

Arkusz ćwiczeń: Czy to jest bezpieczne?

W poniższym arkuszu znajdują się przykłady e-maili i stron internetowych. Twoim zadaniem jest przeanalizowanie każdego z nich i wskazanie podejrzanych elementów. Pod każdym przykładem znajduje się miejsce na Twoją analizę.

Przykład 1: E-mail od "banku"

Od: support@bank-secure.com

Do: Użytkownik

Temat: Pilne! Zablokowanie konta bankowego

Drogi Kliencie,

Wykryliśmy podejrzaną logowanie do Twojego konta. Aby zapobiec zablokowaniu, prosimy o natychmiastowe zalogowanie się i zweryfikowanie swojej tożsamości, klikając w poniższy link:

 [Kliknij tutaj, aby odblokować konto](#)

Jeśli nie podejmiesz działań w ciągu 24 godzin, Twoje konto zostanie zamrożone.

Dziękujemy,

Zespół Bezpieczeństwa Banku

 Twoja analiza (wypisz podejrzane elementy):

1.

2.


3.

Przykład 2: Fałszywa strona logowania

Adres URL: <http://www.paypall-security.com/login>

Strona wygląda jak oryginalna strona PayPal, ale ma kilka podejrzanych elementów:

- Prosi o podanie pełnych danych karty kredytowej.
- Nie ma certyfikatu SSL (brak 'https' w adresie).
- Używa adresu podobnego do prawdziwego, ale nie jest to oficjalny PayPal.

 Twoja analiza (wypisz podejrzane elementy):

1.

2.

3.


Przykład 3: Fałszywy SMS o paczce

Treść SMS:

Twoja paczka nr 123456789 nie mogła zostać dostarczona z powodu braku opłaty 3,50 PLN. Aby ją odebrać, dokonaj płatności tutaj:

 <http://dhl-paczka-secure.com>

Jeśli nie opłacisz przesyłki w ciągu 12 godzin, zostanie ona zwrócona do nadawcy.

 Twoja analiza (wypisz podejrzanе elementy):

1.

2.

3.

Podsumowanie

Wskazówki do analizy:

- Sprawdzaj adresy e-mail i domeny stron.
- Nie klikaj podejrzanych linków.
- Fałszywe wiadomości często stosują presję czasu.
- Zawsze loguj się do serwisów poprzez oficjalne strony, a nie linki z wiadomości.