



STACJA 6

Zatruty haczyk (phishing)



KARTA PRACY DLA DRUŻYNY

Tematyka: Ochrona przed cyberoszustwami, wyłudzeniem haseł i manipulacją w sieci.

Jesteś w środku cyfrowego jeziora. Oszuści rzucają w internecie cyfrowe przynęty. Pytanie, czy złapiesz się na zatruty haczyk? Phishing, to próba oszukania kogoś, aby podał swoje dane osobowe (np. hasło, numer telefonu).

Zadanie 1

Na telefon jednego z was przychodzi SMS: *"Twój profil w grze zostanie zablokowany za 15 minut! Kliknij w ten link: www.bezpieczenstwo_danych.pl i podaj swoje hasło, aby tego uniknąć"*. Zwróć uwagę na to, że może to być cyfrowa pułapka. Co robicie?

Zadanie 2

Połączcie hasło z definicją

Phishing

- Proces zbierania i analizowania zachowań użytkowników w celu stworzenia cyfrowego profilu osoby np. podczas rozgrywki w grze (ruchy, czas reakcji, wybory, częstotliwość logowania).

Profilowanie

- Techniki stosowane w projektowaniu interfejsów (np. gier, aplikacji, stron) w celu manipulowania decyzjami użytkownika np. niezamierzonych zakupów, subskrypcji czy udostępnienia danych osobowych.

Dark patterns

- Rodzaj cyberoszustwa, w którym przestępcy podszywają się pod zaufane instytucje (banki, kurierów, urzędy) lub znajomych, aby wyłudzić poufne dane: hasła, loginy, numery kart kredytowych czy PESEL. Używają do tego fałszywych e-maili, SMS-ów lub stron internetowych, często wywołując presję czasu.



STACJA 6

Zatruty haczyk (phishing)



KARTA MENTORA- OPIEKUNA STACJI

Rola mentora – jesteś przewodnikiem, który zadaje pytania, aby pomóc drużynie rozwiązać zadanie. Nie przekazujesz wiedzy, nie podajesz rozwiązań, ale naprowadzasz tylko pytaniami. Mentor nie krytykuje odpowiedzi drużyny, lecz zadaje jedno z pytań. Możesz wybrać je z zaproponowanej listy pytań pomocniczych. Zaliczenie stacji następuje, gdy uczeń własnymi słowami sformułuje prawidłową odpowiedź związaną z ochroną prywatności.

Instrukcja dla mentora

1. Daj drużynie 1 minutę na przeczytanie „Pigułki wiedzy”.
2. Przekaż drużynie „Kartę pracy” i włącz stoper, czas wykonania zadań to 8 minut.
3. Jeśli drużyna nie zna odpowiedzi, NIE podawaj rozwiązania. Zadawaj pytania naprowadzające oraz pytanie finałowe.
4. Po prawidłowym rozwiązaniu wręczasz drużynie fragment „Kodu odporności cyfrowej”.
5. Jeśli drużyna podjęła złą decyzję – zabierz odpowiedni „Żeton decyzji”.

Żetony decyzji: *Hasło / Tożsamość*, które drużyna oddaje, jeśli udzieli złych odpowiedzi.

Fragment hasła „Kodu odporności cyfrowej”, który drużyna otrzymuje po wykonaniu zadania: „świadomie!”

Cel Mentora: Nauka rozpoznawania próby wyłudzenia danych i procedury bezpiecznego reagowania.

Główne zagadnienia: Cyberszustwa, wyłudzenie haseł/danych osobowych, fałszywe SMS-y/linki, zasada ochrony haseł logowania, zgłaszanie na numer 8080.

Pytania naprowadzające

Na telefon przychodzi SMS: „Twój profil w grze zostanie zablokowany za 15 minut! Kliknij link i podaj hasło”. Jakie dwa sygnały ostrzegawcze wskazują, że to pułapka?

Pytania pogłębiające

Dlaczego hasło do konta traktujemy jak klucz do domu i nie podajemy go nawet najlepszemu przyjacielowi w dowód zaufania?

Co robicie w pierwszej kolejności, gdy otrzymacie podejrzaną wiadomość z nieznanym linkiem?

Dlaczego oszuści w takich wiadomościach dają Wam tak mało czasu na reakcję?

Co należy natychmiast zrobić po otrzymaniu podejrzanego SMS’a lub e-maila?

Na jaki bezpłatny numer w Polsce można zgłosić podejrzanego SMS’a?

Oczekiwana odpowiedź: Bezpłatny numer 8080 – CERT Polska.

Pytanie finałowe (klucz zaliczenia stacji i otrzymania fragmentu „Kodu odporności cyfrowej”)

Jak reaguje “cyfrowy detektyw”, gdy ktoś nieznajomy w sieci żąda od niego podania hasła lub kliknięcia w link?



STACJA 6

Zatruty haczyk (phishing)



KLUCZ ODPOWIEDZI DLA MENTORA – OPIEKUNA STACJI

Tematyka: Ochrona przed cyberoszustwami, wyłudzaniem haseł i manipulacją w sieci.

