finance",
    "contact_count": 2,
    "created_at": "2026-04-10T11:00:00.000Z",
    "updated_at": "2026-05-20T08:15:00.000Z",
    "contacts": [
      { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada",
        "last_name": "Kowalska", "full_name": "Ada Kowalska" }
    ]
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono grupy (być może pustą tablicę).
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.

`POST /accounts/:account_id/groups`

Tworzy grupę w koncie. Nazwy grup ręcznych są normalizowane do snake_case po stronie serwera. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Parametry treści żądania są opakowane w obiekt `group`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
name	body	string	tak	Nazwa grupy (maks. 255). Normalizowana do snake_case; musi być unikalna w obrębie konta (bez rozróżniania wielkości liter, porównywana po normalizacji).
description	body	string	nie	Dowolny opis tekstowy. Dozwolony przez kontroler (model nie ma kolumny `description`, więc jest akceptowany, ale nieutrwalany/ niezwracany).
contact_ids	body	array	nie	Tablica identyfikatorów odbiorców do dodania jako członkowie przy tworzeniu.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "group": { "name": "Finance Team", "contact_ids": [501, 502] } }' \
  https://platform.phishspot.com/api/v1/accounts/11/groups
```

Odpowiedź `201 Created` — utworzona grupa, z tymi samymi polami co punkt końcowy listy powyżej. Zwróć uwagę, że `"Finance Team"` jest zapisywane i zwracane jako `"finance_team"`.

```
{
  "id": 90,
  "account_id": 11,
  "name": "finance_team",
  "contact_count": 2,
  "created_at": "2026-04-10T11:00:00.000Z",
  "updated_at": "2026-04-10T11:00:00.000Z",
  "contacts": [
    { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada", "last_name":
        "Kowalska", "full_name": "Ada Kowalska" },
    { "id": 502, "email": "jan.nowak@example.com", "first_name": "Jan", "last_name":
        "Nowak", "full_name": "Jan Nowak" }
  ]
}
```

Kody statusu

Kod	Kiedy
201	Grupa utworzona.
400	W treści brakuje klucza najwyższego poziomu `group`.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu.
422	Walidacja nie powiodła się (pusta `name` lub nazwa, która po normalizacji jest duplikatem w obrębie konta). Treść to `{ "errors": { … } }`.

`GET /groups/:id`

Pobiera pojedynczą grupę po identyfikatorze, ograniczoną do kont użytkownika tokenu.
Uwierzytelnianie: Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator grupy (`grp_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i identyfikatorem ścieżki.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/groups/grp_xyz789
```

Odpowiedź `200 OK` — grupa, z tymi samymi polami co punkt końcowy listy.

```
{
  "id": 90,
  "account_id": 11,
  "name": "finance",
  "contact_count": 1,
  "created_at": "2026-04-10T11:00:00.000Z",
  "updated_at": "2026-05-20T08:15:00.000Z",
  "contacts": [
    { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada", "last_name":
        "Kowalska", "full_name": "Ada Kowalska" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Grupa znaleziona.
404	Brak grupy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

`PATCH /groups/:id`

Aktualizuje nazwę grupy (i opcjonalnie zastępuje jej członkostwo). Zablokowane, jeśli grupa jest zablokowana przez aktywną kampanię. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Parametry treści żądania są opakowane w obiekt `group`.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator grupy (`grp_…` lub liczba całkowita).
name	body	string	nie	Nowa nazwa grupy (maks. 255). Normalizowana do snake_case; musi pozostać unikalna w obrębie konta.
description	body	string	nie	Akceptowana, ale nieutrwalana (brak kolumny w modelu).
contact_ids	body	array	nie	Zastępuje członkostwo grupy dokładnie tym zestawem identyfikatorów odbiorców.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "group": { "name": "Finance and Ops", "contact_ids": [501, 503] } }' \
  https://platform.phishspot.com/api/v1/groups/grp_xyz789
```

Odpowiedź `200 OK` — zaktualizowana grupa, z tymi samymi polami co punkt końcowy listy.

```
{
  "id": 90,
  "account_id": 11,
  "name": "finance_and_ops",
  "contact_count": 2,
  "created_at": "2026-04-10T11:00:00.000Z",
  "updated_at": "2026-05-21T10:00:00.000Z",
  "contacts": [
    { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada", "last_name":
        "Kowalska", "full_name": "Ada Kowalska" },
    { "id": 503, "email": "ola.wisniewska@example.com", "first_name": "Ola",
        "last_name": "Wisniewska", "full_name": "Ola Wisniewska" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Grupa zaktualizowana.
400	W treści brakuje klucza najwyższego poziomu `group`.
403	Grupa jest zablokowana (używana w kampanii `in_progress` / `paused`), więc nie można jej zmodyfikować.
404	Brak grupy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.
422	Walidacja nie powiodła się (pusta `name` lub nazwa, która po normalizacji jest duplikatem). Treść to `{ "errors": { … } }`.

`DELETE /groups/:id`

Trwale usuwa grupę oraz jej powiązania odbiorca-grupa / kampania-grupa (sami odbiorcy nie są usuwani). Zablokowane, jeśli grupa jest zablokowana przez aktywną kampanię. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator grupy (`grp_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i identyfikatorem ścieżki.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/groups/grp_xyz789
```

Odpowiedź `204 No Content` — pusta treść.

Kody statusu

Kod	Kiedy
204	Grupa usunięta.
403	Grupa jest zablokowana (używana w kampanii `in_progress` / `paused`), więc nie można jej usunąć.
404	Brak grupy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

`POST /groups/:id/add_contacts`

Dodaje jednego lub więcej odbiorców do grupy. Identyfikatory odbiorców są rozwiązywane względem własnego konta grupy — identyfikatory należące do innego konta lub nieistniejące są po cichu odrzucane. Odbiorcy już znajdujący się w grupie są pomijani. Zablokowane, jeśli grupa jest zablokowana. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator grupy (`grp_…` lub liczba całkowita).
contact_ids	body	array	tak	Identyfikatory odbiorców (`cont_…` lub liczby całkowite) do dodania. Identyfikatory spoza konta grupy lub nieistniejące są ignorowane.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "contact_ids": [501, "cont_def456"] }' \
  https://platform.phishspot.com/api/v1/groups/grp_xyz789/add_contacts
```

Odpowiedź `200 OK` — zaktualizowana grupa (po przeładowaniu), z tymi samymi polami co punkt końcowy listy. Odpowiedź nie zawiera osobnej liczby dodanych elementów; porównaj `contact_count` / `contacts` przed i po.


```
{
  "id": 90,
  "account_id": 11,
  "name": "finance",
  "contact_count": 2,
  "created_at": "2026-04-10T11:00:00.000Z",
  "updated_at": "2026-05-22T09:00:00.000Z",
  "contacts": [
    { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada", "last_name":
        "Kowalska", "full_name": "Ada Kowalska" },
    { "id": 540, "email": "marek.zielinski@example.com", "first_name": "Marek",
        "last_name": "Zielinski", "full_name": "Marek Zielinski" }
  ]
}
```


Kody statusu

Kod	Kiedy
200	Zwraca zaktualizowaną grupę (nawet jeśli każdy podany identyfikator został odrzucony/już był obecny — po prostu nic się nie zmieni).
403	Grupa jest zablokowana (używana w kampanii `in_progress` / `paused`).
404	Brak grupy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

`DELETE /groups/:id/remove_contacts`

Usuwa jednego lub więcej odbiorców z grupy. Identyfikatory odbiorców są rozwiązywane względem konta grupy; identyfikatory spoza grupy (lub spoza konta) są ignorowane. Zablokowane, jeśli grupa jest zablokowana. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator grupy (`grp_…` lub liczba całkowita).
contact_ids	body	array	tak	Identyfikatory odbiorców (`cont_…` lub liczby całkowite) do usunięcia z grupy.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "contact_ids": [540] }' \
  https://platform.phishspot.com/api/v1/groups/grp_xyz789/remove_contacts
```

Odpowiedź `200 OK` — zaktualizowana grupa (po przeładowaniu), z tymi samymi polami co punkt końcowy listy.

```
{
  "id": 90,
  "account_id": 11,
  "name": "finance",
  "contact_count": 1,
  "created_at": "2026-04-10T11:00:00.000Z",
  "updated_at": "2026-05-22T09:10:00.000Z",
  "contacts": [
    { "id": 501, "email": "ada.kowalska@example.com", "first_name": "Ada", "last_name":
        "Kowalska", "full_name": "Ada Kowalska" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Zwraca zaktualizowaną grupę (identyfikatory spoza grupy są po prostu ignorowane).
403	Grupa jest zablokowana (używana w kampanii `in_progress` / `paused`).
404	Brak grupy o tym identyfikatorze w jakimkolwiek koncie, do którego należy użytkownik tokenu.

27.7 Dostarczenia, zdarzenia i wyniki

Te trzy zasoby rejestrują telemetrię kampanii per odbiorca. **Dostarczenie** (deliverable) to powiązanie kampanii z kontaktem (jeden wiersz na odbiorcę) i śledzi jego pozycję w lejku zaangażowania poprzez `state`. **Zdarzenie** (event) to w zasadzie niezmienny wpis na osi czasu (sent, opened, clicked, …) identyfikowany przez `genre`. **Wynik** (result) przechowuje odpowiedź/punktację kontaktu dla pojedynczego bloku `block` szkolenia e-learning.

Wszystkie punkty końcowe w tej sekcji autoryzują za pomocą polityki Pundit danego zasobu, która zezwala **każdemu członkowi zespołu** (każdej roli) na odczyt, tworzenie, aktualizację i usuwanie. Nie ma bramki admin/edytor. Listowanie i tworzenie są zagnieżdżone w koncie (`/accounts/:account_id/…`); show/update/destroy są płytkie (`/deliverables/:id` itd.) i ograniczone do kont, do których należy użytkownik tokena — żądanie rekordu spoza tych kont zwraca `404`, nigdy danych innego najemcy.

`GET /api/v1/accounts/:account_id/deliverables`

Listuje wszystkie dostarczenia dla konta, od najnowszych, opcjonalnie ograniczone do jednej kampanii. Użyj go, aby pobrać listę odbiorców i stan lejka kampanii. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
campaign_id	query	string	nie	Ograniczenie do jednej kampanii (`camp_…` lub liczba całkowita). Po pominięciu zwracane są wszystkie dostarczenia dla konta.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/deliverables?campaign_id=42"
```

Odpowiedź `200 OK` — tablica JSON obiektów dostarczenia.

Pole	Typ	Opis
id	integer	Identyfikator dostarczenia.
campaign_id	integer	Kampania będąca właścicielem.
contact_id	integer	Kontakt będący celem.
state	string	Stan lejka (zobacz enum poniżej).
user_agent	string | null	User-agent przechwycony przy otwarciu/kliknięciu, jeśli istnieje.
ip_address	string | null	Adres IP przechwycony przy otwarciu/kliknięciu, jeśli istnieje.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
campaign	object | null	Obecne, gdy kampania się załaduje: `{ id, name, account_id }`.
contact	object | null	Obecne, gdy kontakt się załaduje: `{ id, email, first_name, last_name, full_name }`.
events	array	Obecne tylko wtedy, gdy kontakt ma zdarzenia w tej kampanii; każdy element to `{ id, genre, created_at }`.

`state` przyjmuje jedną z wartości: `pending` (jeszcze niewysłane), `sent`, `delivered`, `bounced`, `opened`, `clicked`, `submitted` (dane wprowadzone na stronie docelowej), `educated` (ukończono szkolenie).


```
[
  {
    "id": 5012,
    "campaign_id": 42,
    "contact_id": 880,
    "state": "clicked",
    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)",
    "ip_address": "203.0.113.7",
    "created_at": "2026-05-30T09:12:44.000Z",
    "updated_at": "2026-05-30T10:01:08.000Z",
    "campaign": { "id": 42, "name": "Q2 Invoice Lure", "account_id": 11 },
    "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
        "last_name": "Kowalski", "full_name": "Jan Kowalski" },
    "events": [
      { "id": 9001, "genre": "sent", "created_at": "2026-05-30T09:12:44.000Z" },
      { "id": 9044, "genre": "opened", "created_at": "2026-05-30T09:58:21.000Z" },
      { "id": 9051, "genre": "clicked", "created_at": "2026-05-30T10:01:08.000Z" }
    ]
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono dostarczenia.
403	Użytkownik tokena nie jest uprawniony do wyświetlenia konta (`account.show?` odmówiono).
404	`account_id` nie należy do użytkownika tokena.

`POST /api/v1/accounts/:account_id/deliverables`

Tworzy dostarczenie, łącząc kontakt z kampanią. `account_id` jest pobierane automatycznie z kampanii (podany segment ścieżki `account_id` wybiera kontekst konta). **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Wszystkie parametry treści żądania są opakowane w obiekt `deliverable`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Nazwa	Gdzie	Typ	Wymagane	Opis
deliverable.campaign_id	body	integer	tak	Kampania, do której ma zostać dołączone. Walidowane `presence`.
deliverable.contact_id	body	integer	tak	Kontakt będący celem. Walidowane `presence`.
deliverable.state	body	string	nie	Stan lejka; domyślnie `pending`. Jedna z wartości enuma `state`. Walidowane `presence`.
deliverable.name	body	string	nie	Akceptowane przez strong params, ale niezapisywane (brak kolumny `name`).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "deliverable": { "campaign_id": 42, "contact_id": 880, "state": "pending" } }' \
  https://platform.phishspot.com/api/v1/accounts/11/deliverables
```

Odpowiedź `201 Created` — utworzone dostarczenie (taki sam kształt jak obiekt show/index powyżej).

```
{
  "id": 5099,
  "campaign_id": 42,
  "contact_id": 880,
  "state": "pending",
  "user_agent": null,
  "ip_address": null,
  "created_at": "2026-06-02T08:00:00.000Z",
  "updated_at": "2026-06-02T08:00:00.000Z",
  "campaign": { "id": 42, "name": "Q2 Invoice Lure", "account_id": 11 },
  "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
       "last_name": "Kowalski", "full_name": "Jan Kowalski" }
}
```

Kody statusu

Kod	Kiedy
201	Utworzono dostarczenie.
404	`account_id` nie należy do użytkownika tokena.
422	Walidacja nie powiodła się (brak `campaign_id` / `contact_id` / `state` lub nieprawidłowa wartość `state`). Treść: `{ "errors": { … } }`.

`GET /api/v1/deliverables/:id`

Pobiera pojedyncze dostarczenie wraz z jego kampanią, kontaktem i osią czasu zdarzeń. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator dostarczenia (`delv_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/deliverables/5012
```

Odpowiedź `200 OK` — pojedynczy obiekt dostarczenia (te same pola co element listy powyżej).

```
{
  "id": 5012,
  "campaign_id": 42,
  "contact_id": 880,
  "state": "clicked",
  "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)",
  "ip_address": "203.0.113.7",
  "created_at": "2026-05-30T09:12:44.000Z",
  "updated_at": "2026-05-30T10:01:08.000Z",
  "campaign": { "id": 42, "name": "Q2 Invoice Lure", "account_id": 11 },
  "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
       "last_name": "Kowalski", "full_name": "Jan Kowalski" },
  "events": [
    { "id": 9001, "genre": "sent", "created_at": "2026-05-30T09:12:44.000Z" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Zwrócono dostarczenie.
404	Brak dostarczenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena.

`PATCH /api/v1/deliverables/:id`

Aktualizuje dostarczenie — zazwyczaj w celu przesunięcia jego `state` lub ponownego powiązania kampanii/kontaktu. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Parametry treści żądania są opakowane w obiekt `deliverable`; wyślij tylko te pola, które chcesz zmienić.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator dostarczenia (`delv_…` lub liczba całkowita).
deliverable.state	body	string	nie	Nowy stan lejka (jedna z wartości enuma `state`).
deliverable.campaign_id	body	integer	nie	Zmiana przypisania kampanii (`presence` nadal wymuszane — nie można wyczyścić).
deliverable.contact_id	body	integer	nie	Zmiana przypisania kontaktu (`presence` nadal wymuszane).
deliverable.name	body	string	nie	Akceptowane, ale niezapisywane (brak kolumny).

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "deliverable": { "state": "submitted" } }' \
  https://platform.phishspot.com/api/v1/deliverables/5012
```

Odpowiedź `200 OK` — zaktualizowany obiekt dostarczenia (taki sam kształt jak show).

Kody statusu

Kod	Kiedy
200	Zaktualizowano dostarczenie.
404	Brak dostarczenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena.
422	Walidacja nie powiodła się (np. nieprawidłowy `state` lub wyczyszczony `campaign_id` / `contact_id`). Treść: `{ "errors": { … } }`.

`DELETE /api/v1/deliverables/:id`

Trwale usuwa dostarczenie (oraz zależne `campaign_replies`). **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/deliverables/5012
```

Odpowiedź `204 No Content` — pusta treść po sukcesie.

Kody statusu

Kod	Kiedy
204	Usunięto dostarczenie.
404	Brak dostarczenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena.

`GET /api/v1/accounts/:account_id/events`

Listuje zdarzenia konta od najnowszych, z opcjonalnym filtrowaniem według kampanii, kontaktu i rodzaju (genre). Użyj go, aby zrekonstruować oś czasu zaangażowania. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
campaign_id	query	string	nie	Ograniczenie do jednej kampanii (`camp_…` lub liczba całkowita).
contact_id	query	string	nie	Ograniczenie do jednego kontaktu (`cont_…` lub liczba całkowita).
genre	query	string	nie	Ograniczenie do jednego rodzaju (zobacz enum poniżej).

`genre` przyjmuje jedną z wartości: `sent`, `delivered`, `bounced`, `opened`, `clicked`, `submitted_data` (dane przesłane na stronie docelowej), `started_training`, `completed_training`, `failed_quiz`, `passed_quiz`, `replied` (odbiorca odpowiedział na e-mail phishingowy).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/events?
        campaign_id=42&genre=clicked"
```

Odpowiedź `200 OK` — tablica JSON obiektów zdarzeń.

Pole	Typ	Opis
id	integer	Identyfikator zdarzenia.
account_id	integer	Konto będące właścicielem.
campaign_id	integer	Kampania, do której należy zdarzenie.
contact_id	integer	Kontakt, do którego należy zdarzenie.

Pole	Typ	Opis
genre	string	Rodzaj zdarzenia (zobacz enum powyżej).
metadata	object	Dowolny JSON (np. `ip_address`, `user_agent`, przesłane pola, dane quizu). Domyślnie `{}`.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
genre_display_name	string	Czytelna nazwa rodzaju (np. `"Submitted data"`); obecne tylko gdy `genre` jest ustawione.
ip_address	string	Wygodna kopia `metadata.ip_address`; obecne tylko gdy ustawione.
user_agent	string	Wygodna kopia `metadata.user_agent`; obecne tylko gdy ustawione.


```
[
  {
    "id": 9051,
    "account_id": 11,
    "campaign_id": 42,
    "contact_id": 880,
    "genre": "clicked",
    "metadata": { "ip_address": "203.0.113.7", "user_agent": "Mozilla/5.0" },
    "created_at": "2026-05-30T10:01:08.000Z",
    "updated_at": "2026-05-30T10:01:08.000Z",
    "genre_display_name": "Clicked",
    "ip_address": "203.0.113.7",
    "user_agent": "Mozilla/5.0"
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono zdarzenia.
404	`account_id` nie należy do użytkownika tokena.

`POST /api/v1/accounts/:account_id/events`

Rejestruje nowe zdarzenie. `account` zdarzenia jest ustawiane na podstawie konta ze ścieżki, a przy zapisie model nadpisuje je tak, aby pasowało do konta kampanii. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Parametry treści żądania są opakowane w obiekt `event`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
event.campaign_id	body	integer	tak	Kampania dla tego zdarzenia. Walidowane `presence`.
event.contact_id	body	integer	tak	Kontakt dla tego zdarzenia. Walidowane `presence`.
event.genre	body	string	nie	Rodzaj zdarzenia; domyślnie `sent`. Jedna z wartości enuma `genre`. Walidowane `presence`.
event.metadata	body	object	nie	Dowolny hash JSON (dozwolony jako `metadata: {}`). Domyślnie `{}`.
event.name	body	string	nie	Akceptowane przez strong params, ale niezapisywane (brak kolumny `name`).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "event": { "campaign_id": 42, "contact_id": 880, "genre": "opened", "metadata":
        { "ip_address": "203.0.113.7", "user_agent": "Mozilla/5.0" } } }' \
  https://platform.phishspot.com/api/v1/accounts/11/events
```

Odpowiedź `201 Created` — utworzony obiekt zdarzenia (taki sam kształt jak element listy powyżej).


```
{
  "id": 9044,
  "account_id": 11,
  "campaign_id": 42,
  "contact_id": 880,
  "genre": "opened",
  "metadata": { "ip_address": "203.0.113.7", "user_agent": "Mozilla/5.0" },
  "created_at": "2026-05-30T09:58:21.000Z",
  "updated_at": "2026-05-30T09:58:21.000Z",
  "genre_display_name": "Opened",
  "ip_address": "203.0.113.7",
  "user_agent": "Mozilla/5.0"
}
```


Kody statusu

Kod	Kiedy
201	Utworzono zdarzenie.
404	`account_id` nie należy do użytkownika tokena.

Kod	Kiedy
422	Walidacja nie powiodła się (brak `campaign_id` / `contact_id` / `genre` lub nieprawidłowy `genre`). Treść: `{ "errors": { … } }`.

`GET /api/v1/events/:id`

Pobiera pojedyncze zdarzenie. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator zdarzenia (`evt_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/events/9044
```

Odpowiedź `200 OK` — pojedynczy obiekt zdarzenia (te same pola co element listy powyżej).

```
{
  "id": 9044,
  "account_id": 11,
  "campaign_id": 42,
  "contact_id": 880,
  "genre": "opened",
  "metadata": { "ip_address": "203.0.113.7" },
  "created_at": "2026-05-30T09:58:21.000Z",
  "updated_at": "2026-05-30T09:58:21.000Z",
  "genre_display_name": "Opened",
  "ip_address": "203.0.113.7"
}
```

Kody statusu

Kod	Kiedy
200	Zwrócono zdarzenie.
404	Brak zdarzenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena. Treść: `{ "error": "Event not found" }`.

`PATCH /api/v1/events/:id`

Aktualizuje rodzaj (genre) lub metadane zdarzenia. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Parametry treści żądania są opakowane w obiekt `event`; wyślij tylko te pola, które chcesz zmienić.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator zdarzenia (`evt_…` lub liczba całkowita).
event.genre	body	string	nie	Nowy rodzaj (jedna z wartości enuma `genre`; `presence` nadal wymuszane).
event.metadata	body	object	nie	Zastępczy hash metadanych.
event.campaign_id	body	integer	nie	Zmiana przypisania kampanii (`presence` wymuszane).
event.contact_id	body	integer	nie	Zmiana przypisania kontaktu (`presence` wymuszane).
event.name	body	string	nie	Akceptowane, ale niezapisywane.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "event": { "metadata": { "note": "manual correction" } } }' \
  https://platform.phishspot.com/api/v1/events/9044
```

Odpowiedź `200 OK` — zaktualizowany obiekt zdarzenia (taki sam kształt jak show).

Kody statusu

Kod	Kiedy
200	Zaktualizowano zdarzenie.
404	Brak zdarzenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena. Treść: `{ "error": "Event not found" }`.
422	Walidacja nie powiodła się (np. nieprawidłowy/pusty `genre`). Treść: `{ "errors": { … } }`.

`DELETE /api/v1/events/:id`

Trwale usuwa zdarzenie. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/events/9044
```

Odpowiedź `204 No Content` — pusta treść po sukcesie.

Kody statusu

Kod	Kiedy
204	Usunięto zdarzenie.
404	Brak zdarzenia o tym identyfikatorze w koncie, do którego należy użytkownik tokena. Treść: `{ "error": "Event not found" }`.

`GET /api/v1/accounts/:account_id/results`

Listuje wyniki e-learningu konta od najnowszych. Ten punkt końcowy nie ma filtrów query.
Uwierzytelnianie: Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/results
```

Odpowiedź `200 OK` — tablica JSON obiektów wyników.

Pole	Typ	Opis
id	integer	Identyfikator wyniku.
block_id	integer	Blok kursu, którego dotyczy ten wynik.
contact_id	integer	Kontakt, który wytworzył wynik.
account_id	integer	Konto będące właścicielem.
metadata	object	Dowolny JSON (np. `answer`, `correct`, `score`, `time_spent`, `completed`). Domyślnie `{}`.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
block	object | null	Obecne, gdy blok się załaduje: `{ id, name }`.
contact	object | null	Obecne, gdy kontakt się załaduje: `{ id, email, first_name, last_name, full_name }`.

```
[
  {
    "id": 7100,
    "block_id": 320,
    "contact_id": 880,
    "account_id": 11,
    "metadata": { "answer": "B", "correct": true, "score": 100, "completed": true },
    "created_at": "2026-05-31T14:20:00.000Z",
    "updated_at": "2026-05-31T14:20:00.000Z",
    "block": { "id": 320, "name": "Spot the Lookalike Domain" },
    "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
        "last_name": "Kowalski", "full_name": "Jan Kowalski" }
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono wyniki.
403	Użytkownik tokena nie jest uprawniony do wyświetlenia konta (`account.show?` odmówiono).
404	`account_id` nie należy do użytkownika tokena.

`POST /api/v1/accounts/:account_id/results`

Rejestruje wynik kontaktu dla bloku kursu. `account` jest pobierane automatycznie z bloku.
Uwierzytelnianie: Bearer; **rola:** odczyt (każda rola).

