Szkolenie z cyberbezpieczeństwa dla niepokornych pracowników

Opis szkolenia: Szkolenie ma na celu zwiększenie świadomości zagrożeń cybernetycznych wśród pracowników, którzy często ignorują zasady bezpieczeństwa lub wykazują opór wobec procedur IT. W przystępny i angażujący sposób przedstawione zostaną realne zagrożenia, skutki nieostrożnych działań oraz dobre praktyki w zakresie ochrony danych i systemów.

Czas trwania: 8 godzin (9:00 – 17:00)

Kategoria: Cyberbezpieczeństwo / Edukacja pracowników

Język wykładowy: język polski

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

Wymagania wstępne: Brak - szkolenie dla każdego pracownika.

Grupa decelowa: Pracownicy różnych branż. Szkolenie może być dopasowane pod konkretną branżę.

Cel szkolenia: Zwiększenie świadomości zagrożeń i zmiana postaw wobec zasad bezpieczeństwa IT.

Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
9:00 – 9:15	15 minut	**Moduł 1: Powitanie i omówienie szkolenia**	Prowadzenie, interaktywna ankieta
9:15 – 10:15	60 minut	**Moduł 2: Zagrożenia w sieci - fakty i mity**	Prezentacja, quiz
10:15 – 10:30	15 minut	Przerwa na kawę	–
10:30 – 11:30	60 minut	**Moduł 3: Socjotechnika i phishing – jak nas łapią?**	Analiza przypadków, ćwiczenia
11:30 – 12:00	30 minut	**Moduł 4: Bezpieczne hasła i uwierzytelnianie**	Demo, warsztat
12:00 – 13:00	60 minut	Przerwa obiadowa	–
13:00 – 13:45	45 minut	**Moduł 5: Zasady bezpiecznej pracy zdalnej i mobilnej**	Prezentacja, dyskusja
13:45 – 14:45	60 minut	**Moduł 6: Incydenty bezpieczeństwa – co robić?**	Symulacja, scenariusze

Godzina	Czas trwania	Moduł	Forma
14:45 – 15:00	15 minut	Popołudniowa przerwa na kawę	–
15:00 – 16:15	75 minut	**Moduł 7: Kultura bezpieczeństwa w organizacji**	Dyskusja, ćwiczenia
16:15 – 16:45	30 minut	**Moduł 8: Podsumowanie, test wiedzy i sesja pytań**	Test, Q&A
16:45 – 17:00	15 minut	**Moduł 9:**	

Szczegółowy program szkolenia

Moduł 1: Powitanie i omówienie szkolenia (15 minut)

- Przedstawienie trenera i uczestników.
- Cele i struktura szkolenia.
- Zasady pracy i materiały szkoleniowe.

Moduł 2: Zagrożenia w sieci – fakty i mity (60 minut)

- Najczęstsze zagrożenia w pracy biurowej.
- Mity na temat bezpieczeństwa IT.
- Statystyki i przykłady ataków.

Moduł 3: Socjotechnika i phishing – jak nas łapią? (60 minut)

- Techniki manipulacji i oszustw.
- Rozpoznawanie podejrzanych wiadomości.
- Ćwiczenia z analizą e-maili.

Moduł 4: Bezpieczne hasła i uwierzytelnianie (30 minut)

- Zasady tworzenia silnych haseł.
- Uwierzytelnianie dwuskładnikowe.
- Zarządzanie hasłami – menedżery haseł.

Moduł 5: Zasady bezpiecznej pracy zdalnej i mobilnej (45 minut)

- Bezpieczne korzystanie z Wi-Fi.
- Zasady pracy na urządzeniach prywatnych.
- Szyfrowanie i ochrona danych.

Moduł 6: Incydenty bezpieczeństwa – co robić? (60 minut)

- Reagowanie na podejrzane sytuacje.
- Zgłaszanie incydentów.
- Symulacja scenariuszy.

Moduł 7: Kultura bezpieczeństwa w organizacji (75 minut)

- Dlaczego warto przestrzegać zasad.
- Rola każdego pracownika w ochronie danych.
- Budowanie pozytywnej kultury bezpieczeństwa.

Moduł 8: Podsumowanie, test wiedzy i sesja pytań (30 minut)

- Powtórzenie kluczowych informacji.
- Test sprawdzający wiedzę.
- Sesja pytań i odpowiedzi.

Zarejestruj się na szkolenie: https://zalnet.pl/edu/szkolenie-z-cyberbezpieczenstwa-dla-niepokornych-pracownikow/