ckbbanka
otp group

Phishing

Tip prevare i način rada

Phishing je vrsta internet prevare, podvrsta socijalnog inženjeringa, koja za cilj ima prikupljanje osjetljivih korisničkih podataka imitiranjem entiteta od povjerenja (banke, državne institucije i sl.). Ova prevara se najčešće sprovodi preko lažnih internet stranica, mejlova ili SMS poruka preko kojih se traži navođenje ličnih podataka.

- Tipičan napad počinje porukom koja izgleda kao da dolazi iz banke, a u njoj se od klijenta zahtijeva da ažurira određene podatke npr. nalog za elektronsko bankarstvo
- Klijent odlazi na link "banke" dostavljen u poruci
- Link usmjerava klijenta na lažni veb-sajt banke koji veoma podsjeća na zvanični veb-sajt
- Klijent unosi korisničko ime i lozinku
- Prevarant dolazi do podataka o nalogu za elektronsko bankarstvo preko lažnog sajta
- Podaci o nalogu za elektronsko bankarstvo koriste se za pristup računima, odnosno za prenos sredstava sa računa vlasnika na račun trećeg lica
- Sredstva se zatim podižu sa računa trećeg lica

Pažnja!

Ova prevara nije ograničena samo na podatke o nalogu za elektronsko bankarstvo. Na jako sličan način možete biti navedeni da unesete i podatke o platnoj kartici, datumu isteka ili podatke o ličnoj karti i pasošu s ciljem dobijanja povjerljivih i osjetljivih podatka kako bi se izvršile lažne finansijske transakcije i prevare.

Nijesu samo banke meta ove vrste prevare, već su veoma česti napadi na korisnike elektronske pošte, društvenih mreža i drugih popularnih onlajn usluga. Neki napadi su takođe usmjereni na širenje virusa, "trojanaca" i drugih prijetnji koje se mogu automatski instalirati klikom na zlonamjerni link.

Mjere predostrožnosti

- Nikada ne otvarajte linkove ili priloge iz mejl poruka, kako biste pristupili bančinoj aplikaciji ili veb-sajtu. Nikada ne unosite kartične podatke ili podatke o nalogu za elektronsko bankarstvo putem linkova dobijenih u mejlu, SMS-u ili na neki sličan način
- Provjerite da li poruka stvarno stiže sa adrese koja je navedena u polju „FROM". Mejl adresa pošiljaoca mora odgovarati domenu banke, odnosno poslije indeksa "@" treba da stoji ckb.me, a prije indeksa "@" jasno razumljiv naziv
- Obratite pažnju na tekst iz mejla. Fišing prevare se često mogu prepoznati po nelogičnim tekstovima ili pravopisnim greškama koje su rezultat grubog prevoda sa nekog stranog jezika
- U ovim porukama uvijek se naziru elementi hitnosti i uslovljavanja koja nijesu karakteristična za obraćanje banke
- Ukoliko posumnjate u tačnost mejla ili SMS poruke odmah pozovite banku
- Sama činjenica da neko od Vas samoinicijativno traži da unesete lične podatke u skladu sa uputstvima iz mejla je sumnjiva

---

NAPOMENA

Banka preduzima sve aktivnosti u cilju sprečavanja phishing napada i ugrožavanja bezbjednog poslovanja svojih klijenata.

Predstavnici Banke, nikada neće zahtijevati od vas preko SMS-a, mejla, društvenih mreža ili drugih vidova komunikacije, da unesete ili saopštite sigurnosne kredencijale (lozinke i PIN-ove za internet/mobilno bankarstvo ili platne kartice). Korisnike koji su dobili ovakve ili slične poruke pozivamo da ne odaju ovu vrstu podataka.

Internet prevare postaju sve sofisticiranije i traže od Vas da uvijek budete na oprezu kako svoje lične podatke i/ili novac ne biste doveli u opasnost. Pokušaji phishing prevara putem mejla, SMS-a, aplikacija i društvenih mreza sve su češći. U slučaju sumnje na vjerodostojnost bilo koje poruke, mejla ili poziva, odmah se obratite banci na broj telefona 19900 ili e-mail porukom na info@ckb.me.