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.

Kod szkolenia: SEC-HIG-01

Kategoria: Security awareness / Cyberbezpieczeństwo / Edukacja pracowników

Trenerka: Beata Zalewa

Czas trwania: 4 godziny (np. 9:00 – 13:00)

Poziom zaawansowania: Podstawowy

Język wykładowy: język polski

Forma szkolenia: zdalne. Po wcześniejszym uzgodnieniu możliwe szkolenie w siedzibie klienta.

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

Wymagania wstępne: Brak wymagań technicznych. Podczas szkolenia uczestnicy będą korzystali z własnych komputerów i licencji.

Grupa decelowa:

- Pracownicy różnych branż, kadra menedżerska. Szkolenie może być dopasowane pod konkretną branżę.

Cel szkolenia: Zrozumienie podstawowych zasad cyberhigieny.

Efekty szkolenia:

- Uczestnik zna fundamentalne zasady bezpiecznego korzystania z sieci, poczty elektronicznej oraz urządzeń służbowych, a także podstawowe rodzaje zagrożeń cyfrowych czyhających na użytkowników w codziennej pracy.
- Uczestnik potrafi wdrożyć w praktyce zasady silnych haseł, poprawnie posługiwać się uwierzytelnianiem wieloskładnikowym (MFA) oraz dbać o fizyczne bezpieczeństwo danych zgodnie z zasadą czystego biurka i zablokowanego ekranu.
- Uczestnik potrafi krytycznie oceniać otrzymywane wiadomości e-mail, identyfikować próby wyłudzenia danych (phishing) oraz właściwie zgłaszać podejrzane incydenty wewnętrznym zespołom IT.
- Uczestnik rozumie ryzyka związane z bezrefleksyjnym korzystaniem z publicznych sieci Wi-Fi, podłączaniem nieznanych nośników pamięci (np. pendrive) oraz instalowaniem nieautoryzowanego oprogramowania.
- Uczestnik rozumie, że jego codzienne nawyki, czujność i stosowanie podstawowych zasad cyberhigieny stanowią kluczowe ogniwo w systemie bezpieczeństwa całej organizacji.

Co otrzymasz?

- Materiały szkoleniowe.
- Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
9:00 - 9:20	20 minut	**Moduł 1: Wstęp i przedstawienie podstawowych pojęć z zakresu cyberhigieny**	Studium przypadku, dyskusja
9:20 – 9:40	20 minut	**Moduł 2: Dlaczego to dotyczy mnie?**	Studium przypadku, dyskusja
9:40 – 10:40	60 minut	**Moduł 3: Inżynieria społeczna i najczęstsze ataki**	Studium przypadku, dyskusja
10:40 – 11:30	50 minut	**Moduł 4: Hasła i uwierzytelnianie**	Studium przypadku, dyskusja
11:30 – 11:40	10 minut	Przerwa kawowa	-
11:40 – 12:15	35 minut	**Moduł 5: Złośliwe oprogramowanie (malware itd.)**	Studium przypadku, dyskusja
12:15– 12:45	30 minut	**Moduł 6: Procedury i reakcja na incydenty**	Studium przypadku, dyskusja
12:45 – 13:00	15 minut	**Moduł 7: Sesja pytań i odpowiedzi**	Q&A, ankieta końcowa

Szczegółowy program szkolenia

Moduł 1: Wstęp

Wprowadzenie do tematu i przedstawienie agendy.

- Przedstawienie prowadzącego i uczestników.
- Omówienie celów i struktury szkolenia.
- Zasady współpracy i interaktywności.
- Przedstawienie podstawowych pojęć z zakresu cyberhigieny.

Moduł 2: Dlaczego to dotyczy mnie?

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 3: Inżynieria społeczna i najczęstsze ataki

- 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 4: Hasła i uwierzytelnianie

- 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 5: Złośliwe oprogramowanie (np. malware)

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

Moduł 6: Procedury i reakcja na incydenty

- 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 7: Podsumowanie, Q&A i kolejne kroki

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

Zarejestruj się na szkolenie: szkolenia@zalnet.pl

https://zalnet.pl/edu/podstawy-cyberhigieny/