I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

Security Awareness - jak być świadomym użytkownikiem

I know IT by softinet

Korzystając z naszego wykładu dowiesz się:

- jak podnieść świadomości pracowników o realnych zagrożeniach w cyberprzestrzeni
- poznasz metody działania hakerów
- jakie są skuteczne metody ochrony
- sposoby pielęgnowania dobrych nawyków związanych z bezpieczeństwem

Czas
1 DZIEŃ

Godziny
9:00 - 13:00

Certyfikat
TAK

OPIS SZKOLENIA

Człowiek w procesie bezpieczeństwa odgrywa bardzo istotną rolę. Jest on ostatnią linią obrony przed zagrożeniami w cyberprzestrzeni. Okazuje się, że to pracownicy są najczęściej na celowniku przestępców, dlatego tak bardzo ważne jest budowanie ich świadomości o potencjalnych zagrożeniach w Internecie. Dzięki temu szkoleniu dowiesz się m. in. czym jest socjotechnika i jak jest wykorzystywana przez przestępców, jak budować bezpieczne hasła oraz czym jest polityka "czystego biurka". Zdobędziesz wiedzę na temat phishing'u- czym jest i jak go rozpoznać i wiele innych ciekawych historii.

CEL SZKOLENIA

Uczestnicy dowiedzą się w jaki sposób radzić sobie z różnymi rodzajami ataków w cyberprzestrzeni. Podczas wykładu bardzo duży nacisk położony jest na przeanalizowanie razem z uczestnikami wielu przypadków ataków aby wykorzystać w praktyce nabytą wiedzę.

FORMA SZKOLENIA

Szkolenie prowadzone jest w formie wykładów.

WYMAGANIA

Wykład przeznaczony jest dla każdego użytkownika.

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"

TRENER - MICHAŁ CYGAN

Inżynier **FORTINET** posiadający doświadczenie w zakresie wdrażania i wsparcia omawianych rozwiązań.

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

(22) 427 37 54 / +48 728 540 162