Praktyczne bezpieczeństwo IT

W dzisiejszych czasach, zagrożenia w **cyberprzestrzeni** stale ewoluują, stwarzając coraz większe wyzwania dla firm i użytkowników indywidualnych. Według najnowszych danych, roczne liczby ataków cybernetycznych znacząco wzrosły, przekraczając obecnie setki tysięcy przypadków rocznie. Nasze szkolenie z zakresu **bezpieczeństwa IT** oferuje kompleksowe podejście do ochrony przed tymi zagrożeniami.

Poprzez interaktywne zajęcia oraz studia przypadków uczestnicy zdobędą aktualną wiedzę na temat najnowszych rodzajów ataków, metod penetracji sieci oraz technik wykorzystywanych przez cyberprzestępców. Szkolenie skupia się na praktycznych aspektach bezpieczeństwa informatycznego, ukazując realne scenariusze i strategie obronne wobec nich.

Szkolenie z bezpieczeństwa informacji jest szkoleniem dedykowanym pracownikom biurowym i administracyjnym (nie jest przeznaczone dla specjalistów IT). Dzięki udziałowi w szkoleniu uczestnik będzie wiedział w jaki sposób utworzyć bezpieczne hasła, jak zidentyfikować potencjalne zagrożenia oraz im zapobiegać. Szkolenie może być traktowane również jako wstępne szkolenie (wprowadzające) nowych pracowników do firmy. Szkolenie Bezpieczeństwo informacji jest oparte o wiele przykładów prawdziwych zdarzeń oraz ataków informatycznych. Prowadzone jest przez trenera praktyka, który w lekki sposób przekazuje informacje dot. ważnych zagadnień bezpieczeństwa biurowego.

Uczestnicy po szkoleniu zdobędą również wiedzę i świadomość jak bezpiecznie korzystać z internetu, portali społecznościowych oraz bankowości elektronicznej zarówno w sferze biznesowej jak i prywatnej.

Zakres tematyczny

Podstawy bezpieczeństwa w firmie

- → Zasada czystego biurka ("clean desk")
- → Zasada czystego ekranu ("clean screen")

Rodzaje zagrożeń – omówienie na przykładach

- → Ataki socjotechniczne – człowiek jako najsłabsze ogniwo systemu zabezpieczeń
  - Na czym polegają
  - Typowe scenariusze
  - Zapobieganie a edukacja
- → Phishing, spear-phishing
- → Scam czyli metoda na "wnuczka" w IT
- → Ransomware – porwanie (komputera) dla okupu (WannaCry, WannaCrypt)
- → Spoofing a więc podszywanie się pod innych
- → Jak nie dać się "złowić"

Bezpieczne hasło

- → Metody autoryzacji – czy hasło to najlepszy sposób ochrony dostępu

Imperium Szkoleniowe
Tel. 22 402 15 04, Fax: 22 258 23 62
biuro@imperiumszkoleniowe.pl

- Jakie hasło jest bezpieczne
- Łamanie haseł
  - Łamanie vs odzyskiwanie haseł
  - Metody łamania haseł
- Przechowywanie haseł – dlaczego hasło nie powinno być przyklejone pod klawiaturą
- Hasła dla różnych usług – jak nie zgubić się w gąszczu haseł
- Kontenery haseł
- Mnemotechniki – jak zapamiętać skomplikowane hasła
- Login w haśle – dlaczego to bardzo zły pomysł
- Autoryzacja 3D – uwierzytelnianie podwójne
- Ochrona PIN – jak chronić swój kod

Bezpieczeństwo komputerów oraz urządzeń mobilnych

- Korzystanie z urządzeń zewnętrznych (USB), urządzenia zakamuflowane (np. pendrive działający jak klawiatura)
- Przenoszenie danych – czy pendrive to dobry pomysł
- Korzystanie z darmowego WiFi – zagrożenia
- Bezpieczne korzystanie z łączności bezprzewodowej (WiFi, Bluetooth)
- Korzystanie z ładowarek w centrach handlowych etc. – wygoda czy zagrożenie
- VPN – bezpieczny zdalny dostęp
- Aktualizacja oprogramowania – przykłady ataków przez niezaktualizowane oprogramowanie
- Kopie zapasowe danych – przywilej czy konieczność
- Przechwytywanie obrazu z kamerki – czy to możliwe oraz metody zapobiegania
- Oprogramowanie antywirusowe na telefonie – standard czy paranoja
- Bezpieczeństwo IoT na podstawie włamania do sieci przez czajnik
- Przechowywanie oraz usuwanie danych (czyli dlaczego lepiej nie sprzedawać aparatu z kartą pamięci)

Bezpieczne praca z aplikacjami

- Programy pakietu Office – wersje online oraz desktop
- Makra – czym są i czy mogą być szkodliwe – jak napisać złośliwy kod w 5 minut
- Przeglądarki internetowe – przechowywanie haseł, strony zabezpieczone/niezabezpieczone
- Co Google o nas wie
- Bezpieczeństwo usług mobilnych – czy każda aplikacja na telefon jest bezpieczna

Bankowość

- Bankowość internetowa – rodzaje dostępów, autoryzacja, zagrożenia
- Korzystanie z bankomatów – metody kradzieży PIN, klonowanie kart

Podsumowanie