MASHTRIMET BANKARE ME SMISHING SMSs

Smishing (një kombinim i fjalëve SMS dhe Phishing) është tentativa e një mashtruesi të përfitojë informacione personale, financiare ose sigurie nga mesazhet tekst.

SI PUNON?

Mesazhi zakonisht do t'ju kërkojë të klikoni mbi një link ose të telefononi një numër telefoni në mënyrë që të 'verifikoni', 'përditësoni'ose 'riaktivizoni' llogarinë tuaj. Por... linku të dërgon në një faqe false dhe numri i telefonit të dërgon drejt një mashtruesi duke pretenduar të jetë kompania legjitime.

ÇFARË MUND TE BËNI?

- Mos klikoni mbi linke, file-t bashkëngjitur apo mbi imazhet **që merrni në tekstin e mesazhit pa verifikuar fillimisht dërguesin.**
- **Mos u nxitoni.** Merrni kohën e nevojshme dhe bëni kontrollet e duhura përpara se të përgjigjeni.
- **Kurrë mos iu përgjigjni një mesazhi** që kërkon PIN-in tuaj apo fjalëkalimin e Internet Banking ose çfarëdo kredenciali tjetër sigurie.
- Nëse mendoni se mund t'i jeni përgjigjur një mesazhi mashtrimi dhe keni dhënë të dhënat bankare, **kontaktoni menjëherë bankën tuaj.**

BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.

HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- **Don't click on links, attachments or images** that you receive in unsolicited text messages without first verifying the sender.
- **Don't be rushed.** Take your time and make the appropriate checks before responding.
- **Never respond to a text message** that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, **contact your bank immediately**.