Parametry

Parametry treści żądania są opakowane w obiekt `result`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
result.block_id	body	integer	tak	Blok kursu, którego dotyczy ten wynik. Walidowane `presence`.
result.contact_id	body	integer	tak	Kontakt wytwarzający wynik. Walidowane `presence`.
result.metadata	body	object	nie	Hash JSON z danymi odpowiedzi/punktacji/ukończenia. Domyślnie `{}`. Dozwolone jako parametr skalarny (`:metadata`), więc wyślij go jako wartość obiektu JSON.
result.name	body	string	nie	Akceptowane przez strong params, ale niezapisywane (brak kolumny `name`).

Nazwa	Gdzie	Typ	Wymagane	Opis
result.state	body	string	nie	Akceptowane przez strong params, ale niezapisywane (Result nie ma kolumny/enuma `state`).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "result": { "block_id": 320, "contact_id": 880, "metadata": { "answer": "B",
        "correct": true, "score": 100, "completed": true } } }' \
  https://platform.phishspot.com/api/v1/accounts/11/results
```

Odpowiedź `201 Created` — utworzony obiekt wyniku (taki sam kształt jak element listy powyżej).

```
{
  "id": 7150,
  "block_id": 320,
  "contact_id": 880,
  "account_id": 11,
  "metadata": { "answer": "B", "correct": true, "score": 100, "completed": true },
  "created_at": "2026-06-02T08:30:00.000Z",
  "updated_at": "2026-06-02T08:30:00.000Z",
  "block": { "id": 320, "name": "Spot the Lookalike Domain" },
  "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
       "last_name": "Kowalski", "full_name": "Jan Kowalski" }
}
```

Kody statusu

Kod	Kiedy
201	Utworzono wynik.
404	`account_id` nie należy do użytkownika tokena.
422	Walidacja nie powiodła się (brak `block_id` / `contact_id`). Treść: `{ "errors": { … } }`.

`GET /api/v1/results/:id`

Pobiera pojedynczy wynik. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator wyniku (`res_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/results/7100
```

Odpowiedź `200 OK` — pojedynczy obiekt wyniku (te same pola co element listy powyżej).


```
{
  "id": 7100,
  "block_id": 320,
  "contact_id": 880,
  "account_id": 11,
  "metadata": { "answer": "B", "correct": true, "score": 100 },
  "created_at": "2026-05-31T14:20:00.000Z",
  "updated_at": "2026-05-31T14:20:00.000Z",
  "block": { "id": 320, "name": "Spot the Lookalike Domain" },
  "contact": { "id": 880, "email": "jan.kowalski@acme.test", "first_name": "Jan",
        "last_name": "Kowalski", "full_name": "Jan Kowalski" }
}
```


Kody statusu

Kod	Kiedy
200	Zwrócono wynik.
404	Brak wyniku o tym identyfikatorze w koncie, do którego należy użytkownik tokena.

`PATCH /api/v1/results/:id`

Aktualizuje wynik, zazwyczaj w celu skorygowania jego metadanych (odpowiedź, punktacja, ukończenie). **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Parametry

Parametry treści żądania są opakowane w obiekt `result`; wyślij tylko te pola, które chcesz zmienić.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator wyniku (`res_…` lub liczba całkowita).
result.metadata	body	object	nie	Zastępczy hash metadanych.
result.block_id	body	integer	nie	Zmiana przypisania bloku (`presence` wymuszane).
result.contact_id	body	integer	nie	Zmiana przypisania kontaktu (`presence` wymuszane).
result.name	body	string	nie	Akceptowane, ale niezapisywane.
result.state	body	string	nie	Akceptowane, ale niezapisywane.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "result": { "metadata": { "answer": "C", "correct": false, "score": 0 } } }' \
  https://platform.phishspot.com/api/v1/results/7100
```

Odpowiedź `200 OK` — zaktualizowany obiekt wyniku (taki sam kształt jak show).

Kody statusu

Kod	Kiedy
200	Zaktualizowano wynik.
404	Brak wyniku o tym identyfikatorze w koncie, do którego należy użytkownik tokena.
422	Walidacja nie powiodła się (np. wyczyszczony `block_id` / `contact_id`). Treść: `{ "errors": { … } }`.

`DELETE /api/v1/results/:id`

Trwale usuwa wynik. **Uwierzytelnianie:** Bearer; **rola:** odczyt (każda rola).

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/results/7100
```

Odpowiedź `204 No Content` — pusta treść po sukcesie.

Kody statusu

Kod	Kiedy
204	Usunięto wynik.
404	Brak wyniku o tym identyfikatorze w koncie, do którego należy użytkownik tokena.

27.8 Trendy konta

Zagregowana analityka podatności na phishing dla konta: jeden punkt danych na każdą dostarczoną kampanię w zakresie dat, plus podsumowanie zbiorcze. Oparte na `Campaigns::TrendService`, który liczy tylko kampanie w stanie `in_progress` lub `done` (scope `delivered`) utworzone w wybranym zakresie.

`GET /accounts/:account_id/trends`

Zwraca metryki podatności dla dostarczonych kampanii konta, uporządkowane od najstarszych, wraz z podsumowaniem (liczba kampanii, średni współczynnik kliknięć, kierunek trendu oraz grupa odbiorców o najwyższej klikalności). Użyj go, aby zasilić panel trendów lub śledzić, czy pracownicy z czasem coraz lepiej (czy gorzej) rozpoznają phishing. **Uwierzytelnianie:** Bearer; **rola:** read (dowolna rola — każdy członek konta).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita). Musi to być konto, do którego należy użytkownik tokena.
start_date	query	string	nie	Początek niestandardowego zakresu, `YYYY-MM-DD` . Parsowany do początku tego dnia. Jeśli jest obecny (z `end_date` lub bez), niestandardowy zakres ma pierwszeństwo przed `range` . Gdy pominięty, ale podano `end_date` , domyślnie przyjmuje datę sprzed 1 roku.
end_date	query	string	nie	Koniec niestandardowego zakresu, `YYYY-MM-DD` . Parsowany do końca tego dnia. Gdy pominięty, ale podano `start_date` , domyślnie przyjmuje teraz.
range	query	string	nie	Predefiniowany zakres, używany tylko wtedy, gdy nie podano ani `start_date` , ani `end_date` . Jedna z wartości `30d` , `90d` , `6m` , `all` . Każda inna/brakująca wartość (w tym domyślna) daje ostatni 1 rok. `all` obejmuje okres od epoki uniksowej do teraz.

> `start_date` / `end_date` tworzą niestandardowy zakres, który **nadpisuje** `range` . Daty są włączne (początek = początek dnia, koniec = koniec dnia). Nieprawidłowe daty zwracają `422` (patrz niżej).

Żądanie

```
curl -X GET -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  "https://platform.phishspot.com/api/v1/accounts/11/trends?
        start_date=2026-01-01&end_date=2026-06-01"
```

Odpowiedź `200 OK` — obiekt z tablicą `campaigns` (jeden wpis na każdą dostarczoną kampanię w zakresie) oraz obiektem `summary` .

Pole	Typ	Opis
campaigns	array	Dostarczone kampanie w zakresie, uporządkowane rosnąco według `created_at`. Każdy element to punkt danych (pola poniżej). Pusta tablica, jeśli brak.
campaigns[].id	integer	Identyfikator kampanii (surowa liczba całkowita).
campaigns[].name	string	Nazwa kampanii.
campaigns[].date	string	Data uruchomienia kampanii, `YYYY-MM-DD` (data ISO 8601). Używa `scheduled_at`, jeśli ustawiono, w przeciwnym razie `created_at`.
campaigns[].open_rate	number (float)	Procent odbiorców, którzy otworzyli e-mail (0.0, gdy brak danych).
campaigns[].click_rate	number (float)	Procent odbiorców, którzy kliknęli link (0.0, gdy brak danych).
campaigns[].submit_rate	number (float)	Procent odbiorców, którzy przesłali dane na stronie docelowej (0.0, gdy brak danych).
campaigns[].total_sent	integer	Liczba odbiorców, do których wysłano kampanię.
summary	object	Zestawienie zbiorcze dla powyższych kampanii (pola poniżej).
summary.total_campaigns	integer	Liczba dostarczonych kampanii w zakresie (`0`, gdy brak).
summary.avg_click_rate	number (float)	Średnia z wartości `click_rate` poszczególnych kampanii, zaokrąglona do 1 miejsca po przecinku (`0.0`, gdy brak).
summary.trend_direction	string	Jedna z wartości `improving`, `worsening`, `stable` lub `neutral`. Porównuje średni współczynnik kliknięć ostatnich do 3 kampanii ze średnią najwcześniejszych do 3; `neutral`, gdy mniej niż 2 kampanie, `stable`, gdy zmiana mieści się w zakresie ±1.0 punktu procentowego.
summary.most_vulnerable_group	string | null	Nazwa grupy odbiorców o najwyższym stosunku kliknięć do wysłanych w zakresie; `null`, gdy brak danych o grupach.

```
{
  "campaigns": [
    {
      "id": 42,
      "name": "Q1 Invoice Lure",
      "date": "2026-01-14",
      "open_rate": 61.5,
      "click_rate": 23.1,
      "submit_rate": 7.7,
      "total_sent": 130
    },
    {
      "id": 57,
      "name": "Password Expiry Notice",
      "date": "2026-04-02",
      "open_rate": 54.0,
      "click_rate": 12.0,
      "submit_rate": 4.0,
      "total_sent": 150
    }
  ],
  "summary": {
    "total_campaigns": 2,
    "avg_click_rate": 17.6,
    "trend_direction": "improving",
    "most_vulnerable_group": "Finance"
  }
}
```


Kody statusu

Kod	Kiedy
200	Zwrócono dane trendów (tablica `campaigns` i `summary` są obecne nawet wtedy, gdy nie ma pasujących kampanii).
404	`account_id` nie należy do użytkownika tokena (`{"error":"Account not found"}`).
422	`start_date` lub `end_date` nie jest możliwą do sparsowania datą `YYYY-MM-DD` (`{"error":"Invalid date; use YYYY-MM-DD."}`).

27.9 Kursy i bloki

Kursy e-learningowe dostarczane pracownikom, którzy dali się nabrać na symulację phishingu. **Kurs** to uporządkowany zbiór **bloków** (tekst, HTML, wideo, quiz itp.). Kursy należą do Twojego konta albo są **globalne** (wyselekcjonowana, współdzielona biblioteka). Bloki są zagnieżdżone w kursie na potrzeby

listowania/tworzenia, ale są adresowalne po własnym płytkim id na potrzeby wyświetlania/aktualizacji/usuwania.

> Wszystkie punkty końcowe w tej sekcji autoryzują przez politykę dla pojedynczego rekordu, która nadaje odczyt **oraz** zapis **każdej roli na koncie** (członek, edytor, admin). Jedyne ograniczenia zapisu to: nie możesz modyfikować kursu/bloku **globalnego**, który nie należy do Twojego konta (`403`), oraz nie możesz aktualizować/usuwać kursu lub bloku, który jest **zablokowany** przez trwającą lub wstrzymaną kampanię.

`GET /api/v1/accounts/:account_id/courses`

Listuje wszystkie kursy dostępne dla konta — kursy należące do Twojego konta plus wszystkie kursy z `global: true` — uporządkowane według nazwy, z dołączonym lekkim podsumowaniem bloków. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokena.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/courses
```

Odpowiedź `200 OK` — tablica JSON obiektów kursu (zobacz pola kursu poniżej).

Pole	Typ	Opis
id	integer	Id kursu.
account_id	integer	Id konta będącego właścicielem.
name	string	Nazwa kursu.
description	string	Opis kursu.
global	boolean	`true` dla współdzielonych/wyselekcjonowanych kursów z biblioteki, `false` dla kursów należących do konta.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
blocks	array	Dołączone podsumowania bloków (zobacz pola poniżej). Uporządkowane tak, jak zapisano w asocjacji.
blocks[].id	integer	Id bloku.
blocks[].name	string	Nazwa bloku.

Pole	Typ	Opis
blocks[].order	integer	Pozycja w kursie liczona od zera.
blocks[].genre	string	Rodzaj bloku (zobacz enum przy punktach końcowych bloków).


```
[
  {
    "id": 7,
    "account_id": 11,
    "name": "Spotting Spoofed Senders",
    "description": "A short course on recognising display-name and domain spoofing.",
    "global": false,
    "created_at": "2026-05-01T09:12:00.000Z",
    "updated_at": "2026-05-14T16:40:11.000Z",
    "blocks": [
      { "id": 31, "name": "Intro", "order": 0, "genre": "html" },
      { "id": 32, "name": "Quick check", "order": 1, "genre": "quiz" }
    ]
  }
]
```


Kody statusu

Kod	Kiedy
200	Kursy zwrócone.
404	`account_id` nie jest kontem, do którego należy użytkownik tokena.

`POST /api/v1/accounts/:account_id/courses`

Tworzy nowy kurs należący do konta. Kurs jest zawsze tworzony pod kontem z ścieżki (nie można ustawić `global` — nowe kursy są prywatne). Zarówno `name`, jak i `description` są wymagane przez model. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — wszyscy członkowie zespołu mogą tworzyć kursy).

Parametry

Parametry treści żądania są opakowane w obiekt `course`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).
course	body	object	tak	Obiekt opakowujący zawierający pola poniżej.
course.name	body	string	tak	Nazwa kursu. Walidowana pod kątem obecności.

Nazwa	Gdzie	Typ	Wymagane	Opis
course.description	body	string	tak	Opis kursu. Walidowany pod kątem obecności.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "course": { "name": "Invoice Fraud 101", "description": "Recognising fake
        supplier invoices." } }' \
  https://platform.phishspot.com/api/v1/accounts/11/courses
```

Odpowiedź `201 Created` — utworzony kurs, taki sam kształt jak element listy (z pustą tablicą `blocks`).

Pole	Typ	Opis
id	integer	Id nowego kursu.
account_id	integer	Id konta będącego właścicielem (konto ze ścieżki).
name	string	Nazwa kursu.
description	string	Opis kursu.
global	boolean	Zawsze `false` dla nowo utworzonych kursów.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
blocks	array	Pusta przy tworzeniu.

```
{
  "id": 19,
  "account_id": 11,
  "name": "Invoice Fraud 101",
  "description": "Recognising fake supplier invoices.",
  "global": false,
  "created_at": "2026-06-02T10:00:00.000Z",
  "updated_at": "2026-06-02T10:00:00.000Z",
  "blocks": []
}
```

Kody statusu

Kod	Kiedy
201	Kurs utworzony.
404	`account_id` nie jest kontem, do którego należy użytkownik tokena.
422	Walidacja nie powiodła się — np. `name` lub `description` puste. Treść: `{"errors": {"name": ["can't be blank"]}}`.

`GET /api/v1/courses/:id`

Pobiera pojedynczy kurs po jego płytkim id. Rozwiązywalne dla kursów należących do Twojego konta lub dowolnego kursu `global`; kurs należący do innego najemcy zwraca `404`. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id kursu (`course_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/courses/7
```

Odpowiedź `200 OK` — jeden obiekt kursu, te same pola co element listy (w tym dołączone podsumowanie `blocks`).

Pole	Typ	Opis
id	integer	Id kursu.
account_id	integer	Id konta będącego właścicielem.
name	string	Nazwa kursu.
description	string	Opis kursu.
global	boolean	Czy kurs pochodzi ze współdzielonej biblioteki.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
blocks	array	Dołączone podsumowania bloków: `id`, `name`, `order`, `genre`.

```
{
  "id": 7,
  "account_id": 11,
  "name": "Spotting Spoofed Senders",
  "description": "A short course on recognising display-name and domain spoofing.",
  "global": false,
  "created_at": "2026-05-01T09:12:00.000Z",
  "updated_at": "2026-05-14T16:40:11.000Z",
  "blocks": [
    { "id": 31, "name": "Intro", "order": 0, "genre": "html" },
    { "id": 32, "name": "Quick check", "order": 1, "genre": "quiz" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Kurs zwrócony.
404	Brak kursu o tym id należącego do Twojego konta, a kurs nie jest globalny.

`PATCH /api/v1/courses/:id`

Aktualizuje pola `name` i/lub `description` kursu. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), z zastrzeżeniem kontroli własności globalnej i blokady opisanych poniżej.

Parametry

Parametry treści żądania są opakowane w obiekt `course`. Dozwolone są tylko `name` i `description`.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id kursu (`course_…` lub liczba całkowita).
course	body	object	tak	Obiekt opakowujący zawierający pola poniżej.
course.name	body	string	nie	Nowa nazwa. Nie może być pusta, jeśli podana (walidacja obecności).
course.description	body	string	nie	Nowy opis. Nie może być pusty, jeśli podany (walidacja obecności).

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "course": { "description": "Updated for the 2026 supplier-fraud wave." } }' \
  https://platform.phishspot.com/api/v1/courses/7
```

Odpowiedź `200 OK` — zaktualizowany kurs (taki sam kształt jak `GET /courses/:id`).

```
{
  "id": 7,
  "account_id": 11,
  "name": "Spotting Spoofed Senders",
  "description": "Updated for the 2026 supplier-fraud wave.",
  "global": false,
  "created_at": "2026-05-01T09:12:00.000Z",
  "updated_at": "2026-06-02T10:05:00.000Z",
  "blocks": [
    { "id": 31, "name": "Intro", "order": 0, "genre": "html" }
  ]
}
```

Kody statusu

Kod	Kiedy
200	Kurs zaktualizowany.
403	Kurs jest `global` i nie należy do Twojego konta, **albo** jest zablokowany przez trwającą/wstrzymaną kampanię.
404	Kurs nieosiągalny dla Twojego konta (nie jest własnością i nie jest globalny).
422	Walidacja nie powiodła się — np. `name` / `description` ustawione na puste. Treść: `{"errors": {...}}`.

`DELETE /api/v1/courses/:id`

Usuwa kurs i (poprzez `dependent: :destroy`) wszystkie jego bloki. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), z zastrzeżeniem kontroli własności globalnej i blokady opisanych poniżej.

Parametry

Brak parametrów poza tokenem bearer i id ze ścieżki.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id kursu (`course_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/courses/19
```

Odpowiedź `204 No Content` — pusta treść po sukcesie.

Kody statusu

Kod	Kiedy
204	Kurs usunięty.
403	Kurs jest `global` i nie należy do Twojego konta, **albo** jest zablokowany przez trwającą/wstrzymaną kampanię.
404	Kurs nieosiągalny dla Twojego konta.

`GET /api/v1/courses/:course_id/blocks`

Listuje bloki kursu, uporządkowane według `order` (rosnąco), zawężone przez Pundit do bloków dostępnych (własnych lub globalnych) kursów. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
course_id	path	string	tak	Id kursu (`course_…` lub liczba całkowita). Musi należeć do Twojego konta lub być globalny.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/courses/7/blocks
```

Odpowiedź `200 OK` — tablica JSON pełnych obiektów bloku (pola poniżej).

Pole	Typ	Opis
id	integer	Id bloku.
name	string	Nazwa bloku.
course_id	integer	Id kursu nadrzędnego.
order	integer	Pozycja w kursie liczona od zera.
genre	string	Jeden z: `text`, `html`, `image`, `video`, `quiz`, `interactive`, `code`, `file_download`.
metadata	object	Dowolny JSON. Dla bloków quizowych przechowuje ładunek z pytaniem/odpowiedziami.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
html_data	string	Wyrenderowany HTML z tekstu sformatowanego. **Obecne tylko wtedy, gdy** blok ma treść ActionText.
locked	boolean	`true`, gdy powiązana kampania jest w toku (bloku nie można aktualizować/usuwać).
quiz_question	string	**Tylko bloki quizowe.** Sparsowany tekst pytania.
quiz_answers	array	**Tylko bloki quizowe.** Tablica hashy odpowiedzi sparsowanych z `metadata`.
url	string	Kanoniczny adres URL API tego bloku (`/api/v1/blocks/:id`).

```
[
  {
    "id": 31,
    "name": "Intro",
    "course_id": 7,
    "order": 0,
    "genre": "html",
    "metadata": {},
    "created_at": "2026-05-01T09:12:00.000Z",
    "updated_at": "2026-05-01T09:12:00.000Z",
    "html_data": "<div>Welcome to the course.</div>",
    "locked": false,
    "url": "https://platform.phishspot.com/api/v1/blocks/31"
  },
  {
    "id": 32,
    "name": "Quick check",
    "course_id": 7,
    "order": 1,
    "genre": "quiz",
    "metadata": [
      { "question_text": "Which sender is spoofed?" },
      { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
      { "answer_text": "no-reply@paypal.com" }
    ],
    "created_at": "2026-05-01T09:13:00.000Z",
    "updated_at": "2026-05-01T09:13:00.000Z",
    "locked": false,
    "quiz_question": "Which sender is spoofed?",
    "quiz_answers": [
      { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
      { "answer_text": "no-reply@paypal.com" }
    ],
    "url": "https://platform.phishspot.com/api/v1/blocks/32"
  }
]
```


Kody statusu

Kod	Kiedy
200	Bloki zwrócone (pusta tablica, jeśli kurs nie ma żadnych).
404	`course_id` nieosiągalny dla Twojego konta (nie jest własnością i nie jest globalny).

`POST /api/v1/courses/:course_id/blocks`

Dodaje blok do kursu. Pole `account` bloku jest ustawiane automatycznie na podstawie kursu; jeśli `order` jest pominięte, jest automatycznie przypisywane na koniec kursu. Wymagania dotyczące treści różnią się w zależności od `genre` (zobacz poniżej). **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), ale nie możesz dodawać bloków do kursu globalnego, który nie należy do Ciebie (`403`).

Parametry

Parametry treści żądania są opakowane w obiekt `block`.

Nazwa	Gdzie	Typ	Wymagane	Opis
course_id	path	string	tak	Id kursu (`course_…` lub liczba całkowita).
block	body	object	tak	Obiekt opakowujący zawierający pola poniżej.
block.name	body	string	tak	Nazwa bloku. Walidowana pod kątem obecności.
block.genre	body	string	tak	Jeden z `text`, `html`, `image`, `video`, `quiz`, `interactive`, `code`, `file_download`. Domyślnie `text`, jeśli pominięty.
block.body	body	string	warunkowo	Treść w zwykłym tekście/markdownie. **Wymagana, chyba że** genre to `quiz`, `html`, `video` lub `file_download`. Dla `video` / `file_download` służy jako opcjonalny opis.
block.html_data	body	string	warunkowo	Treść w formacie rich HTML (ActionText). Dla bloków `html` / `text` podaj `body` albo `html_data`.
block.metadata	body	object/array	warunkowo	Dowolny JSON. **Wymagane dla bloków `quiz`**, gdzie niesie pytanie i odpowiedzi (zobacz ograniczenia quizu).
block.order	body	integer	nie	Pozycja w kursie (liczba całkowita ≥ 0). Automatycznie przypisana na koniec, jeśli pominięta.
block.course_id	body	integer	nie	Dozwolone, ale zwykle nadmiarowe wobec `course_id` ze ścieżki.
block.video_file	body	file	warunkowo	Załącznik wideo. **Wymagany dla bloków `video`.** Musi być `video/mp4` lub `video/webm`, ≤ 300 MB, ≤ 1920×1080, ≤ 600 s, kodek wideo h264/vp8/vp9, kodek audio aac/opus. Puste wartości tekstowe są ignorowane.
block.document_file	body	file	warunkowo	Załącznik dokumentu. **Wymagany dla bloków `file_download`.** Dowolny format, ≤ 100 MB. Puste wartości tekstowe są ignorowane.

Bloki `quiz` muszą mieć od **2 do 6** odpowiedzi w `metadata`, a **co najmniej jedna odpowiedź musi być oznaczona jako poprawna** (odpowiedź jest poprawna, gdy jej wartość `right_answer` / `correct` to `true`, `"on"`, `"true"`, `"1"` lub `"yes"`). W przeciwnym razie tworzenie kończy się błędem `422`.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{
        "block": {
          "name": "Identify the phish",
          "genre": "quiz",
          "metadata": [
            { "question_text": "Which sender is spoofed?" },
            { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
            { "answer_text": "no-reply@paypal.com" }
          ]
        }
      }' \
  https://platform.phishspot.com/api/v1/courses/7/blocks
```

Odpowiedź `201 Created` — utworzony blok (taki sam kształt jak element listy).

```
{
  "id": 33,
  "name": "Identify the phish",
  "course_id": 7,
  "order": 2,
  "genre": "quiz",
  "metadata": [
    { "question_text": "Which sender is spoofed?" },
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "created_at": "2026-06-02T10:10:00.000Z",
  "updated_at": "2026-06-02T10:10:00.000Z",
  "locked": false,
  "quiz_question": "Which sender is spoofed?",
  "quiz_answers": [
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "url": "https://platform.phishspot.com/api/v1/blocks/33"
}
```

Kody statusu

Kod	Kiedy
201	Blok utworzony.

Kod	Kiedy
403	Kurs nadrzędny jest `global` i nie należy do Twojego konta.
404	`course_id` nieosiągalny dla Twojego konta.
422	Walidacja nie powiodła się — brak `name` / `genre`, brak wymaganej treści dla danego genre (`body`, `html_data`, `metadata`, `video_file` lub `document_file`), zbyt mało/zbyt wiele odpowiedzi quizowych, brak poprawnej odpowiedzi quizowej lub niedozwolony plik wideo/dokumentu. Treść: `{"errors": {...}}`.

`GET /api/v1/blocks/:id`

Pobiera pojedynczy blok po jego płytkim id, zawężony do bloków kursów, do których Twoje konto ma dostęp (własnych lub globalnych). **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id bloku (`blk_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/blocks/32
```

Odpowiedź `200 OK` — jeden obiekt bloku (pełne pola jak na liście bloków).

Pole	Typ	Opis
id	integer	Id bloku.
name	string	Nazwa bloku.
course_id	integer	Id kursu nadrzędnego.
order	integer	Pozycja liczona od zera.
genre	string	Rodzaj bloku (zobacz enum powyżej).
metadata	object/array	Dowolny JSON; ładunek quizu dla bloków quizowych.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
html_data	string	Wyrenderowany tekst sformatowany. Obecne tylko, gdy ustawione.
locked	boolean	`true`, gdy powiązana kampania jest w toku.
quiz_question	string	Tylko bloki quizowe.

Pole	Typ	Opis
quiz_answers	array	Tylko bloki quizowe.
url	string	Kanoniczny adres URL API tego bloku.


