CYBERSECURITY FOUNDATION

Bezpieczeństwo Firmy

w rękach jej pracowników

MATERIAŁ POWSTAŁ WE WSPÓŁPRACY Z SHARP

CYBERSECURITY FOUNDATION
RECOMMENDED
SHARP
SHARP SECURITY AWARENESS TRAINING
NOVEMBER 2024

2024

Sharp Security Awareness Training

Skuteczne szkolenia z cyberbezpieczeństwa

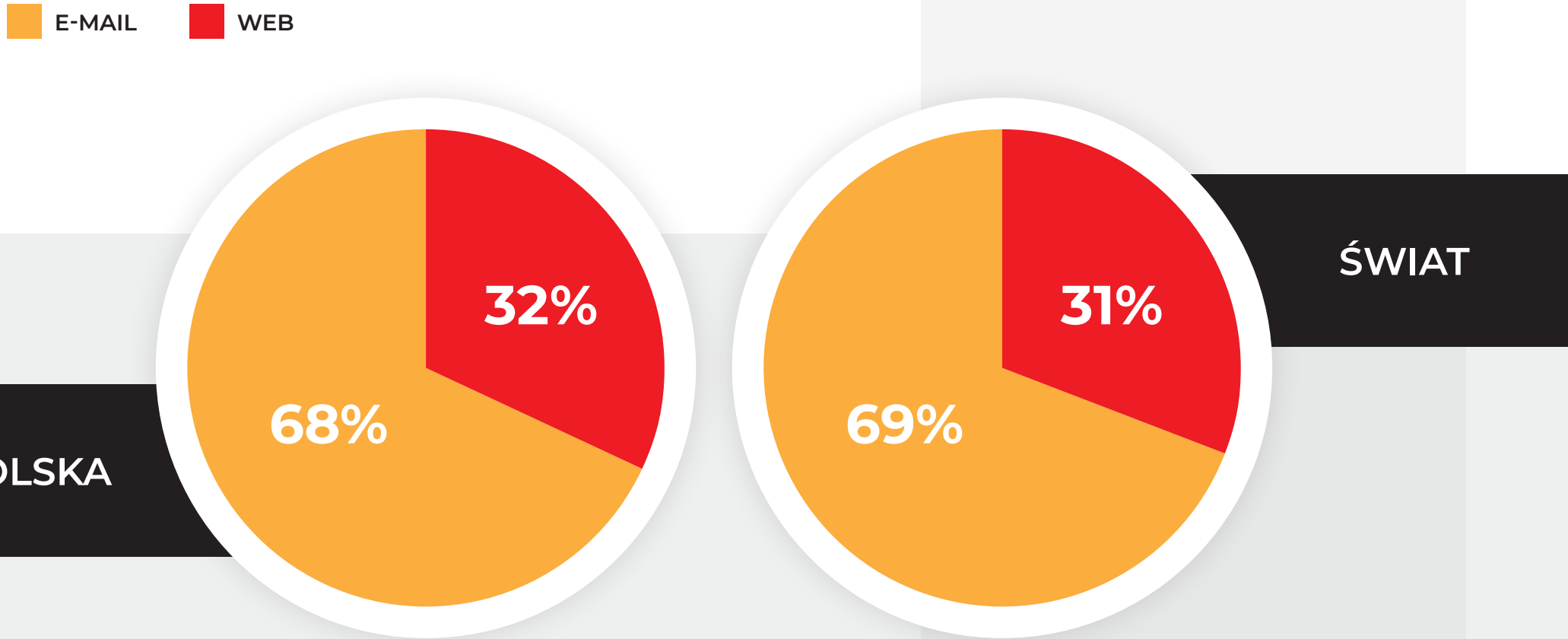
Spis treści

Szkolenia staną się standardem

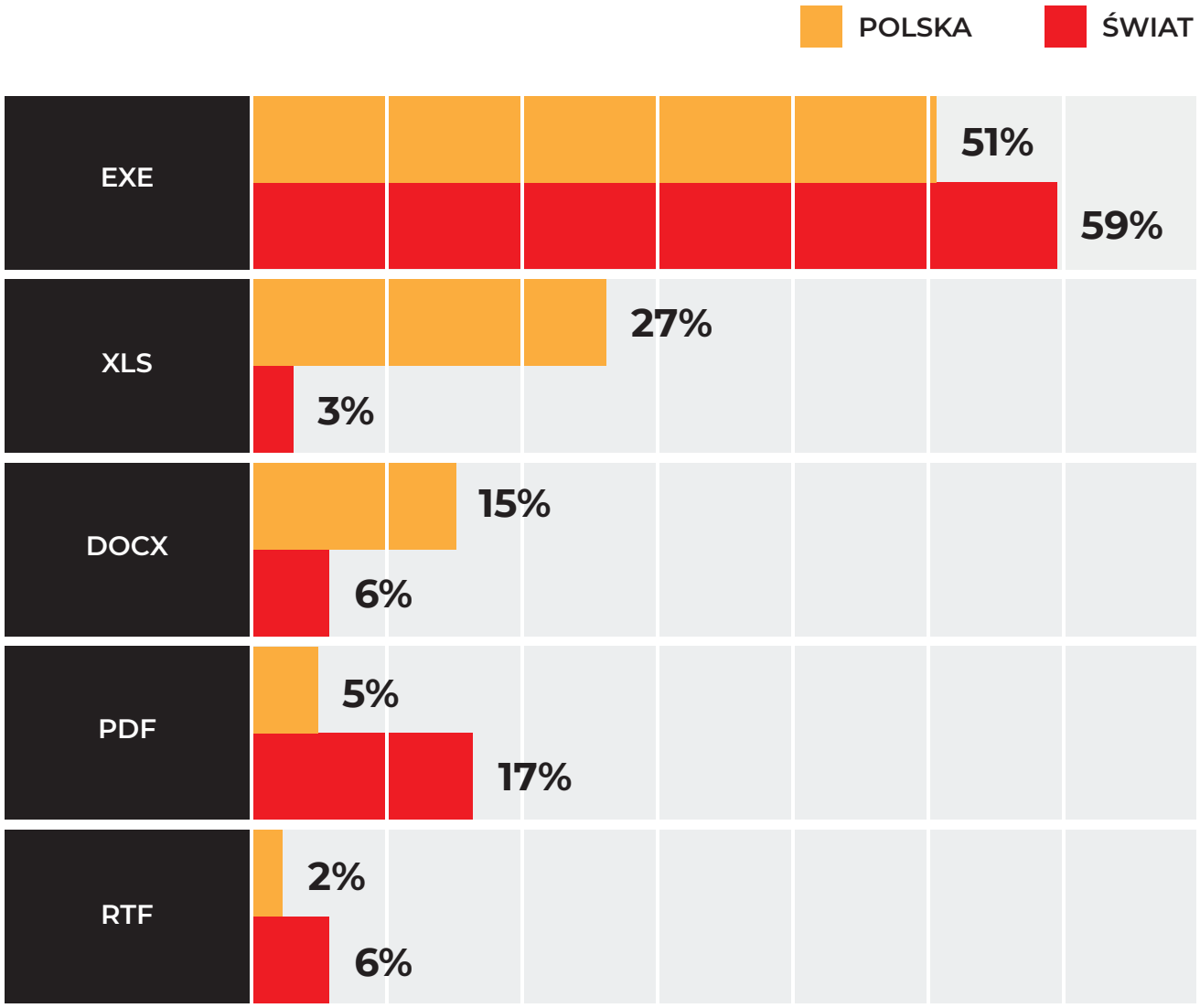
W dobie wielowektorowych zagrożeń cybernetycznych, rola człowieka jako najsłabszego ogniwa w łańcuchu bezpieczeństwa organizacji, jest coraz bardziej odczuwalna. Firmy powinny inwestować w zaawansowane narzędzia i technologie obronne, jednak bez odpowiednio przeszkolonego personelu, każde z tych rozwiązań może się okazać niewystarczające. W Polsce nowy obowiązek prawny w ramach przeprowadzania szkoleń nakłada Krajowy System Cyberbezpieczeństwa (KSC) – operatorzy i dostawcy usług kluczowych muszą zwiększać świadomość pracowników w zakresie zagrożeń cybernetycznych by przeciwdziałać negatywnym konsekwencjom. KSC będzie aktualizowany, aby implementować dyrektywę NIS 2, ale już teraz wiadomo, że nowe przepisy zwiększą odpowiedzialność kadry, która zarządza podmiotami kluczowymi. Za brak wywiązywania się z obowiązków będą grozić firmie kary finansowe, a zarządowi odpowiedzialność osobista i kary dyscyplinarne.

Najnowsze dane firmy Check Point są potwierdzeniem tezy zawartej we wstępie o konieczności zwiększenia świadomości pracowników w zakresie cyberataków. Dane pokazują, że od stycznia 2024 roku cyberprzestępcy najczęściej atakują organizacje nie poprzez luki w systemach informatycznych, lecz z wykorzystaniem socjotechniki. W Polsce oraz na świecie głównym wektorem ataku nadal są aplikacje poczty oraz przeglądarki internetowe obsługiwane przez pracowników. Natomiast autorzy złośliwego oprogramowania najczęściej ukrywają je pod postacią znanych typów plików: EXE, XLS i DOCX (Excel, Word), PDF i RTF (kompatybilny z wieloma edytorami tekstu: OpenOffice, Google Docs, LibreOffice).

Porównanie tego samego wektora ataku w Polsce oraz na świecie:

