Siguria digjitale

Si të mbroheni kur punoni në botën digjitale

Mendoni para se të klikoni

Kriminelët në internet shpesh përdorin tema interesante dhe emocionuese për t'ju tërhequr që të klikoni në ndonjë link keqdashës. Ndaloni dhe mendoni para se të klikoni dhe po ashtu përdorni bitdefender.com ose kaspersky.com

Përdorni softuer për menaxhim të fjalëkalimeve

keepass.info ose buttercup.pw janë mjete të mira për t'i ruajtur të gjitha fjalëkalimet tuaja në një vend, të enkriptuara dhe të mbrojtura. E tëra çfarë duhet të bëni është të mbani mend vetëm një fjalëkalim.

Bëni kopje rezervë të rregullt

Nëse pajisja juaj ndalon së punuari ose është vjedhur, do t'i humbni të gjitha të dhënat tuaja të rëndësishme përgjithmonë. Prandaj është me rëndësi thelbësore që të mbajmë kopje rezervë në një vend të dytë. amanda.org ose backuppc.github.io janë zgjidhje të shkëlqyera softuerike për këtë qëllim.

Përdorni softuer legal dhe azhurnoni atë rregullisht

Përdorimi i softuerit legal dhe azhurnimi i tij i rregullt ju mbron nga softueri keqdashës (malware) dhe e optimizon punën e pajisjes tuaj. Nëse jeni organizatë joqeveritare dhe keni nevojë për softuer legal, techsoupnorthmacedonia.org mund t'ju ndihmojë

Pajisja e sigurt celulare

Përdorni fjalëkalim, PIN ose ndonjë mbrojtje tjetër për ta kyçur pajisjen tuaj celulare. Nëse pajisja juaj celulare është humbur ose vjedhur, atë mund ta gjeni me ndihmën e Find my iPhone, Android Device Manager ose Lookout.

Mos i përdorni të njëjtat fjalëkalime

Përdorimi i vazhdueshëm i fjalëkalimeve të njëjta kudo, mund t'ua lehtësojë punën hakerëve që të fitojnë qasje në të gjitha profilet dhe pajisjet tuaja përnjëherë. Përdorni fjalëkalime të kombinuara (shkronja të mëdha dhe të vogla, simbole, numra) ose disa fjalë të palidhura me një vizë midis tyre.

Shikoni kush ju dërgon mesazhe dhe dokumente në e-mail

Kini kujdes kur klikoni në linke dhe dokumente që ju janë dërguar, pasi ato mund të përmbajnë softuer keqdashës (malware) që do ta dëmtojë pajisjen tuaj.

Mendoni se ku shpërndani informacione private

Informatat personale dhe të ndjeshme siç janë emrat e anëtarëve të familjes, ditëlindjet, numri i targës së automjetit dhe adresa e shtëpisë, të cilat i shpërndani në internet, ndonjëherë mund të përdoren kundër jush.

Përdorni autentifikimin me dy faktorë

Ky nivel shtesë mbrojtjeje e rrit ndjeshëm sigurinë e profileve tuaja. Udhëzimet për aktivizimin e 2FA janë në dispozicion në ueb-faqet e të gjitha shërbimeve kryesore si Facebook, Instagram, Gmail, Twitter dhe të tjerat.

Përdorni VPN

VPN (Rrjeti Virtual Privat) është një mjet për të mbrojtur komunikimin kur përdorni pajisje në Internet. Gjithmonë përdorni protonvpn.com ose psiphon.ca kur përdorni rrjete publike

digitalfirstaid.mk

Mbështetur nga Projekti "The Information Safety & Capacity" (ISC)
Realizuar nga Fondacioni Metamorfozis