```
{
  "id": 32,
  "name": "Quick check",
  "course_id": 7,
  "order": 1,
  "genre": "quiz",
  "metadata": [
    { "question_text": "Which sender is spoofed?" },
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "created_at": "2026-05-01T09:13:00.000Z",
  "updated_at": "2026-05-01T09:13:00.000Z",
  "locked": false,
  "quiz_question": "Which sender is spoofed?",
  "quiz_answers": [
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "url": "https://platform.phishspot.com/api/v1/blocks/32"
}
```


Kody statusu

Kod	Kiedy
200	Blok zwrócony.
404	Blok nieosiągalny dla Twojego konta (jego kurs nie jest ani własnością, ani globalny).

`PATCH /api/v1/blocks/:id`

Aktualizuje blok. Te same dozwolone pola i reguły treści zależne od genre co przy tworzeniu. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), ale nie możesz edytować bloku w kursie globalnym, który nie należy do Ciebie (`403`), a blok `locked?` (kampania w toku) wywołuje błąd not-destroyed podczas aktualizacji.

Parametry

Parametry treści żądania są opakowane w obiekt `block` . Dozwolone klucze: `name` , `body` , `course_id` , `order` , `genre` , `metadata` , `html_data` , `video_file` , `document_file` .

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id bloku (`blk_…` lub liczba całkowita).
block	body	object	tak	Obiekt opakowujący zawierający dowolne z dozwolonych pól.
block.name	body	string	nie	Nowa nazwa (walidacja obecności, jeśli podana).
block.genre	body	string	nie	Zmiana genre; ten sam enum co przy tworzeniu. Zmiana genre może sprawić, że inne pola staną się wymagane.
block.body	body	string	nie	Treść tekstowa. Wymagana, chyba że genre to `quiz` / `html` / `video` / `file_download`.
block.html_data	body	string	nie	Treść w formacie rich HTML.
block.metadata	body	object/array	nie	Dowolny JSON; ładunek quizu (2–6 odpowiedzi, ≥1 poprawna).
block.order	body	integer	nie	Nowa pozycja (liczba całkowita ≥ 0).
block.video_file	body	file	nie	Zastępcze wideo (te same ograniczenia co przy tworzeniu). Puste ciągi ignorowane.
block.document_file	body	file	nie	Zastępczy dokument (≤ 100 MB). Puste ciągi ignorowane.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "block": { "name": "Identify the phishing sender", "order": 1 } }' \
  https://platform.phishspot.com/api/v1/blocks/32
```

Odpowiedź `200 OK` — zaktualizowany blok (taki sam kształt jak `GET /blocks/:id`).

```
{
  "id": 32,
  "name": "Identify the phishing sender",
  "course_id": 7,
  "order": 1,
  "genre": "quiz",
  "metadata": [
    { "question_text": "Which sender is spoofed?" },
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "created_at": "2026-05-01T09:13:00.000Z",
  "updated_at": "2026-06-02T10:15:00.000Z",
  "locked": false,
  "quiz_question": "Which sender is spoofed?",
  "quiz_answers": [
    { "answer_text": "no-reply@paypa1.com", "right_answer": "on" },
    { "answer_text": "no-reply@paypal.com" }
  ],
  "url": "https://platform.phishspot.com/api/v1/blocks/32"
}
```


Kody statusu

Kod	Kiedy
200	Blok zaktualizowany.
403	Kurs bloku jest `global` i nie należy do Twojego konta.
404	Blok nieosiągalny dla Twojego konta.
422	Walidacja nie powiodła się — puste `name`, brak treści wymaganej przez genre, nieprawidłowe odpowiedzi quizowe, niedozwolony plik, **albo** blok jest zablokowany przez kampanię w toku. Treść: `{"errors": {...}}`.

`DELETE /api/v1/blocks/:id`

Usuwa blok. Kontroler najpierw sprawdza, czy blok jest zablokowany przez trwającą kampanię, i odmawia z kodem `422`, jeśli tak jest. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), ale nie możesz usunąć bloku w kursie globalnym, który nie należy do Ciebie (`403`).

Parametry

Brak parametrów poza tokenem bearer i id ze ścieżki.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id bloku (`blk_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/blocks/33
```

Odpowiedź `204 No Content` — pusta treść po sukcesie.

Kody statusu

Kod	Kiedy
204	Blok usunięty.
403	Kurs bloku jest `global` i nie należy do Twojego konta.
404	Blok nieosiągalny dla Twojego konta.
422	Blok jest zablokowany (powiązana kampania jest w toku). Treść: `{"errors": ["Cannot delete block because connected campaign is in progress"]}`.

27.10 Autopiloty

Autopiloty to powtarzalne, bezobsługowe programy phishingowe: opisujesz odbiorców i kadencję, a platforma sama generuje i dostarcza kampanie, dopóki jej nie zatrzymasz. Autopilot powstaje jako `draft`, a następnie przechodzi przez niewielki cykl życia (`draft → running ⇄ paused → stopped`) za pomocą dedykowanych akcji opisanych poniżej.

> Uruchomienie autopilotu aktywuje **działający, wysyłający program** — platforma zacznie generować i dostarczać prawdziwe kampanie phishingowe do wskazanych członków zgodnie ze skonfigurowaną kadencją. Traktuj `POST /autopilots/:id/start` jak akcję uruchamiającą produkcję, nie jak przebieg testowy.

Kilka faktów o modelu, do których odwołujemy się w całym tym rozdziale:

- **Stan** (`state`): jeden z `draft`, `running`, `paused`, `stopped`.
- **Okres intensywności** (`intensity_period`): jeden z `day`, `week`, `month`, `year`.
- **Rodzaj czasu trwania** (`duration_kind`): `continuous` (działa bez końca) lub `until_date` (zatrzymuje się w dniu `ends_on`).
- **Typ akcji końcowej** (`end_action_type`): jeden z `nothing`, `redirect_to_course`, `message_page`, `redirect_to_url` — decyduje, co widzi cel po zakończeniu symulacji.
- **Limit dziennego tempa**: efektywne tempo wysyłki to `intensity_count / period_in_days` i nie może przekroczyć **2 kampanii/dzień** (`day`=1, `week`=7, `month`=30, `year`=365 dni na okres). Przekroczenie powoduje błąd walidacji na `intensity_count`.
- **Edytowalność**: autopilot jest edytowalny, dopóki nie jest `stopped`. Po przejściu w stan `stopped` dostępne pozostają tylko odczyt i usunięcie.

`GET /accounts/:account_id/autopilots`

Listuje wszystkie autopiloty należące do konta, od najnowszych. Użyj, aby wyrenderować panel autopilotów lub znaleźć id autopilotu przed wykonaniem na nim akcji. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — członek, edytor lub admin).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).
state	query	string	nie	Filtruje do pojedynczego stanu. Jeden z `draft`, `running`, `paused`, `stopped`. Każda inna wartość zwraca `422`.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/autopilots?state=running"
```

Odpowiedź `200 OK` — tablica JSON obiektów autopilota (każdy identyczny z odpowiedzią dla pojedynczego autopilotu poniżej).

Pole	Typ	Opis
id	integer	Id autopilotu.
account_id	integer	Id konta będącego właścicielem.
name	string	Nazwa wyświetlana.
state	string	`draft` | `running` | `paused` | `stopped`.
all_groups	boolean	Czy autopilot kieruje się do wszystkich grup (zamiast do wymienionych `groups`).
intensity_count	integer	Liczba kampanii na `intensity_period`.
intensity_period	string	`day` | `week` | `month` | `year`.
duration_kind	string	`continuous` | `until_date`.
ai_optimizer_enabled	boolean	Czy optymalizacja AI jest włączona.
auto_include_new_members	boolean	Czy nowi członkowie są automatycznie dołączani.
language	string	Kod języka docelowego (np. `en`, `pl`).
end_action_type	string	`nothing` | `redirect_to_course` | `message_page` | `redirect_to_url`.
end_action_url	string | null	URL przekierowania (używany, gdy `end_action_type` to `redirect_to_url`).

Pole	Typ	Opis
created_at	string	Znacznik czasu ISO-8601.
updated_at	string	Znacznik czasu ISO-8601.
ends_on	string | null	Data ISO-8601, w której program się zatrzymuje (gdy `duration_kind` to `until_date`), w przeciwnym razie `null`.
started_at	string | null	Znacznik czasu ISO-8601 pierwszego uruchomienia, w przeciwnym razie `null`.
daily_rate	number	Efektywna liczba kampanii/dzień, zaokrąglona do 2 miejsc po przecinku.
progress_percentage	integer | null	Całkowity % oczekiwanych kampanii dostarczonych w bieżącym okresie; `null` dla `draft` / `stopped`.
course_id	integer | null	Id powiązanego kursu e-learningowego, w przeciwnym razie `null`.
editable	boolean	`false` tylko wtedy, gdy `state` to `stopped`.
groups	array	Docelowe grupy. Każda: `{ "id": integer, "name": string }`.
recent_campaigns	array	Do 10 najnowszych wygenerowanych kampanii, od najnowszych. Każda: `{ "id": integer, "name": string, "state": string }`.

```
[
  {
    "id": 7,
    "account_id": 11,
    "name": "Finance team — quarterly drip",
    "state": "running",
    "all_groups": false,
    "intensity_count": 2,
    "intensity_period": "month",
    "duration_kind": "continuous",
    "ai_optimizer_enabled": true,
    "auto_include_new_members": true,
    "language": "en",
    "end_action_type": "redirect_to_course",
    "end_action_url": null,
    "created_at": "2026-05-01T09:00:00Z",
    "updated_at": "2026-06-01T12:30:00Z",
    "ends_on": null,
    "started_at": "2026-05-02T08:00:00Z",
    "daily_rate": 0.07,
    "progress_percentage": 88,
    "course_id": 14,
    "editable": true,
    "groups": [
      { "id": 3, "name": "Finance" }
    ],
    "recent_campaigns": [
      { "id": 102, "name": "Invoice approval — May", "state": "completed" }
    ]
  }
]
```


Kody statusu

Kod	Kiedy
200	Lista zwrócona (być może pusta).
404	`account_id` nie istnieje lub użytkownik tokenu nie jest jego członkiem.
422	Parametr query `state` jest obecny, ale nie jest jednym z `draft`, `running`, `paused`, `stopped`.

`POST /accounts/:account_id/autopilots`

Tworzy nowy autopilot w stanie `draft`. Puste pola są wstępnie wypełniane z ustawień autopilotu konta oraz domyślnych wartości konta (branża, język, URL/HTML akcji końcowej, domyślny kurs), więc nawet minimalna treść żądania daje użyteczny szkic. Autopilot **nie** jest uruchamiany — wywołaj potem `start`, aby przejść na żywo. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor.

Treść żądania jest opakowana w obiekt `autopilot`.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).
name	body	string	tak	Nazwa wyświetlana. Maks. 80 znaków; musi być unikalna w obrębie konta (bez rozróżniania wielkości liter).
all_groups	body	boolean	nie	Kieruj do wszystkich grup. Domyślnie `true`.
group_ids	body	array	nie	Prefiksowane id grup (`grp_…`), do których kierować. Nieznane/obce id → `422`. Używane, gdy `all_groups` to `false`.
intensity_count	body	integer	nie	Liczba kampanii na okres. Musi być ≥ 1. Domyślnie `1`. Wynikowe dzienne tempo (`intensity_count / period_days`) musi być ≤ 2/dzień.
intensity_period	body	string	nie	`day` | `week` | `month` | `year`. Domyślnie `month`.
duration_kind	body	string	nie	`continuous` | `until_date`. Domyślnie `continuous`.
ends_on	body	string (date)	warunkowo	Wymagane (i musi być datą przyszłą), gdy `duration_kind` to `until_date`.
ai_optimizer_enabled	body	boolean	nie	Domyślnie `true`.
auto_include_new_members	body	boolean	nie	Domyślnie `true`.
language	body	string	nie	Kod języka docelowego (np. `en`, `pl`). Wstępnie wypełniany z ustawień/lokalizacji konta, jeśli pusty.
industry_code_id	body	integer	nie	Id kodu branży. Wstępnie wypełniany z ustawień konta, jeśli pusty.
end_action_type	body	string	nie	`nothing` | `redirect_to_course` | `message_page` | `redirect_to_url`. Domyślnie `message_page`.

Nazwa	Gdzie	Typ	Wymagane	Opis
end_action_url	body	string	warunkowo	Wymagane i musi być `http` / `https`, gdy `end_action_type` to `redirect_to_url`.
end_action_html	body	string	warunkowo	Wymagane, gdy `end_action_type` to `message_page` (wstępnie wypełniane z domyślnych wartości konta, jeśli puste).
course_id	body	string	warunkowo	Prefiksowane id kursu (`course_…`); musi należeć do konta albo być kursem globalnym (inaczej `422`). Wymagane, gdy `end_action_type` to `redirect_to_course`.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{
        "autopilot": {
          "name": "Finance team — quarterly drip",
          "all_groups": false,
          "group_ids": ["grp_3a9k"],
          "intensity_count": 2,
          "intensity_period": "month",
          "duration_kind": "continuous",
          "end_action_type": "redirect_to_course",
          "course_id": "course_8h2d"
        }
      }' \
  https://platform.phishspot.com/api/v1/accounts/11/autopilots
```

Odpowiedź `201 Created` — nowo utworzony autopilot, w tym samym kształcie co element listy powyżej (`state` będzie `draft`, a `started_at` i `progress_percentage` `null`).

```
{
  "id": 9,
  "account_id": 11,
  "name": "Finance team — quarterly drip",
  "state": "draft",
  "all_groups": false,
  "intensity_count": 2,
  "intensity_period": "month",
  "duration_kind": "continuous",
  "ai_optimizer_enabled": true,
  "auto_include_new_members": true,
  "language": "en",
  "end_action_type": "redirect_to_course",
  "end_action_url": null,
  "created_at": "2026-06-02T10:15:00Z",
  "updated_at": "2026-06-02T10:15:00Z",
  "ends_on": null,
  "started_at": null,
  "daily_rate": 0.07,
  "progress_percentage": null,
  "course_id": 14,
  "editable": true,
  "groups": [
    { "id": 3, "name": "Finance" }
  ],
  "recent_campaigns": []
}
```


Kody statusu

Kod	Kiedy
201	Autopilot utworzony.
400	Opakowanie treści `autopilot` jest całkowicie nieobecne.
403	Użytkownik tokenu jest `member` (tylko odczyt) na koncie — tylko admini/edytorzy mogą tworzyć.
404	`account_id` nie istnieje lub użytkownik tokenu nie jest jego członkiem.
422	Walidacja nie powiodła się — np. pusta/zduplikowana/zbyt długa `name`, dzienne tempo powyżej limitu 2/dzień, brak `ends_on` dla `until_date`, brak `end_action_url` / `end_action_html` / `course_id` dla wybranego `end_action_type` albo nieznane `group_ids` / `course_id`.

`GET /autopilots/:id`

Pobiera pojedynczy autopilot po jego id. To trasa płaska (niezagnieżdżona) — bez `account_id` w ścieżce; konto jest wnioskowane z autopilotu, a członkostwo użytkownika tokenu jest weryfikowane. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor.

Brak parametrów poza tokenem bearer.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/autopilots/9
```

Odpowiedź `200 OK` — pojedynczy obiekt autopilota (identyczny zestaw pól jak element listy udokumentowany w `GET …/autopilots`).


```
{
  "id": 9,
  "account_id": 11,
  "name": "Finance team — quarterly drip",
  "state": "running",
  "all_groups": false,
  "intensity_count": 2,
  "intensity_period": "month",
  "duration_kind": "continuous",
  "ai_optimizer_enabled": true,
  "auto_include_new_members": true,
  "language": "en",
  "end_action_type": "redirect_to_course",
  "end_action_url": null,
  "created_at": "2026-06-02T10:15:00Z",
  "updated_at": "2026-06-02T10:16:00Z",
  "ends_on": null,
  "started_at": "2026-06-02T10:16:00Z",
  "daily_rate": 0.07,
  "progress_percentage": 100,
  "course_id": 14,
  "editable": true,
  "groups": [
    { "id": 3, "name": "Finance" }
  ],
  "recent_campaigns": []
}
```


Kody statusu

Kod	Kiedy
200	Autopilot zwrócony.
403	Użytkownik tokenu jest `member` (tylko odczyt) na koncie autopilotu — odczyt pojedynczego autopilotu wymaga roli admin/edytor.
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.

`PATCH /autopilots/:id`

Aktualizuje konfigurację autopilotu. Treść żądania jest opakowana w obiekt `autopilot` i przyjmuje te same pola co przy tworzeniu. Przekazanie `group_ids` **zastępuje** cały zestaw docelowych grup. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor — a autopilot musi być edytowalny (nie `stopped`). Trasa płaska (bez `account_id`).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).
name	body	string	nie	Nazwa wyświetlana. Maks. 80 znaków; unikalna w obrębie konta (bez rozróżniania wielkości liter).
all_groups	body	boolean	nie	Kieruj do wszystkich grup.
group_ids	body	array	nie	Prefiksowane id grup (`grp_…`). Gdy obecne, **zastępują** bieżący zestaw grup; nieznane/obce id → `422` .
intensity_count	body	integer	nie	Liczba kampanii na okres (≥ 1; dzienne tempo musi pozostać ≤ 2/dzień).
intensity_period	body	string	nie	`day` | `week` | `month` | `year` .
duration_kind	body	string	nie	`continuous` | `until_date` .
ends_on	body	string (date)	warunkowo	Wymagana data przyszła, gdy `duration_kind` to `until_date` .
ai_optimizer_enabled	body	boolean	nie	Przełącz optymalizację AI.
auto_include_new_members	body	boolean	nie	Przełącz automatyczne dołączanie.
language	body	string	nie	Kod języka docelowego.
industry_code_id	body	integer	nie	Id kodu branży.

Nazwa	Gdzie	Typ	Wymagane	Opis
end_action_type	body	string	nie	`nothing` | `redirect_to_course` | `message_page` | `redirect_to_url`.
end_action_url	body	string	warunkowo	Wymagany URL `http` / `https`, gdy `end_action_type` to `redirect_to_url`.
end_action_html	body	string	warunkowo	Wymagane, gdy `end_action_type` to `message_page`.
course_id	body	string	warunkowo	Prefiksowane id kursu (`course_…`); musi należeć do konta albo być globalne. Wymagane, gdy `end_action_type` to `redirect_to_course`.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "autopilot": { "intensity_count": 1, "intensity_period": "week" } }' \
  https://platform.phishspot.com/api/v1/autopilots/9
```

Odpowiedź `200 OK` — zaktualizowany obiekt autopilota (ten sam kształt co `GET /autopilots/:id`).

```
{
  "id": 9,
  "account_id": 11,
  "name": "Finance team — quarterly drip",
  "state": "running",
  "all_groups": false,
  "intensity_count": 1,
  "intensity_period": "week",
  "duration_kind": "continuous",
  "ai_optimizer_enabled": true,
  "auto_include_new_members": true,
  "language": "en",
  "end_action_type": "redirect_to_course",
  "end_action_url": null,
  "created_at": "2026-06-02T10:15:00Z",
  "updated_at": "2026-06-02T11:00:00Z",
  "ends_on": null,
  "started_at": "2026-06-02T10:16:00Z",
  "daily_rate": 0.14,
  "progress_percentage": 100,
  "course_id": 14,
  "editable": true,
  "groups": [
    { "id": 3, "name": "Finance" }
  ],
  "recent_campaigns": []
}
```


Kody statusu

Kod	Kiedy
200	Autopilot zaktualizowany.
400	Opakowanie treści `autopilot` jest całkowicie nieobecne.
403	Użytkownik tokenu jest `member` (tylko odczyt) **lub** autopilot jest `stopped` (zatrzymane autopiloty są tylko do odczytu — wyłącznie usunięcie).
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.
422	Walidacja nie powiodła się — te same przyczyny co przy tworzeniu (name, limit dziennego tempa, `ends_on`, wymagania akcji końcowej, nieznane `group_ids` / `course_id`).

`DELETE /autopilots/:id`

Trwale usuwa autopilot i jego powiązania z grupami; wygenerowane kampanie są odłączane (nie usuwane). Autopilotu w stanie `running` nie da się usunąć — najpierw go zatrzymaj. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor. Trasa płaska (bez `account_id`).

Brak parametrów poza tokenem bearer.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/autopilots/9
```

Odpowiedź `204 No Content` — puste ciało przy powodzeniu.

Kody statusu

Kod	Kiedy
204	Autopilot usunięty.
403	Użytkownik tokenu jest `member` (tylko odczyt) na koncie autopilotu.
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.
422	Autopilot jest `running` — zatrzymaj go przed usunięciem. (Autopilot `paused` lub `draft` można usunąć bezpośrednio.)

`POST /autopilots/:id/start`

Aktywuje autopilot: ustawia `state` na `running` (oznaczając `started_at` przy pierwszym uruchomieniu), aby platforma zaczęła generować i dostarczać kampanie ze skonfigurowaną kadencją. Użyj, aby przejść na żywo lub wznowić autopilot w stanie `paused`. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor — a autopilot musi być edytowalny (nie `stopped`). Trasa płaska.

> To akcja na żywo: udane wywołanie rozpoczyna wysyłkę prawdziwych symulowanych wiadomości phishingowych do wskazanych członków.

Brak parametrów poza tokenem bearer.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/autopilots/9/start
```

Odpowiedź `200 OK` — obiekt autopilota z `state: "running"` (ten sam kształt co `GET /autopilots/:id`).

```
{
  "id": 9,
  "name": "Finance team — quarterly drip",
  "state": "running",
  "started_at": "2026-06-02T10:16:00Z",
  "editable": true,
  "progress_percentage": 100,
  "daily_rate": 0.07
}
```

Kody statusu

Kod	Kiedy
200	Autopilot uruchomiony/wznowiony; teraz `running`.
403	Użytkownik tokenu jest `member` (tylko odczyt) **lub** autopilot jest `stopped` (zatrzymanego autopilotu nie można uruchomić ponownie).
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.

`POST /autopilots/:id/pause`

Wstrzymuje działający (`running`) autopilot: ustawia `state` na `paused`, więc nie są generowane nowe kampanie. Wznów później przez `start`. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor — a autopilot musi być edytowalny (nie `stopped`). Trasa płaska.

Brak parametrów poza tokenem bearer.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/autopilots/9/pause
```

Odpowiedź `200 OK` — obiekt autopilota z `state: "paused"` (ten sam kształt co `GET /autopilots/:id`).

```
{
  "id": 9,
  "name": "Finance team — quarterly drip",
  "state": "paused",
  "started_at": "2026-06-02T10:16:00Z",
  "editable": true,
  "progress_percentage": 92
}
```

Kody statusu

Kod	Kiedy
200	Autopilot wstrzymany.
403	Użytkownik tokenu jest `member` (tylko odczyt) **lub** autopilot jest `stopped`.
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.

`POST /autopilots/:id/stop`

Zatrzymuje autopilot na stałe: ustawia `state` na `stopped`. Zatrzymany autopilot staje się tylko do odczytu — nie można go już aktualizować, uruchamiać, wstrzymywać ani ponownie zatrzymywać, można go jedynie przeglądać lub usunąć. **Uwierzytelnianie:** Bearer; **rola:** admin/edytor — a autopilot musi być nadal edytowalny (nie już `stopped`). Trasa płaska.

Brak parametrów poza tokenem bearer.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id autopilotu (`auto_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/autopilots/9/stop
```

Odpowiedź `200 OK` — obiekt autopilota z `state: "stopped"` i `editable: false` (ten sam kształt co `GET /autopilots/:id`).

```
{
  "id": 9,
  "name": "Finance team — quarterly drip",
  "state": "stopped",
  "started_at": "2026-06-02T10:16:00Z",
  "editable": false,
  "progress_percentage": null
}
```

Kody statusu

Kod	Kiedy
200	Autopilot zatrzymany.
403	Użytkownik tokenu jest `member` (tylko odczyt) **lub** autopilot jest już `stopped`.
404	Brak autopilotu o tym id lub użytkownik tokenu nie ma aktywnego członkostwa w jego koncie.

27.11 Domeny wysyłkowe

Dwa powiązane zasoby kontrolują, z których domen może wysyłać kampania:

- **Domeny platformy** (`pdm_…`) to domeny atakującego/landingowe obsługiwane przez PhishSpot. Większość należy do platformy (“publiczne” lub przypisane “prywatne” domeny); klienci mogą też dostarczyć własne (BYOD) za pomocą `provision_byod`. Bezpośredni zapis rekordów domen platformy (`POST` / `PATCH` / `DELETE /platform_domains`) jest zarezerwowany dla użytkowników z rolą **admin**; provisioning domeny BYOD jest dostępny dla każdego członka konta.
- **Domeny zabezpieczone** (`sdm_…`) to dowody własności DNS. Klient dodaje domenę, którą kontroluje, umieszcza rekord TXT i weryfikuje go — w ten sposób PhishSpot potwierdza, że nadawca może wysyłać “z” tej domeny.

`GET /api/v1/platform_domains`

Zwraca listę wszystkich domen platformy widocznych dla konta wywołującego tokena — wszystkie operacyjne domeny publiczne oraz wszystkie operacyjne domeny prywatne przypisane do konta. Wyniki są uporządkowane według nazwy. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Brak parametrów poza tokenem bearer.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/platform_domains
```

Odpowiedź `200 OK` — tablica JSON obiektów domen platformy (każdy obiekt używa tych samych pól, co poniższy punkt końcowy show).