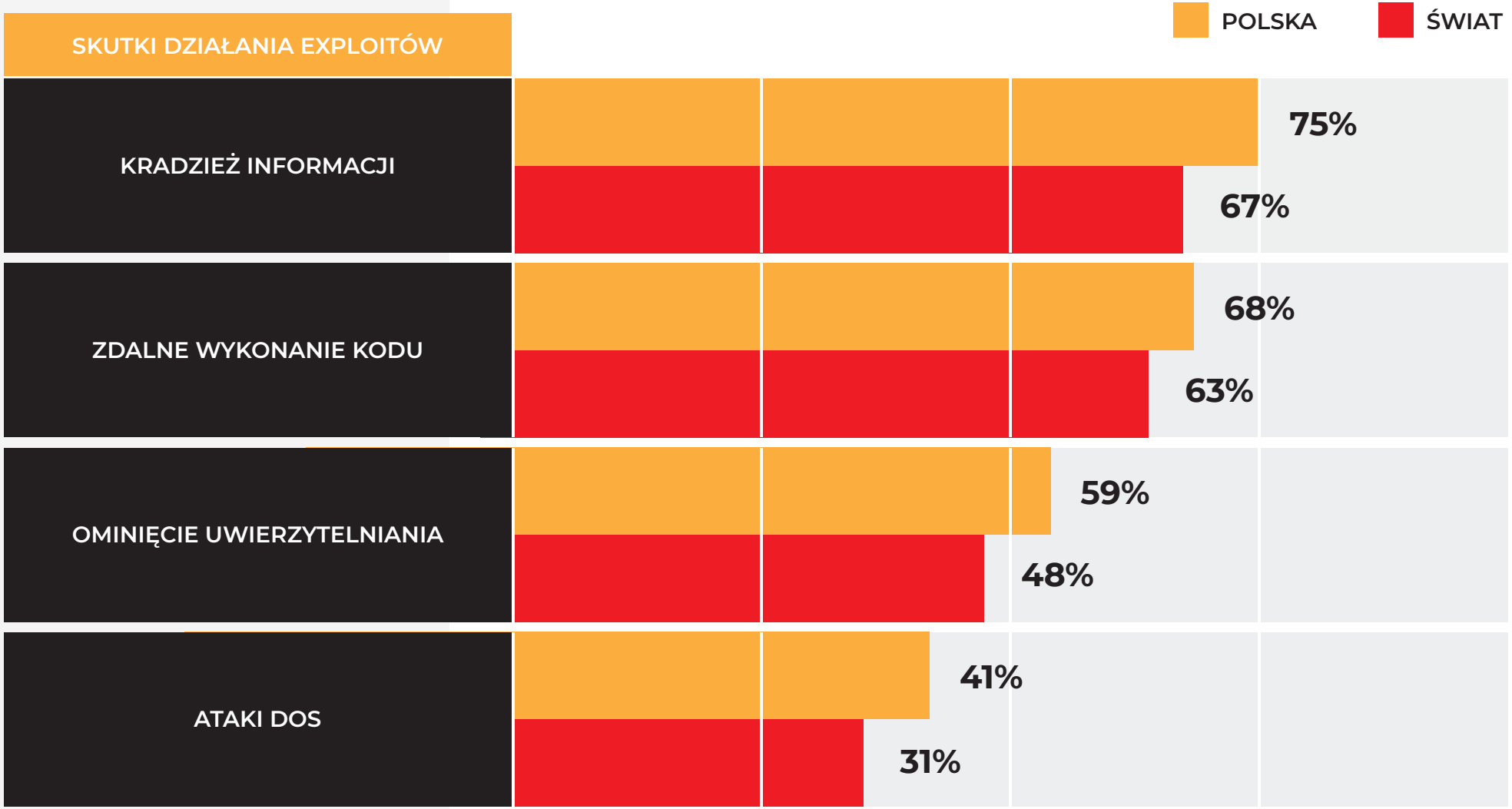


Główne typy zainfekowanych plików dostarczonych przez e-mail



Dane tylko potwierdzają, jak ważną rolę w cyberbezpieczeństwie odgrywa człowiek – brak odpowiedniego przeszkolenia może doprowadzić do zainicjowania ataku przez pracownika. W wyniku błędu ludzkiego niezwykle często dochodzi do ujawnienia poufnych informacji firmowych (75%), zdalnego uruchomienia szkodliwego kodu (68%), przekazania danych logowania (59%) i spowodowania odmowy dostępu do usługi (44%) w wyniku zezwolenia na uruchomienie szkodliwego oprogramowania.

Najczęstsze rodzaje cyberataków w Polsce i na świecie



Opracowano na podstawie danych dostarczonych przez Check Point za Q1 2024.

Dane telemetryczne firmy Malwarebytes o zasięgu globalnym pokazują jeszcze jeden trend. Otóż cyberprzestępcy chętnie używają wizerunku znanych firm oraz usług online, aby ukrywać złośliwe reklamy i linki do złośliwego oprogramowania. Tak zwany malwaretising jest niezwykle atrakcyjną metodą na infekowanie komputerów, ponieważ przybiera szeroki zasięg niskim kosztem finansowym, czasami jest trudny do wykrycia i może rozprzestrzeniać różnego rodzaju niebezpieczne oprogramowanie takie jak: ransomware, spyware, trojany bankowe.

Dla przestępców złośliwe reklamy mają kilka zalet w porównaniu ze złośliwymi załącznikami w wiadomościach e-mail. Użytkownicy są znacznie mniej świadomi takich ataków i rzadko są przeszkoleni w ich wykrywaniu.

5 najczęściej wykorzystywanych hostów do dystrybuowania złośliwego oprogramowania

4Sync

Discord

Dropbox

GitLab

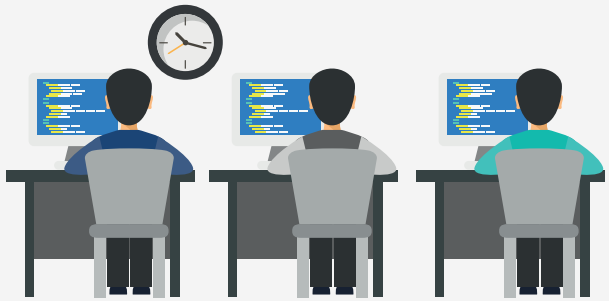
Google

Opracowano na podstawie danych z raportu Malwarebytes pt. „State of Malware 2024: What consumers need to know”
https://www.threatdown.com/typ-state-of-malware-2024/

Z perspektywy osób zarządzających bezpieczeństwem IT, ważną kwestią jest odpowiednie dobranie, wdrożenie i skonfigurowanie rozwiązania, aby podnieść poziom bezpieczeństwa firmy. Inwestowanie w omawiane w tym raporcie szkolenia, staje się nieodłącznym elementem strategii cyberbezpieczeństwa każdej organizacji. Dlatego z myślą o licznych wyzwaniach powstała usługa Sharp Awareness Training – szkolenia, które mają na celu podnoszenie świadomości na temat zagrożeń cybernetycznych wśród pracowników na każdym szczeblu organizacji.

Dobre szkolenie z zakresu cyberbezpieczeństwa powinno odwzorowywać realne scenariusze, z którymi pracownicy mogą spotkać się na co dzień. Pozwala to uczyć się nie tylko teorii, ale przede wszystkim praktycznego podejścia do ochrony przed cyberatakami. Co więcej dobrze przeprowadzone szkolenie minimalizuje liczne ryzyka związane z błędami ludzkimi, a to w jaki sposób zrealizowane kursy z zagadnień ataków socjotechnicznych sprawdzają się w praktyce, omawiamy w tym materiale.

Sharp Security Awareness Training może stanowić istotny krok w kierunku poprawy bezpieczeństwa oraz budowania pewności, że firma jest odpowiednio przygotowana na wyzwania związane z zagrożeniami socjotechnicznymi kolejnych generacji.



Technicznie o Sharp Security Awareness Training

Security Awareness Training od Sharp to usługa szkoleń online dotycząca wielu aspektów bezpieczeństwa IT. Składa się z kilkudziesięciu modułów, które są regularnie aktualizowane. Użytkownicy, którzy zostali zaproszeni do szkolenia, otrzymują wiadomości e-mail z linkami do modułów edukacyjnych wraz z okresowymi przypomnieniami, jeżeli jeszcze nie zapoznali się z daną tematyką. Dodatkowo Sharp automatycznie dba o przeprowadzane symulacje prawdziwych ataków, z których dostępne są szczegółowe raporty. Dostęp do statystyk posiadają osoby z rolą administratora organizacji.

Malicious Activity

All-Time Clicked Simulations and Other Malicious Activity

Search | Filter | Export

Name	Latest activity	Ignored	Clicked	Click Rate
Word Document Macro Malware Malware	2024-09-23	0	1	100%
Microsoft Security Update Malware Malware	2024-10-02	0	2	100%
HR emergency contact Credential Stealing Scam En Fraud	2024-09-27	0	1	100%
Microsoft Credentials Stealer EN Fraud	2024-09-28	0	1	100%
Fake Sender PDF Malware	2024-10-10	0	2	100%
Dropbox file sharing Phishing PL Fraud	2024-10-08	0	1	100%

Możemy wypunktować, że na szeroko rozumiane bezpieczeństwo IT w skali przedsiębiorstwa, składa się kilka czynników. Oprócz dedykowanych rozwiązań ochrony urządzeń końcowych zainstalowanych na urządzeniach pracowników, całościowego monitoringu ruchu sieciowego, rejestrowania dostępu do zasobów, zarządzania podatnościami, uwierzytelnianiem użytkowników i mikro-autoryzacją, kluczowym czynnikiem wciąż pozostają umiejętności techniczne pracowników. Zaawansowane narzędzia potrafią wykrywać, blokować i raportować różne ataki, natomiast nie istnieją w pełni niezawodne rozwiązania, które zapewnią całkowitą ochronę. Dodatkowo systemy zabezpieczające monitorują przepływ informacji wyłącznie na urządzeniach w sieci korporacyjnej, a gdy pracownik do celów służbowych wykorzystuje prywatny sprzęt, nie ma bezpośredniej możliwości ochrony i monitorowania jego aktywności. Zagrożenia związane z brakiem odpowiednich zabezpieczeń nie pojawiają się wyłącznie podczas wykonywania czynności służbowych — pracownik może otrzymać wiadomość phishingową na jednym z serwisów społecznościowych.

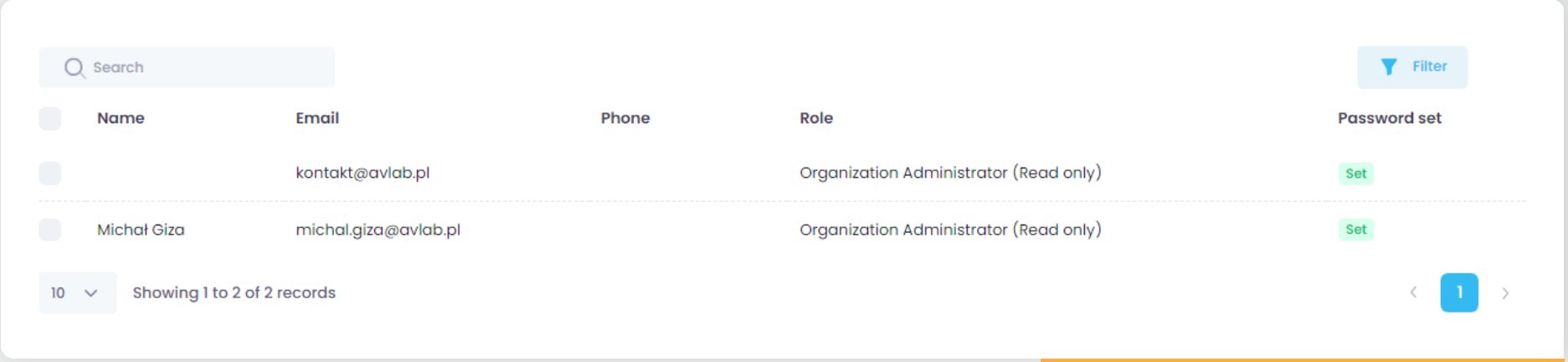
Sposobem na zwiększenie umiejętności pracowników są szkolenia. W praktyce samo przeprowadzenie lekcji edukacyjnych może nie być wystarczające, ponieważ wiedzę możliwą do zdobycia trzeba zweryfikować, utrwalać i uzupełniać – najlepiej na przykładach rzeczywistych ataków. Nawet, jeśli w strukturach firmy znajduje się dział IT, to kompleksowe przygotowanie wartościowego szkolenia z pewnością zajmie znaczną ilość czasu. Dlatego odpowiednim rozwiązaniem może być skorzystanie z zewnętrznych usług w takim zakresie.

Przedmiotem tej analizy są szkolenia Sharp Awareness Training dostępne w ofercie firmy Sharp. Stanowią one przykład dostępnych dla każdego treści z zakresu cyberbezpieczeństwa.

https://www.sharp.pl/uslugi-it/cyberbezpieczenstwo/security-awareness-training-platforma-szkoleniowa-z-zakresu

Backend platformy szkoleniowej to Nimblr

Security Awareness Training od Sharp działa w ramach platformy Nimblr. Wiąże się to z ograniczonymi możliwościami dla klienta końcowego, który m.in. nie posiada uprawnień do samodzielnego zarządzania użytkownikami. Najwyższą możliwą rolą, przykładowo dla pracownika działu IT w firmie, jest Organization Administrator (Read Only).



