Tytuł szkolenia: Cyberbezpieczeństwo i ochrona danych w przedsiębiorstwie

Kod szkolenia: CYBER-BEZP

Wprowadzenie

Adresaci szkolenia

Szkolenie przeznaczone dla przedsiębiorców i ich pracowników, którzy chcą poznać zasady ochrony przed cyberprzestępczością oraz z uwagi na fakt zarządzania danymi osobowymi - ochrony tych danych przed atakami hakerów. Szkolenie dedykowane także dla kadry zarządzającej, menagerów, księgowych, kancelarii prawnych.

UWAGA

Czas trwania: 3 wersje do wyboru – 12/16/24 godzin/y dydaktyczne [45 min].
Zapewniamy materiały szkoleniowe dla uczestników w formie elektronicznej.

Cel szkolenia

Celem szkolenia jest nabycie przez uczestników wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców, wirusami, złośliwym oprogramowaniem - także w zakresie bezpiecznego zarządzania danymi w przedsiębiorstwie, włączając w to wrażliwe dane osobowe oraz zagrożenia płynące z korzystania z Internetu, mediów społecznościowych, poczty e-mail.

Po zakończonym szkoleniu uczestnik:

- zna zasady bezpiecznego korzystania z Internetu, poczty e-mail oraz mediów społecznościowych i chmury
- używa odpowiednich narzędzi do ochrony przed atakami cyberprzestępców oraz przed złośliwym oprogramowaniem
- potrafi rozpoznać zagrożenie i skutecznie je zneutralizować
- tworzy i korzysta z kopii bezpieczeństwa
- zna ryzyko wykradnięcia danych i umie je zminimalizować
- potrafi reagować po wykryciu u siebie w firmie incydentu naruszenia bezpieczeństwa
- wie jak postępować w przypadku wykrycia w swoim sprzęcie komputerowym złośliwego oprogramowania
- zna zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing)
- potrafi rozpoznać fałszywy adres e-mail, aplikację, link, wiadomość na Facebooku
- zna metody wyłudzania danych i umie je zidentyfikować i opisać
- wie jak zarządzać, przetwarzać, szyfrować dane osobowe
- zna sprzętowe możliwości ochrony danych (w tym osobowych)
- rozumie pojęcia typowe dla zagadnień związanych z cyberbezpieczeństwem (VPN, trojan, malware i inne)

Czas i forma szkolenia

- 7 godzin (1 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Jak dbać o swoją tożsamość cyfrową

- wirusy
- szpiegowanie
- sposoby hackowania systemu operacyjnego

2. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich

- phishing
- cracking
- spoofing
- back
- door
- trojan
- DDos
- keyloggin
- session hijacking i inne

3. Hasła i ich bezpieczeństwo. Jak tworzyć, przechowywać i pamiętać swoje hasła w gąszczu pinów, aplikacji, kont internetowych?

4. Zostałeś/łaś shakowany? Co dalej?

- studium przypadków

5. Tryb bezpieczny

- incognito
- monitorowanie zachowań w sieci

6. Programy antywirusowe i ochrona przed atakami hakerskimi

- cookies
- monitorowanie IP
- MAC
- VPN
- aplikacje szpiegowskie

7. Co i jak można wykraść? Jak tego uniknąć?

8. Przeglądarki – Historia. Zarządzanie i ochrona danych – szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku – studium przypadków – incydenty bezpieczeństwa