Security Awareness - jak być świadomym użytkownikiem

Agenda szkolenia:

Czym jest Security Awareness
Motywy osób atakujących
Socjotechnika - stany emocjonalne wykorzystywane przez przestępców
- Zagrożenia w Internecie
- Czym jest Ransomware
- Jak rozpoznać fałszywe bramki płatności
- Co zrobić kiedy Twoje dane wyciekły
- Dezinformacja

Polityka haseł
- Jak tworzyć dobre hasła
- Czym jest uwierzytelnianie dwuskładnikowe (2FA)
- Metody przechowywania haseł

Social Media
- Jakie dane publikujemy w portalach społecznościowych i czym mogą one grozić
- Co robić, gdy nasze konto zostało przejęte
- Jak zadbać o bezpieczeństwo naszych portali

Strony www
- Co to jest domena, subdomena
- Czym są ataki z wykorzystaniem Typosquatting
- Jak sprawdzić wiarygodność linku

Phishing
- Definicja i odmiany phishing'u
- Załączniki w e-mailowych kampaniach phishing'owych
- Jak rozpoznać phishing
- Jak chronić się przed phishingiem

Płatności w Internecie
- Metody płatności w Internecie - dobre i złe strony
- Czym jest charge back?

Bezpieczeństwo urządzeń mobilnych
- Jak podnieść bezpieczeństwo urządzenia mobilnego
- Jak ochronić dane jeżeli straciliśmy smartphone

Bezpieczeństwo pracy zdalnej
- Typowe ataki na osoby pracujące zdalnie
- Jak zabezpieczyć domowy router
- Na co zwrócić uwagę podczas pracy zdalnej

Inne
- Jak bezpiecznie przesyłać wrażliwe dane
- Zabezpieczenie danych na komputerze
- Polityka "czystego biurka"