LISTA ADMINISTRATORÓW DANEJ ORGANIZACJI

Za faktyczną administrację udostępnionej platformy odpowiadają przedstawiciele firmy Sharp. O ile dla zaawansowanych użytkowników może być to pewną niewygodą, to jednak w wielu przypadkach zastosowane podejście jest zaletą, ponieważ nie ma potrzeby zapoznawania administratorów po stronie klienta z technicznymi kwestiami obsługi platformy. Osoby z wymienioną rolą Organization Administrator posiadają pełny dostęp do zawartości szkoleń i śledzenia postępów użytkowników.

III Zakres modułów szkoleniowych

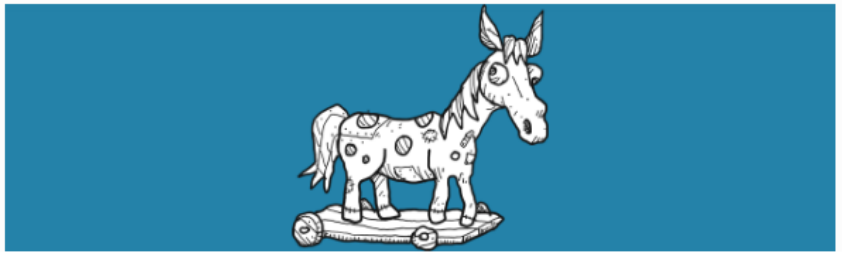
Liczbę dostępnych tematów należy ocenić jednoznacznie pozytywnie. Na czas przygotowywania tej recenzji dostępnych jest kilkadziesiąt szkoleń, w tym jedno jako podstawowe wprowadzenie do tematyki cybersecurity i platformy Nimblr, poruszające w zasadzie każdy znaczący aspekt cyberbezpieczeństwa.

LISTA MODUŁÓW OBEJMUJE NASTĘPUJĄCE TEMATY

- PHISHING
- ZŁOŚLIWE OPROGRAMOWANIE
- ATAKI SOCJOTECHNICZNE
- BEZPIECZEŃSTWO FIZYCZNE
- DOKUMENTY MS OFFICE I ZŁOŚLIWE MAKRA
- NIEBEZPIECZNE KODY QR
- ZAGROŻENIA WEWNĘTRZNE
- BEZPIECZEŃSTWO URZĄDZEŃ MOBILNYCH

Linki do szkoleń są wysyłane do użytkowników w sposób automatyczny. Czas na ich przerobienie jest nieograniczony. Pracownicy otrzymują także okresowe przypomnienia o szkoleniach, które trzeba uzupełnić – maksymalnie jedno w tygodniu dla danego szkolenia. Co więcej, poziom trudności szkoleń jest automatycznie dostosowywany do poziomu wiedzy użytkownika i jego postępów.

PRZYKŁADOWE DOSTĘPNY MODUŁ SZKOLENIOWY



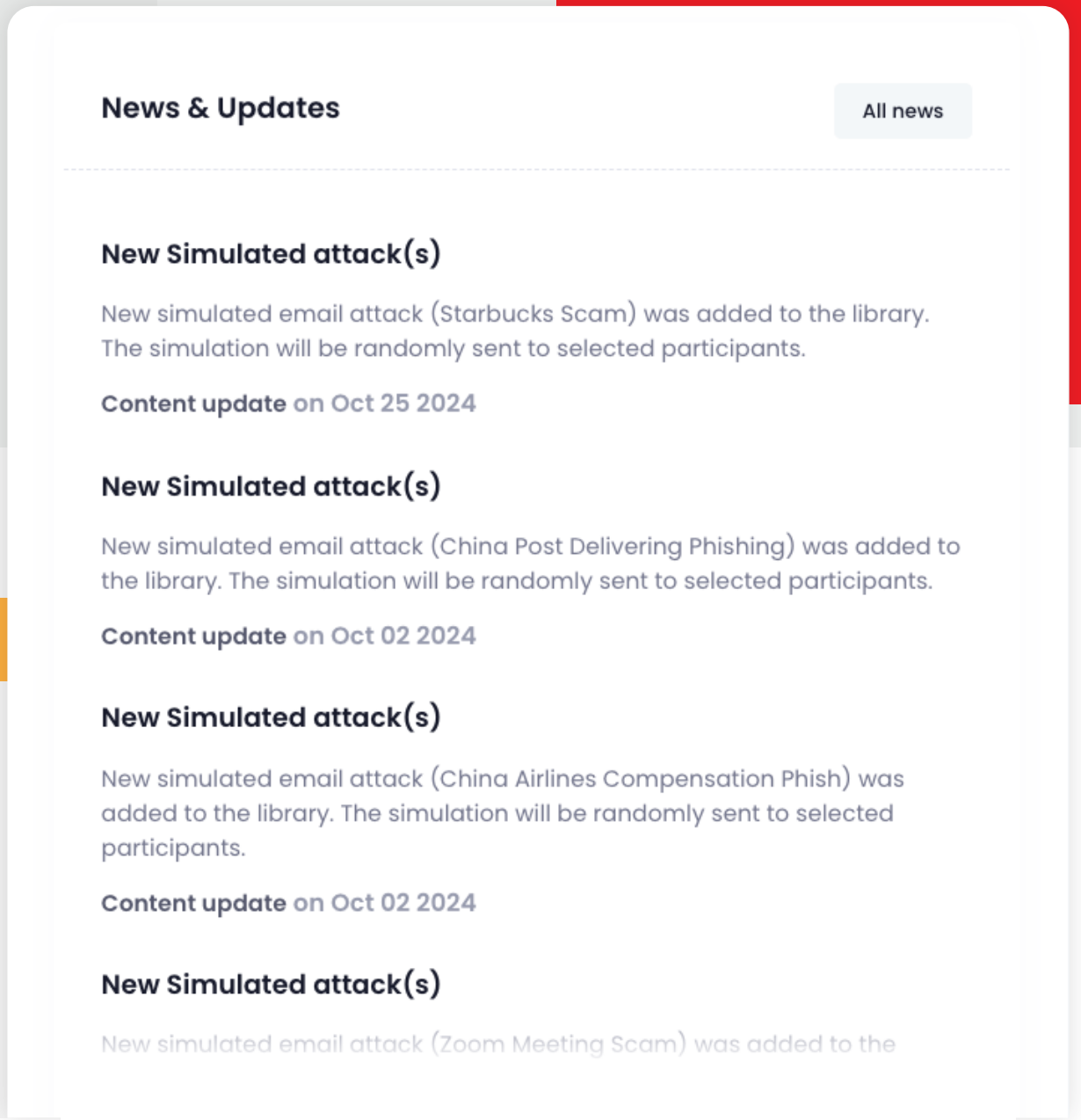
Trojans and Adware

This training module describes what trojans are, and that malicious code can be hidden in legitimate software. The user is made aware of the risks of adware and software downloaded from the internet.

Content update on Jul 29 2024 Preview

Ważnym czynnikiem decydującym o jakości szkoleń jest ich dopasowanie do aktualnych trendów występujących zagrożeń i technik ataków socjotechnicznych. W przypadku usługi Sharp Security Awareness Training to założenie zostało w pełni spełnione. Treść szkoleń jest aktualizowana (także o opisy znaczących podatności 0-day), a lista wprowadzonych zmian jest widoczna w panelu platformy.

NOWE SYMULACJE ATAKÓW DODAWANE SĄ DO PLATFORMY W SPOSÓB AUTOMATYCZNY



That’s the Way It Goes

A hotel with electronic locks was affected by ransomware and inadvertently locked out its guests when the system controlling the locks stopped working.

The Ransomware Attack That Locked Hotel Guests Out of Their Rooms

This is a good demonstration of why electronic systems need physical backups.

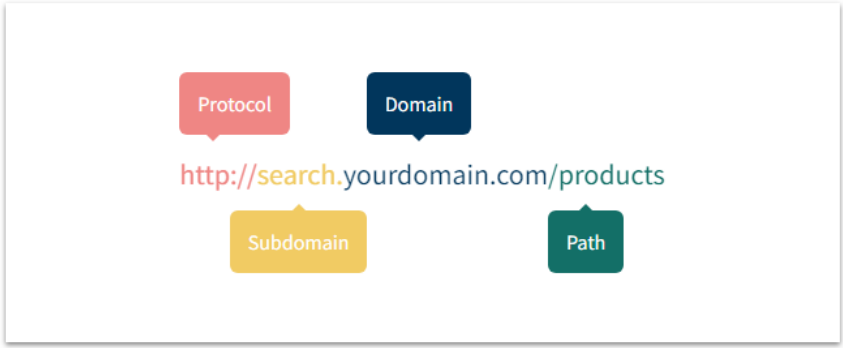
By Josephine Wolff

Romantik Seehotel Jaegerwirt in Austria.

Moduły szkoleniowe są łatwe do zrozumienia i nie powinny stanowić trudności, niezależnie od poziomu dotychczasowej wiedzy użytkownika, ponieważ wszelkie techniczne aspekty, konieczne do lepszego poznania danego zagadnienia, zostały wyjaśnione. Można powiedzieć, że każde szkolenie jest dobrze dopełnione (dany temat został w nim kompleksowo omówiony) i dostosowane do różnych stanowisk, gdyż pomimo zorientowania na użytkownika nietechnicznego, omawiają ważne kwestie.

DUŻĄ ZALETĄ SZKOLENIA JEST PODANIE RZECZYWISTYCH PRZYKŁADÓW ATAKÓW W NIEKTÓRYCH MODUŁACH SZKOLENIOWYCH

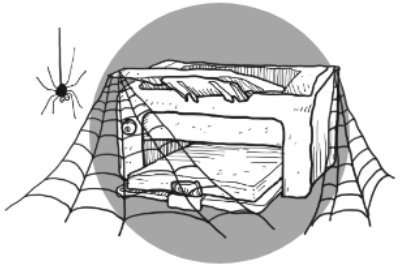
Links



By learning how web pages, links, and domain names work, you can avoid many dangers on the web. Understanding and discerning domain names in links can be crucial to your organization's security.

GRAFICZNE PRZEDSTAWIENIE CZĘŚCI ADRESÓW URL W JEDNYM ZE SZKOLEŃ

Printing and Scanning



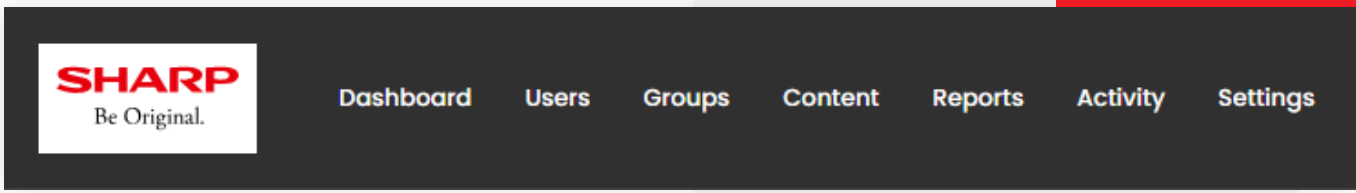
Quickly retrieve printed documents from shared printers and ensure that the entire print job is complete.

