MËNYRA SI TË JENI TË SIGURT ONLINE SI KONSUMATOR

ОПМ
Организација на потрошувачите на Македонија

Министерство за Економија

Interneti na ofron spektër jashtëzakonisht të madh të mundësive dhe zgjedhjeve. Lehtë mund të vendosim lidhje dhe të komunikojmë me familjen dhe miqtë nga tërë bota, të bëjë pazarllëkun tonë javor dhe të të realizojmë pagesën e llogarive tona vetëm me një klik, duke kursyer edhe kohë edhe para. Krejt këto aktivitete në një farë mënyre i përdorin informacionet tona personale - informacionet tona në bankë për të realizuar pagesë, fotografitë dhe komentet tona, adresat tona për të dërguar porosinë. Duke dhënë më tepër informacione për ne onlajn, rreziqet për vjedhje të identitetit, hakim, shantazh dhe mashtrim rriten.

Ja disa punë të rëndomta të cilat mund t'i bëjmë të gjithë për të mbrojtur të dhënat tona personale onlajn dhe të kënaqemi në internet duke u ndjerë të sigurt:

1. Përdorni fjalëkalime të ndryshme dhe origjinale

- Kjo është diçka që mund të ndryshohet më së lehti, por edhe diçka që askush prej nesh nuk e bën. Është shumë me rëndësi të keni PIN ose fjalëkalim të ndryshëm për çdo emër të përdoruesit që kur të jemi në situatë të na hakojnë ndonjërin nga emrat e përdoruesve të tjerët mund të ngelin të mbrojtur. Fjalëkalimin më të rëndësishëm që duhet ta ndërrojmë rregullisht është fjalëkalimi i e-mailit sepse atë mund ta përdorim për të ndërruar fjalëkalimet e emrave të përdoruesve tjerë. Nëse dyshoni se jeni viktimë të hakimit (ndërsa shpesh edhe nuk jemi të vetëdijshëm për atë gjë), ndërroni fjalëkalimin menjëherë dhe të gjitha fjalëkalimet e njëjta që i keni.
- Shmangni përdorimin e fjalëkalimeve të rëndomta dhe të dukshme, si vendi juaj i lindjes ose emri i fëmijës suaj sepse këto të dhëna mësohen lehtë. Në vend të kësaj, përdorni fjalë ose fraza të ndërlikuara të cilat përmbajnë shkronja të mëdha, numra dhe shenja të pikësimit që janë për siguri plotësuese. Mendoni edhe për përdorimin e shërbimit për fjalëkalimeve që do të ruajë të gjitha fjalëkalimet tuaja me atë se do të duhet të mbani ndërmend vetëm një.

2. Shfrytëzoni vegla për siguri

- Shumica e kompanive iu ofrojnë konsumatorëve spektër jashtëzakonisht të madh të opsioneve lidhur me veglat e sigurisë dhe fjalëkalimet. Gjithmonë duhet të keni fjalëkalim në smartfonin (telefonin e mençur) tuaj - është për t'u habitur me numrin e njerëzve që nuk kanë fjalëkalim të tillë- ndërsa pa të gjitha aplikacionet, hartat, kalendarët, kontaktet, informacionet tuaja rreth pagesave dhe numër jashtëzakonisht i madh i të dhënave personale bëhen në dispozicion për t'u lexuar. Ndani kohë t'i lexoni veglat e privatësisë dhe përshtatni ato sipas pirjes suaj dhe mos ngurroni të kërkoni ndihmë nëse hasni në ndonjë problem derisa e bëni këtë gjë.

3. Kini kujdes rreth gjërave që i shkëmbeni në rrjetet sociale

- Nëse iu përmbaheni rregullimeve të dhëna, atëherë çdo kush dhe prej çdo vendi mund të ketë qasje deri të çdo

gjë që shkëmbeni, prandaj para se të shkëmbeni diçka mendoni mirë. Ndani kohë për të lexuar veglat e privatësisë dhe të shmangni shkëmbimin e informacioneve personale me të cilat do të krijonit fotografi të plotë për ju si adresa juaj, vendi i punës, planet për pushime dhe emrat e anëtarëve të familjes tuaj të ngushtë.

4. Kini kujdes me Wi-fi

- Wi-fi falas është shumë e përshtatshme, por siguria mund të jetë problem kur përdorni rrjet të përbashkët me një numër të madh njerëzish. Nëse jeni në wi-fi rrjet përdorni "https" kur të aktivizoni e-mailin tuaj, rrjetet sociale dhe adresa personale tjera të përdoruesit. Nëse jeni në shtëpi, gjithmonë të kini fjalëkalim për të hyrë në rrjetin tuaj.

