NajslabszeOgniwo.pl

SZKOŁA SZTUK WALKI Z CYBERPRZESTĘPCAMI

SZKOLENIA SECURITY AWARENESS – BEZPIECZNY PRACOWNIK

Szkolenia security awareness funkcjonujące też na rynku pod nazwą „bezpieczny pracownik" zyskują coraz większą popularność. Firmy i instytucje, których pracownicy na co dzień korzystają z Internetu i zdobyczy technologicznych nie mogą sobie pozwolić na to, aby z powodu niewiedzy lub braku świadomości zagrożeń naruszona została ich ciągłość biznesowa.

Nie bez powodu w branży związanej z cyberbezpieczeństwem pracownicy firm nazywani są „najsłabszym ogniwem" w łańcuchu zabezpieczeń. To za sprawą ich nieodpowiedzialnych zachowań cyberprzestępcom wystarcza najczęściej kilka minut aby uzyskać nieautoryzowany dostęp do zasobów firmy.

W dobie rosnącej fali ataków ze strony cyberprzestępców, których działalność skutkuje nierzadko milionowymi stratami, zdolność obrony przed nimi jest jednym z najistotniejszych wymogów bezpieczeństwa.

NajslabszeOgniwo.pl jest platformą szkoleniową, która wychodzi na przeciw rosnącemu zapotrzebowaniu na szkolenia security awareness dla pracowników mające na celu podnieść ich świadomość zagrożeń oraz zdolność obrony przed atakami. Szkolenia typu „bezpieczny pracownik" to najefektywniejszy kosztowo sposób na podniesienie bezpieczeństwa infrastruktury teleinformatycznej i danych, a co za tym idzie bezpieczeństwa biznesu.

PRZEWAGA KURSÓW ONLINE

Szkolenia security awareness – bezpieczny pracownik w formie kursów online są odpowiedzią na sygnalizowane nam często przez firmy problemy, takie jak:

- Oderwanie od zajęć większej ilości pracowników w tym samym czasie w celu przeprowadzenia szkolenia stacjonarnego
- Możliwości logistyczne zebrania w jednym miejscu pracowników z odległych lokalizacji
- Brak odpowiednio dużych sal konferencyjnych
- Wypadki losowe uniemożliwiające udział w zaplanowanym szkoleniu (urlopy na żądanie, choroby, pilne do obsłużenia zadania w pracy)
- Skuteczność przekazu w odgórnie narzuconych terminach (pracownicy mogą być w danej chwili rozpraszani pilnymi telefonami, zmęczeni, zdekoncentrowani)
- Brak kontroli nad efektami szkolenia
- Podlegający z czasem obniżeniu poziom bezpieczeństwa (szkolenia stacjonarne przynoszą najwyższe efekty w perspektywie kilku tygodniowej, po tym czasie pracownicy najczęściej zapominają o dobrych praktykach i wracają do starych nawyków)

INNOWACYJNA FORMUŁA

Szkolenia security awareness – bezpieczny pracownik na platformie NajslabszeOgniwo.pl charakteryzują się innowacyjną formułą, która znacznie zwiększa ich skuteczność i długotrwałe efekty. Poniżej najistotniejsze zalety oferowanych przez nas kursów online:

