

Program szkolenia

Cyberbezpieczeństwo dla pracowników

<https://bloomvise.pl/consulting/training/cyberbezpieczenstwo-dla-pracownikow>

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. OSINT – co to jest biały wywiad, czyli jak i gdzie szukać informacji w sieci.

Moduł 3. Przykłady ataków hackerskich – case study. Skutki dla organizacji.

Moduł 4. Regulacje, odpowiedzialności i sankcje.

Moduł 5. Podstawowe informacje o atakach na użytkowników – socjotechnika, phishing, spearphishing, malware, pharming, spoofing, spam, spim, scam, brute force. Przykłady z życia.

Moduł 6. Podstawowe zasady bezpieczeństwa pracy na komputerze, telefonie i tablecie.

Moduł 7. Bezpieczeństwo haseł – budowa, przechowywanie oraz inne bezpieczniejsze metody logowania.

Moduł 8. Bezpieczne korzystanie z poczty elektronicznej.

Moduł 9. Bezpieczne korzystanie z sieci Internet.

Moduł 10. Bezpieczna praca zdalna.

Moduł 11. Szyfrowanie i bezpieczne przechowywanie dokumentów.

Moduł 12. AI a cyberbezpieczeństwo.

Moduł 13. Sprzęt prywatny a sprzęt służbowy.

Moduł 14. Incydenty i reakcja na nie, przydatne linki i narzędzia.

Moduł 15. Moduły personalizowane - do uzgodnienia.