➤ Opis stacji

Jesteś w środku cyfrowego jeziora. Oszuści rzucają w internecie cyfrowe przynęty. Pytanie, czy złapiesz się na zatruty haczyk? Phishing, to próba oszukania kogoś, aby podał swoje dane osobowe (np. hasło, numer telefonu).

Zadanie 1

Na telefon jednego z was przychodzi SMS: *"Twój profil w grze zostanie zablokowany za 15 minut! Kliknij w ten link: www.bezpieczenstwo_danych.pl i podaj swoje hasło, aby tego uniknąć"*. Zwróć uwagę na to, że może to być cyfrowa pułapka. Co robicie?

Klucz odpowiedzi

To typowy phishing połączony z presją czasu. Nie należy klikać w nieznane linki ani podawać haseł. Należy zamknąć wiadomość i zgłosić to osobie dorosłej. Zwróć uwagę na dziwny adres strony www i literówki, presję czasu (15 minut) oraz żądanie podania hasła. Są to trzy wskaźniki cyfrowej pułapki. Możesz zgłosić podejrzany SMS do CERT Polska w NASK na stronie: incydent.cert.pl lub przestać go bezpłatnie na numer 8080 do polskich ekspertów ds. cyberbezpieczeństwa. Ważne jest, aby przekazać całą wiadomość w oryginalnej formie.

Zadanie 2

Połącz hasło z definicją – klucz odpowiedzi

Phishing

- Rodzaj cyberoszustwa, w którym przestępcy podszywają się pod zaufane instytucje (banki, kurierów, urzędy) lub znajomych, aby wyłudzić poufne dane: hasła, loginy, numery kart kredytowych czy PESEL. Używają do tego fałszywych e-maili, SMS-ów lub stron internetowych, często wywołując presję czasu.

Profilowanie

- Proces zbierania i analizowania zachowań użytkowników w celu stworzenia cyfrowego profilu osoby np. podczas rozgrywki w grze (ruchy, czas reakcji, wybory, częstotliwość logowania).

Dark patterns

- Techniki stosowane w projektowaniu interfejsów (np. gier, aplikacji, stron) w celu manipulowania decyzjami użytkownika np. niezamierzonych zakupów, subskrypcji czy udostępnienia danych osobowych.

STACJA 6

Zatruty haczyk (phishing)



PIGUŁKA WIEDZY

Główne zagadnienia

Naucz się chronić swoje hasła logowania oraz rozpoznawać cyfrowe oszustwa wyłudzające dane!

- **Phishing**, to cyfrowe oszustwo, w którym przestępcy rzucają „zanętę” – podszywają się pod banki, kurierów, aplikacje gier lub znajomych, aby wyłudzić Twoje hasła, loginy i numer PESEL.
- **Profilowanie** - proces zbierania i analizowania zachowań użytkowników w celu stworzenia cyfrowego profilu osoby np. podczas rozgrywki w grze (ruchy, czas reakcji, wybory, częstotliwość logowania).
- **Dark patterns tzw. zwodnicze wzorce**
To to podstępne sztuczki i pułapki ukryte w wyglądzie stron internetowych, aplikacji oraz gier. Projektanci tworzą je celowo, aby manipulować decyzjami użytkownika i zmusić go do podjęcia decyzji, której normalnie by nie podjął. Powoduje to nieprzemysłane zakupy, subskrypcje czy udostępnianie danych osobowych.
- **Hasło jest jak klucz do domu**
Twoje hasła do platform z grami, aplikacji gier, e-dziennika i poczty są jak klucze do mieszkania. Muszą być unikalne i tajne. Nie podawaj ich nikomu – nawet najlepszemu przyjacielowi w dowód zaufania.
- **Sztuczka na presję czasu**
Oszuści zawsze łączą phishing z presją czasu (np. SMS: „Twoje konto w grze zostanie zablokowane za 15 minut! Kliknij w link i podaj hasło”). Chodzi o to, abyś zadziałał w emocjach i bez myślenia podał swoje dane!
- **Bezpłatny numer SMS 8080 (CERT Polska)**
Jeśli otrzymasz podejrzanego SMS-a z nieznanym linkiem, zamknij wiadomość i prześlij go bezpłatnie na numer 8080 do polskich ekspertów ds. cyberbezpieczeństwa.



ZŁOTA ZASADA STACJI 6 SUPERMOC DETEKTYWA PRYWATNOŚCI

JEŚLI OTRZYMASZ NIEPOKOJĄCĄ WIADOMOŚĆ Z ŻĄDANIEM PODANIA HASŁA LUB KLIKNIECIA W LINK – NATYCHMIAST ZAMKNIJ OKNO WIADOMOŚCI I POWIADOM DOROSŁEGO, ABY ZGŁOSIĆ PHISHING.

NIE KLIKAJ W „ZATRUTE HACZYKI”!