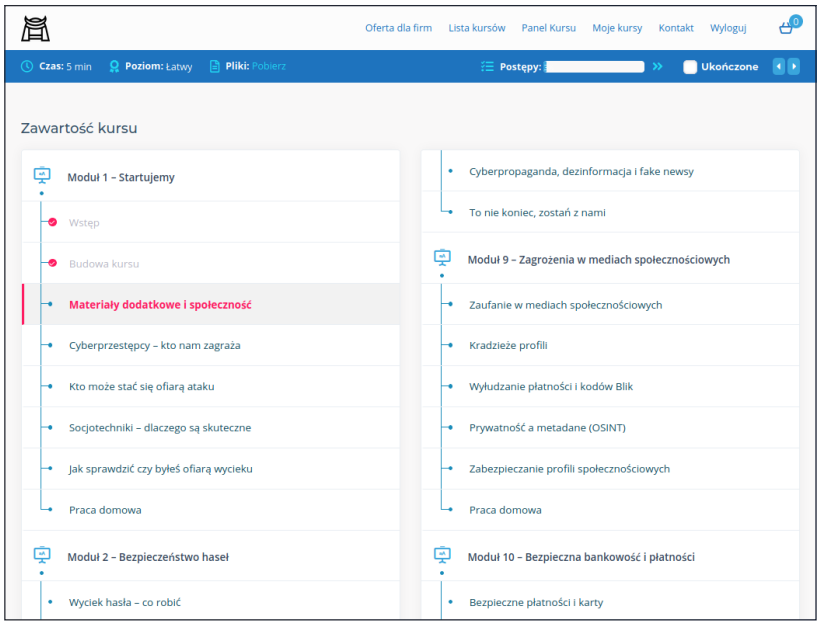
- Szkolenie odbywa się w formie modułów tygodniowych. W każdym tygodniu udostępniany jest nowy moduł składający się z kilku lekcji o łącznej długości od kilkunastu do kilkudziesięciu minut. Uczestnik otrzymuje mailowe powiadomienie o dostępności nowego modułu i przystępuje do niego w dogodnym dla siebie momencie.
- Postępy uczestników są odnotowywane, możliwe jest ich śledzenie i powrót do miejsca, w którym moduł został przerwany. Możliwe jest też śledzenie i raportowanie postępów wszystkich uczestników.
- W każdym module poruszane jest istotne zagadnienie bezpieczeństwa (np. hasła, zagrożenia związane z phishingiem, zagrożenia związane ze złośliwym oprogramowaniem itd.)
- W każdym module poza lekcjami dostępne są materiały dodatkowe w formie plików do pobrania lub artykułów pozwalających poszerzyć wiedzę osobom najbardziej zainteresowanym.
- W każdym module na zakończenie definiowana jest praktyczna „praca domowa", której wykonanie ma na celu przyswojenie wiedzy, wyrobienie dobrych nawyków i podniesienie bezpieczeństwa. Przykładowo może to być polecenie zmiany haseł w systemach, gdzie są one nieunikatowe lub włączenie uwierzytelniania dwuskładnikowego.
- W kolejnych modułach często wspominane są zagadnienia już przerobione, dzięki czemu podtrzymywany jest stały, wysoki poziom bezpieczeństwa i przez wiele miesięcy utrzymywany jest efekt, który w przypadku szkoleń stacjonarnych trwa tylko do kilku tygodni.

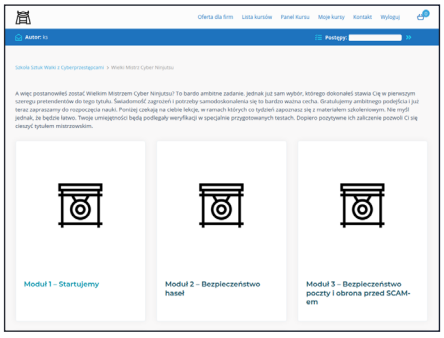
- Uczestnicy przez okres roku mają możliwość wracania do dowolnych, już ukończonych modułów.
- Lekcje dotyczące poszczególnych zagadnień w ciągu roku będą podlegały aktualizacji, stosownie do zmieniających się zagrożeń.
- Każdy uczestnik w ramach kursu otrzyma dostęp do prywatnej grupy kursantów, na której udostępniane będą informacje o nowych zagrożeniach i udzielane praktyczne porady dotyczące bezpieczeństwa.
- Dla uczestników kursu organizowane będą spotkania live w formie webinarów, na których instruktor omawiał będzie nowe zagrożenia i odpowiadał na zapytania kursantów.
- Lekcje są prowadzone przez wykwalifikowanego trenera z wieloletnim doświadczeniem. Mają one charakter video-wykładu prowadzonego w tej samej formule co szkolenie stacjonarne. Przykłady praktyczne omawiane są natomiast z użyciem screencastu, w którym prowadzący udostępnia obraz z komputera. Nie stosujemy nudnego e-learningu, gdzie uczestnik musi sam zapoznawać się z materiałami lub oglądać animacje komentowane przez lektora nieznającego omawianych zagadnień.
- Każdy moduł kończy się quizem sprawdzającym wiedzę uczestnika.
- Każdy uczestnik po pomyślnym zaliczeniu wszystkich quizów otrzymuje certyfikat ukończenia szkolenia security awareness – bezpieczny pracownik.

