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.

ÇFARE MUND TE BENI?

- 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 tuaj 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 u përgjigjni në 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 bëjini një telefonatë.

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

#CyberScams

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

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | INTESA SANPAOLO BANK Albania

BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

HOW DOES IT WORK?

These emails:

may look identical to the types of correspondence that actual banks send.

replicate the logos, layout and tone of real emails.

ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.

WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Be especially vigilant if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- Look at the email closely compare the address with previous real messages from your bank. Check for bad spelling and grammar.
- Don't reply to a suspicious email, instead forward it to your bank by typing in the address yourself.
- Don't click on the link or download the attachment, instead type the address in your browser.
- When in doubt, double check on your bank's website or give the bank a call.

Cybercriminals rely on the fact that people are busy; at a glance, these spoof emails appear to be legitimate.

#CyberScams

Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

INTESA SANPAOLO BANK Albania