Phishing

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 klienta do kliknięcia w link albo otwarcia załącznika. Następnie klient ma przekazać swoje poufne dane, np. numer PESEL, numer dowodu, adres, login i hasło do bankowości internetowej czy numer karty płatniczej.

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

#DbajOBezpieczeństwo

Dbaj o bezpieczeństwo i nie daj się oszustom! Uważaj na phishing. To jedna z metod, z której najczęściej korzystają przestępcy. 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.

Zachowaj ostrożność i dowiedz się więcej o phishingu => www.sgb.pl/phishing

Pamiętaj! Jeśli coś budzi Twoją wątpliwość lub nie działa jak powinno, jak najszybciej skontaktuj się z naszym bankiem lub zadzwoń na Infolinię SGB, czynną 24/7:

- 800 888 888 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).

#DbajOBezpieczeństwo #Bezpieczeństwo #BankiSpółdzielczeSGB #SGB

Czego najczęściej dotyczą fałszywe wiadomości?

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

Jak przebiega takie oszustwo?

- Klient dostaje e-maila lub SMS-a. Wiadomość wygląda jak ze znanej mu firmy.
- Klient ma pilnie zalogować się na stronę banku przez link z wiadomości. Najczęściej po to, aby odebrać rzekome pieniądze.
- Link przekierowuje go na fałszywą stronę, która przypomina stronę jego banku.
- Klient loguje się – podaje swoje dane oraz kod z SMS-a.
- Potem ma wpisać kolejne kody SMS, aby zaktualizować swoje dane.
- Widzi komunikat o błędzie, więc wpisuje je kilka razy.
  Warto pamiętać: zawsze trzeba dokładnie czytać kody SMS – czy treść

powiadomienia z kodem odpowiada temu co klient akurat chce zrobić na stronie?

- Oszust dostał dostęp do konta klienta. 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?

- Warto pamiętać o **zasadzie ograniczonego zaufania**. Zanim klient kliknie w link lub pobierze jakiś plik, powinien się upewnić się, że pochodzą one z zaufanych źródeł.
- Powinno się filtrować spam i zainwestować w oprogramowanie antywirusowe, najlepiej z modułem antyphishingowym. Taki moduł analizuje odwiedzane witryny i sprawdza czy nie są to fałszywe strony.
- Należy czytać powiadomienia push z aplikacji bankowych i na bieżąco kontrolować przelewy na koncie.