Pole	Typ	Opis
id	integer	Numeryczny identyfikator. (W adresach URL używaj identyfikatora z prefiksem `pdm_…`.)
name	string	Nazwa domeny (np. `officelogin.in`).
public	boolean	Starsza flaga publiczna z kolumny.
mail	boolean	Czy jest to domena pocztowa platformy.
state	string	Stan cyklu życia. Jeden z `pending`, `checking`, `confirmed`, `purchasing`, `purchased`, `configuring_dns`, `dns_pending`, `configuring_postal`, `active`, `failed`.
expires_on	string|null	Data wygaśnięcia rejestracji w formacie ISO8601 lub null.
metadata	object	Dowolny JSON (szczegóły provisioningu Cloudflare/Postal, diagnostyka itp.).
created_at	string	Znacznik czasu ISO8601.
updated_at	string	Znacznik czasu ISO8601.
active	boolean	True, gdy `state == "active"`.
byod	boolean	True dla rekordów klienta typu “bring your own domain”.
sending_blocked	boolean	True, gdy domena jest aktywna, ale zablokowana przed rozpoczęciem nowych wysyłek.
nameservers	array	Serwery nazw Cloudflare przypisane do strefy tej domeny (puste, dopóki nie zostaną przechwycone).
cloudflare_error	string|null	Ustawione, jeśli nie udało się utworzyć/odczytać strefy Cloudflare.


```
[
  {
    "id": 42,
    "name": "officelogin.in",
    "public": true,
    "mail": false,
    "state": "active",
    "expires_on": "2027-03-01T00:00:00.000Z",
    "metadata": {},
    "created_at": "2026-01-10T09:00:00.000Z",
    "updated_at": "2026-05-30T14:22:00.000Z",
    "active": true,
    "byod": false,
    "sending_blocked": false,
    "nameservers": [],
    "cloudflare_error": null
  }
]
```


Kody statusu

Kod	Kiedy
200	Domeny zwrócone (możliwe, że pusta tablica).

`GET /api/v1/platform_domains/:id`

Pobiera pojedynczą domenę platformy po identyfikatorze. Przydatne do sprawdzenia stanu, serwerów nazw BYOD oraz `sending_blocked` przed wybraniem jej do kampanii. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny platformy (`pdm_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/platform_domains/pdm_42
```

Odpowiedź `200 OK` — pojedynczy obiekt domeny platformy (te same pola, co powyższy punkt końcowy listy).


```
{
  "id": 42,
  "name": "officelogin.in",
  "public": true,
  "mail": false,
  "state": "active",
  "expires_on": "2027-03-01T00:00:00.000Z",
  "metadata": {},
  "created_at": "2026-01-10T09:00:00.000Z",
  "updated_at": "2026-05-30T14:22:00.000Z",
  "active": true,
  "byod": false,
  "sending_blocked": false,
  "nameservers": [],
  "cloudflare_error": null
}
```


Kody statusu

Kod	Kiedy
200	Domena znaleziona.
404	Brak domeny platformy o tym identyfikatorze.

`POST /api/v1/platform_domains`

Tworzy bezpośrednio rekord domeny należącej do platformy. Jest to operacja administracyjna służąca do zarządzania własną pulą domen platformy — klienci powinni zamiast tego używać `provision_byod`. **Uwierzytelnianie:** Bearer; **rola:** admin.

Parametry — opakowane w obiekt `platform_domain`.

Nazwa	Gdzie	Typ	Wymagane	Opis
platform_domain.name	body	string	tak	Nazwa domeny. Zamieniana na małe litery/przycinana; musi być prawidłową domeną (3–253 znaki, co najmniej jedna kropka, tylko `a–z 0–9 . –`, bez wiodącej/końcowej kropki ani myślnika, bez kolejnych `..` / `--`, etykiety ≤63 znaki). Musi być globalnie unikalna (bez rozróżniania wielkości liter).
platform_domain.public	body	boolean	nie	Starsza flaga publiczna.
platform_domain.metadata	body	object	nie	Dowolne metadane JSON.
platform_domain.expires_on	body	string	nie	Data wygaśnięcia rejestracji w formacie ISO8601.

```
`state`, `genre` i `source` nie są ustawialne przez API; rekord utworzony tutaj
domyślnie przyjmuje `state: "active"`, `genre: "public"`, `source: "manual"`.
```

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "platform_domain": { "name": "secure-portal.co", "public": true } }' \
  https://platform.phishspot.com/api/v1/platform_domains
```

Odpowiedź `201 Created` — utworzony obiekt domeny platformy (te same pola, co punkt końcowy show).

```
{
  "id": 77,
  "name": "secure-portal.co",
  "public": true,
  "mail": false,
  "state": "active",
  "expires_on": null,
  "metadata": {},
  "created_at": "2026-06-02T10:00:00.000Z",
  "updated_at": "2026-06-02T10:00:00.000Z",
  "active": true,
  "byod": false,
  "sending_blocked": false,
  "nameservers": [],
  "cloudflare_error": null
}
```


Kody statusu

Kod	Kiedy
201	Domena utworzona.
403	Wywołujący nie jest administratorem.
422	Walidacja nieudana (np. pusta/zduplikowana/nieprawidłowa `name`). Treść: `{ "errors": { "name": ["..."] } }`.

`PATCH /api/v1/platform_domains/:id`

Aktualizuje rekord domeny należącej do platformy. **Uwierzytelnianie:** Bearer; **rola:** admin.

Parametry — ta sama opakowana treść `platform_domain`, co przy tworzeniu; wszystkie pola opcjonalne.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny platformy (`pdm_…` lub liczba całkowita).
platform_domain.name	body	string	nie	Nowa nazwa domeny (te same reguły walidacji, co przy tworzeniu).
platform_domain.public	body	boolean	nie	Starsza flaga publiczna.
platform_domain.metadata	body	object	nie	Dowolne metadane JSON.
platform_domain.expires_on	body	string	nie	Data wygaśnięcia rejestracji w formacie ISO8601.

```
Zmiana nazwy lub inna aktualizacja domeny powiązanej z trwającą (zablokowaną) kampanią jest odrzucana na poziomie modelu (`ActiveRecord::RecordNotDestroyed`), co objawia się jako błąd z zakresu 500, a nie 422. Unikaj edytowania domen przypisanych do działających kampanii.
```

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "platform_domain": { "expires_on": "2028-01-01T00:00:00Z" } }' \
  https://platform.phishspot.com/api/v1/platform_domains/pdm_42
```

Odpowiedź `200 OK` — zaktualizowany obiekt domeny platformy (te same pola, co punkt końcowy show).

Kody statusu

Kod	Kiedy
200	Domena zaktualizowana.
403	Wywołujący nie jest administratorem.
404	Brak domeny platformy o tym identyfikatorze.
422	Walidacja nieudana. Treść: `{ "errors": { ... } }`.

`DELETE /api/v1/platform_domains/:id`

Usuwa domenę należącą do platformy. Domenę można usunąć tylko wtedy, gdy nie ma blokujących powiązań: domeny należące do platformy nie mogą mieć kampanii ani przypisanych kont; domeny BYOD nie mogą mieć aktywnych (trwających/wstrzymanych) kampanii. **Uwierzytelnianie:** Bearer; **rola:** admin.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny platformy (`pdm_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/platform_domains/pdm_42
```

Odpowiedź `204 No Content` — pusta treść przy powodzeniu.

Kody statusu

Kod	Kiedy
204	Domena usunięta.
403	Wywołujący nie jest administratorem.
404	Brak domeny platformy o tym identyfikatorze.
422	Domena nadal ma aktywne kampanie (lub inne blokujące powiązania). Treść: `{ "error": "Cannot delete platform domain with active campaigns" }`.

`POST /api/v1/platform_domains/:id/check`

Ponownie sprawdza stan provisioningu/kondycji BYOD domeny należącej do konta wywołującego, a następnie zwraca (przeładowaną) domenę. Użyj tego do odpytywania domeny BYOD po delegowaniu serwerów nazw: aktywna domena uruchamia kontrolę kondycji, a domena nadal w trakcie provisioningu odświeża swój status konfiguracji. Przejściowe błędy odświeżania są wyciszane, aby odpytywanie nigdy nie zwracało błędu — otrzymujesz po prostu ostatni utrwalony stan. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola), ale użytkownik tokena musi należeć do konta będącego właścicielem domeny.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny platformy (`pdm_…` lub liczba całkowita). Musi to być domena BYOD należąca do konta, do którego należy wywołujący.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/platform_domains/pdm_88/check
```

Odpowiedź `200 OK` — odświeżony obiekt domeny platformy (te same pola, co punkt końcowy show). Obserwuj `state`, `active`, `nameservers`, `sending_blocked` oraz `cloudflare_error`, aby śledzić postęp.

```
{
  "id": 88,
  "name": "mail.acme-customer.com",
  "public": false,
  "mail": false,
  "state": "dns_pending",
  "expires_on": null,
  "metadata": { "cloudflare_nameservers": ["kara.ns.cloudflare.com",
        "rob.ns.cloudflare.com"] },
  "created_at": "2026-06-01T08:00:00.000Z",
  "updated_at": "2026-06-02T09:30:00.000Z",
  "active": false,
  "byod": true,
  "sending_blocked": false,
  "nameservers": ["kara.ns.cloudflare.com", "rob.ns.cloudflare.com"],
  "cloudflare_error": null
}
```


Kody statusu

Kod	Kiedy
200	Status odświeżony i domena zwrócona.
404	Brak takiej domeny lub domena nie ma konta właściciela / wywołujący nie należy do jej konta właściciela.

`POST /api/v1/accounts/:account_id/platform_domains/provision_byod`

Provisionuje dla konta domenę wysyłkową klienta typu “bring your own domain” (BYOD). Tworzy prywatną domenę platformy BYOD w stanie provisioningu i zwraca serwery nazw Cloudflare, które właściciel domeny musi ustawić u swojego rejestratora; delegacja i weryfikacja kończą się następnie asynchronicznie (odpytuj za pomocą `POST /platform_domains/:id/check`). Idempotentne — ponowny provisioning domeny, którą konto już posiada, po prostu ponownie wyświetla jej serwery nazw. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola, ale wywołujący musi należeć do `account_id`.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita), do którego należy wywołujący.
domain_name	body	string	tak	Domena do provisioningu (np. `mail.acme-customer.com`). Zamieniana na małe litery/przycinana po stronie serwera. Nie opakowana w żaden obiekt — wysyłana jako klucz najwyższego poziomu.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "domain_name": "mail.acme-customer.com" }' \
  https://platform.phishspot.com/api/v1/accounts/11/platform_domains/provision_byod
```

Odpowiedź `201 Created` — wyprovisionowany obiekt domeny platformy wraz ze wskazówkami dotyczącymi provisioningu. Wszystkie pola domeny platformy z punktu końcowego show oraz dodatkowo:

Pole	Typ	Opis
nameservers	array	Serwery nazw Cloudflare, które właściciel domeny musi ustawić u swojego rejestratora. (Obecne także w obiekcie bazowym; powtórzone na najwyższym poziomie dla wygody.)
next_step	string	Czytelna dla człowieka instrukcja opisująca zmianę u rejestratora oraz punkt końcowy `check` do odpytywania.

```
{
  "id": 88,
  "name": "mail.acme-customer.com",
  "public": null,
  "mail": false,
  "state": "dns_pending",
  "expires_on": null,
  "metadata": { "cloudflare_nameservers": ["kara.ns.cloudflare.com",
        "rob.ns.cloudflare.com"] },
  "created_at": "2026-06-02T09:00:00.000Z",
  "updated_at": "2026-06-02T09:00:00.000Z",
  "active": false,
  "byod": true,
  "sending_blocked": false,
  "nameservers": ["kara.ns.cloudflare.com", "rob.ns.cloudflare.com"],
  "cloudflare_error": null,
  "next_step": "At the registrar for mail.acme-customer.com, replace the nameservers
        with the ones above, then poll POST /api/v1/platform_domains/pdm_88/check."
}
```

Kody statusu

Kod	Kiedy
201	Domena wyprovisionowana (lub ponownie wyświetlona, jeśli już należy do tego konta).
403	Wywołujący nie należy do `account_id` (odmowa Pundit `show?`).
404	`account_id` nie znaleziono wśród kont wywołującego. Treść: `{ "error": "Account not found" }`.

Kod	Kiedy
422	Provisioning odrzucony. Treść: `{ "error": "<message>" }`, jeden z: pusta nazwa (`"Domain name is required."`), już zarejestrowana przez inne konto (`"That domain is already registered in PhishSpot by another account."`) lub nieprawidłowa domena (`"That domain name is invalid."`).

`GET /api/v1/accounts/:account_id/secured_domains`

Zwraca listę zabezpieczonych (z potwierdzoną własnością) domen konta, od najnowszej. Opcjonalnie filtruje według stanu weryfikacji. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola, ale wywołujący musi należeć do `account_id`.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita), do którego należy wywołujący.
state	query	string	nie	Filtr według stanu weryfikacji. Jeden z `pending`, `verified`, `failed`. Pomiń, aby uzyskać wszystkie.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/secured_domains?state=verified"
```

Odpowiedź `200 OK` — tablica JSON obiektów domen zabezpieczonych.

Pole	Typ	Opis
id	integer	Numeryczny identyfikator. (W adresach URL używaj identyfikatora z prefiksem `sdm_…`.)
account_id	integer	Identyfikator konta będącego właścicielem.
domain	string	Weryfikowana domena (zamieniona na małe litery).
state	string	Stan weryfikacji: `pending`, `verified` lub `failed`.
verification_attempts	integer	Liczba wykonanych prób weryfikacji DNS.
verified_at	string|null	Znacznik czasu ISO8601 pomyślnej weryfikacji lub null.
created_at	string	Znacznik czasu ISO8601.
updated_at	string	Znacznik czasu ISO8601.

Pole	Typ	Opis
dns_record	object	Rekord TXT, który właściciel musi opublikować, aby udowodnić własność.
dns_record.type	string	Zawsze `"TXT"`.
dns_record.name	string	Host rekordu, np. `_phishspot-verify.example.com`.
dns_record.value	string	Wartość rekordu, np. `phishspot-verify=<64-hex-token>`.

```
[
  {
    "id": 5,
    "account_id": 11,
    "domain": "acme-customer.com",
    "state": "verified",
    "verification_attempts": 2,
    "verified_at": "2026-05-20T11:00:00.000Z",
    "created_at": "2026-05-19T16:30:00.000Z",
    "updated_at": "2026-05-20T11:00:00.000Z",
    "dns_record": {
      "type": "TXT",
      "name": "_phishspot-verify.acme-customer.com",
      "value": "phishspot-verify=3f9a...c2"
    }
  }
]
```

Kody statusu

Kod	Kiedy
200	Domeny zwrócone (możliwe, że pusta tablica).
403	Wywołujący nie należy do `account_id`.
404	`account_id` nie znaleziono wśród kont wywołującego. Treść: `{ "error": "Account not found" }`.

`POST /api/v1/accounts/:account_id/secured_domains`

Dodaje domenę kontrolowaną przez klienta i zwraca rekord TXT do opublikowania w celu weryfikacji własności. Domeny publicznych dostawców poczty (np. gmail.com) są odrzucane. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola, ale wywołujący musi należeć do `account_id`.

Parametry — opakowane w obiekt `secured_domain`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita), do którego należy wywołujący.
secured_domain.domain	body	string	tak	Domena do weryfikacji (np. `acme-customer.com`). Zamieniana na małe litery/przycinana; musi odpowiadać standardowemu formatowi domeny; musi być unikalna w obrębie konta (bez rozróżniania wielkości liter); nie może być zablokowaną domeną publicznego dostawcy poczty.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "secured_domain": { "domain": "acme-customer.com" } }' \
  https://platform.phishspot.com/api/v1/accounts/11/secured_domains
```

Odpowiedź `201 Created` — utworzony obiekt domeny zabezpieczonej (te same pola, co punkt końcowy listy), z `state: "pending"` oraz świeżo wygenerowanym `dns_record` do opublikowania.

```
{
  "id": 6,
  "account_id": 11,
  "domain": "acme-customer.com",
  "state": "pending",
  "verification_attempts": 0,
  "verified_at": null,
  "created_at": "2026-06-02T10:00:00.000Z",
  "updated_at": "2026-06-02T10:00:00.000Z",
  "dns_record": {
    "type": "TXT",
    "name": "_phishspot-verify.acme-customer.com",
    "value": "phishspot-verify=3f9a...c2"
  }
}
```

Kody statusu

Kod	Kiedy
201	Domena dodana; opublikuj zwrócony rekord TXT, a następnie wywołaj `verify_dns`.
403	Wywołujący nie należy do `account_id`.
404	`account_id` nie znaleziono wśród kont wywołującego. Treść: `{ "error": "Account not found" }`.

Kod	Kiedy
422	Walidacja nieudana — pusty/nieprawidłowy format, duplikat dla tego konta lub zablokowana domena publicznego dostawcy poczty. Treść: `{ "errors": { "domain": ["..."] } }`.

`GET /api/v1/secured_domains/:id`

Pobiera pojedynczą domenę zabezpieczoną po identyfikatorze, wraz z rekordem TXT potrzebnym do weryfikacji. Trasa płytka (nie zagnieżdżona pod kontem) — wywołujący musi należeć do konta będącego właścicielem. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola (członek konta).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny zabezpieczonej (`sdm_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/secured_domains/sdm_6
```

Odpowiedź `200 OK` — pojedynczy obiekt domeny zabezpieczonej (te same pola, co powyższy punkt końcowy listy).

Kody statusu

Kod	Kiedy
200	Domena znaleziona.
403	Odmowa Pundit (zwykle nie powinna wystąpić — polityka zezwala każdemu członkowi).
404	Brak takiej domeny lub wywołujący nie należy do konta będącego jej właścicielem.

`DELETE /api/v1/secured_domains/:id`

Usuwa domenę zabezpieczoną. Zablokowane, dopóki jakakolwiek aktywna (trwająca/wstrzymana) kampania wysyła z adresu e-mail w tej domenie. Trasa płytka — wywołujący musi należeć do konta będącego właścicielem. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola (członek konta).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny zabezpieczonej (`sdm_…` lub liczba całkowita).

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/secured_domains/sdm_6
```

Odpowiedź `204 No Content` — pusta treść przy powodzeniu.

Kody statusu

Kod	Kiedy
204	Domena usunięta.
403	Odmowa Pundit (zwykle nie powinna wystąpić).
404	Brak takiej domeny lub wywołujący nie należy do konta będącego jej właścicielem.
422	Domena jest zweryfikowana i używana przez aktywne kampanie. Treść: `{ "error": "Cannot delete secured domain <domain> while it is used by active campaigns: <campaign names>" }`.

`POST /api/v1/secured_domains/:id/verify_dns`

Uruchamia weryfikację DNS: wyszukuje oczekiwany rekord TXT dla domeny i, jeśli go znajdzie, oznacza domenę jako `verified`. Wywołaj to po opublikowaniu rekordu TXT zwróconego przy tworzeniu. Zwraca (przeładowaną) domenę, abyś mógł odczytać wynikowy `state`. Trasa płytka — wywołujący musi należeć do konta będącego właścicielem. **Uwierzytelnianie:** Bearer; **rola:** dowolna rola (członek konta).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator domeny zabezpieczonej (`sdm_…` lub liczba całkowita).

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/secured_domains/sdm_6/verify_dns
```

Odpowiedź `200 OK` — odświeżony obiekt domeny zabezpieczonej (te same pola, co punkt końcowy listy). Przy powodzeniu `state` zmienia się na `"verified"`, a `verified_at` zostaje ustawione; w przeciwnym razie pozostaje `pending` / `failed`, a `verification_attempts` wzrasta.

```
{
  "id": 6,
  "account_id": 11,
  "domain": "acme-customer.com",
  "state": "verified",
  "verification_attempts": 1,
  "verified_at": "2026-06-02T10:05:00.000Z",
  "created_at": "2026-06-02T10:00:00.000Z",
  "updated_at": "2026-06-02T10:05:00.000Z",
  "dns_record": {
    "type": "TXT",
    "name": "_phishspot-verify.acme-customer.com",
    "value": "phishspot-verify=3f9a...c2"
  }
}
```


Kody statusu

Kod	Kiedy
200	Weryfikacja przeprowadzona; sprawdź `state` w odpowiedzi.
403	Odmowa Pundit (zwykle nie powinna wystąpić).
404	Brak takiej domeny lub wywołujący nie należy do konta będącego jej właścicielem.

27.12 Zgłoszone wiadomości

Zgłoszone wiadomości to podejrzane e-maile, które pracownicy oznaczyli — przekazane do skrzynki zgłoszeń konta (`source: inbound_webhook`) albo przesłane przez dodatek do Outlooka (`source: outlook_addin`). Poniższe punkty końcowe odczytu zwracają **wyłącznie metadane** (nadawca, temat, data odebrania, źródło, zgłaszający) — nigdy treści wiadomości, nagłówków ani załączników. Są ograniczone do kont, do których należy użytkownik wywołującego tokenu.

`GET /accounts/:account_id/reported_messages`

Wyświetla listę zgłoszonych wiadomości dla jednego konta, od najnowszych (sortowanie po `received_at` malejąco). Użyj go, aby zasilić kolejkę do weryfikacji lub zsynchronizować zgłoszenia z narzędziami SOC. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita). Musi być kontem, do którego należy użytkownik tokenu.

Nazwa	Gdzie	Typ	Wymagane	Opis
source	query	string	nie	Filtruj według źródła zgłoszenia. Jedna z wartości `inbound_webhook`, `outlook_addin`. Nieznana wartość zwraca `422`. Pomiń, aby zwrócić wszystkie źródła.
limit	query	integer	nie	Rozmiar strony. Domyślnie `50`; ograniczony do zakresu `1` – `500` (wartości `<1` lub `0` przyjmują wartość `50`, wartości `>500` są ograniczane do `500`).
page	query	integer	nie	Numer strony liczony od 1. Domyślnie `1`; wartości poniżej `1` są traktowane jako `1`. Przesunięcie obliczane jest jako `(page - 1) * limit`.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/reported_messages?
        source=outlook_addin&limit=25&page=1"
```

Odpowiedź `200 OK` — tablica JSON obiektów metadanych zgłoszonych wiadomości (bez koperty). Każdy element zawiera następujące pola:

Pole	Typ	Opis
id	integer	Identyfikator zgłoszonej wiadomości.
account_id	integer	Identyfikator konta właściciela.
from_email	string	Adres nadawcy zgłoszonego e-maila.
from_name	string | null	Wyświetlana nazwa nadawcy, jeśli została przechwycona.
subject	string | null	Temat zgłoszonego e-maila.
message_id	string | null	Oryginalny `Message-ID` zgodny z RFC, jeśli został przechwycony.
source	string	Źródło zgłoszenia: `inbound_webhook` lub `outlook_addin`.
received_at	string (ISO 8601)	Kiedy oryginalny e-mail został odebrany.
created_at	string (ISO 8601)	Kiedy zgłoszenie zostało przyjęte do PhishSpot.
from_domain	string	Część domenowa adresu `from_email` zapisana małymi literami (tekst po `@`).
reporter_contact_email	string | null	E-mail odbiorcy z konta, który dokonał zgłoszenia (dopasowany po `from_email`); `null`, gdy nie istnieje pasujący odbiorca.

```
[
  {
    "id": 4821,
    "account_id": 11,
    "from_email": "billing@suspicious-invoice.example",
    "from_name": "Accounts Payable",
    "subject": "Overdue invoice — action required",
    "message_id": "<CADnf9x1@mail.suspicious-invoice.example>",
    "source": "outlook_addin",
    "received_at": "2026-05-28T09:14:00.000Z",
    "created_at": "2026-05-28T09:15:32.000Z",
    "from_domain": "suspicious-invoice.example",
    "reporter_contact_email": "jane.doe@acme.test"
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono zgłoszenia (tablica może być pusta).
403	Użytkownik tokenu jest autoryzowany, ale Pundit odmawia `AccountPolicy#show?` dla tego konta.
404	`account_id` nie jest kontem, do którego należy użytkownik tokenu (zwraca `{ "error": "Account not found" }`).
422	`source` jest podane, ale nie jest jednym z prawidłowych źródeł (zwraca `{ "error": "Unknown source …; valid sources: inbound_webhook, outlook_addin." }`).

`GET /reported_messages/:id`

Pobiera metadane pojedynczej zgłoszonej wiadomości. Jest to trasa **płytka** — przyjmuje identyfikator zgłoszenia bezpośrednio, bez segmentu ścieżki `account_id`. Izolacja kont jest wymuszana po stronie serwera: wyszukiwanie jest ograniczone do kont użytkownika tokenu, więc żądanie zgłoszenia z innego konta zwraca `404`. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator zgłoszonej wiadomości (`rep_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i identyfikatorem w ścieżce.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/reported_messages/rep_4821
```

Odpowiedź `200 OK` — pojedynczy obiekt metadanych zgłoszonej wiadomości z tymi samymi polami co jeden element tablicy indeksu:

Pole	Typ	Opis
id	integer	Identyfikator zgłoszonej wiadomości.
account_id	integer	Identyfikator konta właściciela.
from_email	string	Adres nadawcy zgłoszonego e-maila.
from_name	string | null	Wyświetlana nazwa nadawcy, jeśli została przechwycona.
subject	string | null	Temat zgłoszonego e-maila.
message_id	string | null	Oryginalny `Message-ID` zgodny z RFC, jeśli został przechwycony.
source	string	Źródło zgłoszenia: `inbound_webhook` lub `outlook_addin`.
received_at	string (ISO 8601)	Kiedy oryginalny e-mail został odebrany.
created_at	string (ISO 8601)	Kiedy zgłoszenie zostało przyjęte do PhishSpot.
from_domain	string	Część domenowa adresu `from_email` zapisana małymi literami.
reporter_contact_email	string | null	E-mail pasującego odbiorcy z konta lub `null`.

```
{
  "id": 4821,
  "account_id": 11,
  "from_email": "billing@suspicious-invoice.example",
  "from_name": "Accounts Payable",
  "subject": "Overdue invoice — action required",
  "message_id": "<CADnf9x1@mail.suspicious-invoice.example>",
  "source": "outlook_addin",
  "received_at": "2026-05-28T09:14:00.000Z",
  "created_at": "2026-05-28T09:15:32.000Z",
  "from_domain": "suspicious-invoice.example",
  "reporter_contact_email": "jane.doe@acme.test"
}
```

Kody statusu

Kod	Kiedy
200	Zgłoszenie zostało znalezione i zwrócone.
404	Nie istnieje zgłoszenie o tym identyfikatorze w obrębie kont użytkownika tokenu (zwraca `{ "error": "Resource not found" }`).