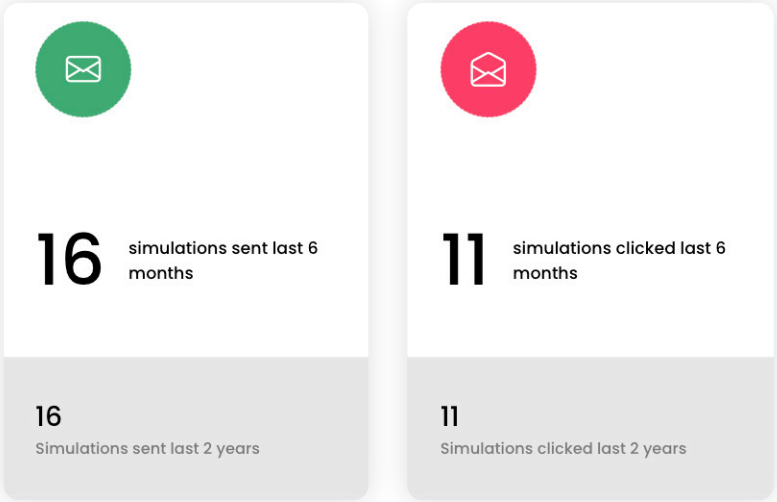
Remember, never leave sensitive documents in a scanner, even if it's a private scanner. Scanners can be activated remotely through networks, allowing unauthorized individuals to access documents left inside.

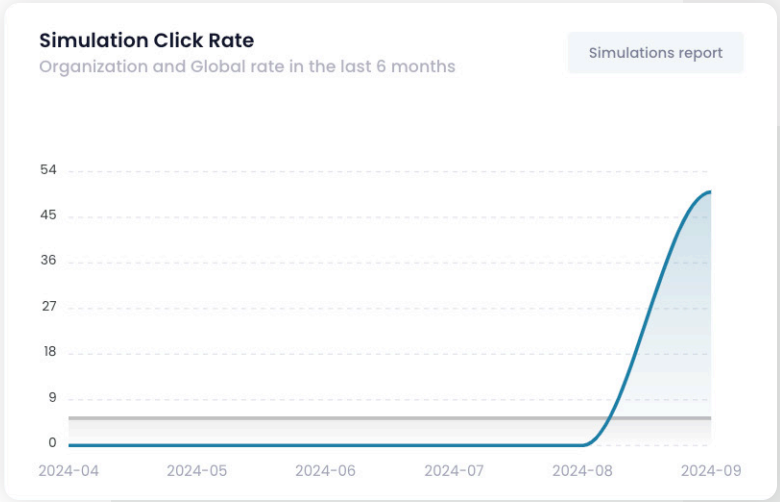
SZKOLENIA ZAWIERAJĄ ŁATWE DO WDROŻENIA I ZAPAMIĘTANIA ZASADY BEZPIECZEŃSTWA

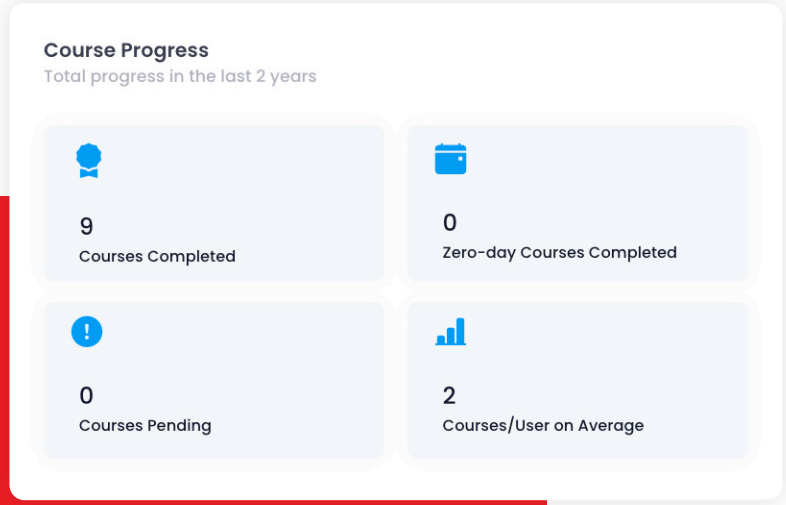
IV Łatwość korzystania w panelu administratora

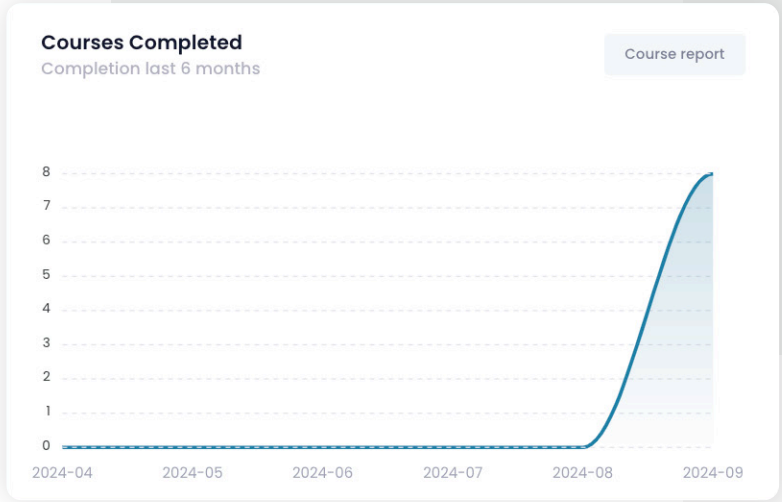
Platforma zapewnia przejrzysty interfejs, którego obsługa nie wymaga dodatkowych instrukcji. Z perspektywy administratora panel został podzielony na siedem zakładek.



