Phishing – co to jest?

To metoda oszustwa, która polega na **wysyłaniu e-maili lub SMS-ów z załącznikami czy linkami do fałszywych stron internetowych**. Wiadomości mają nakłonić Cię do kliknięcia w link albo otwarcia załącznika. Następnie masz przekazać swoje poufne dane, np. numer PESEL, numer dowodu, adres, identyfikator i hasło do bankowości internetowej czy numer karty płatniczej.

Co ważne, oszuści mogą podszywać się pod pewne osoby lub firmy. Chcą uśpić Twoją czujność, więc dbają o to, aby skala podobieństwa była jak największa. Fałszywe strony wyglądają łudząco podobnie do stron firm, które znasz.

Czego najczęściej dotyczą fałszywe wiadomości?

- niewielkiej kwoty, którą masz dopłacić do przesyłki
- bonów, kuponów oraz innych darmowych „nagród", które możesz zdobyć
- podejrzanych logowań na Twoim koncie
- problemów z Twoim kontem lub płatnością
- niekompletnych danych, które musisz potwierdzić
- niezapłaconej faktury, którą masz opłacić.

Jak przebiega takie oszustwo?

- Dostajesz e-maila lub SMS-a. Wiadomość wygląda jak z firmy, którą dobrze znasz.
- Masz pilnie zalogować się na stronę banku przez link z wiadomości. Najczęściej po to, aby odebrać rzekome pieniądze.
- Link przekierowuje Cię na fałszywą stronę, która przypomina stronę Twojego banku.
- Logujesz się – podajesz swoje dane oraz kod z SMS-a.
- Masz wpisać kolejne kody SMS, aby zaktualizować swoje dane.
- Widzisz komunikat o błędzie, więc wpisujesz je kilka razy.

Pamiętaj: zawsze dokładnie czytaj kody SMS – czy treść powiadomienia z kodem odpowiada temu co akurat chcesz zrobić na stronie? Zwracaj też uwagę na to, które urządzenia dodajesz do zaufanych.

- Oszust dostał dostęp do Twojego konta. Od teraz może się na nie logować i z niego korzystać, np. zlecać przelewy czy wypłacać pieniądze z bankomatu za pomocą BLIKA.

Jak się chronić?

- Pamiętaj o **zasadzie ograniczonego zaufania**. Zanim klikniesz w link lub pobierzesz jakiś plik, upewnij się, że pochodzą one z zaufanych źródeł.
- Filtruj spam i zainwestuj w oprogramowanie antywirusowe, najlepiej z modułem antyphishingowym. Taki moduł analizuje odwiedzane przez Ciebie witryny i sprawdza czy nie są to fałszywe strony.
- Czytaj powiadomienia push z aplikacji bankowych i na bieżąco kontroluj przelewy na swoim koncie.

Jeśli dojdzie do oszustwa…

Nie czekaj, reaguj! Jak najszybciej zablokuj dostęp do bankowości elektronicznej oraz skontaktuj się z Bankiem!