SOPHOS
Security made simple.

# Sophos Phish Threat

## Wzmocnij swoją powierzchnię najbardziej narażoną na atak

Atakujący zawzięcie bombardują organizacje spamem, phisingiem i atakami wykorzystującymi zaawansowane metody inżynierii społecznej. Ponadto 41% specjalistów IT zgłasza ataki typu phishing co najmniej raz dziennie. Użytkownicy końcowi są często łatwym celem oraz najsłabszym ogniwem Twojego systemu cyberobrony. Spraw, by Twoi użytkownicy oraz Twoja firma byli bezpieczni, stawiając na rozwiązanie Sophos Phish Threat, które oferuje efektywne symulacje phishingu, automatyczne szkolenia i kompleksowe raportowanie.

## Najważniejsze informacje

- Ponad 140 realistycznych i ambitnych symulacji wspieranych przez najnowszą, globalną bazę wiedzy o zagrożeniach
- Spersonalizowane szkolenie dla użytkowników końcowych uczestniczących w symulowanym ataku
- Automatyczne raportowanie dotyczące phishingu i wyników szkolenia
- Dziewięć wersji językowych
- Wybór międzynarodowych regionów hostingu (Stany Zjednoczone, Irlandia, Niemcy)

## Bezpieczeństwo informacji jest tak skuteczne, jak skuteczne jest najsłabsze ogniwo systemu

Phishing to poważna sprawa. W ostatnich latach liczba ataków tego typu rekordowo wzrosła. 66% złośliwego oprogramowania jest teraz instalowane za pośrednictwem złośliwych załączników e-mail, a zaawansowane ataki typu spear phishing generują w firmach koszty wynoszące średnio 140 000 USD na jeden incydent. Użytkownicy nadal są najłatwiejszym celem osób atakujących systemy cyberobrony większości organizacji, jednak armia przeszkolonych i świadomych phishingu pracowników może stanowić doskonałą ludzką zaporę przed tego typu zagrożeniami.

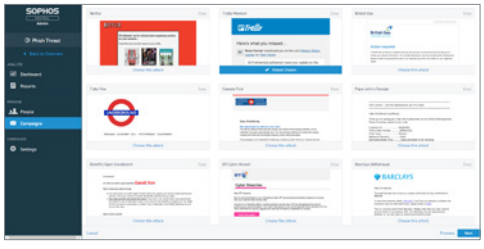
Sophos Phish Threat emuluje szereg różnorodnych ataków typu phishing, dzięki czemu ułatwia identyfikację słabych punktów systemu bezpieczeństwa organizacji oraz zachęca użytkowników do działania poprzez angażujące szkolenia wzmacniające kondycję zabezpieczeń organizacji.

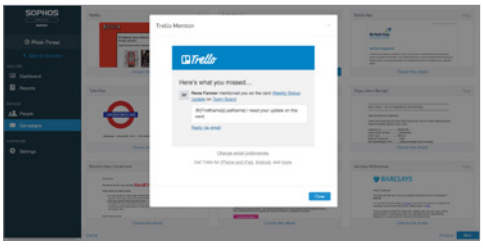
## Najnowsze kampanie

Pozwala symulować ponad 140 realistycznych i wymagających ataków typu phishing zaledwie kilkoma kliknięciami.

Analitycy Sophos, pracujący w laboratoriach SophosLabs na całym świecie, monitorują każdego dnia miliony wiadomości e-mail, adresów URL, plików i innych punktów danych pod kątem najnowszych zagrożeń. Ten stały strumień wiedzy gwarantuje, że szkolenia użytkowników wykorzystują aktualne taktyki obrony przed phishingiem, z szablonami symulacji ataków bazujących na inżynierii społecznej, obejmują wiele scenariuszy i zostały przetłumaczone na dziewięć języków:

- Angielski
- Niemiecki
- Francuski
- Włoski
- Hiszpański
- Portugalski
- Koreański
- Japoński
- Chiński tradycyjny





Zyskaj dostęp do stale powiększającej się biblioteki międzynarodowych szablonów — od poziomu początkującego po zaawansowany

## Efektywne moduły szkoleniowe

Ponad 30 interaktywnych modułów szkoleniowych informuje użytkowników o takich specyficznych zagrożeniach, jak podejrzane wiadomości e-mail, wyłudzanie danych uwierzytelniających, bezpieczeństwo haseł i zgodność z przepisami. Dostępne w dziewięciu językach, informują i angażują użytkowników końcowych, a Ty możesz cieszyć się spokojem ducha w przypadku przyszłych rzeczywistych ataków:

