

Co to jest phishing?

To oszustwo internetowe, w którym osoba trzecia podszywa się pod inny podmiot w celu wyłudzenia informacji, które umożliwią zalogowanie się do bankowości elektronicznej i zlecenie oraz autoryzowanie transakcji płatniczej.

ATAK PHISHINGOWY

111001
00101010010
11011010101101
1011 **HACKED** 1111
01010010000101
101010101010
11110

Jak wyłudzane są informacje?

- osoby podające się za pracowników banku - powołując się na potrzebę zwiększenia bezpieczeństwa – proszą o podanie poufnych informacji;
- przy pomocy złośliwego oprogramowania, które instaluje się po otwarciu załączników do fałszywych e-maili/smsów albo w związku z pobraniem aplikacji mobilnej;
- przez podmianę prawdziwego numeru rachunku bankowego na fałszywy;
- przez podszywanie się pod znajomego na FB i prośbę o wspomoczenie przez np. dot-pay.

Jak chronić swoje internetowe transakcje?

- Zawsze korzystaj z legalnego oprogramowania i regularnie go aktualizuj.
- Stosuj programy antywirusowe oraz firewall.
- Nie wyszukuj stron internetowych banku przez przeglądarki.
- Nie otwieraj e-maili nieznanego pochodzenia, nie odpowiadaj na nie i nie otwieraj załączników lub linków w nich wskazanych.
- Zmieniaj regularnie hasło do konta bankowego.
- Nie kopiuj numerów rachunków ze „schowka”.
- Weryfikuj dane zawarte w SMS-ach autoryzacyjnych: rodzaj dyspozycji i dane transakcji w SMS-ie powinny się zgadzać się z tymi, które wyświetlają się na ekranie.
- Nie loguj się do banku z otwartych sieci WiFi.