`POST /accounts/:account_id/reported_messages`

Tylko dodatek. Przyjmuje nowo zgłoszoną wiadomość z dodatku do Outlooka. Ten punkt końcowy **nie** używa zwykłego tokenu bearer API ani Pundita — wymaga tokenu uprawnień dodatku (`reported_messages:create`), którego przypięty `account_id` odpowiada `:account_id` w adresie URL. Standardowe integracje go nie wywołują; do odczytu służą dwa powyższe punkty końcowe. Treść jest opakowana w obiekt `reported_message` (dozwolone klucze: `from_email`, `from_name`, `subject`, `plain_body`, `html_body`, `received_at`, `message_id`, `headers` oraz tablica `attachments`), a pomyślne wywołanie zwraca `201 Created` z `{ "id": "rep_…", "url": "…" }`. Niezgodność uprawnień/konta zwraca `403`; błędy walidacji zwracają `422`.

> Proces przesyłania z dodatku (uprawnienia tokenu, parowanie i pełny kształt żądania) jest opisany osobno w rozdziale Zgłoszone wiadomości (przyjmowanie z dodatku). Do każdej integracji raportującej lub weryfikacyjnej używaj powyższych punktów końcowych odczytu.

Kody statusu

Kod	Kiedy
201	Zgłoszenie zostało utworzone.
403	Token nie ma uprawnienia `reported_messages:create` albo jego przypięty `account_id` nie odpowiada adresowi URL.
404	`account_id` nie odpowiada istniejącemu kontu (zwraca `{ "error": "Account not found" }`).
422	Usługa przyjmowania odrzuciła ładunek (zwraca `{ "error": "…" }`).

27.13 Biblioteka mediów

Biblioteka mediów przechowuje hostowane pliki graficzne i CSS dla konta. Prześlij plik raz, a następnie odwołuj się do zwróconego `url` w treści HTML wiadomości kampanii, na stronach docelowych i w szablonach. **Zawsze osadzaj hostowany `url`** — klienty pocztowe (Gmail, Outlook) usuwają wbudowane identyfikatory URI `data:`, więc obrazy osadzone jako base64 nie zostaną wyświetlone.

Dozwolone typy zawartości: `image/png`, `image/jpg`, `image/jpeg`, `image/gif`, `image/svg+xml` oraz `text/css`. Maksymalny rozmiar pliku to **5 MB**. Każdy element mediów musi mieć unikalną (bez rozróżniania wielkości liter) `name` w obrębie swojego konta.

Wszystkie punkty końcowe mediów mogą być używane przez dowolnego członka konta (bez ograniczenia do roli admin/edytor). Punkty końcowe kolekcji (`index`, `create`) są zagnieżdżone pod kontem; punkty końcowe pojedynczego elementu (`show`, `update`, `destroy`) są płytkie (`/media/:id`) i rozpoznają tylko media należące do jednego z kont użytkownika tokenu — wszystko inne zwraca `404`.

`GET /accounts/:account_id/media`

Wyświetla wszystkie elementy mediów dla konta, od najnowszego. Użyj go, aby znaleźć hostowany `url` pliku przed osadzeniem go w kampanii. **Uwierzytelnianie:** bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/media
```

Odpowiedź `200 OK` — tablica JSON obiektów mediów (każdy ma kształt opisany poniżej).

Pole	Typ	Opis
id	integer	Identyfikator elementu mediów.
account_id	integer	Identyfikator konta będącego właścicielem.
name	string	Nazwa wyświetlana (unikalna w obrębie konta, bez rozróżniania wielkości liter).
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
url	string|null	Adres URL hostowanego pliku (ścieżka względna); osadź go w HTML. `null`, jeśli żaden plik nie jest dołączony.
filename	string|null	Oryginalna nazwa przesłanego pliku.
content_type	string|null	Typ MIME, np. `image/png`.

```
[
  {
    "id": 42,
    "account_id": 11,
    "name": "phishing-logo",
    "created_at": "2026-06-02T10:15:00.000Z",
    "updated_at": "2026-06-02T10:15:00.000Z",
    "url": "/rails/active_storage/blobs/redirect/eyJfcmFpbHMi.../phishing-logo.png",
    "filename": "phishing-logo.png",
    "content_type": "image/png"
  }
]
```

Kody statusu

Kod	Kiedy
200	Zwrócono listę mediów.
404	`account_id` nie jest jednym z kont użytkownika tokenu.

`POST /accounts/:account_id/media`

Przesyła nowy plik do biblioteki mediów konta. **To żądanie jest typu `multipart/form-data`, a nie JSON** — plik jest wysyłany jako pole formularza, a nie jako ciąg base64 w treści JSON.
Uwierzytelnianie: bearer; **rola:** dowolny członek konta.

Parametry (pola formularza opakowane w obiekt `medium[...]`)

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Identyfikator konta (`acct_…` lub liczba całkowita).
medium[name]	body	string	tak	Nazwa wyświetlana; musi być unikalna (bez rozróżniania wielkości liter) w obrębie konta.
medium[attachment]	body	file	tak	Plik do przesłania. Musi być jednym z `image/png`, `image/jpg`, `image/jpeg`, `image/gif`, `image/svg+xml`, `text/css` oraz ≤ 5 MB.

Żądanie

Zwróć uwagę na flagi `-F` (multipart). **Nie** ustawiaj `Content-Type: application/json`; pozwól curl ustawić granicę multipart. Plik jest odczytywany z dysku za pomocą `@/path`.

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  -F "medium[name]=phishing-logo" \
  -F "medium[attachment]=@./phishing-logo.png;type=image/png" \
  https://platform.phishspot.com/api/v1/accounts/11/media
```

Odpowiedź `201 Created` — utworzony obiekt mediów (taki sam kształt jak element listy powyżej).

Pole	Typ	Opis
id	integer	Identyfikator nowego elementu mediów.
account_id	integer	Identyfikator konta będącego właścicielem.
name	string	Nazwa wyświetlana.
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
url	string	Adres URL hostowanego pliku — osadź go w treści HTML kampanii.

Pole	Typ	Opis
filename	string	Zapisana nazwa pliku.
content_type	string	Typ MIME przesłanego pliku.

```
{
  "id": 42,
  "account_id": 11,
  "name": "phishing-logo",
  "created_at": "2026-06-02T10:15:00.000Z",
  "updated_at": "2026-06-02T10:15:00.000Z",
  "url": "/rails/active_storage/blobs/redirect/eyJfcmFpbHMi.../phishing-logo.png",
  "filename": "phishing-logo.png",
  "content_type": "image/png"
}
```

> Poprzedź zwrócony względny `url` hostem swojej platformy (`https://platform.phishspot.com`), aby uzyskać bezwzględny, osiągalny z zewnątrz adres URL do użycia w treści HTML wiadomości e-mail.

Kody statusu

Kod	Kiedy
201	Utworzono media.
404	`account_id` nie jest jednym z kont użytkownika tokenu.
422	Walidacja nie powiodła się — brakująca/pusta `name`, zduplikowana `name` w koncie, brakujący `attachment`, niedozwolony typ zawartości lub plik większy niż 5 MB. Treść: `{ "errors": { … } }`.

Przykładowa treść `422` (brakujący załącznik):

```
{ "errors": { "attachment": ["can't be blank"] } }
```

`GET /media/:id`

Zwraca pojedynczy element mediów według identyfikatora. Rozpoznaje tylko media należące do jednego z kont użytkownika tokenu. **Uwierzytelnianie:** bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator elementu mediów (`med_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/media/42
```

Odpowiedź `200 OK` — obiekt mediów (te same pola co w odpowiedzi `POST` powyżej).

```
{
  "id": 42,
  "account_id": 11,
  "name": "phishing-logo",
  "created_at": "2026-06-02T10:15:00.000Z",
  "updated_at": "2026-06-02T10:15:00.000Z",
  "url": "/rails/active_storage/blobs/redirect/eyJfcmFpbHMi.../phishing-logo.png",
  "filename": "phishing-logo.png",
  "content_type": "image/png"
}
```

Kody statusu

Kod	Kiedy
200	Zwrócono element mediów.
404	Żaden element mediów o tym identyfikatorze nie należy do jednego z kont użytkownika tokenu.

`PATCH /media/:id`

Aktualizuje element mediów. W praktyce tylko `name` ma znaczenie; można też ponownie przesłać plik, wysyłając nowy `attachment` (multipart). **Uwierzytelnianie:** bearer; **rola:** dowolny członek konta.

Parametry (opakowane w obiekt `medium[...]`)

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator elementu mediów (`med_…` lub liczba całkowita).
medium[name]	body	string	nie	Nowa nazwa wyświetlana; musi pozostać unikalna (bez rozróżniania wielkości liter) w obrębie konta.
medium[attachment]	body	file	nie	Plik zastępczy (wysyłany jako multipart). Te same ograniczenia typu zawartości i 5 MB co przy tworzeniu.

Żądanie

Zmianę samej nazwy można wysłać jako JSON:

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{ "medium": { "name": "phishing-logo-v2" } }' \
  https://platform.phishspot.com/api/v1/media/42
```

Aby zastąpić plik, wyślij zamiast tego multipart (`-F "medium[attachment]=@./new.png;type=image/png"`).

Odpowiedź `200 OK` — zaktualizowany obiekt mediów (te same pola co w `show`).

```
{
  "id": 42,
  "account_id": 11,
  "name": "phishing-logo-v2",
  "created_at": "2026-06-02T10:15:00.000Z",
  "updated_at": "2026-06-02T11:02:00.000Z",
  "url": "/rails/active_storage/blobs/redirect/eyJfcmFpbHMi.../phishing-logo.png",
  "filename": "phishing-logo.png",
  "content_type": "image/png"
}
```

Kody statusu

Kod	Kiedy
200	Zaktualizowano media.
404	Żaden element mediów o tym identyfikatorze nie należy do jednego z kont użytkownika tokenu.
422	Walidacja nie powiodła się — pusta `name`, zduplikowana `name` lub (przy zastępowaniu pliku) niedozwolony typ zawartości / powyżej 5 MB. Treść: `{ "errors": { … } }`.

`DELETE /media/:id`

Trwale usuwa element mediów i dołączony do niego plik. Każda treść HTML kampanii nadal odwołująca się do `url` pliku przestanie działać, więc najpierw usuń odwołania. **Uwierzytelnianie:** bearer; **rola:** dowolny członek konta.

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Identyfikator elementu mediów (`med_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/media/42
```

Odpowiedź `204 No Content` — pusta treść.

Kody statusu

Kod	Kiedy
204	Usunięto media.
404	Żaden element mediów o tym identyfikatorze nie należy do jednego z kont użytkownika tokenu.

27.14 Webhooki

Zarządzaj subskrypcjami wychodzących webhooków i przeglądaj zdarzenia, które PhishSpot wygenerował dla konta. **Punkt końcowy** to adres URL, który rejestrujesz, aby otrzymywać podpisane żądania HTTP POST; **zdarzenie** to niezmienny zapis czegoś, co się wydarzyło (utworzono kampanię, usunięto odbiorcę itp.), rozsyłany do każdego włączonego punktu końcowego subskrybującego jego typ. Mechanikę dostarczania — harmonogram ponawiania, nagłówek HMAC `X-Webhook-Signature` oraz sposób jego weryfikacji za pomocą `signing_secret` — opisano w Dostarczanie webhooków i podpisy.

:::note[Punkty końcowe są globalne dla konta, a nie ograniczone do tenanta] `Webhook::Endpoint` i `Webhook::Event` nie są rekordami wielodostępowymi, dlatego płytkie trasy (`/webhooks/endpoints/:id`, `/webhooks/events/:id`) przyjmują bezpośrednio id rekordu i **nie** zawierają `account_id` w ścieżce. Autoryzacja jest nadal egzekwowana dla każdego rekordu: musisz być członkiem konta będącego właścicielem punktu końcowego/zdarzenia, w przeciwnym razie otrzymasz `403`. Segment `:id` akceptuje zarówno id z prefiksem (`whep_…`), jak i surową liczbę całkowitą. :::

Dostępne wartości `event_type_ids`. Punkt końcowy subskrybuje, wymieniając jeden lub więcej z tych ciągów. Te same ciągi pojawiają się jako `event_type` w emitowanych zdarzeniach:

Typ zdarzenia	Wyzwalane gdy
`campaign.created`	Utworzono kampanię.
`campaign.updated`	Zaktualizowano kampanię.
`campaign.deleted`	Usunięto kampanię.
`contact.created`	Dodano odbiorcę.
`contact.updated`	Zaktualizowano odbiorcę.
`contact.deleted`	Usunięto odbiorcę.
`deliverable.created`	Utworzono pozycję dostarczenia kampanii (wysyłka do jednego odbiorcy).
`deliverable.updated`	Pozycja dostarczenia zmienia stan (wysłana, otwarta, kliknięta itp.).

Typ zdarzenia	Wyzwalane gdy
`spam_whitelist.updated`	Zmienia się migawka listy spamu/dozwolonych nadawców konta.

`GET /accounts/:account_id/webhooks/endpoints`

Wyświetla każdy punkt końcowy webhooka zarejestrowany na koncie, od najnowszych. Użyj tego, aby wyrenderować interfejs zarządzania lub uzgodnić lokalną konfigurację. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/accounts/11/webhooks/endpoints
```

Odpowiedź `200 OK` — tablica JSON obiektów punktów końcowych. `signing_secret` jest **pomijany** w tym widoku listy (jest zwracany wyłącznie w widokach pojedynczego punktu końcowego).

Pole	Typ	Opis
id	integer	Id punktu końcowego. Segment ścieżki/widoku akceptuje również formę z prefiksem `whep_…` .
account_id	integer	Id konta będącego właścicielem.
name	string	Czytelna etykieta punktu końcowego.
url	string	Docelowy adres URL, który otrzymuje żądania POST.
event_type_ids	array of string	Subskrybowane typy zdarzeń (zobacz tabelę powyżej).
enabled	boolean	Czy dostarczenia są obecnie wysyłane.
api_version	integer	Wersja schematu treści (obecnie `1`).
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
total_deliveries	integer	Liczba wszystkich rekordów dostarczenia dla tego punktu końcowego.
successful_deliveries	integer	Liczba dostarczeń w statusie `delivered` .
failed_deliveries	integer	Liczba dostarczeń w statusie `failed` .

```
[
  {
    "id": 42,
    "account_id": 11,
    "name": "Production listener",
    "url": "https://hooks.example.com/phishspot",
    "event_type_ids": ["campaign.created", "deliverable.updated"],
    "enabled": true,
    "api_version": 1,
    "created_at": "2026-05-30T09:14:22Z",
    "updated_at": "2026-06-01T12:03:10Z",
    "total_deliveries": 128,
    "successful_deliveries": 121,
    "failed_deliveries": 7
  }
]
```


Kody statusu

Kod	Kiedy
200	Zwrócono punkty końcowe (pusta tablica, jeśli brak).
403	Wywołujący nie jest członkiem `account_id`.
404	`account_id` nie istnieje lub wywołujący nie jest członkiem.

`POST /accounts/:account_id/webhooks/endpoints`

Rejestruje nowy punkt końcowy webhooka. Odpowiedź zawiera `signing_secret` **dokładnie raz** — zapisz go natychmiast, ponieważ jest potrzebny do weryfikacji podpisów dostarczeń i nigdy więcej nie jest pokazywany w całości, z wyjątkiem operacji `show` / `update` / `toggle` na tym samym punkcie końcowym. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — wystarczy członkostwo w koncie).

:::caution[Punkty końcowe startują wyłączone, chyba że wybierzesz inaczej] Nowo utworzony punkt końcowy domyślnie ma `enabled: true` w modelu, ale przekaż `enabled: false`, aby zarejestrować go jako uśpiony i włączyć go później za pomocą punktu końcowego toggle, gdy zweryfikujesz swój odbiornik. `url` jest walidowany pod kątem bezpieczeństwa: akceptowane są wyłącznie schematy `http` / `https`, a adresy URL wskazujące na `localhost`, `127.0.0.1`, `::1`, zakresy IP RFC 1918 / link-local / loopback / unique-local lub dowolny host `*.phishspot.com` są odrzucane z kodem `422`. :::

Parametry

Parametry treści są opakowane w obiekt `webhook_endpoint`.

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).

Nazwa	Gdzie	Typ	Wymagane	Opis
webhook_endpoint.name	body	string	tak	Czytelna etykieta. Walidowana pod kątem obecności.
webhook_endpoint.url	body	string	tak	Docelowy adres URL. Musi być prawidłowym adresem URL `http` / `https` i przejść opisane powyżej kontrole bezpieczeństwa.
webhook_endpoint.event_type_ids	body	array of string	tak	Jeden lub więcej typów zdarzeń do subskrybowania (zobacz tabelę). Walidowane pod kątem obecności — wymagany co najmniej jeden.
webhook_endpoint.enabled	body	boolean	nie	Czy punkt końcowy ma startować jako włączony. Domyślnie `true`.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{
        "webhook_endpoint": {
          "name": "Production listener",
          "url": "https://hooks.example.com/phishspot",
          "event_type_ids": ["campaign.created", "deliverable.updated"],
          "enabled": false
        }
      }' \
  https://platform.phishspot.com/api/v1/accounts/11/webhooks/endpoints
```

Odpowiedź `201 Created` — utworzony punkt końcowy, w tym jednorazowy `signing_secret`. Pola są takie same jak w widoku listy, plus `signing_secret`:

Pole	Typ	Opis
id	integer	Id punktu końcowego.
account_id	integer	Id konta będącego właścicielem.
name	string	Czytelna etykieta.
url	string	Docelowy adres URL (przycięty/znormalizowany).
event_type_ids	array of string	Subskrybowane typy zdarzeń.
enabled	boolean	Czy dostarczenia są aktywne.
api_version	integer	Wersja schematu treści (`1`).
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.

Pole	Typ	Opis
signing_secret	string	64-znakowy sekret HMAC w formacie hex. **Zwracany tutaj — zapisz go teraz.**
total_deliveries	integer	`0` dla nowego punktu końcowego.
successful_deliveries	integer	`0` dla nowego punktu końcowego.
failed_deliveries	integer	`0` dla nowego punktu końcowego.


```
{
  "id": 42,
  "account_id": 11,
  "name": "Production listener",
  "url": "https://hooks.example.com/phishspot",
  "event_type_ids": ["campaign.created", "deliverable.updated"],
  "enabled": false,
  "api_version": 1,
  "created_at": "2026-06-02T10:00:00Z",
  "updated_at": "2026-06-02T10:00:00Z",
  "signing_secret": "9f2c1e7b4a6d8f0c3e5a7b9d1f3c5e7a9b1d3f5c7e9a1b3d5f7c9e1a3b5d7f9c",
  "total_deliveries": 0,
  "successful_deliveries": 0,
  "failed_deliveries": 0
}
```


Kody statusu

Kod	Kiedy
201	Utworzono punkt końcowy.
403	Wywołujący nie jest członkiem `account_id`.
404	`account_id` nie istnieje lub wywołujący nie jest członkiem.
422	Walidacja nie powiodła się — brak `name` / `url` / `event_type_ids`, nieprawidłowy adres URL lub adres URL wskazujący na localhost / prywatny IP / host `*.phishspot.com`.

`GET /webhooks/endpoints/:id`

Pobiera pojedynczy punkt końcowy, w tym jego pełny `signing_secret` i statystyki dostarczeń z całego okresu. Użyj tego, aby ponownie odczytać sekret, jeśli go zgubisz, lub aby monitorować kondycję dostarczeń. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — musisz być członkiem konta będącego właścicielem).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id punktu końcowego (`whep_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i id w ścieżce.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/webhooks/endpoints/whep_8xk2p9
```

Odpowiedź `200 OK` — jeden obiekt punktu końcowego z tymi samymi polami co odpowiedź na tworzenie (zawiera `signing_secret`).

```
{
  "id": 42,
  "account_id": 11,
  "name": "Production listener",
  "url": "https://hooks.example.com/phishspot",
  "event_type_ids": ["campaign.created", "deliverable.updated"],
  "enabled": true,
  "api_version": 1,
  "created_at": "2026-05-30T09:14:22Z",
  "updated_at": "2026-06-01T12:03:10Z",
  "signing_secret": "9f2c1e7b4a6d8f0c3e5a7b9d1f3c5e7a9b1d3f5c7e9a1b3d5f7c9e1a3b5d7f9c",
  "total_deliveries": 128,
  "successful_deliveries": 121,
  "failed_deliveries": 7
}
```

Kody statusu

Kod	Kiedy
200	Zwrócono punkt końcowy.
403	Wywołujący nie jest członkiem konta będącego właścicielem punktu końcowego.
404	Brak punktu końcowego o tym id.

`PATCH /webhooks/endpoints/:id`

Aktualizuje nazwę punktu końcowego, adres URL, subskrybowane typy zdarzeń lub flagę włączenia. `signing_secret` nie jest regenerowany i nie może zostać zmieniony za pomocą tego wywołania. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — musisz być członkiem konta będącego właścicielem).

Parametry

Parametry treści są opakowane w obiekt `webhook_endpoint`; wyślij tylko te pola, które chcesz zmienić.

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id punktu końcowego (`whep_…` lub liczba całkowita).
webhook_endpoint.name	body	string	nie	Nowa etykieta. Nie może zostać wyczyszczona (walidowana pod kątem obecności).
webhook_endpoint.url	body	string	nie	Nowy docelowy adres URL. Ponownie walidowany pod kątem bezpieczeństwa (te same reguły co przy tworzeniu).
webhook_endpoint.event_type_ids	body	array of string	nie	Zastępczy zestaw subskrybowanych typów zdarzeń. Nie może zostać opróżniony.
webhook_endpoint.enabled	body	boolean	nie	Włącz/wyłącz.

Żądanie

```
curl -X PATCH -H "Authorization: Bearer $TOKEN" -H "Content-Type: application/json" \
  -d '{
        "webhook_endpoint": {
          "event_type_ids": ["campaign.created", "campaign.updated", "campaign.deleted"]
        }
      }' \
  https://platform.phishspot.com/api/v1/webhooks/endpoints/whep_8xk2p9
```

Odpowiedź `200 OK` — zaktualizowany obiekt punktu końcowego (te same pola co `show`, w tym `signing_secret`).

```
{
  "id": 42,
  "account_id": 11,
  "name": "Production listener",
  "url": "https://hooks.example.com/phishspot",
  "event_type_ids": ["campaign.created", "campaign.updated", "campaign.deleted"],
  "enabled": true,
  "api_version": 1,
  "created_at": "2026-05-30T09:14:22Z",
  "updated_at": "2026-06-02T11:20:45Z",
  "signing_secret": "9f2c1e7b4a6d8f0c3e5a7b9d1f3c5e7a9b1d3f5c7e9a1b3d5f7c9e1a3b5d7f9c",
  "total_deliveries": 128,
  "successful_deliveries": 121,
  "failed_deliveries": 7
}
```


Kody statusu

Kod	Kiedy
200	Zaktualizowano punkt końcowy.
403	Wywołujący nie jest członkiem konta będącego właścicielem.
404	Brak punktu końcowego o tym id.
422	Walidacja nie powiodła się — pusty `name`, pusty `event_type_ids` lub nieprawidłowy/niebezpieczny `url`.

`DELETE /webhooks/endpoints/:id`

Trwale usuwa punkt końcowy i wszystkie jego rekordy dostarczenia. Same zdarzenia nie są usuwane. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — musisz być członkiem konta będącego właścicielem).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id punktu końcowego (`whep_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i id w ścieżce.

Żądanie

```
curl -X DELETE -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/webhooks/endpoints/whep_8xk2p9
```

Odpowiedź `204 No Content` — pusta treść w przypadku powodzenia.

Kody statusu

Kod	Kiedy
204	Usunięto punkt końcowy.
403	Wywołujący nie jest członkiem konta będącego właścicielem.
404	Brak punktu końcowego o tym id.

`POST /webhooks/endpoints/:id/toggle`

Przełącza flagę `enabled` punktu końcowego — włącza wyłączony punkt końcowy lub wyłącza włączony. Użyj tego, aby wstrzymać/wznowić dostarczenia bez usuwania punktu końcowego ani utraty jego sekretu. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — musisz być członkiem konta będącego właścicielem).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id punktu końcowego (`whep_…` lub liczba całkowita).

Brak parametrów poza tokenem bearer i id w ścieżce — nowy stan jest wyprowadzany z bieżącego.

Żądanie

```
curl -X POST -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/webhooks/endpoints/whep_8xk2p9/toggle
```

Odpowiedź `200 OK` — punkt końcowy z przełączoną wartością `enabled` (te same pola co `show`, w tym `signing_secret`).

```
{
  "id": 42,
  "account_id": 11,
  "name": "Production listener",
  "url": "https://hooks.example.com/phishspot",
  "event_type_ids": ["campaign.created", "deliverable.updated"],
  "enabled": false,
  "api_version": 1,
  "created_at": "2026-05-30T09:14:22Z",
  "updated_at": "2026-06-02T11:30:00Z",
  "signing_secret": "9f2c1e7b4a6d8f0c3e5a7b9d1f3c5e7a9b1d3f5c7e9a1b3d5f7c9e1a3b5d7f9c",
  "total_deliveries": 128,
  "successful_deliveries": 121,
  "failed_deliveries": 7
}
```

Kody statusu

Kod	Kiedy
200	Stan przełączony; zwrócono zaktualizowany punkt końcowy.
403	Wywołujący nie jest członkiem konta będącego właścicielem.
404	Brak punktu końcowego o tym id.