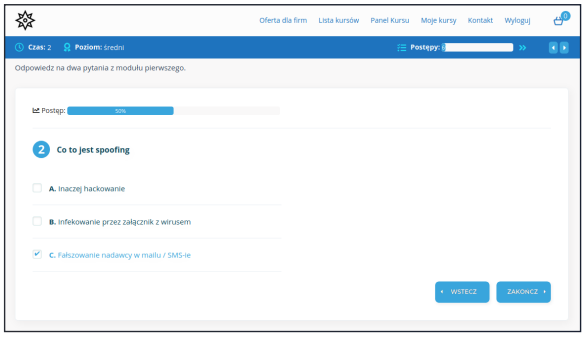
Gdyby tego wszystkiego było mało, to na dokładkę w planach mamy jeszcze cykliczny podcast oraz biuletyn bezpieczeństwa dla wszystkich kursantów.

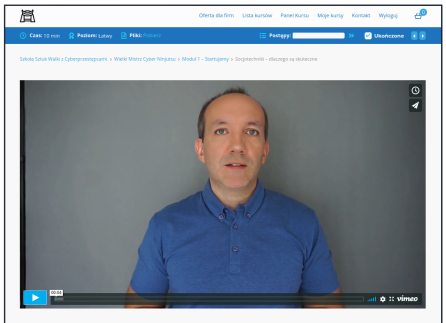
PRZYJAZNY INTERFEJS NASZEJ PLATFORMY

Poniżej zamieszczamy kilka zdjęć prezentujących przyjazny interfejs naszej platformy, m.in. zawartość lekcji, nawigację i śledzenie postępów, quiz sprawdzający i jego wyniki.

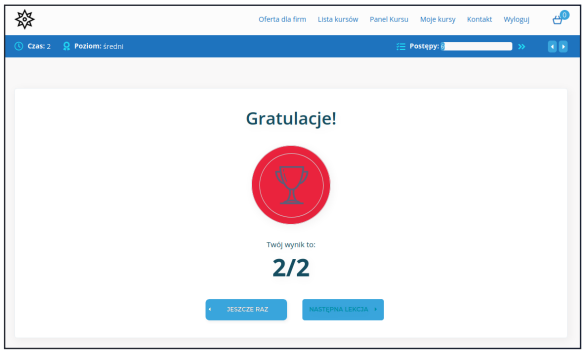








Poniżej znajdziesz pliki, które przydadzą się w Twojej pracy domowej.



DOŚWIADCZENIE I OPINIE

W branży szkoleniowej, a zwłaszcza tej związanej z cyberbezpieczeństwem doświadczenie trenerów odgrywa najwyższą rolę. Nasze kursy przygotowane i prowadzone są przez certyfikowanych specjalistów zajmujących się cyberbezpieczeństwem oraz trenerów, którzy w zawodzie pracują od ponad 10 lat. W szkoleniach stacjonarnych przeszkoliliśmy już tysiące pracowników z największych Polskich firm. Z usług naszych trenerów korzystają aktualnie największe w kraju firmy szkoleniowe. Poniżej zamieszczamy przykładowe opinie uczestników prowadzonych przez nas szkoleń

Opinie na temat przeprowadzonych szkoleń cyber awareness:

- *Szkolenia poruszały ciekawe zagadnienia związane z bezpieczeństwem zarówno od strony technicznej jak i ludzkiej, wskazywały miejsca na które należy zwrócić szczególną uwagę aby do minimum zminimalizować możliwe ataki. Szkolenie uważam za bardzo ciekawe i potrzebne aby zapewnić jak najwyższy poziom bezpieczeństwa.*
- *Szkolenie umożliwia nabycie podstawowej wiedzy dotyczącej poruszania się w internecie i bezpieczne korzystanie z niego. Uczy zachowań, prawidłowych nawyków i zwracania uwagi na pewne szczegóły, o których ludzie nie wiedzą, bądź z chęci zaoszczędzenie czasu ignorują.*
- *Świadomość cyber przestępczości jest bardzo mała. Szkolenie pozwala spojrzeć z innej perspektywy na codzienne wykonywanie czynności z telefonem/ komputerem.*
- *Nasi pracownicy byli pod ogromnym wrażeniem prezentacji, do teraz dostaje zapytania od pracowników którzy byli (również naszego szefostwa), że szkolenie było świetne i czy będzie możliwość jeszcze się z nim zapoznać.*