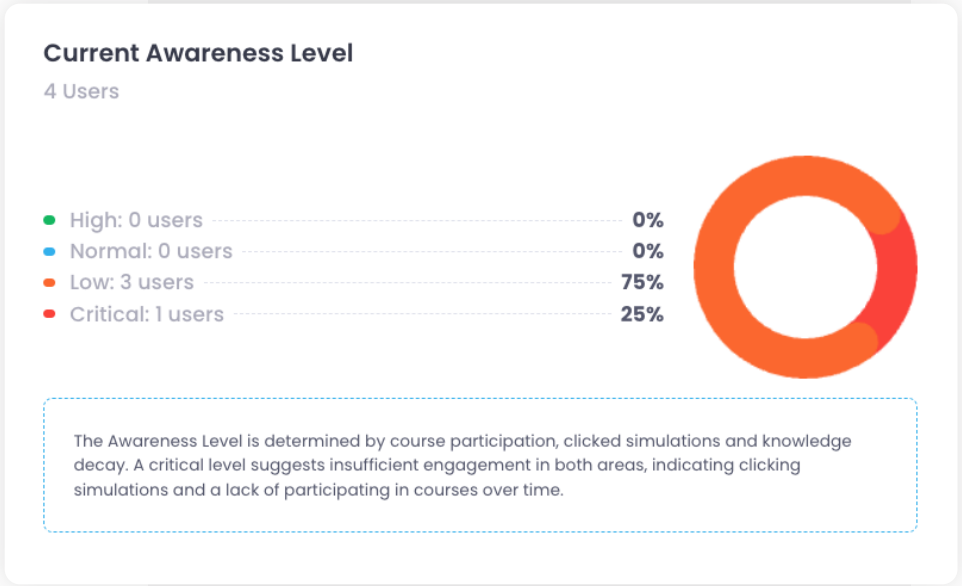


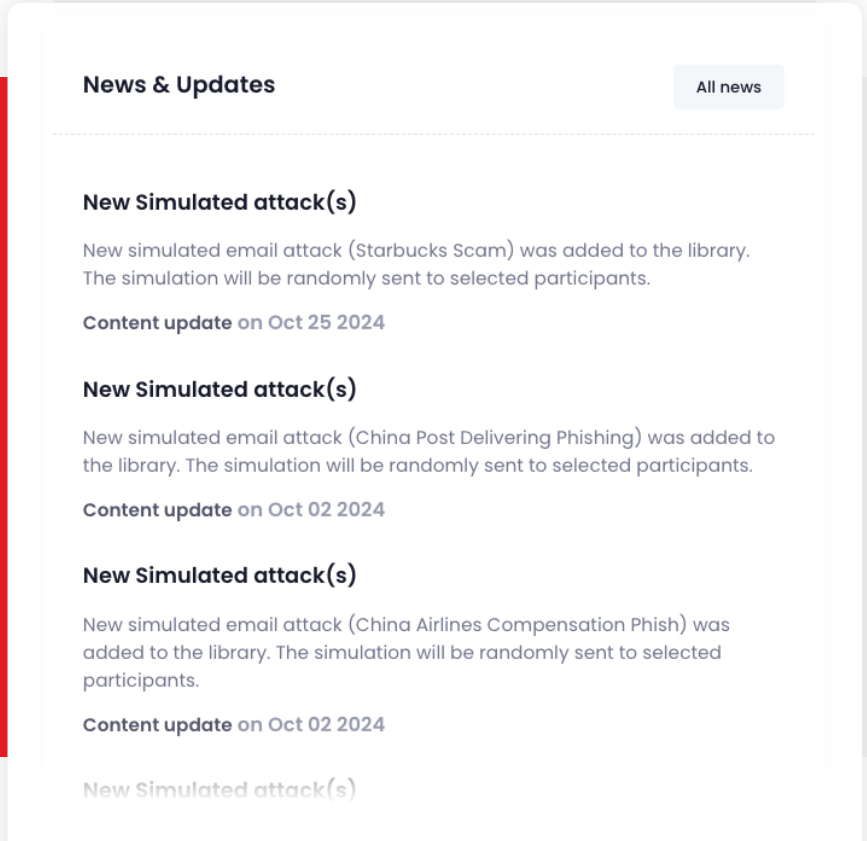




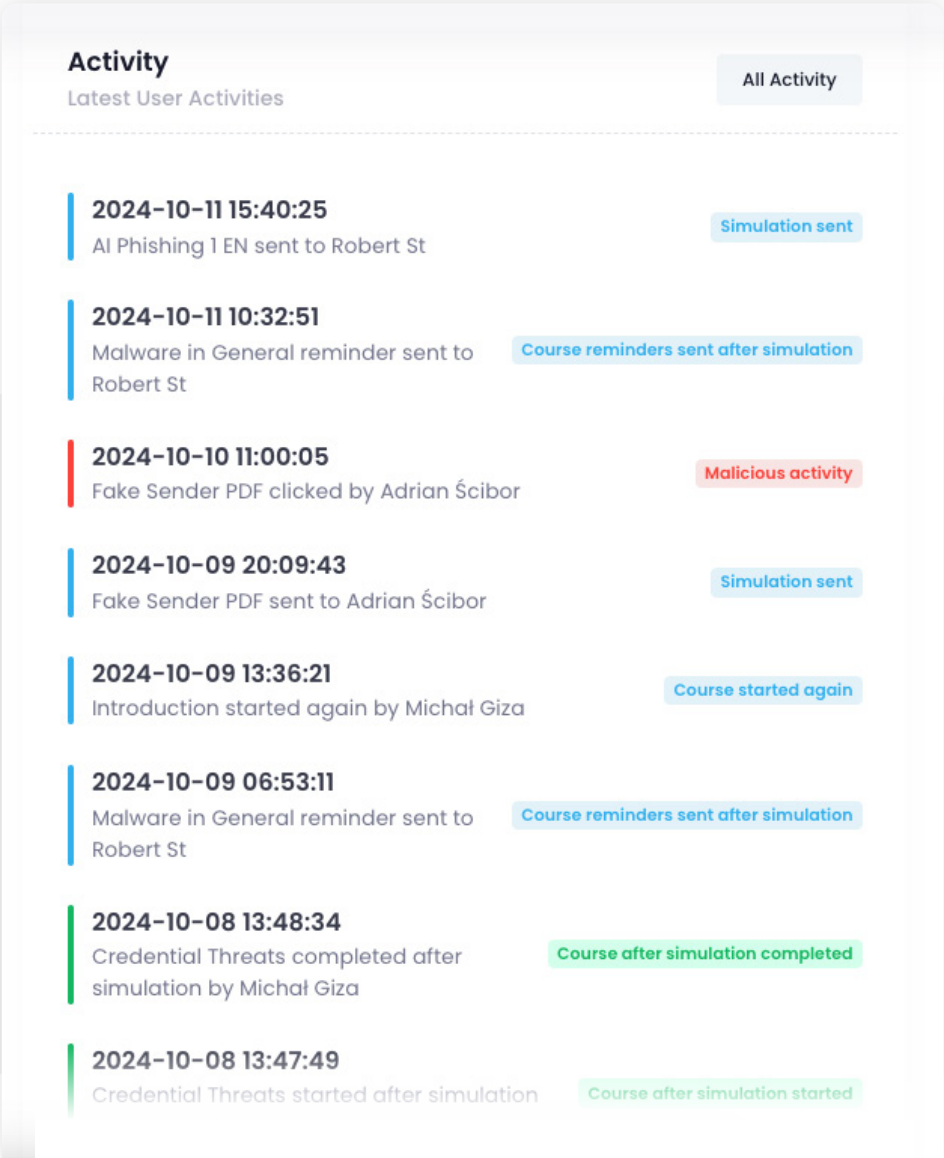


Domyślną zakładką po zalogowaniu jest Dashboard, który umożliwia wygodny podgląd stanu platformy. Dostarcza informacji o liczbie ukończonych szkoleń i symulacji, statystykach poziomu świadomości użytkowników, liczbie zalogowanych użytkowników czy ostatnich aktywnościach.





Dashboard w Sharp Security Awareness Training umożliwia monitorowanie postępów oraz analizowanie wyników. W widoku można przeglądać statystyki, wyniki ukończonych modułów (poziom wiedzy uczestników) i wskaźniki efektywności postępów. Dzięki takim informacjom możliwa jest identyfikacja obszarów wiedzy pracowników, która wymaga szczególnej uwagi.



ZAPROSZENIE DO NOWEGO SZKOLENIA

Avlab Trial Security Awareness Training

Phishing – e-mail i strony internetowe

Tutaj wyjaśniono pojęcie "phishingu" i zaprezentowano przykłady, w jaki sposób fałszywe wiadomości e-mail i strony internetowe próbują wyłudzić od Ciebie poufne informacje, a także dobre rady i konkretne wskazówki, jak rozpoznać próbę phishingu.

Szkolenie trwa około 3-6 minut.

Zacznij szkolenie!

Możesz również rozpocząć kurs, korzystając z tego linku:
https://awrns.net/course/phishing-email-and-web-pages/32b4a154-2e0b-4d2e-96b5-83e090d10c84

Ostatnio ukończone kursy

Phishing – e-mail i strony internetowe	Wrzesień 26, 2024	★
Linki i domeny	Wrzesień 22, 2024	★
Wstęp	Wrzesień 17, 2024	★

Ostatnie symulacje

Microsoft Credentials.....	Wrzesień 27, 2024	Kliknięty
Fake LinkedIn InMail	Wrzesień 27, 2024	Zatwierdzone

WIADOMOŚCI ZAWIERAJĄ LISTĘ OSTATNIO PRZEROBIONYCH SZKOLEŃ I OTRZYMANYCH SYMULACJI

Jeśli uczestnik szkolenia nie wykazuje aktywności tzn. moduł nie został od pewnego czasu ukończony, użytkownik otrzymuje przypomnienie. W przypadku szkoleń istotne jest zachowanie systematyczności, dlatego ta funkcjonalność zdecydowanie spełnia swoje zadanie.

PRZYPOMNIENIE O MOŻLIWOŚCI UKOŃCZENIA SZKOLENIA

Avlab Trial Security Awareness Training

Zagrożenia dla danych uwierzytelniających

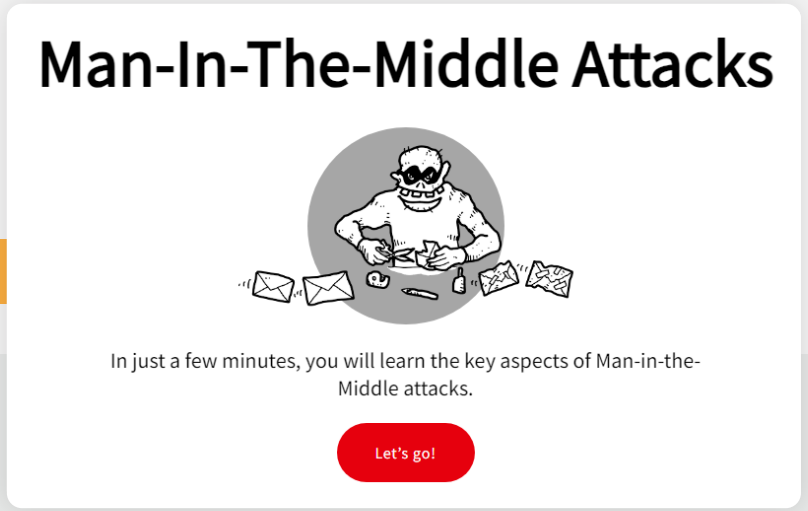
To jest przypomnienie. Nie dokończyłeś szkolenia: Zagrożenia dla danych uwierzytelniających. Szkolenie trwa około 3-6 minut.

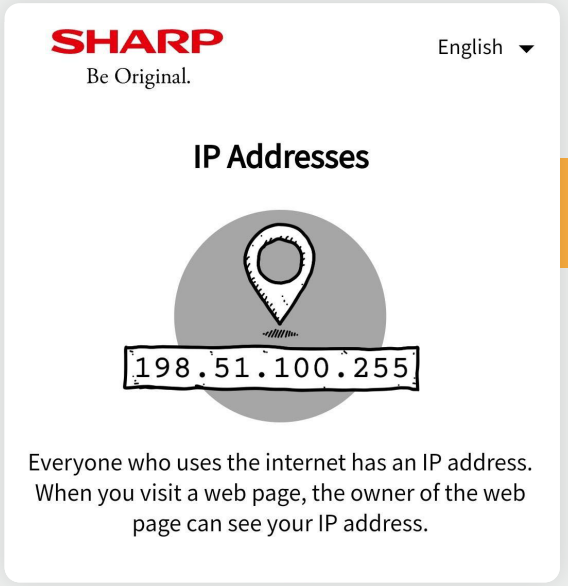
Zacznij szkolenie!

Możesz również rozpocząć kurs, korzystając z tego linku:
https://awrns.net/course/credential-threats/32b4a154-2e0b-4d2e-96b5-83e090d10c84

Moduły szkoleniowe zawierają slajdy i (ewentualnie) pytania dotyczące przekazanej wiedzy. Zostały przetłumaczone na różne języki, w tym na język polski. Widoczny jest też pasek postępu w przybliżeniu określający ilość pozostałych slajdów w module.

EKRAN POCZĄTKOWY MODUŁU SZKOLENIOWEGO



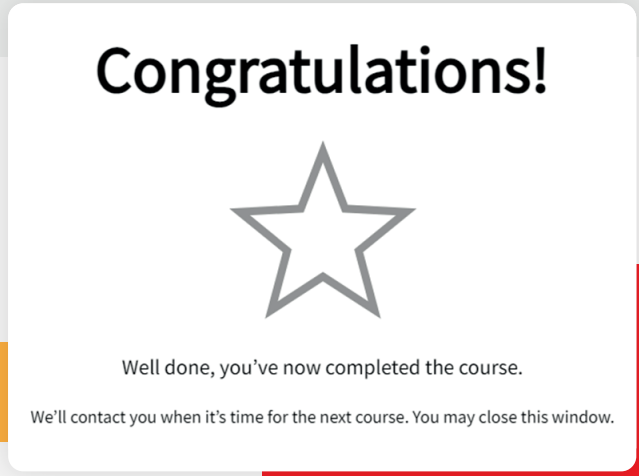


PLATFORMA JEST RESPONSYWNA I WYGODNA W UŻYCIU NA URZĄDZENIACH MOBILNYCH

Slajdy składają się z niedużej ilości tekstu, co zachęca do czytania. Taka forma jest często atrakcyjniejsza dla odbiorcy niż tzw. ściany tekstu. Należy mieć świadomość, że szkolenia z cyberbezpieczeństwa dla wielu osób nie stanowią szczególnie interesującej lektury, a samo zaliczenie szkolenia to zwykle kolejny służbowy obowiązek. Dzięki niewielkiej ilości informacji, zwiększone są szanse, że wiedza zostanie utrwalona na przyszłość.

Z perspektywy użytkownika szkoleń nie ma możliwości sprawdzenia swoich statystyk, postępów, zdobycia certyfikatów itp. Użytkownik otrzymuje jednak natychmiastowo feedback – w przypadku udzielenia błędnej odpowiedzi czy kliknięcia odnośnika w symulacji ataku (wysyłanej w losowych porach na przypisany adres e-mail).

