Szkolenie z cyberbezpieczeństwa dla niepokornych pracowników

Opis szkolenia: Czy te sytuacje brzmią znajomo?

- Czy Twoi pracownicy regularnie **ignorują zasady bezpieczeństwa** lub wykazują wyraźny opór wobec procedur wdrażanych przez dział IT?
- Obawiasz się, że mimo setek ostrzeżeń ktoś w firmie **wciąż klika w podejrzane linki** i daje się złapać na sprytne sztuczki phishingu?
- Czy masz stuprocentową pewność, że Twoi podwładni stosują **silne hasła** i potrafią poprawnie korzystać z menedżerów haseł oraz uwierzytelniania dwuskładnikowego?
- Czy wiesz, w jaki sposób Twój zespół chroni firmowe dane podczas **pracy zdalnej**, korzystając z publicznych sieci Wi-Fi lub prywatnego sprzętu?
- Czy w razie realnego cyberataku pracownicy potrafiliby **zachować zimną krew**, odpowiednio zareagować i natychmiast zgłosić incydent?

Odpowiedzią na te wyzwania jest nasze intensywne szkolenie! Poprzez praktyczne warsztaty, analizę studiów przypadku i symulacje realnych scenariuszy zmieniamy podejście najbardziej opornych uczestników, co na koniec weryfikujemy testem wiedzy i potwierdzamy certyfikatem.

Kod szkolenia: SEC-NIEP-01

Kategoria: Cyberbezpieczeństwo / Edukacja pracowników / Security awareness

Trenerka: Beata Zalewa

Czas trwania: 1 dzień / 8 godzin (9:00 – 17:00)

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 - szkolenie dla każdego pracownika.

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

Cel 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.

Efekty szkolenia:

- Uczestnicy zdobędą pełną świadomość realnych zagrożeń cybernetycznych oraz negatywnych skutków, jakie mogą nieść za sobą ich nieostrożne działania.
- Szkolenie ma na celu trwałą zmianę postaw uczestników, którzy do tej pory wykazywali opór wobec procedur IT lub ignorowali zasady bezpieczeństwa.

ZALNET
Beata Zalewa
+48 600 926 031
info@zalnet.pl
www.zalnet.pl
Wola Radzięcka 62
23-440 Frampol
NIP 717 111 99 64

- Uczestnicy zrozumieją rolę każdego członka zespołu w ochronie informacji i systemów oraz dowiedzą się, dlaczego warto bezwzględnie przestrzegać wdrożonych zasad.
- Uczestnicy dowiedzą się, w jaki sposób mogą aktywnie pomagać w budowaniu pozytywnej kultury bezpieczeństwa w strukturach całej organizacji.

Co otrzymasz?

- Materiały szkoleniowe.
- 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 – 12:30	60 minut	Moduł 4: Bezpieczne hasła i uwierzytelnianie	Demo, warsztat
12:30 – 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
14:45 – 15:00	15 minut	Popołudniowa przerwa na kawę	–

Godzina	Czas trwania	Moduł	Forma
15:00 – 16:30	90 minut	Moduł 7: Kultura bezpieczeństwa w organizacji	Dyskusja, ćwiczenia
16:30 – 17:00	30 minut	Moduł 8: Podsumowanie, test wiedzy i sesja pytań	Test, Q&A

Szczegółowy program szkolenia

Moduł 1: Powitanie i omówienie szkolenia

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

Moduł 2: Zagrożenia w sieci – fakty i mity

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

Moduł 3: Socjotechnika i phishing – jak nas łapią?

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

Moduł 4: Bezpieczne hasła i uwierzytelnianie

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

Moduł 5: Zasady bezpiecznej pracy zdalnej i mobilnej

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

Moduł 6: Incydenty bezpieczeństwa – co robić?

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

Moduł 7: Kultura bezpieczeństwa w organizacji

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

Moduł 8: Podsumowanie, test wiedzy i sesja pytań

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

Zarejestruj się na szkolenie: szkolenia@zalnet.pl

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