Jak rozpoznać Phishing?

Opracowanie: Danuta Bartnik, Anna Grzesiakowska

Jednym z najczęstszych zagrożeń, z jakim spotykamy się w Internecie jest Phishing i różne odmiany ataków socjotechnicznych. **Jak rozpoznać, że jestem celem ataku?**

Atak Phishing przyjmuje zwykle formę wiadomości wysyłanych w imieniu zaufanej osoby lub instytucji, które zachęcają do wykonania określonych czynności, np. uruchomienia załącznika, wejścia na wskazaną stronę Web, przekazania danych, itp.

Fałszywe wiadomości wysłane są na wiele sposobów, m.in.:

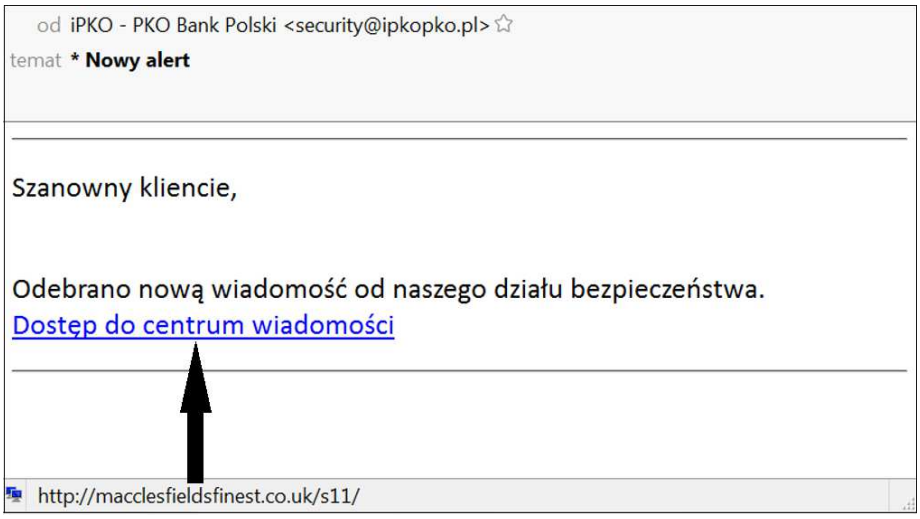
- email,
- SMS,
- portale społecznościowe,
- grupy dyskusyjne i fora internetowe,
- Youtube, Skype, itd.

Szczególnie w poczcie elektronicznej otrzymujemy ogromną liczbę wiadomości wysyłanych przez przestępców, którzy starają się przekonać nas do jakiegoś działania, które przyniesie im korzyści, np. aktywować konto na fałszywym serwerze banku, przez które przestępcy uzyskają nasze poufne dane.

Pierwszy krok

Pierwsza czynność jaką należy zrobić to zastanowić się czy takiej wiadomości się spodziewaliśmy. Następnie gdy w wiadomości jest zawarty link (adres URL) to zaznaczamy go myszką (**bez klikania!**) i odczytujemy gdzie prowadzi. Jeżeli link prowadzi do domeny innej niż nadawca email to wiadomość prawdopodobnie jest fałszywa.

Przykład ataku Phishing



Pamiętajmy, że tylko w niektórych przypadkach Phishing można wykryć analizując zawarte w treści adresy. Większość wiadomości Phishing jest tak profesjonalnie przygotowana, że użytkownik nie potrafi odróżnić ich od prawdziwych wiadomości. Wiadomości mogą być przygotowane zgodnie z szablonem danej instytucji. Mogą zawierać poprawne logo instytucji. W polu "Nadawca" e-mail może znaleźć się prawdziwy adres e-mail danej instytucji, itd.

Drugi krok

Często jedynym sygnałem rozpoznawczym ataku Phishing jest prośba o wykonanie jakiejś niebezpiecznej czynności jak udostępnienie poufnych danych, wejście na wskazaną stronę WWW, otwarcie jakiegoś pliku lub zainstalowanie aplikacji. Należy wtedy kierować się zdrowym rozsądkiem i ostrożnością.

Oszuści wykorzystują różne sposoby manipulacji:

- Prośba o przekazywanie danych jako odpowiedź na atrakcyjną ofertę pracy.
- Groźba zablokowania dostępu do aplikacji (np. konta e-banking).
- Informacje o wygranej lub innych nagrodach.
- Informacje związane ze śmiercią znanych osób lub katastrofą (np. katastrofą smoleńską).
- Informacje o promocjach filmów (np. Piraci z Karaibów) lub gier (np. World of Warcraft).
- Kartki świąteczne, imieninowe, itp.
- Prywatne zdjęcia znanych ludzi.
- Panika wokół świńskiej grypy, AIDS lub innego zagrożenia.
- Zemsta na dziewczynie za zdradę (zdjęcia nagiej dziewczyny).
- I wiele, wiele innych pomysłów!

Nie dajmy się temu zwieść!

Tematyce ochrony przed atakami Phishing i innym zagrożeniom z Internetu poświęcone są szkolenia Security Awareness. Dostępne w portalu edukacyjnym BezpiecznyPracownik.PL szkolenia oferowane są w interaktywnej formie e–learningowej i dzięki temu organizacje, mogą efektywnie kosztowo kształcić wszystkich swoich pracowników oraz rozwijać kulturę bezpieczeństwa informacji w skali całej organizacji.