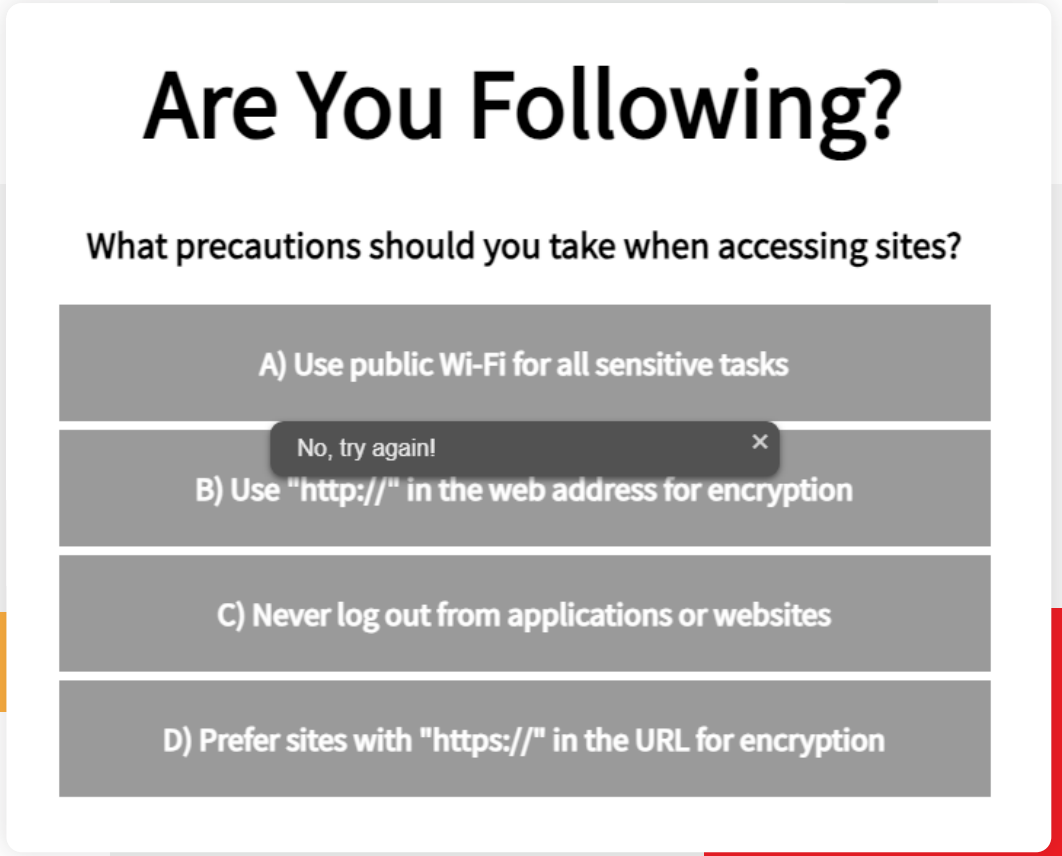
PO SKOŃCZENIU KAŻDEGO MODUŁU WYŚWIETLANE JEST POWIADOMIENIE



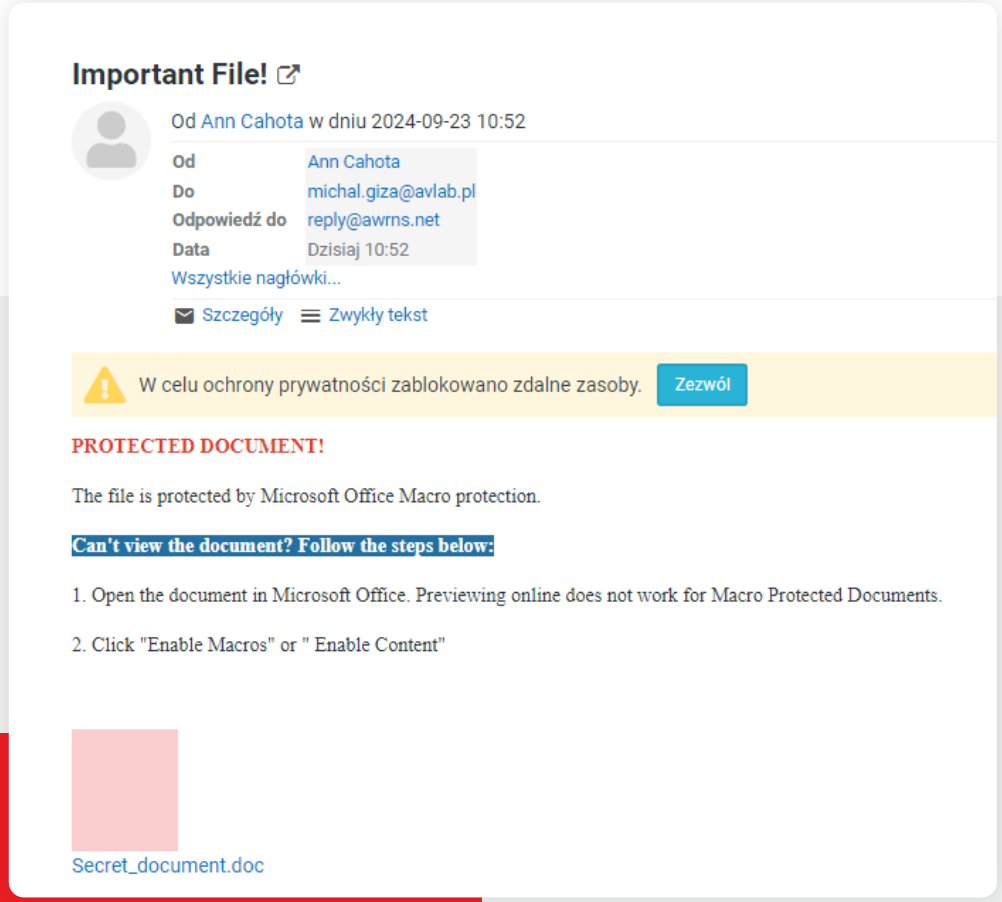
Ważnym elementem szkoleń, a już szczególnie dla osób niezainteresowanych prezentowaną tematyką, mogą okazać się elementy „interaktywne”. W usłudze Nimblr, oprócz pytań kontrolnych (niezbyt skomplikowanych, co też de facto jest ich zaletą), będących integralną częścią modułów szkoleniowych, pojawiają się wspomniane symulacje.

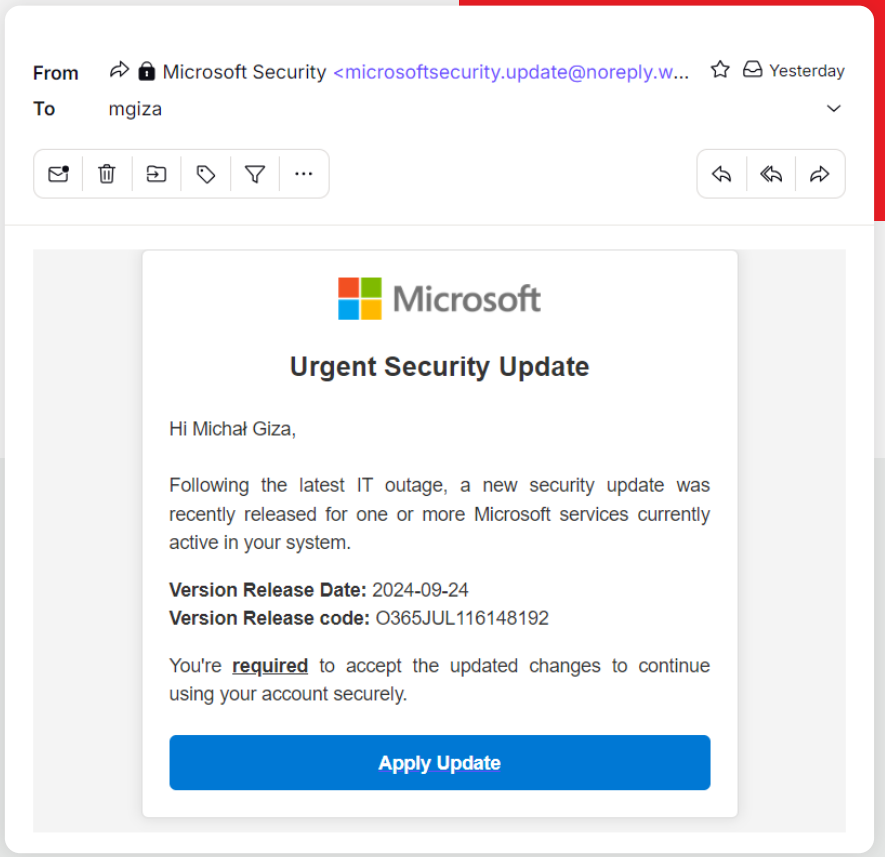
Każde pytanie z zestawu jest jednokrotnego wyboru i nie ma możliwości udzielania błędnej odpowiedzi – użytkownik może „strzelać” do skutku, ale system uwzględni prawdopodobny brak umiejętności i po pewnym czasie wyśle dodatkowe materiały związane z tematem szkolenia.

PRZYKŁADOWE PYTANIE I KOMUNIKAT WIDOCZNY PODCZAS UDZIELENIA BŁĘDNEJ ODPOWIEDZI



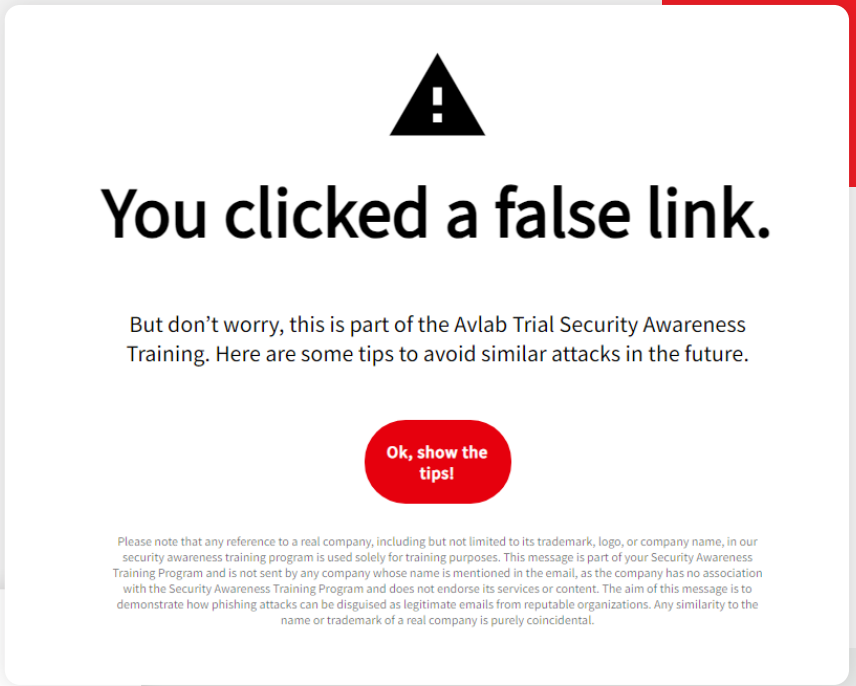
Świetnym dodatkiem są symulacje. Przykładowa wiadomość dostarczona do użytkownika może wyglądać np. tak:

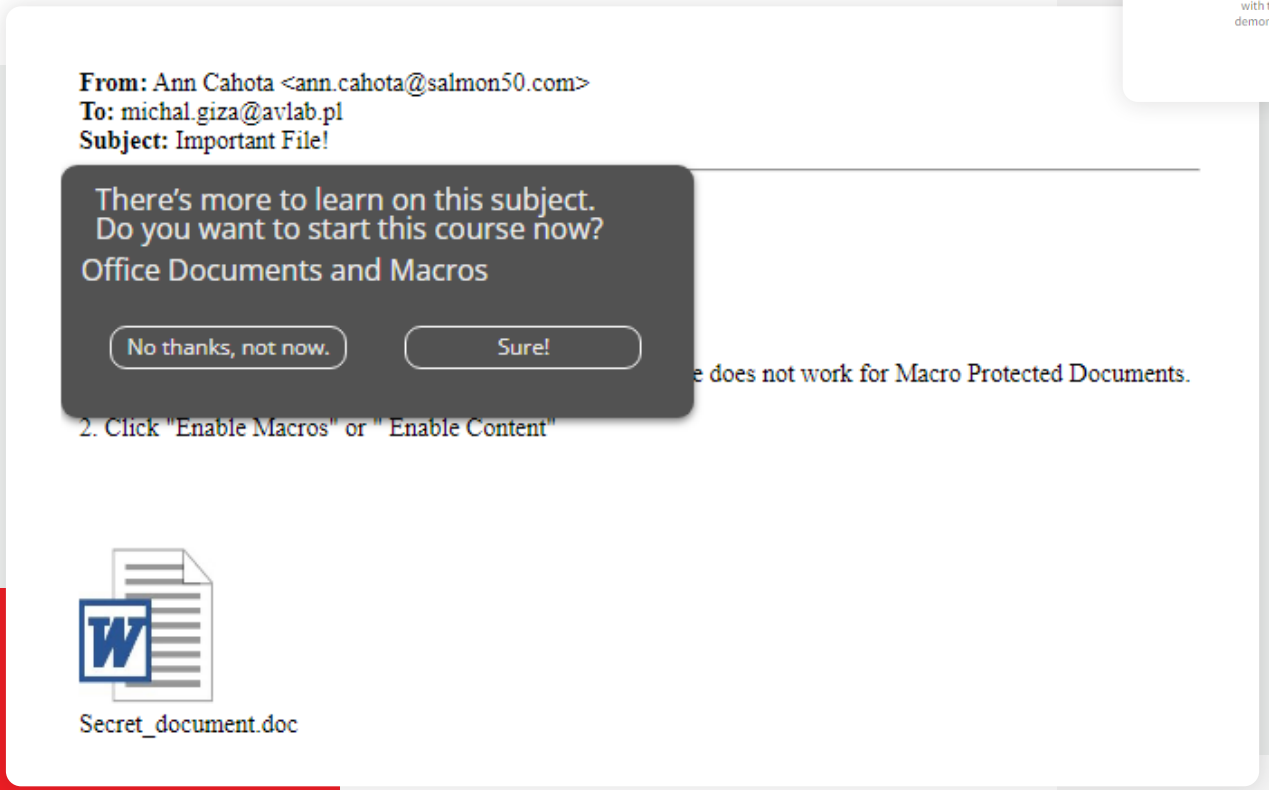




Kolejny przykład to symulacja próby podszycia się pod firmę Microsoft. Wiadomość informuje o rzekomej aktualizacji i zachęca użytkownika do jej zastosowania.

