 Përdorimi i kompjuterëve, laptopëve, celularëve inteligjentë dhe i pajisjeve elektronike për komunikim rritet dita ditës. Shfrytëzuesit e tyre janë të moshave dhe profileve të ndryshme, duke u nisur nga shkollarët, studentët, profesorët, punëtorët, amviset duke mos anashkaluar edhe të moshuarit.

Të arriturat e teknologjisë nuk kanë të ndalur, përparime të mëdha bëhen në fusha të ndryshme si në harduer (hardware – pjesë elektronike për kompjuter, tabletë apo celularë) ashtu edhe në softuer (software - aplikacione). Falë këtij përparimi të teknologjisë ne sot dërgojmë porosi elektronike, fotografi, video të formateve dhe madhësive të ndryshme.

Një grup i caktuar njerëzish falë teknologjisë sot në pronësi kanë miliona dollarë, edhe atë falë një ideje dhe një mundi modestë.

Kompani të ndryshme lansojnë produkte (aplikacione) të të gjitha llojeve, postë elektronike, rrjete sociale, sisteme inteligjente, aplikacione për komunikim në kohë reale etj.

Të gjitha këto shpikje u bënë për të mirën e njerëzimit, për të na lehtësuar punën neve, e në veçanti për trashjen e xhepave të tyre.

Sido që të jetë po bëhet një punë e madhe dhe shumë frytdhënëse.

Disa nga të mirat dhe dobitë i përmendëm këtu, ka dhe shumë për tu përmendur mirëpo qëllimi ynë në këtë artikull është të ndalemi në aspektin e sigurisë gjatë përcjelljes së të dhënave në rrjet sociale (përmes internetit).

Sa prej nesh para se të dërgojnë një të dhënë qoftë në fejsbuk, twitter apo në cilindo rrjet social mendojnë për sigurinë, gjegjësisht kush do të ketë qasje në të dhënat që po dërgojmë, sa janë gjasat për keqpërdorim, të dhënat ruhen vetëm në pajisjen e pranuesit të porosisë apo edhe diku tjetër etj. E sidomos në dërgimin e porosive intime, fotografi- video personale, fjalëkalime, dokumente të ndjeshme etj., sa është masa e sigurisë kur dërgohen porosi me përmbajtje të tilla.

Rrjetet sociale në përgjithësi kanë bashkëpunim të ngushtë me shërbimet sekrete, po qe puna

juaj në interesin e tyre keni mbaruar.

Çdo e dhënë e cila ngarkohet në rrjetet sociale edhe pas fshirjes së të njëjtës ajo mbetet e ruajtur në bazën e të dhënave të kompanisë e cila ofron shërbimin. Një kompani e tillë ka informacione për ne nga dita që e kemi hapur llogarinë në sistemin e tyre e deri në ditën e bllokimit apo fshirjes së llogaris. Ka nga ato sisteme që indirekt kanë qasje edhe në të dhënat e kompjuterit, tabletit apo celularit tënd andaj kujdes.

Edhe pas aplikimit të masave të sigurisë që ofrojnë rrjetet sociale ato sërish nuk janë të sigurta, ne dëgjojmë çdo ditë për thyerje të sigurisë qoftë në fejsbuk apo twitter. Pas ndodhive të këtilla ne me automatizëm biem pre e krimeve kibernetike edhe pse jo direkt.

Andaj çdo shfrytëzues kompjuteri në përgjithësi dhe shfrytëzuesit e rrjeteve sociale në veçanti duhet t'i kenë parasysh këto këshilla:

• Zgjedhja e një fjalëkalimi të fortë (strong paswword), duke përdorë shkronja dhe numra.
• Aplikimi i masave të sigurisë që ofron rrjeti social.
• Kanalizimi i porosive.
• Enkriptimi i të dhënave.
• Të dhënat e ndjeshme të ruhen në mediume që nuk kanë qasje në rrjet.
• Mbrojtja e të dhënave me fjalëkalim.
• Etj.

Besojmë që pas aplikimit të këtyre këshillave të dhënat tuaja do të jenë më të sigurta edhe pse çdo gjë është relative.

Ylber Veliu