

Szkolenie Security awareness - Podstawy cyberhigieny

Opis szkolenia: Wprowadzenie pracowników w świat cyberbezpieczeństwa i wyposażenie ich w podstawową, uniwersalną wiedzę, która pozwoli im identyfikować i unikać najczęstszych zagrożeń. Program ma charakter prewencyjny i ma na celu uświadomienie, że bezpieczeństwo cyfrowe dotyczy każdego. Szkolenie może zostać dopasowane do poziomu grupy i branży.

Czas trwania: 3 godziny (np. 9:00 – 12:00)

Kategoria: Security awareness

Język wykładowy: język polski

Materiały: w języku polskim. Na życzenie klienta materiały w języku angielskim.

Wymagania wstępne: Brak wymagań technicznych.

Forma szkolenia: Zdalne. Możliwe także przeprowadzenie szkolenia w siedzibie klienta (skontaktuj się w celu uzgodnienia szczegółów).

Liczba pracowników: nielimitowana

Grupa docelowa:

- Pracownicy różnych branż
- Kadra menedżerska

Cel szkolenia: Zrozumienie podstawowych zasad cyberhigieny.

Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
9:00 – 9:20	20 minut	Moduł 1: Wprowadzenie: dlaczego to dotyczy mnie?	Studium przypadku, dyskusja
9:20 – 10:00	40 minut	Moduł 2: Inżynieria społeczna i najczęstsze ataki	Studium przypadku, dyskusja
10:00 – 10:30	30 minut	Moduł 3: Hasła i uwierzytelnianie	Studium przypadku, dyskusja
10:30 – 11:00	30 minut	Moduł 4: Złośliwe oprogramowanie (malware itd.)	Studium przypadku, dyskusja

Godzina	Czas trwania	Moduł	Forma
11:00– 11:40	40 minut	Moduł 5: Procedury i reakcja na incydent	Studium przypadku, dyskusja
11:40 – 12:00	20 minut	Moduł 6: Sesja pytań i odpowiedzi	Q&A, ankieta końcowa

Szczegółowy program szkolenia

Moduł 1: Wprowadzenie: dlaczego to dotyczy mnie? (20 minut)

Wprowadzenie do tematu i przedstawienie agendy.

- Przedstawienie prowadzącego i uczestników.
- Omówienie celów i struktury szkolenia.
- Zasady współpracy i interaktywności.
- Wytłumaczenie koncepcji *security awareness* i podkreślenie, że cyberbezpieczeństwo to nie tylko problem firmy, ale także osobista korzyść – ochrona rodziny i danych w życiu prywatnym.

Moduł 2: Inżynieria społeczna i najczęstsze ataki (40 minut)

- Omówienie psychologicznych mechanizmów manipulacji.
- Szczegółowa analiza phishingu – zjawiska podszywania się pod wiarygodne źródła w celu wyłudzenia danych.
- Przykłady obejmują wiadomości e-mail z zainfekowanymi załącznikami, fałszywe strony logowania (np. bankowe), oszustwa na BLIK czy fałszywe wezwania do zapłaty.
- Wskazówki, jak weryfikować nadawcę i unikać klikania w podejrzane linki.

Moduł 3: Hasła i uwierzytelnianie (30 minut)

- Prezentacja zasad tworzenia silnych haseł: minimalna długość, unikalność, kombinacja wielkich, małych liter, cyfr i symboli.
- Omówienie popularnych błędów, takich jak używanie tego samego hasła na wielu stronach.
- Wytłumaczenie roli i korzyści z używania menedżerów haseł oraz uwierzytelniania dwuskładnikowego (MFA) jako kluczowej warstwy ochrony.

Moduł 4: Złośliwe oprogramowanie (np. malware) (30 minut)

- Ogólne wprowadzenie do pojęcia malware. Krótki opis najczęściej spotykanych typów, takich jak ransomware (szyfrowanie danych), trojany (podszywanie się pod legalne oprogramowanie), czy keyloggers (rejestrowanie naciskanych klawiszy).
- Prezentacja, jak malware dostaje się na urządzenia (np. przez załączniki w fałszywych wiadomościach).

Moduł 5: Procedury i reakcja na incydent (40 minut)

- Wskazanie, co należy robić w przypadku podejrzenia ataku.

- Omówienie jasnych procedur zgłaszania incydentów, które powinny być zrozumiałe i łatwe do zastosowania dla każdego pracownika.
- Podkreślenie znaczenia natychmiastowej reakcji i weryfikacji informacji poprzez inne kanały komunikacji.

Moduł 6: Podsumowanie, Q&A i kolejne kroki (20 minut)

- Podsumowanie i wnioski.
- Sesja pytań i odpowiedzi.
- Ankieta końcowa i informacje o certyfikacie.

Zarejestruj się na szkolenie: <https://szkolenia.zalnet.pl/szkolenia/podstawy-cyberhigieny/>

