Opis szkolenia

Dane o szkoleniu

Kod szkolenia: 5044426

Temat: Higiena Cyberbezpieczeństwa - szkolenie dla urzędów i firm

28 Kwiecień Transmisja ONLINE, Internet ,

Kod szkolenia: 5044426

Koszt szkolenia: 640.00 + 23% VAT

Program

Cele szkolenia

- **Zwiększenie świadomości cyberzagrożeń – uczestnicy poznają aktualne metody ataków (np. phishing, deepfake, vishing).**
- **Zrozumienie roli cyberhigieny w ochronie informacji i bezpieczeństwie organizacji.**
- **Nabycie praktycznych umiejętności rozpoznawania zagrożeń w codziennej pracy (e-mail, komunikatory, internet, AI).**
- **Wypracowanie właściwych nawyków bezpieczeństwa – reagowanie na incydenty, stosowanie dobrych praktyk.**
- **Poznanie odpowiedzialności pracowników i działów IT w utrzymaniu bezpieczeństwa organizacji.**
- **Przygotowanie do nowych ryzyk związanych z pracą zdalną, mediami społecznościowymi i sztuczną inteligencją.**

Korzyści z udziału

- **Zmniejszenie ryzyka incydentów bezpieczeństwa dzięki lepszym reakcjom pracowników.**
- **Ochrona danych organizacji i informacji wrażliwych (szczególnie istotne w administracji publicznej).**
- **Większa odporność na ataki socjotechniczne (np. fałszywe maile od „przełożonego").**
- **Lepsza współpraca z działem IT/cyberbezpieczeństwa i sprawniejsza komunikacja w sytuacjach zagrożenia.**
- **Świadome i bezpieczne korzystanie z narzędzi cyfrowych, w tym AI i pracy zdalnej.**
- **Wykształcenie automatycznych, właściwych reakcji w sytuacjach ryzykownych (tzw. „odruchy bezpieczeństwa").**

---

1. Wprowadzenie do cyberbepieczeństwa
2. Cyberbezpieczeństwo a ochrona informacji
3. Cyberhigiena – co to i po co
a. Całościowe podejście do cyberbezpieczeństwa
b. Rola i znaczenie cyberhigieny w cyebrbezpieczeństwie
c. Rola działów IT/Cyberbezpieczeństwa w cyberbezpieczeństwie
d. Rola pracowników w zachowaniu cyberbezpieczeństwe organizacji
4. Główne cele cyberprzestępców w ataku na organizacje takie jak administracja publiczna
5. Główne ryzyka związane z cyberbezpieczeństwem
a. Phishing – wprowadzenie
b. Korespondencja mailowa
c. Korespondencja za pomocą komunikatorów
d. Korzystanie z zewnętrznych źródeł internetowych, przesyłanie plików
e. Stosowanie czatów AI (chat gpt, gemini, Anthropic itp.)
f. Uwierzytelnianie w usługach zewnętrznych przez pracowników
6. Nowe ryzyka
a. Social media pracownika
b. Sztuczna Inteligencja jako nowe źródło ryzyk
c. Praca zdalna
d. Deepfake, generatory głosu, vising
e. Dezinformacja ukierunkowana
f. Sieci internetowe wi-fi itp.
7. Reagowanie
a. Świadomość jest ważna ale nie najważniejsza
b. Komunikacja z IT

c. Rola trenowania odruchów
d. Włączanie i przestrzeganie mechanizmów kontrolnych
8. Przykłady dobrych praktyk
a. Nowe strony internetowe
b. Nietypowe komunikaty od szefa
c. Stosowanie haseł
d. Stosowanie mechanizmów uwierzytelnienia
e. Powściągliwość w komunikacji internetowej
9. Zakończenie szkolenia – pytania i odpowiedzi.