ATAK PHISHINGOWY

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.

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 wspomożenie przez np. dot-pay.

Jak chronić swoje internetowe transakcje?

1. Zawsze korzystaj z legalnego oprogramowania i regularnie go aktualizuj.

2. Stosuj programy antywirusowe oraz firewall.

3. Nie wyszukuj stron internetowych banku przez przeglądarki.

4. Nie otwieraj e-maili nieznanego pochodzenia, nie odpowiadaj na nie i nie otwieraj załączników lub linków w nich wskazanych.

5. Zmieniaj regularnie hasło do konta bankowego.

6. Nie kopiuj numerów rachunków ze „schowka”.

7. 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.

8. Nie loguj się do banku z otwartych sieci WiFi.

Rzecznik Finansowy
www.rf.gov.pl

CEO
CENTRUM EDUKACJI OBYWATELSKIEJ