Garante per la Privacy

Kujdes të dhënat personale që ruhen në telefonat inteligjentë (*smartphone)* dhe *tablet*

Duhet të bëhet shumë kujdes në ruajtjen e informacionit personal në *smartphone* dhe *tablet* sepse këto të fundit mund t'iu humbasin, të vidhen ose të sulmohen nga piratët elektronike. Ju kurrë nuk duhet të mbani për shembull, fjalëkalimet, kodet e hyrjes dhe të dhënat bankare në mënyrë të dukshme.

Mbani mend, *se smartphone* dhe *tablet* i përdorur, i dhuruar apo që është për t'u hedhur, ende mund të përmbajë të dhëna personale. Nëse ju duhet ta hiqni atë, atëherë, duhet të përpiqeni të merrni disa masa të vogla të sigurisë të tilla si:

- Të rivendosni parametrat e fabrikës;
- Të hiqni kartën SIM dhe kartën e kujtesës;
- Të fshini të gjitha *backups* të ruajtura në kujtesë.

Mbroni të dhënat tuaja

Nëse ju doni të parandaloni dikë të lexojë fshehurazi emailet dhe mesazhet tuaja pa dijeninë tuaj, duhet të merrni disa masa paraprake.

Gjithmonë vendosni një PIN mjaft të komplikuar, duke shmangur, për shembull, të përdorni emrin tuaj, datën e lindjes, emrat e fëmijëve ose kafshëve shtëpiake, ose çfarëdo fjale tjetër që është lehtësisht e kopjueshme.

Ndoshta është mirë të vendosni dhe një kod bllokimi që aktivizohet automatikisht kur telefoni është i ndezur por nuk është në përdorim për një kohë të caktuar. Gjithashtu, në këtë rast është mirë të shmangen kodet pak a shumë të lehtë për t'u zbuluar.

Kujdes! Ruani numrin IMEI, të cilin mund ta gjeni në kutinë e produktit që keni blerë dhe në rast të vjedhjes ose humbjes së aparatit tuaj *smartphone* ose *tablet* mund ta përdorni për ta bllokuar në distancë.

Kur lundroni në Internet nëpërmjet *smartphone* dhe *tablet*

Nëse ju lidheni në internet dhe rrjete sociale nëpërmjet *smartphone* dhe *tablet*, kontrolloni politikat e privatësisë dhe lexoni kushtet e përdorimit të shërbimeve.

Nëse lundroni në internet, instaloni - nëse është e mundur –antivirus ose programe të sigurisë kompjuterike për t'u mbrojtur nga ndërhyrjet e hakerave.
Sigurohuni që lundrimi të jetë i mbrojtur me protokollet e shkëmbimit të të dhënave të kriptuara dhe që faqet e vizituara të përmbajnë protokollin e autentifikimit **https**. Kujdes të veçantë duhet pasur për sigurinë në përdorimin e faqeve bankare apo dhe emailit.

Aplikacionet (app.)

Nëse shkarkoni aplikacione dhe nuk jeni në gjendje për të vlerësuar besueshmërinë e burimit - për shembull, duke lexuar komentet e lëna nga përdoruesit e tjerë - për të kuptuar nëse ka rreziqe apo probleme shmangi burimet e panjohura dhe gjithmonë përdorni tregun zyrtar.

Pas instalimit të një app, kontrolloni nëse kërkon qasje në përmbajtje të *smartphon*-it ose në *tablet*-ën tuaj (për shembull, foto apo kontaktet në librin tuaj të adresave) dhe lexoni me kujdes kushtet e përdorimit të shërbimit, sidomos për të shmangur pasojën e pagesës për shërbimet e pakërkuara ose për të mos ekspozuar të dhëna personale (p.sh..: foto, video, kontakte, etj).

Kujdes nga spamet

Kini kujdes nga linket që ju shfaqen në email, mesazhe apo *chat*-e të ndryshme. Mund të përmbajnë viruse apo përmbajtje të tjera të padëshiruara.

Jo gjithmonë duam të tregojmë se ku ndodhemi

Smartphone dhe tablet kanë funksione gjeolokalizimi, por jeni ju ata që vendosni nëse, kur dhe kush mund të njohë pozicionin tuaj. Për të çaktivizuar gjeolokalizimin, ju mund të fikni – kontrolloni - parametrat e *smartphon*-it ose tablet-ës tuaj- lidhjen me GPS ose Ëi-Fi, kur ju nuk përdorni këto shërbime apo shërbime të tjera që lidhen me to.

Është gjithashtu praktikë e mirë kontrollimi i parametrave të gjeolokalizimit gjatë përdorimit të rrjeteve sociale në *smartphone* apo *tablet.* Zgjedhja përfundimtare për t'iu bërë të ditur njerëzve se ku ndodheni, pas të gjitha, është gjithmonë e juaja.