`GET /accounts/:account_id/webhooks/events`

Wyświetla zdarzenia wygenerowane dla konta, od najnowszych, ze stronicowaniem. Każde zdarzenie rejestruje, co się wydarzyło, i dołącza liczby dostarczeń przypadające na zdarzenie. Użyj tego, aby skontrolować, co PhishSpot próbował wysłać, niezależnie od jakiegokolwiek pojedynczego punktu końcowego. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
account_id	path	string	tak	Id konta (`acct_…` lub liczba całkowita).
event_type	query	string	nie	Filtruj do pojedynczego typu zdarzenia (np. `deliverable.updated`). Pomiń, aby uwzględnić wszystkie typy.
page	query	integer	nie	Numer strony. Domyślnie `1`.
per_page	query	integer	nie	Liczba elementów na stronę. Domyślnie `50`.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  "https://platform.phishspot.com/api/v1/accounts/11/webhooks/events?
        event_type=deliverable.updated&page=1&per_page=50"
```

Odpowiedź `200 OK` — tablica JSON obiektów zdarzeń.

Pole	Typ	Opis
id	integer	Id zdarzenia. Segment widoku akceptuje również formę z prefiksem/surową.
account_id	integer	Id konta będącego właścicielem.
subject_id	integer	Id rekordu, którego dotyczy zdarzenie (kampania, odbiorca, pozycja dostarczenia, …).
subject_type	string	Nazwa klasy podmiotu (np. `Campaign`, `Contact`, `Deliverable`).
event_type	string	Jeden z typów zdarzeń z tabeli powyżej.
api_version	integer	Wersja schematu treści (`1`).

Pole	Typ	Opis
uuid	string	Stabilne unikalne id tego zdarzenia (używane również jako `payload.id`).
created_at	string	Znacznik czasu ISO 8601.
updated_at	string	Znacznik czasu ISO 8601.
data	object	Dane specyficzne dla zdarzenia opisujące zmianę (kształt różni się w zależności od `event_type`).
payload	object	Dokładna treść JSON dostarczana do punktów końcowych (zobacz poniżej).
deliveries	object	Liczby dostarczeń przypadające na zdarzenie.
deliveries.total	integer	Wszystkie rekordy dostarczenia dla tego zdarzenia.
deliveries.delivered	integer	Dostarczenia w statusie `delivered`.
deliveries.failed	integer	Dostarczenia w statusie `failed`.
deliveries.pending	integer	Dostarczenia w statusie `pending`.

Obiekt `payload` to dokładnie to, co otrzymują odbiorniki, o następującym kształcie: `id` (`uuid` zdarzenia), `type` (`event_type`), `created_at` (ISO 8601), `data` (takie samo jak `data` na najwyższym poziomie) oraz `api_version`.

```
[
  {
    "id": 9001,
    "account_id": 11,
    "subject_id": 305,
    "subject_type": "Deliverable",
    "event_type": "deliverable.updated",
    "api_version": 1,
    "uuid": "3f1c8a02-7d4e-4b9a-9c1e-2a6b5d8f0e11",
    "created_at": "2026-06-02T09:58:12Z",
    "updated_at": "2026-06-02T09:58:12Z",
    "data": { "deliverable_id": "dlv_4k2m", "state": "clicked" },
    "payload": {
      "id": "3f1c8a02-7d4e-4b9a-9c1e-2a6b5d8f0e11",
      "type": "deliverable.updated",
      "created_at": "2026-06-02T09:58:12Z",
      "data": { "deliverable_id": "dlv_4k2m", "state": "clicked" },
      "api_version": 1
    },
    "deliveries": { "total": 2, "delivered": 1, "failed": 0, "pending": 1 }
  }
]
```

Kody statusu

Kod	Kiedy
200	Zwrócono zdarzenia (pusta tablica, jeśli żadne nie pasuje).
403	Wywołujący nie jest członkiem `account_id`.
404	`account_id` nie istnieje lub wywołujący nie jest członkiem.

`GET /webhooks/events/:id`

Pobiera pojedyncze zdarzenie po id, w tym jego pełne `data`, dostarczony `payload` oraz liczby dostarczeń. Użyj tego, aby sprawdzić dokładnie, co zostało wysłane w przypadku jednego wystąpienia. **Uwierzytelnianie:** Bearer; **rola:** odczyt (dowolna rola — musisz być członkiem konta będącego właścicielem).

Parametry

Nazwa	Gdzie	Typ	Wymagane	Opis
id	path	string	tak	Id zdarzenia (z prefiksem lub surowa liczba całkowita).

Brak parametrów poza tokenem bearer i id w ścieżce.

Żądanie

```
curl -H "Authorization: Bearer $TOKEN" \
  https://platform.phishspot.com/api/v1/webhooks/events/9001
```

Odpowiedź `200 OK` — jeden obiekt zdarzenia, o identycznym kształcie jak pojedynczy element tablicy indeksu powyżej.

```
{
  "id": 9001,
  "account_id": 11,
  "subject_id": 305,
  "subject_type": "Deliverable",
  "event_type": "deliverable.updated",
  "api_version": 1,
  "uuid": "3f1c8a02-7d4e-4b9a-9c1e-2a6b5d8f0e11",
  "created_at": "2026-06-02T09:58:12Z",
  "updated_at": "2026-06-02T09:58:12Z",
  "data": { "deliverable_id": "dlv_4k2m", "state": "clicked" },
  "payload": {
    "id": "3f1c8a02-7d4e-4b9a-9c1e-2a6b5d8f0e11",
    "type": "deliverable.updated",
    "created_at": "2026-06-02T09:58:12Z",
    "data": { "deliverable_id": "dlv_4k2m", "state": "clicked" },
    "api_version": 1
  },
  "deliveries": { "total": 2, "delivered": 1, "failed": 0, "pending": 1 }
}
```


Kody statusu

Kod	Kiedy
200	Zwrócono zdarzenie.
403	Wywołujący nie jest członkiem konta będącego właścicielem zdarzenia.
404	Brak zdarzenia o tym id.

27.15 Wersja dodatku Outlook (publiczna)

`GET /outlook/version`

Zwraca metadane bieżącego wydania dodatku Outlook. **Nie wymaga uwierzytelniania.** Buforowane na ~5 minut.

Parametry: brak.

```
curl https://platform.phishspot.com/api/v1/outlook/version
```

Odpowiedź `200 OK`

Pole	Typ	Opis
`latest`	string	Najnowsza wersja dodatku.
`min_supported`	string	Najstarsza wersja, która nadal może być uruchamiana.

Pole	Typ	Opis
`bundle_filename`	string	Nazwa pliku pakietu sideload.
`bundle_sha256`	string	SHA-256 pakietu.

```
{ "latest": "1.1.0", "min_supported": "1.0.0", "bundle_filename": "phishspot-outlook-
        sideload-v1.1.0.zip", "bundle_sha256": "…" }
```

Przydatne dla narzędzi inwentaryzacyjnych weryfikujących, którą wersję dodatku powinny uruchamiać Twoje urządzenia. Zobacz Rozdział 20.

27.16 Pobieranie białej listy antyspamowej (osobny system tokenów)

Samoobsługowy URL dla administratora poczty z Rozdziału 22 korzysta z innego schematu — 64-znakowego tokenu osadzonego w ścieżce, **bez** nagłówka `Authorization`:

`GET /integrations/spam/:token/:format`

Nazwa	Gdzie	Typ	Wymagane	Opis
`token`	path	string (64 hex)	tak	Token białej listy z panelu Integracje.
`format`	path	enum	nie	Jeden z `txt` (domyślny), `json`, `csv`, `md`, `microsoft365`, `google-workspace`, `mimecast`, `proofpoint`, `postfix`, `spamassassin`.

Posiadanie URL-a jest jedynym poświadczeniem — traktuj go jak hasło i rotuj z poziomu **Ustawienia konta → Integracje → Biała lista filtra antyspamowego**, jeśli wycieknie.

27.17 Limity zapytań

Throttling Rack::Attack obowiązuje per źródłowe IP dla punktów końcowych bez uwierzytelniania oraz per token dla tych uwierzytelnionych:

Powierzchnia	Limit
Generowanie kodu parowania Outlook	10 / minutę / IP
Odpytywanie kodu parowania Outlook	60 / minutę / IP
Przyjmowanie zgłoszeń phishingowych (dodatek)	30 / minutę / IP
Pobieranie białej listy antyspamowej	60 / minutę / token

Przekroczenie limitu zwraca `429 Too Many Requests` z nagłówkiem `Retry-After`. Ogólne uwierzytelnione API nie podlega innym limitom zapytań poza ochroną przed nadużyciami na poziomie

infrastruktury; utrzymuj użycie poniżej kilkuset żądań/minutę/token lub skontaktuj się z nami, aby je zwiększyć.

27.18 Odsyłacze

- Tworzenie i zarządzanie tokenami API w panelu administracyjnym: Rozdział 14 Tokeny API.
- Sterowanie tymi samymi funkcjami z klienta AI za pomocą języka naturalnego: Rozdział 29 Serwer MCP.
- Odpowiednik tych punktów końcowych oparty na powiadomieniach push zamiast odpytywania: Rozdział 26 Webhooki.
- Punkt końcowy białej listy antyspamowej w kontekście: Rozdział 22 Biała lista filtra antyspamowego.
- Dodatek Outlook korzystający z `outlook/version`: Rozdział 20 Dodatek Outlook.

Entra ID: ryzyka i kompromisy przed połączeniem

PhishSpot umie połączyć się z Microsoft Entra ID (dawniej Azure AD) i pobierać użytkowników oraz grupy bezpośrednio z Twojego katalogu — opisuje to Rozdział 25 Synchronizacja katalogu. Wspieramy tę integrację, klienci używają jej na produkcji, działa zgodnie z dokumentacją.

Ten rozdział istnieje dlatego, że w przypadku większości organizacji **nie uważamy, że powinieneś jej włączać.** Nadanie scope'ów odczytu katalogu zewnętrznemu dostawcy SaaS to nie drobiazg, a korzyść w wygodzie jest mniejsza niż się wydaje, gdy policzysz pracę operacyjną, bezpieczeństwa i compliance, którą to faktycznie generuje. Prostsza alternatywa — kwartalny import z CSV — spełnia każdą realistyczną potrzebę programu symulacji phishingowych, przy ułamku ryzyka.

Przeczytaj zanim klikniesz **Połącz z Microsoft**. Jeśli już połączyłeś, przeczytaj przed kolejnym przeglądem nadanych zgód OAuth.

28.1 Krótko — co polecamy

- **Rekomendacja domyślna: nie podłączaj Entra ID.** Użyj importu z CSV ze swojego systemu HR — patrz Rozdział 5 Kontakty i operacje masowe w §5.6.
- **Trzy powody w jednym tchu:** (1) zgoda OAuth rozszerza Twoją powierzchnię ataku, dając PhishSpot dostęp do odczytu całego katalogu; (2) integracja sprzęga Twój program phishingowy z dostępnością Microsoft i decyzjami polityki Twojego tenanta; (3) platforma do symulacji phishingu, która uczy pracowników podejrzliwości wobec promptów MS, sama nie powinna być promptem MS.
- **Jeśli mimo to podłączasz:** review scope'ów z security team, wpis do rejestru przetwarzania u DPO, time-boxed zgoda OAuth i ponowny audyt co sześć miesięcy. Patrz §28.9.

28.2 Co właściwie przyznajesz łącząc Entra

Połączenie Entra w PhishSpot żąda trzech scope'ów Microsoft Graph podczas zgody administracyjnej:

- `User.Read.All` — odczyt **pełnego** obiektu użytkownika dla każdego konta w tenancie.
- `Group.Read.All` — odczyt każdej definicji grupy security i Microsoft 365.
- `Directory.Read.All` — odczyt członkostwa w grupach i danych katalogowych organizacji.

PhishSpot używa małego wycinka tego — email, imię/nazwisko, stanowisko, dział, lokalizacja, telefon, flaga `accountEnabled` i członkostwo w grupach. Reszty nie tyka. Ale scope to **odczyt wszystkiego**: telefonu komórkowego, łańcucha menedżerów, przypisanych licencji, ustawień skrzynki, metadanych logowań i kilkudziesięciu innych atrybutów, które Entra wystawia per użytkownik. Token OAuth, który PhishSpot zapisuje po zgodzie admina, może pobrać dowolne z tych pól, w dowolnym momencie, dopóki go nie cofniesz.

Import CSV odwraca tę logikę. To Ty wybierasz, które kolumny wyeksportować ze swojego systemu HR (`first_name, last_name, email, department, title`). Nic poza tym nie trafia do PhishSpot — nie dlatego, że odmówilibyśmy, ale dlatego, że tego nie wysłałeś.

To jest **zasada minimalizacji danych** z art. 5 ust. 1 lit. c RODO: dane osobowe muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane". Nadanie `Directory.Read.All` w celu „prowadzenie symulacji phishingu" jest na pierwszy rzut oka trudne do obrony.

28.3 Bezpieczeństwo — rozszerzenie powierzchni ataku

Tutaj nakładają się trzy sub-argumenty.

Token OAuth rozszerza Twoją powierzchnię ataku. PhishSpot przechowuje w swojej bazie tenant-scoped token Microsoft Graph. Jeśli PhishSpot zostanie skompromitowany — luka w naszym kodzie, źle skonfigurowany zasób chmurowy, błąd uprzywilejowanego użytkownika po naszej stronie — atakujący odchodzi z dostępem read-only do **Twojego** katalogu. Zanim się połączyłeś, Twój katalog był chroniony przez Twój własny perimeter bezpieczeństwa. Po — jest chroniony też przez nasz. Podwoiłeś liczbę organizacji, które muszą pozostać bezpieczne, żeby Twój katalog pozostał prywatny.

Ironia symulacji phishingowych. Cały sens PhishSpot to uczenie pracowników podejrzliwości wobec nieoczekiwanych promptów Microsoft: maila „Twoje hasło wygasa dziś", linku „Kliknij aby zobaczyć udostępniony dokument w OneDrive", niespodziewanego ekranu logowania. Prosząc użytkowników o SSO przez Microsoft, by mieli dostęp do **naszej** platformy, trenujemy ich w przeciwnym kierunku — że MS-brandowany prompt logowania, w kontekście phishspot.com, jest normalny i oczekiwany. Zbudowaliśmy konia trojańskiego, przed którym ostrzega nasze własne szkolenie. (Ta ironia dotyczy mocniej Rozdziału 24 Logowanie przez Microsoft 365; ta sama zasada jest istotna tutaj, bo integracja Entra i SSO dzielą tę samą powierzchnię OAuth.)

Ślad audytowy przeżywa integrację. Gdy nadasz zgodę administracyjną PhishSpot, zgoda OAuth zostaje zapisana w logu audytowym Entra na zawsze. Późniejsze odłączenie tego rekordu nie usuwa. Za pięć lat nowy audytor compliance pyta „dlaczego ta organizacja nadała `Directory.Read.All` zewnętrznemu dostawcy phishingu?" — i Ty, albo Twój następca, musisz to wyjaśnić.

28.4 Sprzężenie operacyjne

Gdy polegasz na pliku CSV, polegasz na pliku CSV. Gdy polegasz na synchronizacji Entra, polegasz na:

- **Dostępności Microsoft Graph.** Awaria Grafu — nawet częściowa — degraduje albo zatrzymuje synchronizację. PhishSpot retryje, ale jeśli awaria trwa kilka dni, lista kontaktów odpływa od rzeczywistości.
- **Politykach Conditional Access.** Polityki CA Twojego tenanta mogą po cichu blokować flow daemon PhishSpot. Następna zaplanowana synchronizacja kończy się niejasnym błędem — ale Ty tego nie widzisz, dopóki nie otworzysz strony integracji, co dla większości adminów oznacza „gdy coś wygląda na zepsute".

- **Zmianach schematu Microsoft Graph.** Microsoft aktualizuje API Graph swoim rytmem. Zmiana nazwy pola, deprecation, przemapowanie uprawnień — i nasza logika synchronizacji musi się dostosować. Robimy to, ale luka między „Microsoft wypuszcza zmianę" a „PhishSpot wypuszcza poprawkę" może wynosić dni.
- **Czasie życia tokena i odświeżaniu.** Tokeny aplikacji wygasają. Odświeżamy je. Przeważnie. Gdy odświeżenie się nie uda — admin zmienił hasło, conditional access się zacieśnił, aplikacja została oznaczona jako ryzykowna w MDM — synchronizacja gaśnie.

CSV nie ma żadnego z tych trybów awarii. Wgrywasz, dane się ładują, i jedyne co kiedykolwiek się zmienia, to gdy wgrasz nowy plik.

28.5 RODO — minimalizacja danych

W §28.2 wspomnieliśmy już o art. 5 ust. 1 lit. c RODO. Jest więcej.

- **Podstawa prawna.** Art. 6 wymaga, byś miał podstawę prawną przetwarzania danych osobowych. „Prawnie uzasadniony interes" to typowa podstawa dla symulacji phishingu — ale wymaga testu balansującego, a „pobraliśmy cały katalog, bo to było wygodne" nie przechodzi tego testu, gdy „pobraliśmy pięć potrzebnych pól z CSV" było dostępne.
- **Rejestr czynności przetwarzania (art. 30).** Połączenie Entra z PhishSpot to nowa czynność przetwarzania, z nowym przepływem danych, nowym subprocesorem, nowym pytaniem o retencję. Należy do RCP. Importy CSV zwykle mieszczą się w istniejącym wpisie „symulacje phishingu"; Entra dodaje świeży.
- **Review DPO.** W większości organizacji EU/UK nadanie `Directory.Read.All` dostawcy SaaS uruchamia ocenę skutków dla ochrony danych (DPIA) wg art. 35. To tygodnie procesu, często miesiące. Import CSV, z tymi samymi podmiotami danych, często nie uruchamia DPIA w ogóle — zakres danych jest węższy, a relacja z subprocesorem prostsza.

28.6 Ukryty koszt po stronie admina

Pitch dla synchronizacji Entra to „ustaw raz, zapomnij". Rzeczywistość to więcej pracy.

- Global Administrator musi nadać zgodę. W większości org to jedna albo dwie osoby — a ich kalendarze są pełne.
- Review DPO i prawników, wpis RCP, DPIA (czasem).
- Wyjątki w Conditional Access, jeśli Twoje domyślne polityki blokują flow app-only.
- Kwartalny audyt nadanych zgód OAuth w tenancie (dobra higiena bezpieczeństwa).
- Ponowna zgoda, gdy Microsoft przemianowuje scope'y albo wymaga zaktualizowanej rejestracji aplikacji.
- Reakcja na incydent, gdy synchronizacja po cichu pada przez tydzień, a następna kampania trafia do byłych pracowników.

Przeciw alternatywie CSV: dowolny admin eksportuje pięciokolumnowy CSV z systemu HR raz na kwartał, wgrywa, gotowe. Bez zaangażowania global admina, bez telefonu do DPO, bez follow-upu audytowego. „Oszczędność czasu" automatyki Entra to w większości iluzja, gdy policzysz pracę, którą sama generuje.

28.7 Ironia programu uświadamiającego, w szczegółach

Ten argument zasługuje na własną sekcję, bo jest jedynym powodem specyficznym dla PhishSpot, który nie dotyczy innych integracji SaaS.

Udany program uświadamiający uczy pracowników kilku odruchów:

- Nieoczekiwany MS-brandowany prompt logowania zasługuje na drugie spojrzenie.
- Ekran „nadaj tej aplikacji dostęp do swojego konta" to coś, co się czyta przed kliknięciem.
- Prompt, który przychodzi mailem i prosi o dane logowania, jest domyślnie wrogi, dopóki się go nie zweryfikuje.

Integracja Entra w PhishSpot i SSO Microsoft 365 zaprzeczają każdemu z tych odruchów w naszym własnym UX:

- **Wysyłamy** użytkownikom prompt logowania Microsoft pod `platform.phishspot.com/users/sign_in`. Klikają, robią MFA i odruch „ufać promptowi Microsoft w tym kontekście" się wzmacnia.
- **Prosimy** Global Administratora, by przeklikał ekran zgody Microsoft nadający naszej aplikacji `Directory.Read.All`. Odruch, którego chcemy — „przeczytaj ten ekran, zapytaj o ten scope" — jest w sprzeczności z integracją, którą sami prosimy go ukończyć.

Wynik: populacja pracowników lepiej wytrenowana wobec symulacji, które wysyłamy, ale nieco gorzej wytrenowana wobec prawdziwych ataków, przed którymi ma być chroniona. Trening gorzej się przenosi na „nieznany MS-brandowany prompt poza PhishSpot", bo zrobiliśmy jeden **w środku** PhishSpot znanym.

To nie jest wada śmiertelna — większość programów uświadamiających akceptuje pewną niedoskonałość — ale jest powodem, by domyślnie wybierać prostszą ścieżkę integracji, która tej sprzeczności nie produkuje.

28.8 Co polecamy

W niemal każdej organizacji, z którą pracujemy, właściwa ścieżka to:

1. **Import CSV przez Rozdział 5 Kontakty.** Wybierz kolumny, których faktycznie potrzebujesz (`first_name, last_name, email, department, title, groups`). Wyeksportuj z systemu HR albo Active Directory przez PowerShell. Wgraj przez UI PhishSpot.
2. **Kwartalne odświeżenie.** Re-eksport i re-import raz na kwartał, albo po większych zmianach w org (duże fale rekrutacji, reorganizacje, M&A). Operacje masowe w §5.6 obsłużą usuwanie.
3. **Członkostwo w grupach w CSV.** PhishSpot akceptuje rozdzieloną przecinkami kolumnę `groups` — ten sam efekt co odzwierciedlanie grup z Entra, bez synchronizacji.
4. **Risk score nadal działa.** Risk score jest liczony przez PhishSpot na podstawie wyników kampanii, nie z Entra. Wyłączenie synchronizacji Entra nic nie zmienia w zachowaniu risk score.

Ta ścieżka pokrywa 95% potrzeb programu symulacji phishingowych. Tej ścieżki używają nasi długo-letni klienci nawet wtedy, gdy ich tenanty są całkowicie zdolne wesprzeć synchronizację Entra.

28.9 Jeśli mimo to się łączysz

Wspieramy synchronizację Entra. Klienci ją podłączają. Czasem są realne powody: organizacja 5 000+ pracowników, gdzie kwartalny CSV nie nadąża za zmianami org; środowisko regulowane, gdzie IT wymaga onboardingu opartego o katalog dla wszystkich SaaS; fazowane wdrożenie, gdzie program symulacji to jedno z wielu narzędzi w tym samym pipeline Entra.

Jeśli zdecydujesz się podłączyć Entra ID, zrób to świadomie:

- **Review scope'ów z security.** Niech Twój zespół security potwierdzi, że `User.Read.All` / `Group.Read.All` / `Directory.Read.All` są akceptowalne w Twoim frameworku vendor risk.
- **Time-box zgody OAuth.** Ustaw przypomnienie w kalendarzu na review zgody co sześć miesięcy. Jeśli przestałeś używać synchronizacji, cofnij.
- **Zarejestruj przetwarzanie.** Dodaj wpis do RCP. Jeśli działasz w EU/UK i DPO wymaga DPIA — przeprowadź ją.
- **Monitoruj zdrowie synchronizacji.** Log aktywności w §25.6 to jedyny sygnał degradacji. Skonfiguruj swój zespół operacji, by sprawdzał po każdym zaplanowanym przebiegu — albo postaw webhook na limicie `contact.updated`.
- **Trzymaj CSV w pogotowiu.** Miej aktualny eksport CSV na dzień, w którym zechcesz się odłączyć — onboarding nowych kontaktów z CSV po odejściu Entra jest łatwiejszy, gdy plik został pod ręką.

Następnie idź do Rozdziału 25 Synchronizacja katalogu po instrukcje techniczne.

28.10 Odnośniki

- Rozdział 5 Kontakty — ścieżka importu CSV, którą polecamy zamiast.
- Rozdział 25 Synchronizacja katalogu — techniczne instrukcje dla integracji Entra, przeciw której argumentuje ten rozdział.
- Rozdział 24 Logowanie przez Microsoft 365 — osobna decyzja od synchronizacji katalogu; argument o ironii symulacji z §28.7 dotyczy też SSO.
- Art. 5 RODO — zasada minimalizacji danych w prawie EU.

Te same argumenty dotyczą każdej przyszłej synchronizacji katalogu Google Workspace, którą mogłybyśmy zaoferować. To nie są argumenty przeciwko Microsoft jako dostawcy — to są argumenty przeciwko OAuth-owej synchronizacji katalogu między dwoma niepowiązanymi produktami SaaS w ogóle, i przeciwko specyficznemu niedopasowaniu między treningiem antyphishingowym a ciasną integracją z Microsoft w szczególności.

Serwer MCP (Integracja AI)

PhishSpot udostępnia serwer MCP (Model Context Protocol), dzięki czemu klient AI, np. Claude, może obsługiwać PhishSpot w Twoim imieniu — językiem naturalnym, na tych samych danych i zasadach co aplikacja webowa. Zestaw narzędzi odzwierciedla teraz większość tego, co może zrobić człowiek w panelu: przeglądać bibliotekę szablonów, budować i planować kampanie, wgrywać hostowane obrazy, zarządzać kontaktami/grupami/kursami/domenami/webhookami/autopilotami oraz odczytywać wszystkie wyniki i trendy.

29.1 Punkt końcowy

Serwer MCP jest dostępny pod adresem:

