INFORMACION
I RËNDËSISHËM

Mashtruesit mund të përdorin emra të besueshëm institucionesh si banka, institucione publike, operatorë telekomunikacioni, kompani softuerësh të përdorur gjerësisht si Apple, Microsoft etj.

Ata mund të dërgojnë SMS ose e-mail në emër të kompanive/institucioneve të tilla në lidhje me përditësimin e të dhënave të klientëve si numrat e kartave, data e skadencës së kartës, kodi i sigurisë së kartës, pini i kartës, numri i sigurimeve shoqërore, fjalëkalimi i e-banking/mobile banking, e-mail, fjalëkalimet e Windows, mbiemri i vajzërisë etj.

Institucione të tilla nuk kërkojnë kurrë një informacion kaq të rëndësishëm me e-mail, SMS ose çdo kanal tjetër komunikimi. Mos ndani informacionin tuaj personal me askënd!

BKT
BANKA KOMBETARE TREGTARE

E-MAIL PHISHING NGA BANKA

Phishing i referohet e-mail-eve mashtruese të cilat mashtrojnë marrësin për të ndarë informacione personale, financiare apo sigurie.

SI FUNKSIONON?

Këto e-mail-e:

mund të duken identike me korrespondencën aktuale që dërgon banka.

kopjojnë logot, formatin dhe pamjen e e-mail-it të vërtetë.

përdorin gjuhë që nënkuptojnë urgjencë.

ju kërkon të shkarkoni një dokument bashkëngjitur ose të klikoni në një link.

Kriminelët kibernetikë përfitojnë nga fakti që njerëzit janë të zënë; në pamje të parë këto e-mail-e duken legjitime.

Kujdes kur përdorni aparatin celular. Mund të jetë e vështirë të dalloni një e-mail mashtrues nga celulari apo tableti.

ÇFARË MUND TË BËNI?

- **Mbani programet të përditësuara, duke** përfshirë shfletues-it, antivirusin dhe **sistemin operativ.**
- Jini veçanërisht vigjilent nëse një e-mail "banke" ju kërkon informacion sensitiv (p.sh. fjalëkalimin e llogarisë suaj në Internet Banking).
- **Shikoni me kujdes adresën e e-mail: krahasoni adresën dërguese me atë të korrespondecave të mëparshme me bankën. Shikoni për gabime gramatikore** dhe ortografike.
- **Mos iu përgjigjni një e-mail të dyshimtë, por dërgojeni atë në bankë duke e shkruar vetë adresën.**
- **Mos klikoni mbi link dhe mos shkarkoni dokumentet bashkangjitur, por shkruani** vetë adresën në shfletues.
- Nëse keni dyshime referojuni faqes zyrtare të Bankës ose telefononi bankën.

#CyberScams

BKT
BANKA KOMBETARE TREGTARE

SMS SMISHING NGA BANKA

Smishing (një kombinim i fjalëve SMS dhe Phishing) i referohet mesazheve mashtruese të cilat mashtrojnë marrësin për të ndarë informacionë personale, financiare apo sigurie nëpërmjet mesazheve.

SI FUNKSIONON?

Mesazhi, i cili në dukje duket legjitim do t'ju kërkojë të klikoni një link ose të telefononi një numër telefoni sepse:

- Keni fituar një dhuratë
- Duhet të "verifikoni", "rifreskoni" ose "riaktivizoni" llogarinë tuaj
- Duhet"të rifreskoni" numrin tuaj të telefonit
- Duhet "të mësoni më shumë" rreth një çështjeje që ju përket

Linku në të vërtetë ju drejton në një website dhe numër telefoni të mashtruesit që pretendon të jetë banka ose një institucion shtetëror.

ÇFARË MUND TË BËNI?

- **Mos klikoni në linqe, dokumenta apo foto të bashkangjitura** që ju merrni nëpërmjet mesazheve të pakërkuara nga ju, pa verifikuar dërguesin.
- **Mos nxitoni.** Merrni kohën tuaj për të bërë verifikimet e duhura para se të përgjigjeni.
- **Asnjëherë mos iu përgjigjni** një mesazhi që kërkon kodin tuaj PIN ose fjalëkalimin e online banking tuaj ose kredenciale tjetër sigurie.
- Nëse mendoni që i jeni përgjigjur një mesazhi smishing duke dhënë të dhënat tuaja, **telefononi menjëherë bankën tuaj**.

Shënim: Pronësia dhe përgjegjësia e kredencialeve si dhe ndarja e kredencialeve me palë të treta të pakonfirmuara i përket klientit.

BKT
BANKA KOMBETARE TREGTARE

#CyberScams