  Najbardziej merytoryczna prezentacja, na której byłam, dodatkowo świetnie poprowadzona!
- *Chyba ze wszystkich prelegentów, których słuchałem, mówił najbardziej konkretnie i opowiedział wciągającą historię.*
- *Zachęciłbym znajomych do wykonania tego szkolenia.*
- *Szkolenie jest bardzo poruszające dla pracowników biur i nie tylko, również w codziennych sytuacjach i problemach z bezpieczeństwem.*
- *Bardzo ciekawe szkolenie. Podane przykłady z życia codziennego — spotykamy się z tym na co dzień w pracy.*
- *Treść szkolenia istotna w dzisiejszych czasach, w dobie internetu. Zbyt duża ufność ludzi danymi prezentowanymi w sieci.*

- *Problem cyber przestępczości jest bardzo powszechny, zaś problematyka jej unikania jest stosunkowo mało rozpowszechniana. Szkolenie jasno przedstawia popularne problemy i metody ich unikania.*
- *Tematyka szkolenia była bardzo interesująca i przyda się w codziennym życiu.*
- *Bardzo przydatne szkolenie, życiowe, zwracające uwagę na ważne aspekty bezpieczeństwa poruszania się w internecie.*

Opinie o trenerze:

- *Dobrze przygotowany merytorycznie, jasne i przejrzyście ukazanie tematu.*
- *Trener tłumaczył jasno, dokładnie, zrozumiale. Bardzo sympatyczny w odbiorze.*
- *Przekazane informacje i prowadzenie szkolenia było jasne i zrozumiałe.*
- *Przekazane informacje w przystępnej formie z ciekawymi przykładami oraz sugestie, na co należy zwracać uwagę.*
- *Pan prowadzący opowiadał ciekawie, potrafił zainteresować.*
- *Dobrze przygotowany merytorycznie, przykłady z „życia wzięte". Łatwość komunikacji.*
- *Pan Jakub korzystnie prowadził szkolenie, wiedział, o czym mówił. Dobrze przygotowany.*
- *Dobrze przygotowany, ciekawie opowiadał.*
- *Wyraźne nakreślenie tematu.*
- *Bardzo konkretne przykłady jeśli chodzi o zagrożenia, przemiły głos, duża wiedza.*
- *Profesjonalny, jasny przekaz, trener dobrze przygotowany. Ciekawie opowiada, płynnie, szybko, treściwie.*
- *Osoba posiadająca wiedzę praktyczną, opowiada na konkretnych przykładach.*
- *Bardzo dobry poziom komunikacji i duża wiedza merytoryczna.*

LISTA LEKCJI

Poniżej prezentujemy listę 90 lekcji składających się na 16 modułów w najbardziej rozbudowanej formie naszego kursu security awareness – bezpieczny pracownik. Tak ogromna ilość wiedzy byłaby niemożliwa do przekazania nawet w formie całodniowego szkolenia stacjonarnego. Ponadto jego efektem byłoby przeładowanie uczestników wiedzą i spowodowanie jednego z dwóch niepożądanych efektów – przerażenia bądź rezygnacji. To pokazuje jeszcze jedną przewagę platformy NajslabszeOgniwo.pl, w której wiedza przekazywana jest w sposób usystematyzowany, pozwalający na stopniowe budowanie dobrych nawyków bezpieczeństwa i przynoszący długotrwałe efekty.

Moduł 1:
STARTUJEMY
- Wstęp
- Budowa kursu
- Materiały dodatkowe i społeczność
- Cyberprzestępcy – kto nam zagraża
- Kto może stać się ofiarą ataku
- Socjotechniki – dlaczego są skuteczne
- Jak sprawdzić czy nie byłeś ofiarą wycieku danych
- Praca domowa

Moduł 2:
BEZPIECZEŃSTWO HASEŁ
- Wyciek hasła – co robić
- Wszystko co musisz wiedzieć o hasłach
- Bezpieczne przechowywanie haseł
- Uwierzytelnianie dwuskładnikowe
- Praca domowa

Moduł 3:
BEZPIECZEŃSTWO POCZTY I OBRONA PRZED SCAM-EM
- Poczta tradycyjna
- Mail i SMS spoofing – jakie to łatwe
- Zasady weryfikacji nadawcy
- Przykładowe ataki spoofingowe
- Na co zwrócić uwagę
- Jak weryfikować załączniki i linki
- Praca domowa

