FIŠING

Tip prevare

Imitiranjem entiteta od poverenja (banke, trgovca, državne institucije i sl.) preko kanala elektronske komunikacije navode žrtvu da otkrije lične podatke.

Način rada

- Prevarant šalje e-mail poruku lažno se predstavljajući kao banka u smislu da e-mail adresa pošiljaoca liči ili je ista kao adresa banke, zahtevajući od klijenta da ažurira podatke npr. nalog za elektronsko bankarstvo,
- Klijent odlazi na link "banke" dostavljen u poruci,
- Link usmerava klijenta na **lažni** veb sajt banke koji izuzetno **liči** na oficijelni,
- Klijent unosi korisničko ime i lozinku,
- Prevarant dolazi do podataka o nalogu za elektronsko bankarstvo preko lažnog veb sajta,
- Podatke o nalogu za elektronsko bankarstvo prevarant koristi za pristup računima žrtve, odnosno za prenos sredstava sa računa žrtve na račun trećeg lica,
- Prevarant zatim podiže sredstva sa računa trećeg lica kojem inače ima pristup.

Ova prevara nije ograničena samo na podatke o nalogu za elektronsko bankarstvo ili na imitiranje banke, na sličan način prevaranti vas mogu navesti da unesete i podatke o platnoj kartici i njenom PIN-u, ili podatke o ličnoj karti i pasošu itd. imitiranjem neke druge institucije od poverenja.

Preventivne mere

- Nikada ne otvarajte linkove iz e-mail poruka. Umesto toga pristupajte veb sajtu banke (ili neke druge institucije) na način da direktno ukucavate veb adresu u vaš internet pretraživač.
- Koristite uobičajene procedure za ažuriranje vaših podataka. Banka nikada neće zahtevati detalje o vašim ličnim/poverljivim podacima putem elektronske pošte.
- Uporedite veb adresu iz primljene e-mail poruke sa realnom internet adresom banke (ili neke druge institucije).
- Ukoliko posumnjate u legitimnost e-mail poruke, pozovite vašu banku .
- Nikada nemojte odati vašu lozinku nikome.
- Izbegavajte izvršenje transakcija preko javnih WiFi mreža.