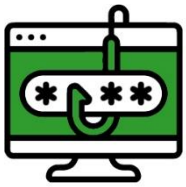
Phishing



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.

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.

Vishing i spoofing

Vishing i spoofing - czym są?

Vishing to metoda oszustwa, która polega na **podszywaniu się pod pracowników banków i innych zaufanych instytucji**, np. policjantów. Oszuści chcą w ten sposób zdobyć poufne dane klienta (np. login i hasło do bankowości internetowej) lub nakłonić o do określonych czynności (np. zainstalowania aplikacji do zdalnej obsługi urządzenia).

Spoofing to metoda oszustwa, która polega na **podszywaniu się pod inne urządzenia lub innego użytkownika**. Oszuści zmieniają numer telefonu, adres e-mail czy adres IP, z których się kontaktują. Co więcej, mogą też wybrać i zmienić płeć osoby dzwoniącej, jej kraj pochodzenia, a nawet akcent. Zawsze dobrze przygotowują się do rozmowy, aby była ona wiarygodna i uśpiła czujność klienta.

Jak przebiega takie oszustwo?

Oszuści stosują wyćwiczone techniki manipulacji. **Podszywają się pod prawdziwe numery telefonów!** Kiedy dzwonią, na telefonie klienta może wyświetlić się inny, znany numer lub nazwa banku.

Choć nie ma jednego schematu działania, przykładowa rozmowa może przebiegać tak:

- Klient odbiera telefon od oszusta.
- Oszust przekazuje klientowi informację o rzekomej płatności na jego koncie i prosi o potwierdzenie jej wykonania. Często oszuści przekazują też informację o logowaniu spoza granic Polski.
- Klient odpowiada na wszystkie pytania, których oficjalnym celem jest jego weryfikacja.
- Oszust informuje klienta, że musi zablokować rzekomą fałszywą transakcję lub przeprowadzić „zdalne skanowanie antywirusowe”. W tym celu klient ma zainstalować specjalną aplikację, np. AnyDesk lub TeamViewer.
- Klient instaluje aplikację, a jego dane trafią do oszusta – ma dostęp do konta klienta i pieniędzy na nim.

Jak się chronić?

- Nigdy nie wolno podawać loginu i hasła do bankowości internetowej, danych karty płatniczej (numer karty, CVV, data ważności). To informacje poufne, powinny być znane tylko klientowi.
- Zawsze warto czytać treść SMS-ów i komunikatów z aplikacji mobilnej. Należy zwrócić na nie szczególną uwagę podczas połączenia z rzekomym przedstawicielem banku lub innej instytucji. Z ich treści może wynikać, że akceptuje się transakcję, którą przygotowali przestępcy.
- Jeżeli jakakolwiek rozmowa wzbudza wątpliwości lub niepokój klienta, niech się rozłączy. Warto odczekać minimum 30 sekund, a następnie samodzielnie połączyć się z instytucją, z której dzwonił rzekomy przedstawiciel. Koniecznie należy wpisać numer samodzielnie – **nie oddzwaniać na wcześniejsze połączenie**.
- Nie powinno się instalować dodatkowego oprogramowania na urządzeniach, za pomocą których klient loguje się do aplikacji bankowej.
- Nie wolno zgadzać się na alternatywny kontakt mailowy czy SMSowy. Oszust może chcieć wysłać link lub załącznik, który może zainfekować urządzenie klienta.

Fałszywe inwestycje

Fałszywe inwestycje - czym są?

To metoda oszustwa, która polega na **podszywaniu się pod maklerów i brokerów giełdowych**. Proponują nowe możliwości zainwestowania środków klienta, które np. wcześniej nie były dostępne na rynku dla każdego. Doskonale przedstawiona oferta staje się przekonująca, przez co ciężko rozpoznać kłamstwo. Co więcej, oszuści bardzo często wykorzystują wizerunki znanych osób czy firm. Dzięki temu oferta i możliwość szybkiego oraz wysokiego zarobku wydają się jeszcze bardziej wiarygodne.

Jak przebiega takie oszustwo?

Jak się chronić?

- Nigdy nie podawać loginu i hasła do bankowości internetowej czy danych karty płatniczej (numer karty, CVV, data ważności) – te informacje są poufne, powinny być znane tylko klientowi.
- Nie instalować dodatkowego oprogramowania (np. Any Desk) na urządzeniach, z których klient loguje się do aplikacji bankowej.
- Jeśli klient otrzyma przelew z obcego rachunku, który wygląda jak „zwykły” od innej osoby, nie może przekazywać go dalej. Jeśli to zrobi, weźmie udział w przestępstwie.
- Jeśli klient podejrzewa, że to oszustwo, powinien zadzwonić na policję.