Po kliknięciu w odnośnik (w realnym ataku mógłby z dużym prawdopodobieństwem kierować do strony phishingowej lub zawierającej malware) użytkownik jest przenoszony na jedną z testowych domen (np. 135461223.site), następuje też przekierowanie do domeny platformy. Użytkownik dowiaduje się, że jego zachowanie umożliwiło przeprowadzenie ataku.





Po wybraniu opcji „Ok, show the tips!", na przykładzie wysłanej wiadomości, są prezentowane elementy, które powinny zwrócić uwagę użytkownika, świadczące o możliwej próbie ataku. Bezpośrednio można także przejść do dedykowanego modułu szkoleniowego.

V

Personalizacja szkoleń dla firm w usłudze Sharp

Nimblr zapewnia możliwość podstawowej personalizacji szkoleń i symulacji. Uprawnione osoby mogą m.in. wskazać rzeczywistych pracowników odpowiedzialnych za dany dział, wybrać narzędzia stosowane w firmie, godziny otwarcia biura, ustalić priorytet dla modułów szkoleniowych (np. oszustwa „na CEO", ataki ransomware, ataki socjotechniczne, złośliwe skrypty i makro, zarządzanie hasłami i inne). Dzięki temu zwiększa się atrakcyjność szkoleń, a w przypadku symulacji także „szansa na otwarcie złośliwego linku" przez pracownika.

OSZUSTWO „NA PREZESA"

Pilne!

Adrian Ścibor <kontakt@avlab.pl>

To: Michał Giza

Dzień dobry,

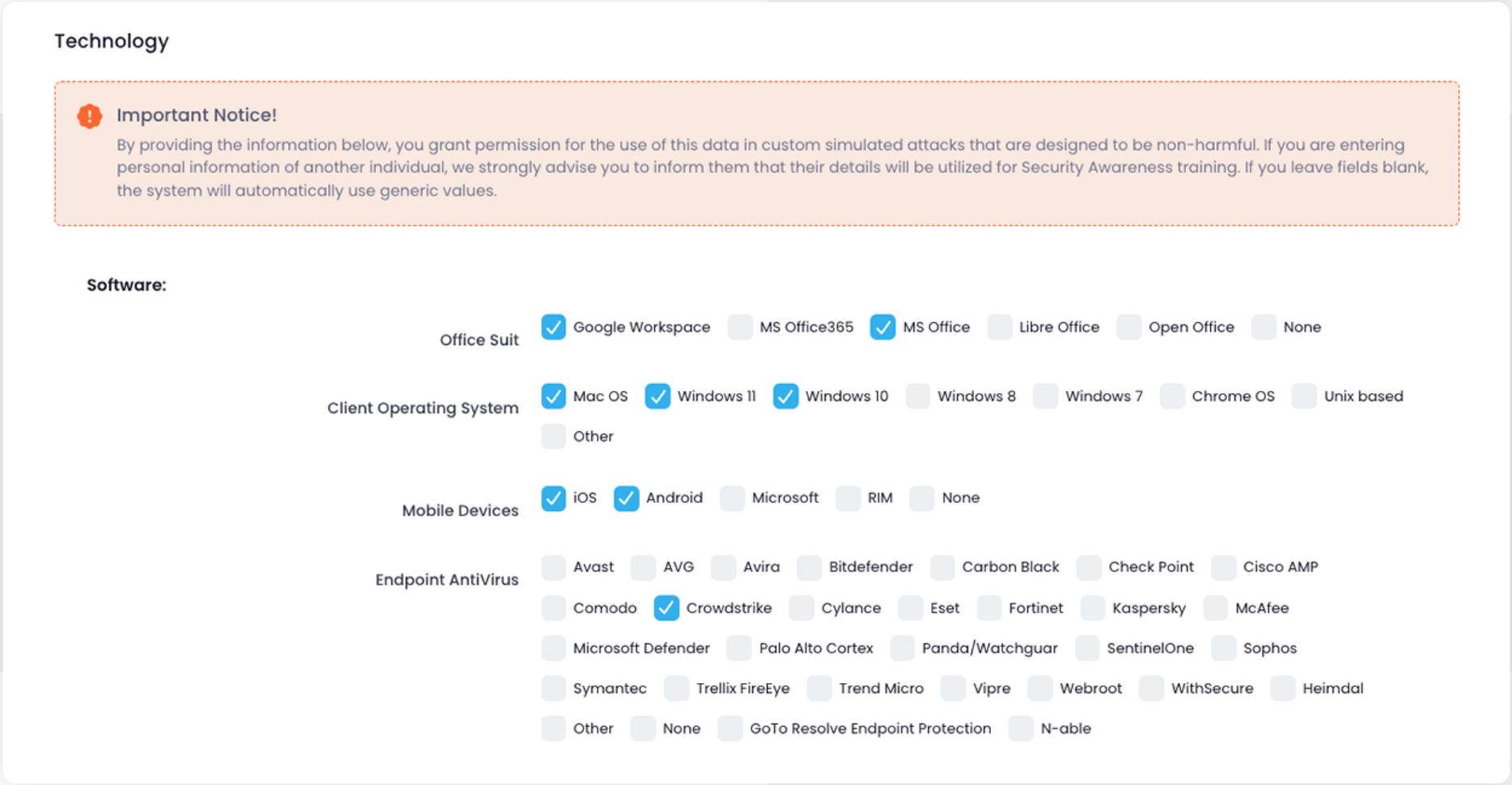
Jestem służbowo w Niemczech i nie mogę zalogować się do naszego banku internetowego. Potrzebujemy jak najszybszej wpłaty depozytu dla naszego dostawcy, czy możesz poprosić dział księgowości o przelanie 35 000 EUR na konto 2299-3688881-3156-55 w Deutsche Bank?

Proszę o potwierdzenie, kiedy tylko zostanie to zrobione, najlepiej dziś po południu!

Z poważaniem
Adrian Ścibor

Wysłane z mojego iPhone'a

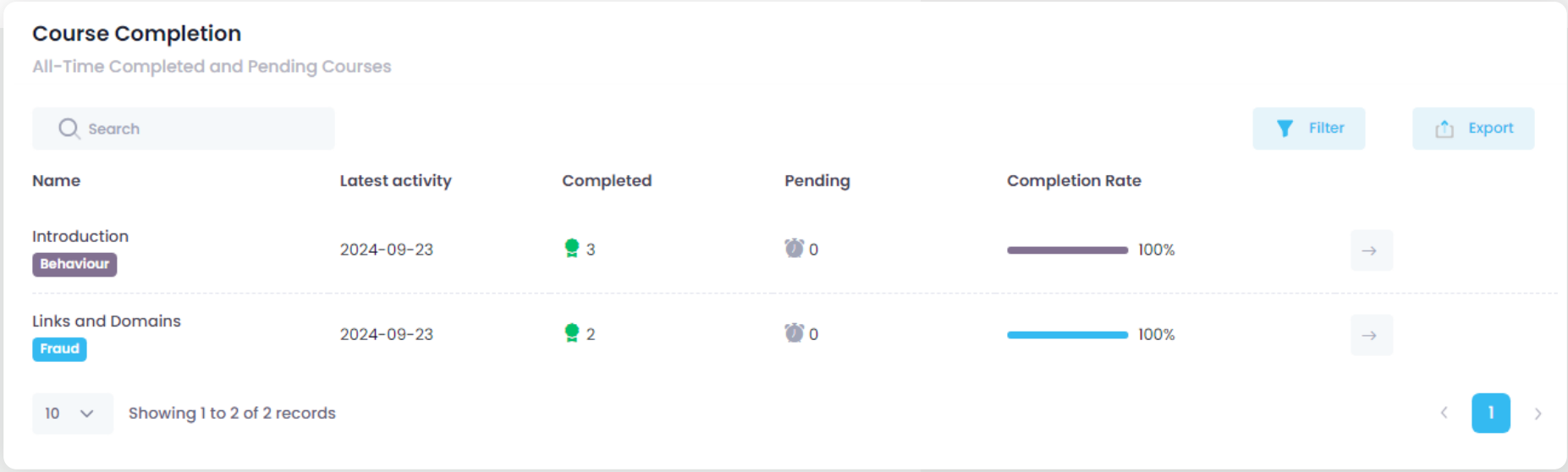
Podczas wstępnej konfiguracji platformy wymagane jest także podanie listy pracowników (wedle uznania). Możliwe jest automatyczne pobranie tych informacji z Microsoft Entra ID lub Google Workspace. Dane pracowników są używane jako przykłady w modułach szkoleniowych oraz symulacjach.



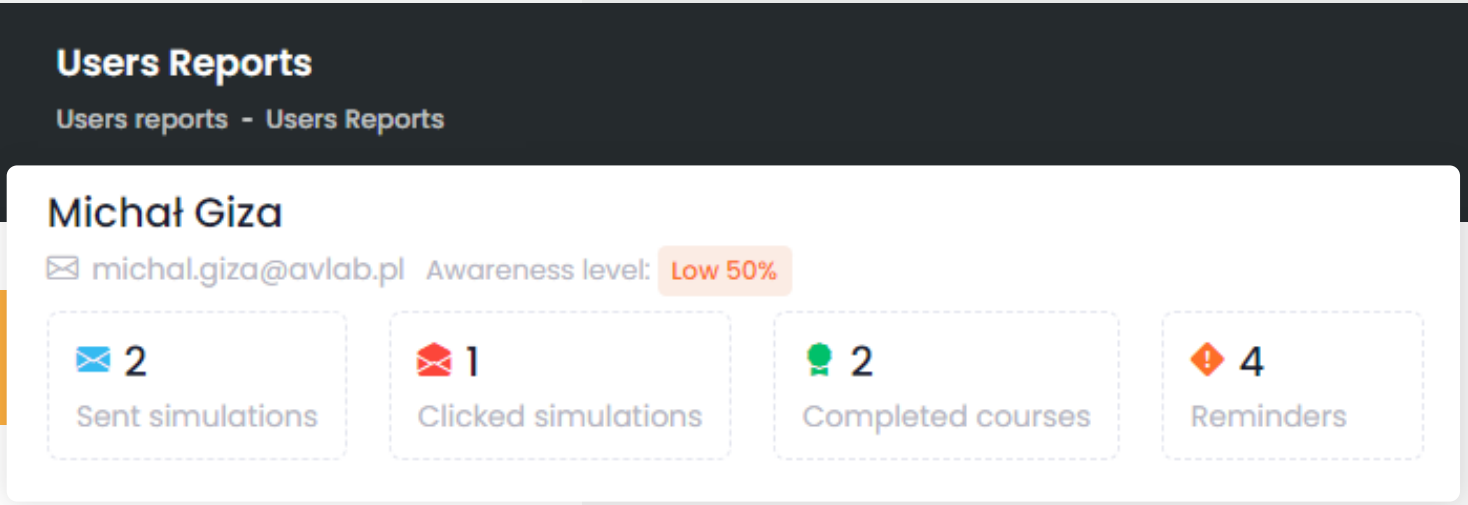
Niestety na tym kończą się opcje dalszego dostosowania do indywidualnych potrzeb. Nie możemy przykładowo wskazać konkretnego zestawu szkoleń dla wybranych pracowników – wszyscy będą otrzymywać dokładnie te same moduły. Poziom szkoleń jest przystępny dla każdego i nie powinny wystąpić problemy z ich zrozumieniem. Natomiast brak wspomnianej funkcjonalności to wada tej platformy. Trzeba jednak wspomnieć, że w ofercie Nimblr dostępna jest usługa przygotowania dedykowanych szkoleń i symulacji.