Moduł 4:
OBRONA PRZED PHISHINGIEM
- Phishing
- Przykładowe ataki phishingowe
- Jak czytać adresy URL i domeny
- Pułapki w nazwach domen
- Typosquoting / cybersquoting
- Problem „zielonej kłódeczki”
- Praca domowa

Moduł 5:
BEZPIECZEŃSTWO PRZEGLĄDAREK
- Bezpieczeństwo przeglądarek
- Ciasteczka i zapamiętywanie haseł
- Clickjacking, likejacking, camjacking
- Ostrzeżenia o certyfikatach
- Praca domowa

Moduł 6:
JESZCZE WIĘCEJ SOCJOTECHNIK I JAK ICH UNIKAĆ
- Ataki z wykorzystaniem telefonu
- Nieznane nośniki danych
- Niebezpieczne gadżety
- Złośliwe reklamy
- Porady praktyczne
- Praca domowa

Moduł 7:
JESZCZE WIĘCEJ ZAGROŻEŃ
- Ataki techniką wodopoju
- Zagrożenia związane z WIFI
- Smartfon w prezencie (albo z aukcji)
- Ataki na konto bankowe przez duplikat SIM
- Praca domowa

Moduł 8:
STRZEŻ SIĘ – TO TEŻ JEST MOŻLIWE
- Sztuczna inteligencja w służbie przestępczości
- Zagrożenia IoT (Internetu Rzeczy)
- Cyberpropaganda, dezinformacja i fake newsy
- To nie koniec, zostań z nami

Moduł 9:
ZAGROŻENIA W MEDIACH SPOŁECZNOŚCIOWYCH
- Zaufanie w mediach społecznościowych
- Kradzieże profili
- Wyłudzanie płatności i kodów Blik
- Prywatność a metadane (OSINT)
- Zabezpieczanie profili społecznościowych
- Praca domowa

Moduł 10:
BEZPIECZNA BANKOWOŚĆ I PŁATNOŚCI
- Bezpieczne płatności i karty
- Pośrednicy płatności
- Bankowość mobilna
- Blik
- Praca domowa

Moduł 11:
NAJLEPSZE PRAKTYKI I NAWYKI
- Dobre praktyki bezpieczeństwa
- Wrogi pracownik
- Bezpieczne usuwanie danych
- Aktualizacje
- Praca domowa

Moduł 12:
OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM
- Złośliwe oprogramowanie – poznaj wroga
- Czym jest darknet i czy nam zagraża
- Antywirus
- Bezpieczne kopie zapasowe
- Praca domowa

Moduł 13:
BEZPIECZEŃSTWO TELEFONÓW I TABLETÓW
- Telefon to też komputer
- Uprawnienia a inwigilacja
- Zabezpieczenia i dobre praktyki
- Bezpieczeństwo dzieci
- Praca domowa

Moduł 14:
STRZEŻ SIĘ TYCH URZĄDZEŃ
- Urządzenia hackerskie na które należy uważać
- Wrogie USB
- Implanty sieciowe
- Złudna kontrola dostępu
- Praca domowa

Moduł 15:
REAKCJA NA INCYDENT BEZPIECZEŃSTWA
- Incydent bezpieczeństwa – rozpoznanie
- Jak i gdzie zgłosić incydent
- Co mogę zrobić samemu
- Praca domowa

Moduł 16:
PRACUJ BEZPIECZNIE I BROŃ SIĘ SKUTECZNIE
- Czym jest hardening
- Przeglądarka, która Cię nie zdradzi
- Bezpieczna poczta
- Bezpieczny komunikator
- Bezpieczna sieć w podróży
- Sprzętowe 2FA
- Blokady usług premium
- Praca domowa

ZAPYTAJ O OFERTĘ

Mamy nadzieję, że już dłużej nie musimy Cię przekonywać. Jeżeli jesteś zainteresowany szkoleniem pracowników w Twojej firmie, zapytaj nas o ofertę podając orientacyjną ilość uczestników. Oczywiście możesz też zapytać o szkolenia w tradycyjnym, stacjonarnym modelu.

Napisz na adres szkolenia@najslabszeogniwo.pl

NajslabszeOgniwo.pl

SZKOŁA SZTUK WALKI Z CYBERPRZESTĘPCAMI

Możesz się z nami skontaktować przez:
email: szkolenia@najslabszeogniwo.pl
tel.: +48 733 296 894
FB: https://www.facebook.com/najslabszeogniwo/