```
https://platform.phishspot.com/mcp
```

Komunikuje się przez JSON-RPC po HTTP. Skonfiguruj dowolnego klienta MCP na ten adres, używając **transportu HTTP**.

29.2 Uwierzytelnianie

Serwer MCP korzysta z **tokenów API** PhishSpot. Token musi mieć jawnie nadany dostęp MCP.

1. Przejdź do **Ustawienia** → **Tokeny API** → **Nowy token**.
2. Nadaj nazwę i zaznacz **Zezwól na dostęp MCP**.
3. Skopiuj wartość tokenu (wyświetlana raz).

> Token może działać na **każdym koncie, do którego należysz**, a operacje **zapisu** MCP wymagają roli **administratora lub edytora** na danym koncie. Traktuj token jak hasło.

29.3 Łączenie z Claude

Dla **Claude Code** uruchom (zastąp `YOUR_TOKEN`):

```
claude mcp add --transport http phishspot https://platform.phishspot.com/mcp \
  --header "Authorization: Bearer YOUR_TOKEN"
```

Dla **Claude Desktop** lub innego klienta dodaj wpis serwera:

```
{
  "mcpServers": {
    "phishspot": {
      "type": "http",
      "url": "https://platform.phishspot.com/mcp",
      "headers": { "Authorization": "Bearer YOUR_TOKEN" }
    }
  }
}
```

29.4 Bezpieczeństwo: co wysyła, a co nie

Niemal wszystko, co może zrobić AI, jest **tylko do odczytu** lub **tylko przygotowuje**. Narzędzia kampanii `build_*`, `create_*` i `set_*` przygotowują kampanię do kroku **przeglądu** i **nigdy nie wysyłają e-maili do odbiorców** — to człowiek uruchamia każdą kampanię w panelu PhishSpot.

Niewielki, jasno oznaczony zestaw **narzędzi-akcji** może wywołać realną wysyłkę, dzięki czemu AI może na Twoją prośbę poprowadzić kampanię od początku do końca. Ich opisy zaczynają się od ostrzeżenia i wymagają roli administratora/edytora:

Narzędzie-akcja	Skutek
`schedule_campaign`	**Wysyła prawdziwe e-maile** — planuje gotową kampanię do faktycznej wysyłki o zadanej porze.
`reschedule_campaign`	**Wysyła prawdziwe e-maile** — zmienia czas wysyłki zaplanowanej kampanii.
`start_autopilot`	**Uruchamia żywy program** — aktywuje autopilota, który cyklicznie generuje i wysyła kampanie.

`cancel_schedule`, `pause_autopilot` i `stop_autopilot` to bezpieczne odpowiedniki — **zatrzymują** wysyłki. Dodanie domeny wysyłkowej powoduje jej skonfigurowanie i zwrócenie serwerów nazw do ustawienia u rejestratora — **nie** rejestruje ani nie kupuje domeny.

> Jeśli chcesz, aby AI nigdy nie wysyłało samodzielnie, po prostu nie proś o zaplanowanie ani uruchomienie czegokolwiek — każde inne narzędzie zostawia człowiekowi decyzję o uruchomieniu.

29.5 Dostępne narzędzia

Niemal każde narzędzie powiązane z kontem przyjmuje `account_id` (`acct_…`). Najpierw wywołaj **`whoami`**, aby poznać konta i role dostępne dla tokenu. Poniżej narzędzia pogrupowano według funkcji.

Tożsamość i domeny wysyłkowe

Narzędzie	Co robi
`whoami`	Pokazuje zalogowanego użytkownika oraz konta/role, na których token może działać.
`list_sending_domains`	Lista aktywnych i konfigurowanych domen wysyłkowych konta.
`provision_sending_domain`	Dodaje domenę BYOD i zwraca serwery nazw do ustawienia u rejestratora.
`check_sending_domain`	Sprawdza delegację domeny, rekordy poczty i gotowość do wysyłki.
`list_platform_domains`	Lista wszystkich domen widocznych dla konta (współdzielone + BYOD) ze stanem i gotowością.
`get_platform_domain`	Pełne szczegóły jednej domeny: status weryfikacji, oczekiwane rekordy DNS, diagnostyka, powód blokady.

Kontakty i grupy

Narzędzie	Co robi
`list_contacts`	Lista kontaktów na koncie (stronicowana).
`import_contacts`	Importuje kontakty z CSV lub JSON; kolumna `groups` modeluje fale/segmenty.
`update_contact`	Aktualizuje pola kontaktu i/lub zastępuje jego przynależność do grup.
`delete_contacts`	Usuwa kontakty (pomija zablokowane przez aktywną kampanię).
`list_groups`	Lista grup kontaktów na koncie.
`create_group`	Tworzy nową grupę kontaktów.
`delete_group`	Usuwa grupę (chyba że jest zablokowana przez aktywną kampanię).
`add_contacts_to_group`	Dodaje kontakty do grupy (pomija duplikaty).
`remove_contacts_from_group`	Usuwa kontakty z grupy.

Biblioteka szablonów phishingowych

Narzędzie	Co robi
`list_phishing_templates`	Lista szablonów wbudowanych lub własnych, z filtrowaniem po kategorii i wyszukiwaniem.
`get_phishing_template`	Pełna treść jednego szablonu: e-mail + HTML/CSS strony docelowej i akcja po kliknięciu.

Narzędzie	Co robi
`list_phishing_categories`	Drzewo kategorii szablonów (szablony trzymają tylko kategorie liściowe).
`build_campaign_from_template`	Buduje roboczą kampanię z szablonu; opcjonalnie dodaje wszystkie kontakty i zatrzymuje na przeglądzie. Nie wysyła.

Szkolenia e-learningowe

Narzędzie	Co robi
`list_courses`	Lista kursów dostępnych dla konta (własne + globalne) z liczbą bloków i statystykami ukończeń.
`get_course`	Szczegóły jednego kursu i uporządkowane podsumowanie jego bloków.

Biblioteka mediów (hosting obrazów)

Narzędzie	Co robi
`upload_media`	Wgrywa obraz lub plik CSS (z URL lub base64) i zwraca **hostowany URL** do e-maili/stron.
`list_media`	Lista hostowanych mediów konta.
`delete_media`	Usuwa plik media.

> Klienty pocztowe (Gmail, Outlook) usuwają obrazy z URI `data:`, więc w HTML kampanii osadzaj hostowany URL z `upload_media` zamiast wklejać base64.

Budowanie kampanii

Narzędzie	Co robi
`list_campaigns`	Lista kampanii ze stanem i postępem kreatora.
`get_campaign`	Pełny status jednej kampanii, w tym co blokuje uruchomienie.
`create_campaign`	Tworzy roboczą kampanię (ustawienia).
`set_campaign_email`	Ustawia temat i treść HTML e-maila.
`set_campaign_landing`	Ustawia stronę docelową oraz domenę wysyłkową/landingową.
`set_campaign_post_click`	Ustawia akcję po kliknięciu (szkolenie, strona edukacyjna lub przekierowanie).
`add_campaign_recipients`	Dodaje odbiorców (wszyscy, grupa lub wybrane kontakty). Zostawia kampanię w przeglądzie.

Narzędzie	Co robi
`build_campaign_from_spec`	Buduje całą roboczą kampanię jednym wywołaniem (ustawienia → odbiorcy).
`duplicate_campaign`	Powiela kampanię do nowej kopii roboczej (z odbiorcami). Nie wysyła.

Planowanie kampanii

Narzędzie	Co robi
`schedule_campaign`	⚠ **Wysyła prawdziwe e-maile** — planuje gotową kampanię do wysyłki o zadanej porze.
`reschedule_campaign`	⚠ **Wysyła prawdziwe e-maile** — zmienia czas wysyłki zaplanowanej kampanii.
`cancel_schedule`	Anuluje oczekującą zaplanowaną wysyłkę i przywraca kampanię do wersji roboczej.

Wyniki i raporty (tylko odczyt)

Narzędzie	Co robi
`get_campaign_results`	Lejek zaangażowania oraz podział na grupy i działy.
`get_campaign_recipients`	Etap dostarczenia, status szkolenia i flaga odpowiedzi per odbiorca (z filtrami).
`get_recipient_timeline`	Chronologiczna oś zdarzeń jednego kontaktu w kampanii.
`get_campaign_replies`	Odpowiedzi, które odbiorcy odesłali na e-mail phishingowy.
`list_account_trends`	Trendy podatności na phishing w kampaniach w zadanym zakresie dat.
`list_events`	Surowe zdarzenia zaangażowania, z filtrami po kampanii / kontakcie / typie.
`list_reported_messages`	Podejrzane e-maile zgłoszone przez pracowników (tylko metadane nadawcy/tematu).

Webhooki

Narzędzie	Co robi
`list_webhook_endpoints`	Lista wychodzących punktów końcowych webhooków.
`get_webhook_endpoint`	Jeden punkt końcowy wraz z ostatnimi dostawami (sekret podpisu zamaskowany).

Narzędzie	Co robi
`create_webhook_endpoint`	Tworzy (wyłączony) punkt końcowy; jednorazowo zwraca sekret podpisu.
`update_webhook_endpoint`	Aktualizuje nazwę, URL lub subskrypcje zdarzeń.
`delete_webhook_endpoint`	Usuwa punkt końcowy i historię dostaw.
`toggle_webhook_endpoint`	Włącza lub wyłącza punkt końcowy.
`list_webhook_event_types`	Lista typów zdarzeń do subskrypcji (bez konta).

Autopiloty (programy automatyczne)

Narzędzie	Co robi
`list_autopilots`	Lista programów autopilota i ich stan/postęp.
`get_autopilot`	Konfiguracja jednego autopilota, grupy docelowe i ostatnie kampanie.
`create_autopilot`	Tworzy autopilota w wersji **roboczej**. Nie uruchamia go.
`update_autopilot`	Aktualizuje edytowalnego (niezatrzymanego) autopilota.
`delete_autopilot`	Usuwa autopilota (nie podczas działania).
`start_autopilot`	⚠ **Uruchamia żywy program**, który cyklicznie wysyła kampanie phishingowe.
`pause_autopilot`	Wstrzymuje działającego autopilota.
`stop_autopilot`	Trwale zatrzymuje autopilota (nieodwracalne).

29.6 Dodawanie domeny wysyłkowej (BYOD)

Aby wysyłać kampanię z własnej domeny (np. `twoja-firma.pl`):

1. Poproś AI o wywołanie `provision_sending_domain` z domeną.
2. Ustaw zwrócone **serwery nazw** u rejestratora domeny.
3. Odpytuj `check_sending_domain`, aż domena będzie **aktywna** i **gotowa do wysyłki**.

Po aktywacji domena pojawia się w `list_sending_domains` / `list_platform_domains` i może być użyta jako domena wysyłkowa/landingowa kampanii. Zobacz też Domeny.

29.7 Przykład: zbuduj kampanię z szablonu

Typowy przebieg sterowany przez AI — wszystko tylko przygotowuje, dopóki nie zdecydujesz się zaplanować wysyłki:

1. `whoami` → wybierz `account_id`.

2. `list_phishing_categories` i `list_phishing_templates` → wybierz szablon.
3. `build_campaign_from_template` (opcjonalnie `quick_launch`) → robocza kampania z odbiorcami, w kroku przeglądu.
4. `get_campaign` → potwierdź brak błędów gotowości.
5. Uruchom ją samodzielnie w panelu lub poproś AI o `schedule_campaign` na konkretny czas (**to wysyła naprawdę**).
6. Po wysyłce `get_campaign_results`, `get_campaign_recipients` i `list_account_trends` podsumują, kto dał się nabrać.

Każde narzędzie trafia na produkcję z każdym wdrożeniem — bez dodatkowej konfiguracji, bez migracji i bez ustawień per narzędzie.

Projektowanie skutecznych kampanii

Rozdział 4 pokazuje, *gdzie kliknąć* w kreatorze kampanii. Ten przewodnik wyjaśnia, *co tam wpisać* — jak zaprojektować symulację, która zachowuje się jak prawdziwy atak, poprawnie personalizuje treść, śledzi każdą interakcję i kończy się momentem edukacyjnym. Zakładamy, że znasz już rozdział Kampanie, i skupiamy się na decyzjach projektowych w obrębie każdego kroku.

Kampania w PhishSpot składa się z pięciu elementów, a dobry projekt to dopasowanie ich do siebie:

1. **Tożsamość nadawcy** — nazwa i adres, z których pozornie pochodzi e-mail.
2. **E-mail** — temat i treść HTML, personalizowane dla każdego odbiorcy.
3. **Strona docelowa** — to, co odbiorca widzi po kliknięciu (opcjonalna).
4. **Akcja końcowa** — „moment edukacyjny” po kliknięciu lub wysłaniu formularza.
5. **Odbiorcy** — kto otrzymuje wiadomość i jak jest ona do nich dopasowana.

Kolejne sekcje omawiają każdy z tych elementów, ze szczególnym naciskiem na mechanikę platformy — tagi scalające i klucze śledzenia — która do tej pory nie była szczegółowo opisana.

30.1 Personalizacja za pomocą tagów scalających („klucze”)

Tagi scalające to `{{symbole}}`, które wstawiasz w treść, a PhishSpot zastępuje je prawdziwymi danymi każdego odbiorcy w chwili wysyłki. To najskuteczniejsza dźwignia, jaką masz: wiadomość zaadresowana do „Jana” od „Twojego działu IT w [Twojej firmie]” jest znacznie bardziej przekonująca niż masowa, bezosobowa wysyłka.

Składnia. Otocz nazwę tagu podwójnymi nawiasami klamrowymi: `{{first_name}}`. Tagi **nie rozróżniają wielkości liter** i tolerują spacje — `{{First_Name}}` oraz `{{ first_name }}` działają tak samo. Tag, którego PhishSpot nie rozpoznaje, pozostaje w wiadomości **dosłownie**, więc literówka typu `{{frist_name}}` trafi do odbiorcy jako widoczny tekst. Zawsze wyślij test (zob. §30.6), aby je wychwycić.

Dostępne tagi różnią się między **e-mailem** a **stroną docelową**, ponieważ każde z nich renderowane jest w innym kontekście. Używaj tylko tagów dozwolonych w danym miejscu — edytor to weryfikuje i nie pozwoli zapisać e-maila odwołującego się do tagu dostępnego wyłącznie na stronie docelowej.

Temat i treść e-maila — dostępne tagi:

Tag	Zastępowany przez	Przykład
`{{first_name}}`	Imię odbiorcy	Jan
`{{last_name}}`	Nazwisko odbiorcy	Kowalski
`{{full_name}}`	Imię i nazwisko	Jan Kowalski
`{{email}}`	Adres e-mail odbiorcy	jan.kowalski@firma.pl
`{{position}}`	Stanowisko odbiorcy	Starszy Analityk

Tag	Zastępowany przez	Przykład
`{{department}}`	Dział odbiorcy	Finanse
`{{company}}`	Nazwa Twojego konta	Acme Sp. z o.o.
`{{campaign_name}}`	Nazwa kampanii	Test faktur Q2
`{{landing_url}}`	Śledzony link odbiorcy	https://officelogin.in/l/ab12cd34?d=…

Strona docelowa i wiadomość edukacyjna — dostępne tagi:

Tag	Zastępowany przez
`{{first_name}}`, `{{last_name}}`, `{{full_name}}`, `{{email}}`	Jak wyżej
`{{company}}`	Nazwa Twojego konta
`{{landing_url}}`	Śledzony link odbiorcy
`{{elearning_url}}`	Link szkoleniowy odbiorcy (używany na stronie edukacyjnej)

> `{{landing_url}}` to śledzony link phishingowy — nie istnieje tag `{{phishing_url}}`. `{{company}}` zwraca nazwę *Twojego* konta (organizacji prowadzącej symulację), dzięki czemu działają preteksty typu „wiadomość od Twojej własnej firmy". Pełny wykaz znajdziesz w rozdziale Zmienne szablonów.

Wskazówki projektowe:

- Personalizuj **temat**, nie tylko treść — `Jan, wymagane działanie na Twoim koncie` podnosi współczynnik otwarć bardziej niż ogólny temat.
- Umieść `{{landing_url}}` za realistycznym przyciskiem lub linkiem, nigdy jako surowy adres URL. Odbiorcy rzadko klikają widoczny link.
- Używaj `{{department}}` / `{{position}}`, aby dopasować pretekst do roli (faktura dla Finansów, informacja o świadczeniach dla HR). Strategię targetowania opisuje Socjotechnika i perswazja.
- Lepiej pominąć tag, niż ryzykować, że będzie pusty — niezręczne „Szanowny ," (bez imienia) zdradza symulację. Puste wartości renderują się jako pusty tekst, więc upewnij się, że dane kontaktów są kompletne dla pól, na których polegasz.

30.2 Jak działa śledzenie i jak wpływa na projekt

PhishSpot rejestruje drogę każdego odbiorcy przez lejek kampanii — **Wysłano** → **Dostarczono** → **Otwarto** → **Kliknięto** → **Przesłano** → **Przeszkolono**. Zrozumienie, *jak* wykrywany jest każdy etap, pomaga zaprojektować treść, która mierzy to, na czym faktycznie Ci zależy.

- **Otwarto** wykrywane jest przez niewidzialny piksel śledzący 1×1, automatycznie osadzany w każdym e-mailu. Klient poczty odbiorcy ładuje go przy wyświetleniu wiadomości. Ponieważ wiele

klientów (zwłaszcza Apple Mail Privacy Protection i niektóre bramy korporacyjne) blokuje lub wstępnie pobiera zdalne obrazy, traktuj współczynnik otwarć jako sygnał *miękki* — nie projektuj kampanii, której sukces zależy wyłącznie od śledzenia otwarć.

- **Kliknięto** wykrywane jest, gdy odbiorca odwiedzi swój spersonalizowany link. Link zawiera nieprzejrzysty **klucz** przypisany do odbiorcy — identyfikator deliverable — jako parametr `d`:

  ```
  https://<Twoja-domena-docelowa>/l/<losowa-ścieżka>?d=<id-deliverable>
  ```

  To właśnie wartość kryjąca się za `{{landing_url}}`. Klucz identyfikuje dokładnie jedną parę (kampania, odbiorca), dzięki czemu PhishSpot przypisuje kliknięcie konkretnej osobie, nie umieszczając jej adresu e-mail w adresie URL. **Nigdy nie edytuj ręcznie ani nie wpisuj linku na sztywno** — zawsze wstawiaj `{{landing_url}}`, aby zachować klucz odbiorcy. Statyczny adres URL przypisałby każde kliknięcie do nikogo.

- **Przesłano** wykrywane jest, gdy odbiorca wyśle formularz na Twojej stronie docelowej (§30.3). Każde wpisane pole jest przechwytywane, z wyjątkiem pól routingu i zabezpieczeń — mierzysz więc nie tylko *to*, że ktoś wysłał formularz, lecz także *co* był gotów ujawnić.

Kampanie wyłącznie śledzące. Jeśli chcesz jedynie zmierzyć, kto kliknie — bez hostowania fałszywego logowania — możesz wyłączyć stronę docelową (Krok 3). Link nadal rejestruje kliknięcie dzięki kluczowi, a następnie od razu uruchamia akcję końcową (np. przejście wprost do strony edukacyjnej). To najmniej inwazyjny projekt, który w ogóle nie przechwytuje danych logowania.

30.3 Projektowanie strony docelowej

Włączona strona docelowa jest celem `{{landing_url}}`. To zwykły HTML, który kontrolujesz, hostowany na wybranej domenie platformy. Typowe wzorce:

- **Klon logowania** — kopia ekranu logowania Microsoft 365, Google lub portalu wewnętrznego. Klasyczny test wyłudzania danych logowania.
- **Udostępnianie pliku / dokument** — „udostępniono Ci dokument, zaloguj się, aby go wyświetlić”.
- **Powiadomienie / strona akcji** — „potwierdź swoje dane”, „zapoznaj się z polityką”.

Formularze. Nie musisz konfigurować akcji formularza — PhishSpot automatycznie przepisuje każdy `<form>` na stronie tak, by wysyłał dane z powrotem na adres śledzący. Dowolne pola, które dodasz (login, hasło itp.), są przy wysyłce przechwytywane do rekordu zdarzeń odbiorcy, z pominięciem wewnętrznych pól routingu i zabezpieczeń. Zaprojektuj formularz tak, by odzwierciedlał to, co imitujesz.

Możesz tu również używać tagów scalających dostępnych dla strony docelowej (§30.1) — np. wstępne wypełnienie pola loginu wartością `{{email}}` to mocny akcent realizmu.

> Świadomie zdecyduj, czy przechwytywać hasła. Zarejestrowanie *samego faktu* przesłania formularza zwykle wystarcza, by uruchomić szkolenie, a przechowywanie prawdziwych haseł — nawet na krótko, nawet własnych pracowników — podnosi stawkę ćwiczenia. Wiele programów rejestruje przesłanie bez zapisywania wartości hasła. Dostosuj to do polityki bezpieczeństwa i HR.

Techniczną stronę poprawnego renderowania strony (a zwłaszcza e-maila) opisuje Kompatybilność z klientami poczty.

30.4 Moment edukacyjny (akcja końcowa)

To, co dzieje się po kliknięciu lub przesłaniu formularza przez odbiorcę, decyduje, czy symulacja zamieni się w szkolenie. PhishSpot oferuje cztery akcje końcowe (Krok 4):

Akcja końcowa	Działanie	Stosuj, gdy
Nic	Pusta strona	Wystarczy zarejestrowanie kliknięcia/przesłania; minimalne zakłócenie
Przekierowanie do kursu	Kieruje odbiorcę do przypisanego kursu e-learningowego	Chcesz natychmiastowego szkolenia w kontekście — najsilniejszy moment edukacyjny
Strona z wiadomością edukacyjną	Pokazuje własną stronę „to była symulacja” (HTML, który piszesz, obsługuje tagi scalające)	Chcesz markowego, uspokajającego wyjaśnienia bez pełnego kursu
Przekierowanie do adresu URL	Kieruje do dowolnego zewnętrznego adresu URL	Chcesz, by odbiorca trafił np. na prawdziwy portal lub wewnętrzną politykę

Najskuteczniejszy projekt to **przekierowanie do kursu**: odbiorca jest najbardziej otwarty na naukę w sekundach po tym, jak zorientuje się, że dał się nabrać. Połącz kampanię z krótkim, trafnym kursem — zob. Kursy.

Na stronie edukacyjnej możesz użyć `{{first_name}}`, by zwrócić się do odbiorcy, oraz `{{elearning_url}}`, by zaproponować dodatkową lekcję. Utrzymaj ton niekarzący (więcej w Socjotechnika i perswazja §32.7).

30.5 Tożsamość nadawcy i dostarczalność

Najstaranniej przygotowany e-mail jest bezwartościowy, jeśli trafi do spamu. Nadawcę definiują dwa pola (Krok 1):

- **Nazwa wyświetlana** (`from_name`) — to, co widnieje jako nadawca, np. `IT Security`.
- **E-mail nadawcy** (`from_email`) — adres, który musi należeć do **domeny platformy** wybranej dla kampanii.

Kilka realiów, które warto uwzględnić w projekcie:

- Domena wysyłkowa musi być **aktywna i nie zablokowana**, aby uruchomić kampanię. Wybierz domenę, której nazwa wspiera pretekst — `officelogin.in` czyta się zupełnie inaczej niż `losowy-ciag.xyz`. Zobacz Domeny, aby poznać proces provisioningu i konfigurację BYOD.

- Dostarczalność zależy od SPF/DKIM/DMARC domeny i jej reputacji, konfigurowanych podczas konfiguracji domeny. Zupełnie nowa domena bez rozgrzewki może trafiać do spamu niezależnie od treści.
- Jeśli test trafia do spamu, zajrzyj do Whitelist filtra antyspamowego — być może administrator poczty odbiorców musi dopuścić źródło symulacji.

Dopasuj nazwę wyświetlaną i domenę do pretekstu: e-mail „od Microsoftu" z `acme-internal.com` jest niespójny i uczy odbiorców rozpoznawania niewłaściwego sygnału.

30.6 Test i weryfikacja przed uruchomieniem

Nigdy nie uruchamiaj kampanii, której nie widziałeś wyrenderowanej. Przed Krokiem 6:

1. **Wyślij testowy e-mail** do siebie (Akcje kampanii → Wyślij testowy e-mail). Sprawdź: czy tagi scalające się rozwinęły (brak osieroconych `{{…}}`), czy link działa i prowadzi na właściwą stronę, czy obrazy się ładują i czy formatowanie się trzyma.
2. **Sprawdź wersję na komputer i na telefon.** Po uruchomieniu podgląd per odbiorca w Raporty i analityka §11.5 pokazuje dokładny e-mail, który otrzymała każda osoba, z przełącznikiem desktop/mobile — użyj go do weryfikacji renderowania i personalizacji.
3. **Przejdź całą ścieżkę** — kliknij własny testowy link, wyślij formularz i potwierdź, że akcja końcowa (kurs, strona edukacyjna lub przekierowanie) uruchamia się zgodnie z zamierzeniem.

Szybka lista kontrolna przed uruchomieniem:

- [ ] Temat i treść personalizują się poprawnie (testowy e-mail dotarł i został odczytany)
- [ ] `{{landing_url}}` jest pod przyciskiem/linkiem, kliknięcie jest śledzone
- [ ] Strona docelowa się renderuje; formularz wysyła dane; przesłanie zarejestrowane
- [ ] Akcja końcowa uruchamia się i wskazuje właściwy kurs/stronę/URL
- [ ] Domena nadawcy jest aktywna; test nie trafił do spamu
- [ ] E-mail renderuje się poprawnie na komputerze **i** telefonie

---

Zobacz też: Kampanie · Zmienne szablonów · Kompatybilność z klientami poczty · Socjotechnika i perswazja · Domeny · Raporty i analityka

Kompatybilność z klientami poczty

E-mail symulacyjny zadziała tylko wtedy, gdy wyrenderuje się tak, jak go zaprojektowano. W przeciwieństwie do strony WWW — która działa w jednej z kilku nowoczesnych przeglądarek — e-mail otwierany jest w dziesiątkach klientów, każdy z własnym silnikiem renderującym, a wiele z nich pozostaje lata za standardami sieci. Ten przewodnik opisuje praktyczne zasady pisania HTML e-maili, które przetrwają drogę do skrzynki. Stanowi uzupełnienie rozdziału Projektowanie skutecznych kampanii, który zajmuje się stroną *treści*.

Treść e-maila wpisujesz w edytorze kodu HTML w **Kroku 2** kreatora kampanii (zob. Kampanie §4.2). Wszystko poniżej dotyczy tego, jaki HTML/CSS tam umieścić.

31.1 Dlaczego HTML e-maila to nie HTML strony WWW

Nie istnieje jeden „standard e-maila”. Każdy klient sam decyduje, ile HTML i CSS obsługuje:

Klient / silnik	Czego się spodziewać
Outlook (Windows, 2007–2021)	Renderuje silnikiem Microsoft Word. Brak obsługi `float`, `position`, obrazów tła (bez obejść), nowoczesnego CSS oraz niezawodnych `margin` / `padding` na `<div>`. Najbardziej restrykcyjny cel.
Outlook 365 / outlook.com / nowy Outlook	Oparty na webview, znacznie lepszy — ale wciąż w pewnych kontekstach usuwa `<style>` i przepisuje CSS.
Gmail (web i aplikacja)	Dobra obsługa CSS, ale historycznie usuwa `<head>` / `<style>` w niektórych widokach, przycina długie wiadomości i proxuje obrazy.
Apple Mail (macOS i iOS)	Renderowanie najwyższej klasy, niemal jak w przeglądarce. Respektuje `@media`. Privacy Protection wstępnie ładuje obrazy (wpływa na śledzenie otwarć).
Mobilne klienty webview (aplikacje Gmail/ Outlook, Samsung Mail)	Zmienne; zakładaj wąski ekran i niespójną obsługę `@media`.

Złota zasada: projektuj pod najgorszy klient używany przez Twoich odbiorców, a potem ulepszaj. W korporacyjnej symulacji phishingu prawie zawsze oznacza to **Outlooka na Windows**. Jeśli e-mail działa w Outlooku, działa niemal wszędzie.

31.2 Układaj treść tabelami, nie `div`-ami

Nowoczesny układ CSS (`flexbox`, `grid`, `float`) nie działa w Outlooku. Niezawodne, sprawdzone od dekad podejście to **zagnieżdżone tabele HTML** z kolumną treści o stałej szerokości (zwykle 600px), wyśrodkowaną w tabeli tła o pełnej szerokości.

