Si të shmangim kërcënimet e inxhinierisë sociale.

KËSHILLA TË PËRGJITHSHME

Siguroni pajisjet tuaja kompjuterike.
Instaloni një program anti-virus, aktivizoni firewalls , aktivizoni filtrat e emailit dhe mbajini ato të përditësuara.

Kujdes! Mashtruesit duan që ju të veproni shpejt dhe pa menduar mirë! Nëse një email ju kërkon veprime urgjente, tregohuni skeptik; kurrë mos lejoni që të ndikojë në kujdesshmërinë tuaj.

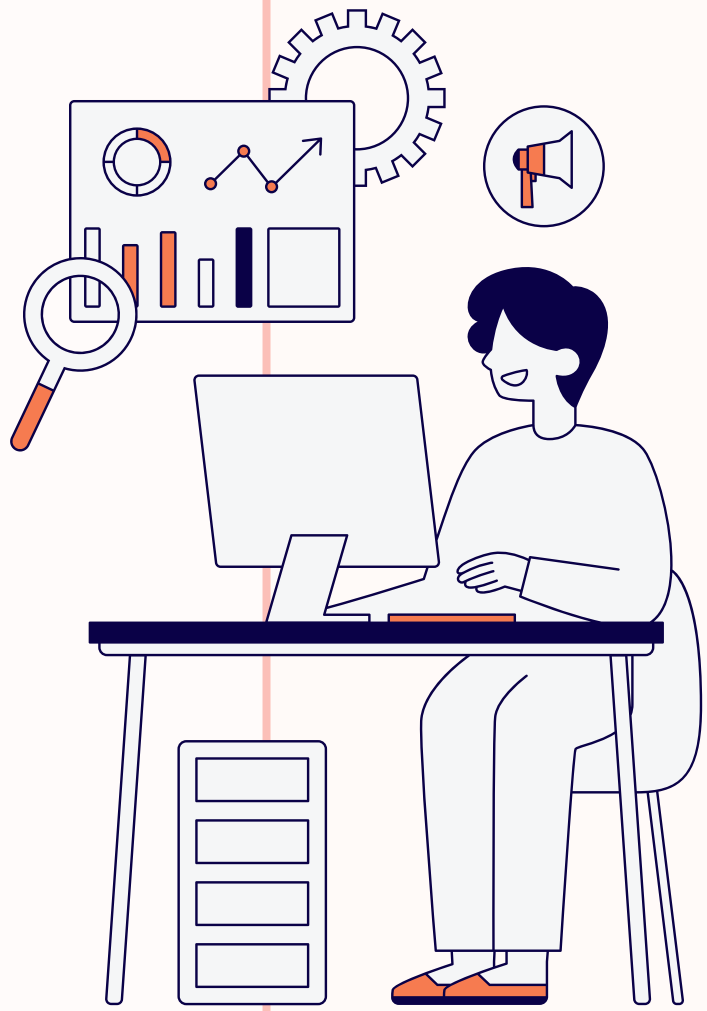
KËSHILLA PËR TË DHËNAT

Jini të kujdesshëm ndaj të dhënave **personale që i bëni publike përmes rrjeteve sociale** dhe metodave të tjera.

Sa më shumë informacione publike për ju, aq më e lehtë është për sulmuesit që të krijojnë **mesazhe phishing** më bindëse.

Jini të kujdesshëm kur një i panjohur ju telefonon ose ju takon dhe ju bën shumë **pyetje.**

Nëse është e mundur**,** përdorni **enkriptimin** për dërgimin e të dhënave të rëndësishme**.**



KËSHILLA PËR EMAIL-IN

Gjithmonë kontrolloni dërguesin.
Nëse emaili është i rëndësishëm telefononi dërguesin për t'u siguruar që është vërtet ai që dërgoi emailin.

Kujdes! Mund të merrni email nga kontaktet tuaja që kanë rënë pre e sulmeve.
Mos klikoni në **linqe të dyshimta.**

Fshini emailet që nuk ju nevojiten më.

Mos hapni dokumente të bashkëngjitura në email nga **dërgues të panjohur.**
Përdorni mjete specifike për të kontrolluar URL-të ose skedarët.

KËSHILLA PËR FJALËKALIMET

Mos përdorni **të njëjtin fjalëkalim** kudo.

Vendosni fjalëkalime të gjata, me numra, shkronja të mëdha, të vogla, karaktere speciale, të cilat nuk kanë **kuptim të veçantë.**

Mos aktivizoni në browser opsionin i cili ruan fjalëkalimet tuaja.

Nëse është e mundur, përdorni **autentifikimin me shumë faktorë.**