

Program szkolenia

Cyberbezpieczeństwo dla personelu medycznego

<https://bloomwise.pl/consulting/training/cyberbezpieczenstwo-dla-personelu-medycznego>

Poniższy zakres stanowi bazę, którą możemy dopasować do specyfiki Twojej marki, zespołu i modelu pracy z klientem.

Moduł 1. Wprowadzenie, czyli jak działają cyberprzestępcy?

Moduł 2. Przykłady ataków hackerskich – case study. Skutki dla placówki medycznej, pracownika i pacjenta.

Moduł 3. Podstawowe informacje o atakach na użytkowników – socjotechnika, phishing, spearphishing, malware, pharming, spoofing, spam, spim, scam, brute force. Przeprowadzenie warsztatów z identyfikowania ataków hackerskich.

Moduł 4. Podstawowe zasady bezpieczeństwa pracy na komputerze, telefonie i tablecie.

Moduł 5. Bezpieczeństwo haseł – budowa, przechowywanie oraz inne bezpieczniejsze metody logowania.

Moduł 6. Bezpieczne korzystanie z poczty elektronicznej.

Moduł 7. Bezpieczne korzystanie z sieci Internet.

Moduł 8. Kontakt z pacjentem i osobami upoważnionymi a cyberbezpieczeństwo.

Moduł 9. AI a cyberbezpieczeństwo.

Moduł 10. Sprzęt prywatny a sprzęt służbowy.

Moduł 11. Incydenty i reakcja na nie, przydatne linki i narzędzia.

Moduł 12. Moduły personalizowane - do uzgodnienia.