```
<!-- Wrapper o pełnej szerokości trzyma tło; tabela wewnętrzna trzyma treść. -->
<table role="presentation" width="100%" cellpadding="0" cellspacing="0" border="0"
       style="background-color:#f4f4f4;">
  <tr>
    <td align="center" style="padding:24px 12px;">
      <!-- Kolumna treści 600px, wyśrodkowana -->
      <table role="presentation" width="600" cellpadding="0" cellspacing="0" border="0"
             style="width:600px; max-width:600px; background-color:#ffffff;">
        <tr>
          <td style="padding:32px; font-family:Arial, sans-serif; font-size:16px;
                     line-height:24px; color:#333333;">
            Witaj {{first_name}}, Twoje konto wymaga uwagi…
          </td>
        </tr>
      </table>
    </td>
  </tr>
</table>
```

Kluczowe punkty:

- Ustaw `cellpadding="0" cellspacing="0" border="0"` na każdej tabeli — w przeciwnym razie Outlook doda domyślne odstępy.
- `role="presentation"` informuje czytniki ekranu, że tabela służy do układu, a nie do danych.
- Odstępy realizuj przez `padding` na `<td>`, nie `margin` na elementach wewnętrznych — `margin` jest w Outlooku zawodny.
- Używaj **atrybutu** `width` *oraz* stylu `width` / `max-width`; Outlook czyta atrybut, nowoczesne klienty czytają styl.

31.3 Wstawiaj CSS inline

Wiele klientów usuwa bloki `<style>` z `<head>` (Gmail historycznie robi to w kilku widokach). Bezpieczny domyślny wybór to **style inline** na każdym elemencie:

```
<td style="font-family:Arial,sans-serif; font-size:16px; color:#333; padding:16px;">…</
        td>
```

Blok `<style>` w `<head>` rezerwuj **wyłącznie** dla tego, co tego wymaga — głównie reguł `@media` dla responsywności (§31.5) i stanów `:hover` — i traktuj je jako ulepszenie, które część klientów zignoruje. Nigdy nie polegaj na klasie zdefiniowanej w `<head>` dla układu, który musi działać wszędzie.

Pozostałe zasady inline:

- Używaj czcionek bezpiecznych dla sieci (Arial, Helvetica, Georgia, Tahoma, Verdana) z fallbackiem generycznym. Niestandardowe czcionki webowe działają tylko w kilku klientach.
- Zawsze ustawiaj jawnie `font-family`, `font-size`, `line-height` i `color` na komórkach z tekstem — nie polegaj na dziedziczeniu.

31.4 Niezbędnik przetrwania w Outlooku

Silnik Outlooka na Windows (Word) jest źródłem większości problemów typu „u mnie w teście wyglądało dobrze, a u połowy odbiorców się rozsypało". Praktyczne zabezpieczenia:

- **Kuloodporne przyciski.** Przycisk `<a>` stylowany CSS-em zapada się w Outlooku. Użyj przycisku opartego na tabeli, opcjonalnie z VML dla Outlooka:

```
<table role="presentation" cellpadding="0" cellspacing="0" border="0">
  <tr>
    <td align="center" bgcolor="#0067b8"
        style="border-radius:4px; mso-padding-alt:14px 28px;">
      <a href="{{landing_url}}"
         style="display:inline-block; padding:14px 28px; font-family:Arial,sans-
        serif;
                font-size:16px; color:#ffffff; text-decoration:none;">
        Zweryfikuj konto
      </a>
    </td>
  </tr>
</table>
```

  Zwróć uwagę na `mso-padding-alt` — właściwość wyłącznie dla Outlooka, przywracającą padding, który silnik Word usuwa.

- **Komentarze warunkowe.** Celuj w Outlooka konstrukcją `<!--[if mso]> … <![endif]-->`, aby dodać poprawki (np. stałe szerokości, VML) ignorowane przez inne klienty.

- **Unikaj `background-image`** na elementach — Outlook ignoruje większość z nich. Użyj jednolitego `bgcolor` lub prawdziwego `<img>`.

- **Odstępy pod obrazami.** Outlook dodaje białą przestrzeń pod obrazami. Ustaw `display:block;` i `border:0;` na każdym `<img>` oraz `font-size:0; line-height:0;` na komórkach zawierających wyłącznie obraz.

- **Nie polegaj na `border-radius`, `box-shadow`, gradientach ani `max-width` w Outlooku** — są ignorowane. Traktuj je jako dodatek dla zdolniejszych klientów.

31.5 Responsywność: komputer i telefon

Symulacja musi być użyteczna na telefonie — duża część odbiorców czyta pocztę najpierw na urządzeniu mobilnym, a rozsypany układ mobilny czyta się jak „fałszywka".

- **Zacznij od pojedynczej kolumny o stałej szerokości (≤600px)**, która już wygląda akceptowalnie na komputerze i degraduje się łagodnie — wiele klientów mobilnych nie respektuje `@media` niezawodnie, więc układ bazowy musi bronić się sam.

- **Ulepsz zapytaniami `@media`** w bloku `<style>` w `<head>` dla klientów, które je obsługują (Apple Mail, większość natywnych aplikacji mobilnych):

```
<style>
  @media only screen and (max-width:600px) {
    .container { width:100% !important; }
    .stack     { display:block !important; width:100% !important; }
    .mobile-pad { padding:16px !important; }
  }
</style>
```

- **Składaj kolumny na telefonie.** Dwukolumnowy wiersz na komputerze powinien stać się dwoma pełnoszerokościowymi blokami jeden pod drugim na telefonie (wzorzec `.stack` powyżej).
- **Cele dotyku:** przyciski o wysokości co najmniej ~44px, przyjazne pełnej szerokości na telefonie.
- **Rozmiary czcionek:** tekst podstawowy ≥14px (16px bezpieczniej); cokolwiek mniejszego jest nieczytelne na telefonie i wygląda podejrzanie.

31.6 Obrazy

- **Hostuj obrazy, nigdy ich nie osadzaj.** URI `data:` w base64 są usuwane przez Gmaila i Outlooka. Wgraj obrazy do Biblioteki mediów §10 i odwołuj się do hostowanego adresu URL. (To również powód, dla którego platforma serwuje obrazy kampanii z prawdziwego adresu URL.)
- **Zawsze dołączaj tekst `alt`.** Wiele klientów domyślnie blokuje obrazy, więc pierwsze wrażenie z e-maila często jest *bez obrazów*. Sensowny `alt` na logo i kluczowych obrazach utrzymuje spójność wiadomości — a dobry pretekst powinien czytać się także przy wyłączonych obrazach.
- **Ustawiaj jawnie atrybuty `width` i `height`**, aby układ nie skakał podczas ładowania obrazów i aby zastępcze ramki przy zablokowanych obrazach miały właściwy rozmiar.
- **Retina:** eksportuj obrazy w rozmiarze 2× względem wyświetlanego i ogranicz przez `width` / `height` dla ostrości na ekranach o wysokiej gęstości.
- **Nie buduj całego e-maila jako jednego dużego obrazu** — to uruchamia filtry antyspamowe, łamie się przy wyłączonych obrazach i uniemożliwia zaznaczanie/personalizację.

31.7 Tryb ciemny

Wiele klientów (Apple Mail, Outlook, aplikacja Gmail) zmienia kolory e-maili w trybie ciemnym, czasem nieprzewidywalnie odwracając tła i tekst.

- Nie zakładaj białego tła — logo ciemne na przezroczystym tle zniknie na ciemnym tle. Użyj logo z bezpiecznym tłem lub wersji działającej na obu.
- Przetestuj tryb ciemny przynajmniej w Apple Mail i aplikacji mobilnej Gmail.
- Unikaj czystego tekstu `#000000` na czystym `#ffffff`; lekko odchylone wartości odwracają się łagodniej.

31.8 Linki i preheader

- **Nie rozbijaj adresów URL.** Nie przenoś linku do nowej linii ani nie wstawiaj go jako surowego tekstu w środku zdania. W PhishSpot śledzony link wstawiasz przez `{{landing_url}}` (zob. §30.2) — platforma obsługuje klucz odbiorcy, więc tag scalający umieszczasz tylko pod przyciskiem lub linkiem.
- **Preheader** — fragment podglądu pokazywany na liście skrzynki — domyślnie jest pierwszą linią treści. Dodaj celowy preheader (ukryty lub widoczny) blisko góry, aby podgląd w skrzynce wspierał pretekst, a nie pokazywał „Wyświetl w przeglądarce” czy przypadkowego URL-a:

```
<div style="display:none; max-height:0; overflow:hidden; mso-hide:all;">
  Wymagane działanie na Twoim koncie przed piątkiem.
</div>
```

31.9 Testuj za każdym razem

Nic nie zastąpi zobaczenia e-maila w prawdziwych klientach:

1. **Wyślij testowy e-mail** z kampanii (Akcje kampanii → Wyślij testowy e-mail) do kontrolowanych przez siebie skrzynek — najlepiej po jednej w **Outlooku desktop, Gmailu (web + aplikacja) i Apple Mail (Mac + iOS)**.
2. **Sprawdź podgląd per odbiorca** w Raporty i analityka §11.5, który renderuje dokładny e-mail otrzymany przez każdego odbiorcę, z **przełącznikiem desktop/mobile**.
3. **Obejrzyj z wyłączonymi obrazami** i **w trybie ciemnym** co najmniej raz.

Lista kontrolna renderowania przed wysyłką:

- [ ] Układ zbudowany na zagnieżdżonych tabelach, stała kolumna treści ≤600px
- [ ] Cały istotny CSS jest inline; `<style>` tylko dla `@media` / `:hover`
- [ ] Przyciski oparte na tabeli/VML (przetrwają Outlooka)
- [ ] Obrazy hostowane (bez base64), z `alt`, jawnymi wymiarami, `display:block`
- [ ] Renderuje się na komputerze **i** telefonie; kolumny się składają; tekst ≥14px
- [ ] Wygląda akceptowalnie z wyłączonymi obrazami i w trybie ciemnym
- [ ] Ustawiony preheader; śledzony link wstawiony przez `{{landing_url}}`

Zobacz też: Projektowanie skutecznych kampanii · Kampanie · Biblioteka mediów · Raporty i analityka · Whitelist filtra antyspamowego

Socjotechnika i perswazja

Symulacja phishingu jest przydatna tylko wtedy, gdy jest przekonująca. Wiadomość, na którą nikt się nie nabiera, niczego nie mierzy; wiadomość, na którą nabierają się wszyscy, niczego nie uczy, jeśli jest tanią sztuczką. Ten przewodnik wyjaśnia, *dlaczego* ludzie klikają — zasady perswazji wykorzystywane przez prawdziwych atakujących — oraz jak zastosować je w PhishSpot, by budować symulacje dające uczciwe wyniki i, co najważniejsze, moment edukacyjny.

Tekst napisano z myślą o zespołach bezpieczeństwa i świadomości prowadzących **autoryzowane** symulacje wobec własnej organizacji. Celem nigdy nie jest zawstydzenie pracowników — chodzi o znalezienie i zamknięcie luk, zanim zrobi to prawdziwy atakujący. Trzymaj otwarty obok Projektowanie skutecznych kampanii: tamten przewodnik opisuje *mechanikę*, ten — *psychologię*.

32.1 Dlaczego ludzie klikają

Nabranie się na phishing rzadko wynika z braku inteligencji. Atakujący odnoszą sukces, wyzwalając szybkie, automatyczne decyzje — wykorzystując to, jak zajęci ludzie przetwarzają zalew poczty na autopilocie. Niemal każdy skuteczny phishing opiera się na tych samych sześciu zasadach wpływu (spopularyzowanych przez Roberta Cialdiniego):

Zasada	Dźwignia	Przykładowy pretekst
Autorytet	Podporządkowujemy się osobom u władzy	„Wiadomość od prezesa”, „Aktualizacja polityki IT Security”
Pilność / niedobór	Termin wyłącza czujność	„Twoje konto zostanie zablokowane za 24 godziny”
Dowód społeczny	Podążamy za tym, co robią inni	„12 współpracowników już to ukończyło”
Wzajemność	Odwzajemniamy przysługi	„Oto Twoja informacja o premii — potwierdź, by ją otrzymać”
Strach	Zagrożenie zawęża uwagę	„Wykryto podejrzane logowanie na Twoim koncie”
Ciekawość	Otwarta pętla domaga się zamknięcia	„Udostępniono Ci dokument”

Każda z nich mapuje się wprost na preteksty, które zbudujesz w PhishSpot. Najskuteczniejsze symulacje łączą **jedną** dominującą zasadę z mocnym realizmem — nakładanie trzech czy czterech sprawia, że wiadomość czyta się jak oszustwo.

32.2 Projektowanie wiarygodnego pretekstu

Pretekst to *historia*, którą opowiada e-mail. Wiarygodność bierze się ze spójności, nie z pomysłowości:

- **Prawdopodobny kontekst.** Wiadomość powinna pasować do czegoś, czego odbiorca faktycznie się spodziewa — faktura dla kogoś z Finansów, udostępniony plik dla współpracownika, powiadomienie o wygaśnięciu hasła odzwierciedlające Wasz realny proces IT.

- **Spójny nadawca.** Nazwa wyświetlana, adres i domena muszą pasować do historii (zob. §30.5). E-mail „od Microsoftu” z niepowiązanej domeny uczy złej lekcji.
- **Właściwy ton i branding.** Dopasuj głos i styl wizualny do tego, co podszywasz. Korporacyjne powiadomienie IT jest zwięzłe i formalne; marka konsumencka — przyjazna. Użyj technik HTML e-maila, by przekonująco odtworzyć wygląd marki.
- **Jedno, jasne wezwanie do działania.** Prawdziwy phishing prosi o jedną rzecz. Wiele próśb rozmywa pilność i wzbudza podejrzliwość.
- **Tyle personalizacji, ile trzeba.** Użyj `{{first_name}}` i danych o roli, by wiadomość sprawiała wrażenie skierowanej do osoby — ale nie personalizuj w sposób niemożliwy dla prawdziwego zewnętrznego atakującego (to testuje inny model zagrożeń; zob. §32.3).

32.3 Targetowanie i poziom trudności

Nie każdy odbiorca powinien dostać ten sam e-mail. Dopasowanie pretekstu do odbiorców zwiększa realizm i pokazuje, gdzie naprawdę leży ryzyko.

- **Świadomość roli / działu.** Wykorzystaj dane kontaktów (`{{department}}`, `{{position}}`), by dobrać pasujące preteksty: przynęty fakturowe i płatnicze dla Finansów, resetu danych logowania dla zespołów technicznych, świadczeń i HR dla wszystkich, „prośby od zarządu” dla asystentów i osób zatwierdzających płatności (klasyczny wektor Business Email Compromise). Podziel odbiorców na Grupy i prowadź targetowane kampanie.
- **Ogólny vs. ukierunkowany (spear).** Szeroka, lekko spersonalizowana przynęta („Twoja skrzynka jest pełna”) modeluje masowy phishing. Symulacja spear-phishingu odwołuje się do realnego projektu, dostawcy czy osoby — znacznie trudniejsza do wykrycia i właściwy test dla celów o wysokiej wartości. Świadomie zdecyduj, który model zagrożeń mierzysz.
- **Stopniowanie trudności.** W ramach programu eskaluj. Zacznij od łatwych, oczywistych przynęt, by ustalić punkt odniesienia i zbudować nawyk zgłaszania; przechodź do subtelniejszych, dobrze zbrandowanych, kontekstowych wiadomości. Powtarzany łatwy test zawyża liczby, nie poprawiając odporności.

32.4 Czerwone flagi, które zasiewasz

Każdy symulowany phishing powinien zawierać *sygnały do nauki*, które chcesz, by pracownicy nauczyli się rozpoznawać. Wprowadzaj je celowo, a potem odnoś do nich wyniki:

- **Niezgodna / łudząco podobna domena nadawcy** (`micros0ft-support.com`).
- **Pilność i groźby** („działaj teraz albo stracisz dostęp”).
- **Ogólne powitanie** — właśnie dlatego nim sterujesz: wyślij części odbiorców wersję z `{{first_name}}`, a części ogólną, i porównaj. Jeśli personalizacja mocno podnosi współczynnik kliknięć, to wniosek wart przekazania.
- **Nieoczekiwany załącznik lub link**, niezgodność między tekstem linku a celem przy najechaniu.
- **Prośby o dane logowania lub płatność** omijające zwykły proces.

Podczas omówienia (przez kurs lub stronę edukacyjną) wskaż pracownikom konkretne flagi, które zawierała *ta* wiadomość. Konkret bije abstrakcję: „ten e-mail prosił o zalogowanie przez link z błędnie zapisaną domeną” trafia lepiej niż „uważaj w sieci”.

32.5 Lokalizacja i kultura

Przetłumaczony phishing to słaby phishing. Idiom, poziom formalności i lokalne normy biznesowe — wszystko to sygnalizuje autentyczność:

- Polscy odbiorcy reagują na treść napisaną naturalną polszczyzną, we właściwym rejestrze i z lokalnymi odniesieniami — nie na maszynowo przetłumaczony angielski. Wyselekcjonowane polskie szablony PhishSpot są **z tego powodu pisane przez polskojęzyczny zespół**, a nie tłumaczone automatycznie (zob. Szablony phishingowe).
- Lokalizuj pretekst, nie tylko język: podszywane marki, banki, firmy kurierskie i instytucje publiczne powinny być tymi, z których Twoi odbiorcy faktycznie korzystają.
- Dla odbiorców międzynarodowych segmentuj według języka/regionu i prowadź równoległe zlokalizowane kampanie, zamiast jednego e-maila „najmniejszego wspólnego mianownika".

32.6 Uczenie się z wyników

Perswazja to hipoteza; lejek w Raporty i analityka jest jej testem. Czytaj wyniki jako sygnał, nie jako tablicę wyników:

- Porównuj współczynnik **kliknięć** i **przesłań** — wiele osób klika z ciekawości, ale zatrzymuje się przed podaniem danych logowania. Różnica pokazuje, gdzie świadomość się broni.
- Rozbij wyniki według **działu/grupy**, by znaleźć skoncentrowane ryzyko, nie tylko średnią dla całej organizacji.
- Obserwuj **trend w czasie** w ramach programu — poprawa odporności z kampanii na kampanię to prawdziwa miara sukcesu, nie pojedynczy niski wynik.
- Śledź **zgłaszanie**, nie tylko klikanie — pracownik, który zgłosi symulację, to warunek zwycięstwa. Zob. Zgłoszone wiadomości.

32.7 Etyka i higiena programu

Granica między pożyteczną a szkodliwą symulacją to staranność, jaką wkładasz. Program, który upokarza ludzi, niszczy zaufanie i obniża zgłaszalność — czyli odwrotność tego, czego chcesz.

- **Pozostań w zakresie i autoryzacji.** Symuluj wyłącznie wobec własnej organizacji, za zgodą kierownictwa i (gdy wymagane) rady pracowniczej/HR. To szkolenie ze świadomości bezpieczeństwa, nie atak.
- **Unikaj okrutnych pretekstów.** Nie kuś premiami, podwyżkami, zwolnieniami, wynikami COVID/medycznymi ani niczym, co wykorzystuje realny lęk osobisty. Realistyczny ≠ bezduszny; takie tematy wywołują prawdziwe cierpienie i sprzeciw oraz trafiały na nagłówki z niewłaściwych powodów.
- **Szkól, nie zawstydzaj.** Niech akcja końcowa będzie momentem konstruktywnym — krótkim kursem lub uspokajającym „to była symulacja, oto na co zwracać uwagę" — nigdy publiczną listą tych, którzy zawiedli.

- **Wzmacniaj zgłaszanie.** Nagradzaj pożądane zachowanie: chwal osoby, które zgłaszają, ułatw zgłaszanie (zob. Dodatek do Outlooka) i traktuj kliknięcie jako okazję do coachingu, nie jako punkt karny.
- **Chroń dane.** Rozważ ponownie przechwytywanie prawdziwych haseł (zob. §30.3); często zarejestrowanie *samego faktu* przesłania wystarcza do uruchomienia szkolenia bez przechowywania wrażliwych wartości.

Prowadzona w ten sposób symulacja robi to, do czego służy: zamienia chwilę „prawie się na to nabrałem” w trwały nawyk ostrożności — i daje dane potwierdzające, że program działa.

Zobacz też: Projektowanie skutecznych kampanii · Kompatybilność z klientami poczty · Szablony phishingowe · Kursy · Grupy · Raporty i analityka · Zgłoszone wiadomości

Skróty klawiszowe i porady

- Skorzystaj z przełącznika kont na górze paska bocznego, aby szybko przemieszczać się pomiędzy zespołami.
- Edytor kodu Monaco obsługuje standardowe skróty klawiszowe: Ctrl+Z (cofnij), Ctrl+S (zapisz), Ctrl+F (szukaj).
- Klikaj nagłówki kolumn w widokach list, aby sortować dane.
- PhishSpot używa standardowej nawigacji URL — możesz używać przycisków Wstecz/Dalej w przeglądarce.

Słowniczek

Termin	Definicja
Kampania	Działania oparte na inscenizacji zdarzeń hakerskich — symulacji ataku wycelowanej w wybrany przez organizatorów zespół osób
Kontakt	Wewnętrzny lub zewnętrzny pracownik wyznaczonej przez operatorów komórki organizacyjnej z perspektywą na bycie zidentyfikowanym z systemami kampanijnymi
Grupa	Zespolony organizm klasyfikujący, służący do łączenia ludzi wedle założeń planistycznych danej misji w jeden zunifikowany twor decyzyjny
Szablon	Niestandardowy, bądź zaprezentowany użytkownikowi moduł roboczy pod ewentualne użycie dla systemów imitujących środowiska włamywaczy komputerowych
Strona Docelowa	Wygenerowany element stron opartych na sieci web wymuszający na nieprzygotowanym personelu uległość w procesie akwizycji niejawnych poufnych danych korporacyjnych po zalogowaniu na witrynę wskazaną linkiem wiadomości
Zabezpieczona Domena	Poświadczona własność domen e-mail służących przedsiębiorstwu jako główny punkt wyjściowy dla testów phishingowych
Domena Platformy	Strefa dedykowana na hostowanąe linków odsyłających do fikcyjnych podzespołów witryny platformowej opartej o mechanizmy kampanijne phishingu
Kurs	Zunifikowana jednostka szkoleniowa z zakresu budowania ogólnej ostrożności — przypisywana adresatom ulegającym atakom
Blok	Sekwencja edukacyjna — rozbita na mniejsze oddziały materiałowe jednostka sprawdzająca posiadana bądź przekazana wiedzę
Lejek	Wykres reprezentujący schemat weryfikacji etapowej przebiegu danej operacji: Wysłane → Otwarte → Kliknięte → Przesłane
Ocena Ryzyka	Określana wielostopniową jednostką matematyczną miara obnażająca skalę bezradności i potencjalnego braku doświadczenia badanej jednostki w zetknięciu ze wskaźnikami kampanii
Webhook	Zautomatyzowana metoda oparta na standardach przesyłu protokołu internetowego (HTTP) przekazująca raport incydentalny na system nadzorujący

Termin	Definicja
Token API	Elektroniczna forma przepustki — akredytacja dopuszczająca maszynowe zapytania zewnętrzne od obcego softwaru do głównych złącz struktury operacyjnej serwisu PhishSpot

Koniec dokumentu