Puna në distancë

(Remote Working)

Puna në distancë ka sjellë fleksibilitet dhe mundësi të reja për shumë njerëz, por është e rëndësishme të keni parasysh disa këshilla sigurie për të mbrojtur veten dhe të dhënat e organizatës suaj.

Rrjeti Privat Virtual (VPN)

Një VPN ju lejon të punoni në një rrjet të sigurt duke konvertuar të gjithë informacionin tuaj në një kod, për të bërë më të vështirë aksesin për hakerat.

Wi-Fi & Hotspotet Publike

Wi-Fi dhe hotspotet publike kanë siguri të kufizuar, duke e bërë të lehtë për hakerat të kenë akses në çdo informacion të ndjeshëm që dërgoni, merrni ose aksesoni gjatë kohës që jeni në këto rrjete.

Hapësirat Publike

Mashtruesit mund të aksesojnë informacion thjesht duke parë ekranin tuaj (e njohur ndryshe si 'shoulder surfing'). Kini kujdes kur punoni në distancë dhe mos e lini kurrë pajisjen tuaj pa mbikëqyrje në hapësira publike.

Autentifikimi me Dy Faktorë (2FA)

Kurdoherë që është e mundur, përdorni autentifikimin me dy faktorë kur lidheni në internet. Kjo kërkon dy mënyra për të vërtetuar identitetin tuaj, duke shtuar një shtresë tjetër sigurie që mund të mbrojë llogaritë dhe të dhënat tuaja.

Fjalëkalimi

Fjalëkalimi "Password" kërkon vetëm 0,29 milisekonda për t'u thyer. Hakerët përdorin një sërë mjetesh për të thyer fjalëkalimet në kohë rekord. Merrni parasysh përditësimin e fjalëkalimeve tuaja në fraza kalimi (passphrases); ato janë të lehta për t'u mbajtur mend dhe më të vështira për t'u hakuar.

Përditësimet e Softuerit & Backup i të Dhënave

Nëse kompjuteri juaj prishet, hakerohet ose jeni të bllokuar, të dhënat tuaja mund të zhduken përgjithmonë. Sigurohuni që të bëni kopje rezervë të skedarëve tuaj rregullisht për të parandaluar çdo humbje të të dhënave.