

Security Awareness - socjotechnika

Korzyści dla Biznesu:

- Podniesienie bezpieczeństwa w organizacji
- Zwiększenie świadomości pracowników będących najsłabszym ogniwem bezpieczeństwa firmy

Korzyści dla uczestników

- Podczas szkolenia uczestnicy poznają sposoby i metody wykorzystywane przez hakerów i sposoby ochrony przed nimi
- Zapoznają się z tematyką socjotechniki i ataków socjotechnicznych

Zarys Agendy:

1. Historia systemów operacyjnych, Internetu oraz obecna struktura sieci
2. Terminologia bezpieczeństwa IT
3. Polityka bezpieczeństwa w firmie
4. Strategie zabezpieczania danych
5. Czym jest socjotechnika? Jak hakerzy przeprowadzają ataki?
6. Przykłady ataków i formy obrony
7. Korzystanie z prywatnych kont np. Facebook
8. Phishing
9. Błędy certyfikatów i ryzyko podsłuchania
10. Bezpieczeństwo haseł
11. Uwierzytelnianie dwuskładnikowe - najlepsze zabezpieczenie

Czas trwania	Język szkolenia	Forma szkolenia:
1 dzień (4 godzin)	Polski lub Angielski	Wykłady, prezentacje, ćwiczenia
Szkolenie dostosowujemy do jednego z poziomów: • PODSTAWOWY • ŚREDNIOZAAWANSOWANY • ZAAWANSOWANY		



Kontakt

Patryk Dynowski

Business Development Manager

T: +48 577 255 112

E: patryk.dynowski@testarmy.com

