Fałszywy mejl

Kluczowe pytanie: Nie daj sobie ukraść hasła.

Czas: 20 min.

Materiały: karty pracy: treść mejla i 10 cech fałszywych mejli

Metoda pracy: burza mózgów, dyskusja

Przebieg ćwiczenia:

1.

Rozdaj uczniom karty pracy. Poproś, aby przeczytali mejla, którego mają przed sobą. Powiedz, że jest to autentyczny mejl, być może ktoś z twoich uczniów otrzymał podobną wiadomość.

- Zapytaj, co zrobiliby w tej sytuacji. Zbierz opinie uczniów.
- Zapytaj, czy widzą coś niepokojącego w tym mejlu (błędy ortograficzne, ostrzeżenie itp.)

2.

Po rozmowie na temat treści i formy mejla, rozdaj uczniom karty pracy: **10 cech fałszywych mejli** według serwisu PayPal. Zapytaj czy znajdują odzwierciedlenie tych punktów w mejlu z pierwszego ćwiczenia. Poproś o wskazanie minimum czterech z nich.

Podsumuj ćwiczenie. Zapoznaj uczniów z pojęciem i zjawiskiem **„phishingu”:** to określenie działalności przestępczej polegającej na tworzeniu i wykorzystywaniu fałszywych przesyłek poczty elektronicznej oraz stron internetowych – zaprojektowanych tak, by nie różniły się one od przesyłek i stron dobrze znanych firm, instytucji finansowych czy instytucji publicznych, w celu wyłudzenia haseł użytkowników.

Fałszywy mejl
karta pracy

Do: Marta.rutkowska@o2.pl
Od: no_reply@facebook.com
Odpowiedz do: no_reply@facebook.com

Włamanie na Twoje konto Facebook!

Drogi użytkowniku! Ktoś próbował przejąć Twoje konto w serwisie Facebook! Musisz natychmiast zainteresować się tą sprawą!
Aby temu zapobiec wygenerowaliśmy dla Ciebue nowe hasło. Wyślij nam swoje stare hasło, a następnie udaj się pod Adres: http://facebook.com/marta.r

Aby w pełni w pełni bezpiecznie odzyskać swoje konto
Postępuj zgodnie z instrukcjami zawartymi na stronie.
Z poważaniem Facebook Group.

Rozwiązanie (dla nauczyciela)

Do: Marta.rutkowska@gmail.com
Od: **no_reply@facebook.com fałszywy adres e-mail**
Odpowiedz do: no_reply@facebook.com

Włamanie na Twoje konto Facebook!

Drogi użytkowniku! *Ogólna treść powitania*
Ktoś próbował przejąć Twoje konto w serwisie Facebook! Musisz natychmiast zainteresować się tą sprawą! *ton charakterystyczny dla sprawy niecierpiącej zwłoki*
Aby temu zapobiec wygenerowaliśmy dla **Ciebue** *błędy w pisowni* nowe hasło. Wyślij nam swoje stare hasło, a następnie udaj się pod Adres: **http://facebook.com/marta.r** *fałszywe łącza, serwisy bez zabezpieczeń*

Aby w pełni w pełni bezpiecznie odzyskać swoje konto
Postępuj zgodnie z instrukcjami zawartymi na stronie.
Z poważaniem Facebook Group.

PayPal
10 sposobów na rozpoznawanie fałszywych wiadomości e-mail

1. **Ogólny charakter powitania**. Wiele fałszywych wiadomości e-mail rozpoczyna się ogólnie brzmiącym powitaniem, np.: „Drogi Użytkowniku serwisu PayPal!" Brak Twojego imienia i nazwiska w liście od razu powinien budzić podejrzenia – nie należy wtedy klikać żadnych łączy ani przycisków.
2. **Fałszywy adres nadawcy**. Fałszywa wiadomość zwykle jest opatrzona podrobionym adresem nadawcy w polu „Od". Zawartość tego pola bardzo łatwo jest modyfikować.
3. **Ton charakterystyczny dla spraw niecierpiących zwłoki**. Wiele tego typu wiadomości stara się wywołać fałszywe wrażenie zagrożenia związanego z kontem, któremu zapobiec może tylko natychmiastowa aktualizacja zapisanych na koncie danych. Wiadomość może także sugerować, że na Twoim koncie zarejestrowano nieautoryzowaną transakcję lub że PayPal aktualizuje właśnie dane klientów i potrzebuje jak najszybciej potwierdzić ich prawidłowość.
4. **Fałszywe łącza.** Zanim klikniesz dane łącze, zawsze sprawdzaj, dokąd prowadzi. Umieść nad nim kursor myszy i sprawdź, co wyświetla się na pasku stanu przeglądarki lub programu pocztowego. Łącze, którego opis wprowadza w błąd, może być niebezpieczny. Jego kliknięcie może mieć różne skutki:
   - ➔ Skierowanie do sfałszowanej strony internetowej, której zadaniem jest pobieranie danych osobowych odwiedzającego.
   - ➔ Zainstalowanie oprogramowania szpiegowskiego w systemie użytkownika. Oprogramowanie szpiegowskie to program, który pozwala osobom niepowołanym obserwować poczynania użytkownika i wykradać wpisywane z klawiatury hasła lub numery kart kredytowych.
   - ➔ Spowodować pobranie wirusa, który uszkodzi system.
5. **Wiadomości e-mail wyglądające jak strony internetowe**. Niektóre wiadomości e-mail przybierają formę stron internetowych, które zachęcają do wprowadzenia danych osobowych. Serwis PayPal nigdy nie prosi o podanie tych informacji w wiadomości e-mail.
6. **Zwodnicze adresy URL**. Hasło dostępu do konta PayPal należy wprowadzać wyłącznie na stronach należących do serwisu PayPal
7. **Błędy pisowni i gramatyki**. Fałszywe wiadomości e-mail często zawierają błędy w pisowni, błędy gramatyczne, braki wyrazów lub nieścisłości logiczne. Pomyłki takie pomagają oszustom w obchodzeniu filtrów spamu.
8. **Serwisy bez zabezpieczeń**. Adres każdej strony, na której podajesz swoje dane osobowe, powinien rozpoczynać się od członu „https". Końcówka „s" jest bardzo ważna i świadczy o tym, że działają mechanizmy bezpieczeństwa. Jeśli nie ma członu „https", sesja przeglądarki nie jest zabezpieczona i nie należy wprowadzać żadnych danych.

9. **Pojawiające się okna podręczne**. Wiadomości z serwisu PayPal nigdy nie powodują wyświetlania okien podręcznych, ponieważ okna podręczne nie zapewniają żadnych zabezpieczeń.
10. **Załączniki.** Obok zwodniczych łączy, załączniki są drugą, często spotykaną i niebezpieczną cechą fałszywych wiadomości e-mail. Nigdy nie należy klikać załącznika. Może to spowodować pobranie programu szpiegowskiego lub wirusa. Serwis PayPal nigdy nie wysyła swoim użytkownikom wiadomości e-mail z załącznikami lub aktualizacjami oprogramowania, prosząc o ich instalację na komputerze.

Materiał ze strony: https://www.paypal.com/pl/cgi.-.bin/webscr?cmd=xpt/Help/popup/RecognizeSpoof-outside, dostęp na dzień 18.01.2015