Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Cyberbezpieczeństwo dla osób nie-technicznych: budowanie cyfrowej odporności (Human Firewall)

Opis

Wygenerowany przez AI fałszywy e-mail do księgowości czy fałszywa faktura mogą w kilka chwil sparaliżować działanie całej firmy. Na szczęście budowanie odporności na cyberataki nie wymaga specjalistycznej wiedzy IT – to po prostu kwestia dobrych nawyków.

Podczas jednodniowego, praktycznego szkolenia nauczymy Ciebie I Twój zespół, jak skutecznie wyłapywać pułapki w sieci, dbać o hasła i bezpiecznie pracować w biurze oraz zdalnie.

Zapisz się na kurs i zyskaj pewność, że Twoja codzienna praca opiera się na najlepszych, sprawdzonych standardach bezpieczeństwa a Twoja firma jest dobrze chroniona.

Dlaczego warto?

Prosty język, zero technicznego żargonu → Szkolimy na przykładach z życia. Nie musisz mieć zaawansowanej wiedzy IT, by skutecznie chronić siebie i firmę

Praktyczne symulacje → Zobaczysz przykłady, jak wygląda prawdziwy atak hakerski i przeanalizujesz go krok po kroku

Psychologia ataku→ Pokazujemy, że najsłabszym ogniwem nie jest system, ale ludzkie emocje. Uczymy, jak hakerzy wykorzystują strach i ciekawość oraz jak się nie złapać.

Check-listy – Wracasz do pracy z gotowymi procedurami do wdrożenia w życie

Umiejętności

Dzięki szkoleniu:

- Nauczysz się szybko identyfikować phishing e-mailowy, fałszywe SMS-y (smishing) oraz próby wyłudzenia danych przez telefon (vishing)
- Skonfigurujesz i zaczniesz korzystać z menedżerów haseł, kluczy bezpieczeństwa oraz weryfikacji dwuetapowej (2FA/MFA)
- Nauczysz się, jak nie ulegać manipulacji i presji czasu stosowanej przez oszustów
- Zdobędziesz wiedzę, jak bezpiecznie korzystać z publicznego Wi-Fi, pendrive'ów oraz jak dbać o aktualizacje i backupy podczas pracy zdalnej
- Otrzymasz gotowe procedury i checklisty, dzięki którym będziesz wiedzieć, kogo powiadomić i co kliknąć, gdy przypadkowo padniesz ofiarą ataku

Dla kogo jest to szkolenie?

Poruszane zagadnienia są ważne dla każdego, a w szczególności dla pracowników biurowych i administracyjnych oraz działów HR, Finasów, Księgowości oraz kadry zarządzającej jako osób najbardziej zagrożonych na cyberataki.

Szczegółowy program szkolenia

1. Najczęstsze zagrożenia w codziennej pracy

- Phishing – jakie są skuteczne metody bezbłędnej identyfikacji fałszywych wiadomości, złośliwych załączników i nieprawdziwych nadawców
- Smishing (SMS) – jak wykrywać fałszywe wiadomości tekstowe oraz podejrzane linki do płatności
- Vishing (voice) – weryfikowanie tożsamości dzwoniącego, bezpieczna rozmowa i ochrona poufnych danych przez telefon
- Spear phishing – dlaczego ataki ukierunkowane na konkretne działy i osoby są najgroźniejsze i jak je powstrzymać?
- Procedury sprawdzania autentyczności dokumentów płatniczych oraz numerów kont bankowych
- Szybkie rozpoznawanie nietypowej aktywności logowania (przejęcie konta) i błyskawiczne odcinanie dostępu
- Jak wykrywać wyłudzenia tworzone przez sztuczną inteligencję (AI) oraz oszustwa typu deepfake

2. Bezpieczne hasła i uwierzytelnianie

- Zasady tworzenia unikalnych, trudnych do złamania i łatwych do zapamiętania fraz dostępowych
- Menedżer haseł – jak zautomatyzować generowanie, bezpieczne przechowywanie i uzupełnianie danych logowania
- Dwuetapowa weryfikacja 2FA/MFA w praktyce jako podstawowy standard ochrony kont służbowych
- Zastosowanie fizycznych kluczy jako nieprzenikalnej bariery dla cyberprzestępcó.

3. Social engineering i manipulacja

- Demaskowanie psychologicznych sztuczek na podstawie najczęstszych scenariuszy ataków
- Jak zachować zimną krew pod presją czasu i weryfikować podejrzane prośby?

- Kontekst prawny i RODO – ochrona danych osobowych w organizacji a uniknięcie dotkliwych kar finansowych.

4. Praca zdalna

- Bezpieczne korzystanie z domowych i publicznych sieci bezprzewodowych przy użyciu szyfrowania VPN
- Ryzyka związane z zewnętrznymi nośnikami pamięci i zasady ochrony przed złośliwym oprogramowaniem
- Aktualizacje i backupy – jak prawidłowo tworzyć i weryfikować kopie zapasowe kluczowych dokumentów na wypadek awarii?
- Korzystanie z prywatnych urządzeń do celów służbowych

5. A co zrobić, gdy już staniemy się ofiarą?

- Procedura działania – zarządzanie kryzysowe bez paniki
- Kogo i jak błyskawicznie poinformować w przypadku incydentów, by powstrzymać rozprzestrzenianie się ataku?
- Gotowa check-lista ratunkowa krok po kroku

6. Praktyka

- Interaktywne symulacje w bezpiecznych, kontrolowanych warunkach warsztatowych
- Analiza case studies –wnioski z realnych ataków na polskie i zagraniczne firmy

Liczba dni, liczba godzin szkoleniowych

1 dzień, 8 godzin szkoleniowych

Ścieżka rozwoju po szkoleniu

OSINT dla pracowników biurowych

Etyczny hacking- Pentesty w Kali Linux