

ÇFARË JANË SULMET SMISHING DHE VISHING DHE SI TË MBROHEMI



Smishing dhe vishing janë lloje të sulmeve phishing që përpiqen të manipulojnë viktimat përmes mesazheve SMS dhe mesazheve zanore. Kërcënuesit kibernetik i përdorin këto lloje sulmesh për të fituar akses në informacionin tuaj personal.



Sulmet Smishing dhe Vishing

1. Verifikoni se kush po ju dërgon mesazhe

Nëse merrni një mesazh të dyshimtë që pretendon se është nga banka juaj, duhet të telefononi bankën nga një numër telefoni që ju i besoni.



2. Jini të kujdesshëm ndaj mesazheve që përcjellin një ndjenjë urgjence

Nëse merrni një mesazh me tekst ose një telefonatë që nuk jep shumë informacion dhe ju informon se ekziston një kërcënim urgjent që duhet adresuar shpejt, ky mesazh mund të jetë i rremë.



3. Kërkesa të papritura për informacion personal

Në shumicën e rasteve, një kërkesë legjitime nga një organizatë me reputacion nuk do t'ju kërkojë të jepni informacione konfidenciale me tekst ose nga një numër jozyrtar.



4. Shmangni klikimin e linqeve brenda një mesazhi

Mashtroesit jo gjithmonë kanë nevojë që ju të zbuloni informacionin tuaj të ndjeshëm për të fituar akses në llogaritë tuaja. Ndonjëherë qëllimi i tyre kryesor është t'ju mashτροjnë që të klikoni në një link dhe të shkarkoni malware ose spyware në pajisjen tuaj.



5. Tregoni kujdes ndaj mesazheve me gabime drejtshkrimore dhe gramatikore

Nëse merrni një mesazh me shumë gabime ose mesazhi nuk ka kuptim, kjo mund të jetë një shenjë e një mashtrimi.



6. Mos ndani informacione personale në mediat sociale

Duhet të jini të kujdesshëm në lidhje me informacionin që ndani në internet. Para se të postoni, mendoni se çfarë po postoni dhe kush ka akses në të.

