



Tetor

Muaji i ndërgjegjësimit për sigurinë kibernetike Mbroni veten!

1. Kini kujdes nga emailët phishing

Phishing është kur kriminelët kibernetikë përpiqen të vjedhin informacione me emailë të rreme. Ata shtiren si dikush tjetër dhe përpiqen t'ju nxisin të klikoni në lidhje të rrezikshme. Nëse një email ju duket i çuditshëm, kini kujdes, kontrolloni se kush e ka dërguar dhe nëse emaili përputhet me atë që thonë se janë.

2. Përdorni autentikimin me shumë faktorë (MFA)

Merrni një shtresë shtesë mbrojtjeje kundër hakerave kur hyni me MFA. Është si një mesazh me një kod sekret që skadon pas një përdorimi.

3. Përdorni një fjalëkalim ose një frazëkalim të fortë

Mos përdorni të njëjtën fjalëkalim kudo! Përdorni shkronja, numra dhe simbole. Sa më gjatë, aq më mirë, dhe frazëkalimet mund të ndihmojnë.

4. Mbajeni softuerin tuaj të përditësuar

Ai redukton rrezikun e infektimit nga softuerët e instaluar nga hakerat që mund të vjedhin informacionet tuaja ose të përhapin viruse në kompjuterin tuaj.

5. Qëndroni të zgjuar, qëndroni të sigurt në rrjetet sociale!

Ndarja e informacionit personal, si ditëlindja juaj e plotë, adresa e shtëpisë ose vendndodhja juaj, mund të përdoret për vjedhje identiteti ose bullizim.

6. Mbrohuni – përdorni rrjet Wi-Fi të sigurt

Rrjetet publike nuk janë të sigurta. Dikush mund të shohë se çfarë po bëni në internet, duke përfshirë hyrjen në email dhe llogaritë bankare.

7. Kini kujdes nga mashtrimet me inteligjencë artificiale

Kriminelët kibernetikë përdorin inteligjencë artificiale të përparuar për të krijuar imazhe, tekst, zë dhe video realiste. Kjo e bën më të vështirë zbulimin e phishing-ut dhe mashtrimeve të tjera. Qëndroni vigjilentë dhe kontrolloni dy herë (p.sh., verifikoni burimin, kërkoni për sinjale paralajmëruese të inteligjencës artificiale dhe "artefakte" si gjuhë urgjente, zëra të panatyrshëm ose imazhe paksa të shtrembëruara etj.) përpara se t'i besoni ndonjë komunikimi të papritur.