Autoryzowane Centrum Szkoleniowe CLICO

CYBER-BEZPIECZEŃSTWO

DLA PRACOWNIKÓW BIUROWYCH

UNIKALNE KORZYŚCI DLA UCZESTNIKÓW SZKOLENIA:

- rozpoznawanie podejrzanych wiadomości e-mail, stron internetowych i innych form komunikacji, które mogą być probą phishingu czy innego scamu
- świadome korzystanie z haseł o silnej złożoności i praktyowanie bezpiecznego zarządzania nimi.
- zrozumienie konsekwencji otwierania załączników z nieznanych źródeł oraz otwierana podejrzanych linków.
- wykazywanie się ostrożnością przy udostępnianiu poufnych informacji online, zarówno na platformach społecznościowych jak i podczas korzystania z aplikacji służbowych
- jak reagować i kiedy zgłaszać podejrzane zachowania lub incydenty związane z bezpieczeństwem IT odpowiednim osobom w firmie
- myślenie krytyczne a więc jak odnajdywać się w sieci szybko rozprzestrzeniających się fake newsów
- teoretyczne i praktyczne przyswojenie wiedzy dzięki prezentacji i nagraniom z przygotowania wybranych form ataków i realizacji ich w rzeczywistości

CEL SZKOLENIA:

Celem szkolenia jest zwiększenie świadomości pracowników biurowych na temat różnorodnych zagrożeń cybernetycznych, takich jak phishing, malware, ataki ransomware itp. Poprzez przekazanie praktycznej wiedzy oraz konkretnych przykładów, chcemy wyposażyć uczestników w umiejętności identyfikacji podejrzanych sytuacji oraz sposobów reakcji na nie. Ponadto, celem szkolenia jest także edukacja w zakresie właściwego korzystania z narzędzi i aplikacji używanych w pracy biurowej, aby minimalizować ryzyko naruszenia bezpieczeństwa danych firmowych, ale też prywatnych.

AGENDA

DZIEŃ 1

Wprowadzenie

- Podstawowe pojęcia bezpieczeństwa systemów informatycznych.
- Kim są cyberprzestępcy i jakie są ich motywy.

Krytyczne obszary bezpieczeństwa pracowników

- Włamania, złośliwe programy i inne zagrożenia w sieci i Internecie.
- Phishing i różne odmiany ataków socjotechnicznych oraz ich skutki.
- Zestawianie Reverse Shell pomiędzy systemami Windows i Linux.
- Łamanie haseł i jak się przed tym chronić + Wprowadzenie do Yubico

Bezpieczne przeglądanie stron WWW

- Szyfrowanie
- Certyfikaty SSL
- Adblocker

Wykorzystanie sprzętu służbowego do użytku prywatnego i na odwrót

- Bezpieczne przechowywanie danych na laptopie i zewnętrznych zasobach dyskowych
- Aktualizacja oprogramowania
- Praca z urządzeniami mobilnymi + zastrzeganie PESEL

OSINT

- W jaki sposób pozyskać dane na swój temat
- Jak ograniczać dostęp do danych
- Myślenie krytyczne w kontekście dezinformacji

Quiz

Cena szkolenia: 600 zł netto od osoby
(dla grup min. 10 osób)