POŠTOVANI KLIJENTI,

Hipotekarna banka primjenjuje visoke standarde u zaštiti IT sistema i iste stalno unapređuje saglasno razvoju softvera i prakse za informatičku bezbjednost. Kako se povremeno na različitim tržištima, pa i crnogorskom, javljaju sajber (eng. cyber) napadi preko korisnika bankarskih usluga, niže možete naći više informacija o ovoj vrsti kriminala.

Želimo da istaknemo uobičajeni cyber napad kojeg bi svi trebali biti svjesni –"pecanje" (eng. phishing).

"Phishing" je najčešća vrsta cyber napada koja kao metu ima organizacije poput naše. Napadi krađe identiteta mogu biti u mnogim oblicima, ali svi imaju zajednički cilj – da vas natjeraju da dijelite osjetljive informacije poput povjerljivih podataka za prijavu, podataka o kreditnoj kartici ili podataka o bankovnom računu.

Iako imamo sigurnosne sisteme i kontrole kojima štitimo naše mreže i računare od cyber prijetnji, oslanjamo se na vas kao našu prvu liniju odbrane.

Izdvojili smo nekoliko različitih vrsta phishing napada na koje morate paziti:

Phishing:	U ovoj vrsti napada, hakeri se lažno predstavljaju u pravom preduzeću da bi došli do vaših podataka za prijavu. Možete primiti e-mail sa zahtjevom da **potvrdite detalje svog računa** pomoću linka koji vas vodi do forme za prijavu koja vaše podatke dostavlja direktno napadačima.
Spear phishing:	Spear phishing predstavlja sofisticiraniji phishing napad koji uključuje prilagođene informacije zbog kojih napadač izgleda kao legitimni izvor. Oni mogu koristiti vaše ime i telefonski broj i u e-mailu će se pozivati na Banku kako bi vas **naveli da imaju vezu s vama**, čineći vjerovatnijim da kliknete na vezu ili prilog koji vam daju.
Whaling:	Popularna zavjera koja ima za cilj da e-mail napadom prebaci novac ili pošalje osjetljive informacije napadaču **lažnim predstavljanjem** pravog izvršnog direktora kompanije. Koristeći lažni domen koji izgleda slično našem, oni izgledaju kao uobičajena e-pošta od visokog zvaničnika kompanije, obično generalnog ili izvršnog direktora i traže od vas osetljive informacije (uključujući korisnička imena i lozinke).
Dijeljenje zajedničkih dokumenata:	Možda ćete primiti e-poštu koja **izgleda** kao da dolazi sa web lokacija za dijeljenje fajlova kao što su Dropbox ili Google Drive koji vas obavještavaju da je dokument podijeljen sa vama. Link naveden u tim e-mailovima odvešće vas na lažnu stranicu za prijavu koja oponaša stvarnu stranicu za prijavu i ukrašće akreditive vašeg računa.

HIPOTEKARNA BANKA
Vama posvećena

ŠTA MOŽETE DA URADITE:

Da biste izbjegli ove krađe identiteta, pridržavajte se najboljih praksi e-pošte:

- ✓ Ne klikajte na veze ili priloge pošiljalaca koje ne prepoznajete. Budite posebno oprezni sa .zip ili drugim komprimovanim ili izvršnim tipovima datoteka (npr .exe).
- ✓ Ne šaljite osjetljive lične podatke (poput korisničkih imena i lozinki) putem e-pošte.
- ✓ Pazite na pošiljaoce e-pošte koji koriste sumnjiva ili pogrešna imena domena.
- ✓ Pažljivo pregledajte URL adrese da biste se uvjerili da su legitimne i ne namještaju web lokacije.
- ✓ Ne pokušavajte da otvorite zajednički dokument koji ne očekujete da će vam biti poslat.
- ✓ Budite posebno oprezni prilikom otvaranja priloga ili klika na linkove ako primite e-poštu koja sadrži upozorenje koje obavještava da potiče iz spoljašnjeg izvora.
- ✓ Budite posebno oprezni kod promjena standardnih ino instrukcija dobavljača.
- ✓ Budite svjesni da Hipotekarna banka nikada ne traži od vas lične podatke putem e-pošte: podatke o kartici, CVV, PIN, korisničko ime i šifra za elektronsko bankarstvo.

Hvala vam još jednom što pomažete u očuvanju mreže i činite našu saradnju bezbjednom od ovih cyber prijetnji.

Budite slobodni da, ukoliko imate i najmanju nedoumicu ili sumnju, kontaktirate vašeg ličnog bankara ili naš kontakt centar.

19905
www.hb.co.me

HIPOTEKARNA BANKA
Vama posvećena