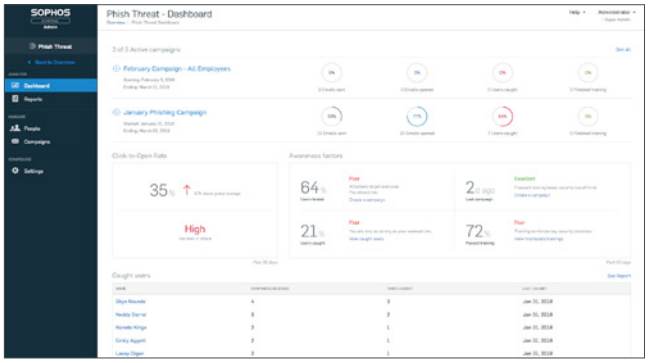

Angażuj użytkowników poprzez szereg interaktywnych modułów szkoleniowych

## Kompleksowe raportowanie

Poznaj kondycję bezpieczeństwa swojej organizacji i zaprezentuj faktyczny zwrot z inwestycji za pomocą intuicyjnego panelu sterowania z raportem o efektach działania dostępnym na życzenie. Panel sterowania Phish Threat pozwala szybko sprawdzić, jak kampania wpływa na podatność użytkowników, oraz zmierzyć ogólny poziom ryzyka w całej grupie użytkowników za pomocą danych mających wpływ na współczynnik świadomości, takich jak:

- Bieżący wskaźnik podatności użytkowników
- Całkowita liczba przetestowanych użytkowników
- Całkowita liczba oszukanych użytkowników
- Liczba dni od ostatniej kampanii
- Średni pozytywny wynik szkolenia

Raporty drążenia danych zapewniają głębszy wgląd na wydajność na poziomie organizacji lub poszczególnych użytkowników, dając lepsze spojrzenie na temat ogólnej kondycji bezpieczeństwa organizacji.




Interaktywne raporty mierzą ogólny poziom ryzyka i wydajności użytkowników

## Phish Threat to składnik pakietu Sophos Central

Phish Threat to składnik pakietu Sophos Central, naszej bazującej na chmurze, zintegrowanej konsoli do zarządzania bezpieczeństwem, dlatego jest łatwo dostępny w całej organizacji IT. Oznacza to, że nie jest konieczna instalacja żadnego sprzętu ani oprogramowania, a Ty możesz korzystać z jedynego rozwiązania umożliwiającego zarządzanie symulacjami ataków typu phishing i szkoleniami użytkowników, jak również bezpieczeństwem poczty e-mail, urządzeń końcowych, urządzeń przenośnych, i wiele więcej. Otrzymujesz pojedynczą, aktualną i obsługiwaną przez Sophos platformę, która jest intuicyjna i łatwa w obsłudze. Dowiedz się więcej pod adresem sophos.com/central.

## Łatwe rozpoczęcie pracy

Sophos Phish Threat można wygodnie uruchomić z poziomu przeglądarki internetowej. Aby mieć pewność, że wiadomości e-mail Phish Threat są pomyślnie dostarczane, wystarczy dodać do białej listy adresy IP przedstawione w konsoli Sophos Central oraz adresy i domeny e-mail używane w Twoich kampaniach Phish Threat. Następnie wystarczy zaimportować użytkowników z pliku CSV albo za pomocą wygodnego narzędzia synchronizacji usługi Active Directory. Po wczytaniu użytkowników można rozpocząć swoją pierwszą kampanię.

## Jak kupić?

Cena pojedynczej licencji Sophos Phish Threat zależy od liczby użytkowników: od 1 do ponad 5000. Obowiązuje nieograniczona liczba testów na jednego użytkownika, dzięki czemu można skupić się na ochronie użytkowników i firmy przed dzisiejszymi zaawansowanymi atakami typu phishing.

## Wypróbuj bezpłatnie przez 30 dni

Zarejestruj się pod adresem sophos.com/phish-threat, aby otrzymać bezpłatną wersję testową dla 100 użytkowników.

Dział sprzedaży w Polsce:Sophos Ltd. (Poland)
ul. Rzymowskiego 53, 02-697 Warszawa
Email: salesee@sophos.com



2018.luty. DSPL (NP)

SOPHOS