VI Raportowanie i analiza postępów

Platforma zapewnia funkcjonalność śledzenia postępów użytkowników. Wszelkie raporty dostępne są po wejściu w zakładkę Reports. Co istotne, zebrane dane można eksportować do pliku CSV bądź XLSX.



MOŻNA SPRAWDZAĆ RÓWNIEŻ POSTĘPY KONKRETNEGO UŻYTKOWNIKA.



Dużą wartość dostarcza pełny zapis aktywności dostępny w zakładce Activity

Recent Activity

Most Recent Course and Simulation Activity

Search

Filter

Export

Created	Action	Description	Group
2024-09-23 18:20:10	Course completed	Introduction completed by Michał Giza	Avlab Trial group
2024-09-23 16:18:04	Course completed	Links and Domains completed by Michał Giza	Avlab Trial group
2024-09-22 18:24:44	Course completed	Links and Domains completed by Adrian Ścibor	Avlab Trial group
2024-09-19 15:31:35	Course completed	Introduction completed by Michał Giza	Avlab Trial group
2024-09-17 17:20:14	Course completed	Introduction completed by Adrian Ścibor	Avlab Trial group

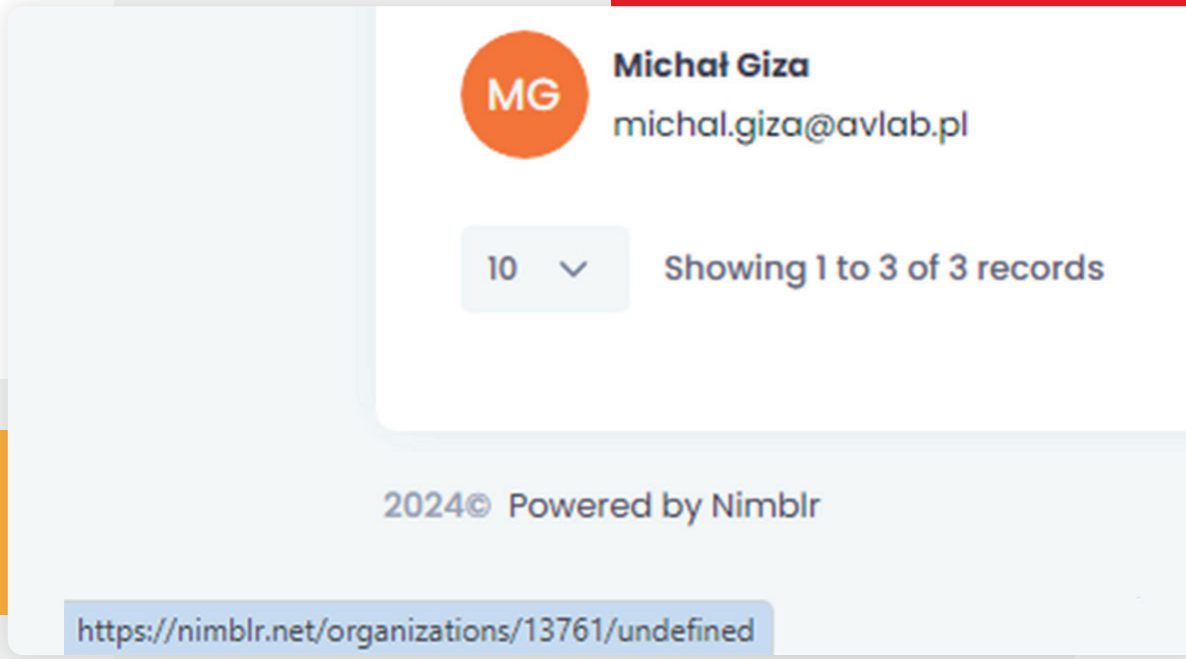
50 Showing 1 to 5 of 5 records (filtered from 36 total entries)

1

Użytkownicy nie otrzymują żadnego rodzaju raportów o postępie zdobywania umiejętności. Dostęp do całości informacji posiadają administratorzy. Na podstawie aktywności (m.in. liczbie kliknięć na linki dostarczone w symulacjach) mogą oni wyciągać wnioski i przykładowo typować osoby wymagające większego wsparcia w zakresie bezpieczeństwa.

VII Wydajność aplikacji

Podczas korzystania z platformy nie zauważono problemów ze stabilnością. Obsługa zarówno panelu zarządzania, jak i modułów szkoleniowych, odbywała się w sposób efektywny.
Jedyny znaleziony błąd dotyczy zakładki Users oraz karty Users – w edycji grupy odnośniki nie są poprawnie generowane.



DO PRZYGOTOWANIA APLIKACJI UŻYTO SPRAWDZONEGO FRAMEWORK'A LARAVEL (PHP), JAKO SERWER WWW ZASTOSOWANO WYDAJNE ROZWIĄZANIE NGINX

W praktyce wydajność wymaga jednak poprawy. Test przeprowadzony w serwisie GTmetrix dla samej strony logowania wskazuje na pewne problemy, bo ogólna ocena to D. Mimo wszystko z perspektywy docelowego odbiorcy istotne są wyłącznie moduły szkoleniowe, które standardowo ładują się szybko, ponieważ mają formę prostych slajdów. Do panelu administratora, który pod względem wydajności jest przeciwieństwem modułów szkoleniowych, dostęp został przewidziany jedynie dla osób decyzyjnych w organizacji. Wcześniej zostały opisane czynności dostępne w tym panelu, np. przeglądanie dostępnych szkoleń czy raportów, co nie wymaga wysokiej wydajności aplikacji. Prostym sposobem na optymalizację jest często modyfikacja konfiguracji PHP-FPM (NGINX obsługuje wyłącznie ten tryb) i zwiększenie kluczowych parametrów PHP, np. memory_limit czy max_execution_time. Nie można zapominać też o optymalizacji silnika bazy danych i samego serwera WWW.

Istnieje opcja integracji platformy Nimblr z innymi systemami, jednakże obejmuje to udostępnianie naszej własnej usługi zewnętrznym klientom. Szczegóły zostały opisane na stronie https://www.nimblrsecurity.com/partner/integrated-partner

VIII Podsumowanie

Inwestycja w szkolenia cyberbezpieczeństwa jest uzasadniona

Szkolenia przygotowane przez wewnętrzny dział pracowników IT albo usługa taka jak Sharp Security Awareness Training z finansowego punktu widzenia są jedną z bardziej uzasadnionych strategicznych decyzji w organizacji. Udostępnienie pracownikom dużej dawki łatwo przyswajalnej wiedzy, to większa wartość dodana niż zakup zaawansowanej zapory sieciowej, która nie będzie odpowiednio skonfigurowana, nie będzie obsługiwana przez wyszkolonych pracowników, nie będzie miała cyklicznie przedłużanych licencji na kluczowe moduły zabezpieczające. Eksperci od cyberbezpieczeństwa są zgodni, że wkład finansowy w regularne szkolenia szybko się zwróci. Postępy edukacyjne pracowników można oceniać za pomocą raportów z ukończonych modułów, jak również poprzez portfel firmowy – większą odporność na ataki złośliwego oprogramowania i wyłudzenia finansowe.

Podsumowując szkolenia mają znaczący wpływ na budowanie ogólnej kultury cyberodporności firmy. Ich zaletą jest to, że zwiększają świadomość na temat licznych zagrożeń i uczulają pracownika na potencjalne ryzyka. Ostatecznie inwestycja w edukację zawsze się zwraca, a w tym przypadku zwiększa ostrożność i odpowiedzialność pracowników podczas wykonywanych obowiązków.

AVLab rekomenduje SHARP Security Awareness Training

Kluczowe aspekty szkoleń uświadamiających

MINIMALIZOWANIE BŁĘDU LUDZKIEGO

Najczęstszą przyczyną udanych cyberataków są błędy ludzkie. Pracownicy, którzy uczestniczą w szkoleniach, stają się mniej podatni na triki cyberprzestępców.

ZWIĘKSZENIE ŚWIADOMOŚCI ZAGROŻEŃ

Szkolenia dostarczają wiedzy na temat najnowszych cyberzagrożeń, takich jak phishing, malware, ataki socjotechniczne i ransomware.

BUDOWANIE DOBRYCH NAWYKÓW

Pracownicy zaczną korzystać z silnych haseł, będą unikać podejrzanych stron, nie będą klikać w podejrzane linki i załączniki, dowiedzą się o aktualizowaniu oprogramowania.

LEPSZE REAGOWANIE NA INCYDENTY

Najlepszą metodą jest prewencja. Kiedy już dojdzie do ataku, pracownicy wiedzą, jak reagować, do kogo zgłosić problem, jak minimalizować szkody.

WIĘKSZE ZAANGAŻOWANIE

Jeżeli poważnie traktujesz kwestie bezpieczeństwa, to wśród pracowników rośnie poczucie odpowiedzialności za środowisko pracy.

PROCEDURY CYBERBEZPIECZEŃSTWA

Szkolenia pomagają w standaryzacji procedur bezpieczeństwa w całej organizacji.

Fundacja AVLab dla Cyberbezpieczeństwa jako niezależna organizacja stoimy na straży ochrony prywatności i bezpieczeństwa w Internecie. Budujemy świadomość użytkowników z zakresu ochrony cyfrowej. Wydajemy opinie, techniczne analizy oraz testy rozwiązań informatycznych w sferze cyberbezpieczeństwa. Udostępniamy również blog o bezpieczeństwie, na którym zamieszczamy artykuły o nowościach w zakresie bezpieczeństwa IT, lukach w zabezpieczeniach i rozwiązaniach IT.

Przeprowadzamy regularne testy różnych programów ochronnych i publikujemy wyniki na naszej stronie internetowej. Testy te obejmują szeroki zakres próbek złośliwego oprogramowania, w tym zarówno znane, jak i nieznane zagrożenia, i oceniają skuteczność każdego programu w ich wykrywaniu i usuwaniu. Pomaga to użytkownikom porównać skuteczność różnych programów bezpieczeństwa i podejmować świadomą decyzję przy wyborze rozwiązania do ochrony komputera.

Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, dzięki którym jesteśmy rozpoznawalni na całym świecie, jako jedno z najpopularniejszych laboratoriów testujących.

Aby poznać szczegóły techniczne producenci mogą kierować swoje zapytania na adres: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl