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

COMARCH
Szkolenia

E- Wprowadzenie do phisingu

Cele szkolenia

Szkolenie ma na celu podniesienie świadomości na temat zagrożeń związanych z phishingiem oraz wyposażenie uczestników w umiejętności i narzędzia niezbędne do skutecznej ochrony przed tego rodzaju atakami.

Cele są podzielone na trzy główne obszary:

- edukacja,
- identyfikacja
- oraz ochrona i reakcja.

Umiejętności

Uczestnicy tego szkolenia zyskają:

- **Świadomość zagrożeń:** Lepsze zrozumienie, jakie ryzyka niesie phishing dla danych osobowych oraz poufnych informacji firmowych.
- **Zdolność szybkiego reagowania:** Umiejętność natychmiastowego rozpoznania prób phishingowych oraz szybka reakcja w przypadku potencjalnego zagrożenia.
- **Zwiększenie bezpieczeństwa organizacji:** Nabyte kompetencje pozwolą przyczynić się do wzmocnienia kultury bezpieczeństwa w organizacji, co może zminimalizować ryzyko wycieku danych.

Profil uczestników

Szkolenie to skierowane jest zarówno do pracowników technicznych, jak i nietechnicznych, zapewniając kompleksowe podejście do ochrony przed phishingiem w różnych środowiskach pracy i życia prywatnego.

Przygotowanie uczestników

Aby w pełni skorzystać ze szkolenia, uczestnicy powinni spełniać następujące minimalne wymagania:

1. Podstawowa wiedza o obsłudze komputera i internetu
2. Dostęp do urządzenia z dostępem do internetu
3. Podstawowa znajomość środowiska pracy - jeśli szkolenie dotyczy phishingu w środowisku zawodowym, uczestnicy powinni znać ogólne zasady pracy z firmowymi systemami, np. korzystanie z firmowej poczty elektronicznej czy innych aplikacji używanych w organizacji.

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

Szczegółowy program szkolenia

1. **Wstęp**
    - Krótkie wprowadzenie do phishingu oraz jego znaczenia w dzisiejszym świecie cyfrowym.
2. **Phishing z lotu ptaka**
    - **Czym jest phishing?** Wprowadzenie do phishingu, w tym omówienie technik i motywacji stojących za atakami phishingowymi.
    - **Powody ataków phishingowych** Omówienie, dlaczego przeprowadza się ataki phishingowe, m.in. dla zysków finansowych i kradzieży informacji.
    - **Pułapki phishingu** Sposoby, w jakie atakujący projektują pułapki, aby oszukać swoje ofiary.
    - **Psychologiczne bariery w ochronie przed phishingiem** Jak psychologia człowieka wpływa na podatność na ataki phishingowe i jak przezwyciężyć te słabości.
3. **Rodzaje ataków phishingowych**
    - **Vishing (phishing telefoniczny)** Przegląd phishingu przeprowadzanego za pomocą rozmów telefonicznych.
    - **Phishing w mediach społecznościowych** Ataki phishingowe wykorzystujące platformy mediów społecznościowych.
    - **Spear phishing** Wysoce ukierunkowane ataki phishingowe skierowane na konkretne osoby lub organizacje.
    - **Smishing (phishing przez SMS)** Ataki phishingowe za pomocą wiadomości tekstowych.
    - **Inne kreatywne ataki phishingowe** Omówienie nietypowych i innowacyjnych technik phishingowych.
4. **Jak wykryć phishing**
    - **Dlaczego phishing jest skuteczny** Analiza, dlaczego ataki phishingowe często się udają, od luk technicznych po błędy ludzkie.
    - **Sztuka rozpoznawania phishingu** Praktyczne strategie i oznaki, które mogą pomóc w rozpoznawaniu prób phishingowych.
    - **Rzeczywiste przypadki i strategie oszustów** Wgląd w rzeczywiste przykłady phishingu i techniki stosowane przez atakujących.
5. **Obrona przed phishingiem**
    - **Jak się chronić przed phishingiem** Najlepsze praktyki i nawyki pozwalające uniknąć stania się ofiarą phishingu.
    - **Jak może w tym pomóc technologia** Narzędzia i technologie, które wspierają wykrywanie i zapobieganie phishingowi.
    - **Ćwicz rozpoznawanie phishingu** Ćwiczenia praktyczne mające na celu poprawę umiejętności wykrywania phishingu.
6. **Co zrobić, jeśli padłeś ofiarą phishingu?**
    - **Phishing w pracy** Kroki, które należy podjąć, jeśli padniesz ofiarą phishingu w kontekście zawodowym.
    - **Phishing w domu** Strategie odpowiedzi na ataki phishingowe w życiu prywatnym.
7. **Podsumowanie**

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

COMARCH
Szkolenia

Metoda realizacji szkolenia

Szkolenie elektroniczne (on-line).

Materiał szkoleniowy, udostępniany przez Internet, wzbogacony jest prezentacjami video, obrazami (zrzutami ekranu), opisami tekstowymi. Dzięki formie e-learningu uczestnicy dostają możliwość zapoznania się z materiałem w dowolnym czasie, w swoim własnym tempie, z dowolnego miejsca.

Zastosowane metody i narzędzia:

- Prezentacja treści (tekst wraz z komentarzem Trenera)
- Symulacja systemu (film prezentujący funkcjonalności z narracją Trenera)
- Podsumowanie (tekst/ilustracja z komentarzem Trenera)
- Quizy

Liczba godzin szkoleniowych

90 minut materiału video

Ścieżka rozwoju po szkoleniu

Szkolenia z zakresu cyberbezpieczeństwa:
e-learning
https://www.comarch.pl/szkolenia/e-learning/cyberbezpieczenstwo/

szkolenia stacjonarne/zdalne
https://www.comarch.pl/szkolenia/cyberbezpieczenstwo/