5. Mos lejoni të ju mashtrojnë me e-maila ose SMS dhe mesazhe tjera të rrejshme

- Lehtë mund të josheni nga ndonjë letër në e-mail e cila pohon se ju takojnë para si shpërblim ose ndonjë pjesë e trashëgimisë së humbur që moti, por kini kujdes! Mos ju besoni ofertave ose shpërblimeve të cilat tingëllojnë tepër mirë për të qenë të vërteta, sepse me gjasë edhe janë. Nëse pranoni e-mail i cili thotë se ju takon një shumë jashtëzakonisht e madhe parash dhe se duhet të jipni detaje të llogarisë suaj bankare që t'i merrni ato - kujdes! Kjo është mënyrë e lehtë që hakerët të marrin informacionet tuaja bankare dhe të kryejnë mashtrim.
- Nëse pranoni letër në e-mail nga banka ose kompania juaj në të cilën kërkohen informacionet tuaja, para se të jepni çfarëdo informacioni letrën përcilleni deri te shërbimet e tyre që të siguroheni se pohimi i tillë është i saktë.

6. Shmangni hapjen e shtojcave në e-mail ose me linqe të pazakonshme

- Viruset më së shpeshti dërgohen përmes shtojcave në e-mail ose linqe. Viruset mund t'i shkaktojnë dëm pajisjes suaj si dhe të sigurojnë hyrje deri te të dhënat tuaja personale. Nëse nuk e njihni dërguesin ose nuk e dinë se çka është shtojca në e-mail, mos e hapni. E njëjta vlen edhe për linqe nga miqtë tuaj. Nëse ju kanë dërguar diçka që duket pak e çuditshme, ndërsa është me emër të përdoruesit të mikut tuaj, gjithmonë pyetni për atë para se ta hapni sepse ka mundësi të madhe që e-maili i tyre të ketë qenë i hakuar.

7. Shfrytëzoni e-mail të përkohshëm

- Kur të lidheni në ndonjë web-faqe shpesh prej jush kërkohet të jepni të dhëna për e-mailin tuaj dhe informacionet për kontakt, madje edhe nëse shërbimet i shfrytëzoni vetëm një herë. Nëse dëshironi të shmangni pranimin e e-mailave për marketing dhe shitje, mund të përdorni e-mail adresë të përkohshme. Kjo ju jep mjaft kohë të t lidheni në atë faqe, të merrni të dhënat që ju nevojiten. E-maili i përkohshëm pastaj shkatër-

rohet me automatizëm pa i ruajtur të dhënat tuaja personale. Shfrytëzimi i e-mailave të përkohshëm ofron mënyrë të sigurt për lidhje në web-faqe pa e zbuluar e-mailin tuaj të vërtetë. Ka shumë web-faqe të cilat e ofrojnë këtë shërbim, vetëm kërkoni termin "temporary email addresses" për të zbuluar mundësitë e tyre.

8. Sigurohuni që pagesat tuaja të jenë të sigurta

- Kur bëni pagesë onlajn kërkoni web-adresa, të cilat fillojnë me "https://", e jo vetëm me "https://" sepse shkronja "s" në fund donë të thotë siguri. Kjo donë të thotë se të dhënat deshifrohen derisa udhëtojnë prej web-faqes deri te kompjuteri juaj. Gjithashtu, në anën e majtë ose të djathtë krahas emrit të web-adresës duhet të ketë një ikonë në formë të drynit që tregon se ajo web-faqe është e sigurt.

- Është e dobishme të krijoni shprehi që rregullisht t'i kontrolloni llogaritë bankare dhe raportet e bankës pasi të kryeni çdo pagesë që të vërtetoni se gjatë transaksionit është deponuar shuma e vërtetë dhe se nuk ka pasur kurrfarë mashtrimi.

9. Rregullisht bëni ripërtëritje të softuerit

- Aktivizimi automatik i sistemit operativ dhe softuerit tuaj është më të vërtetë mënyrë e lehtë të siguroheni se e keni mbrojtjen më të mirë ashtu që çdo ripërtëritje ofron siguri plotësuese automatikisht. Nëse keni softuer të vjetër, tek ai do të mungojnë mbrojtjet më të reja, prandaj aktivizoni ripërtëritjet automatike në të gjitha pajisjet tuaja.

10. Instaloni dhe ripërtërini muret mbrojtëse (firewalls), antivirusin dhe softuerin kundër spiunimit

- Është me rëndësi të keni në dispozicion këtë mundësi rregullimi në të gjitha pajisjet tuaja sepse muret mbrojtës parandalojnë që persona të paautorizuar të hakojnë kompjuterin, softuerin tuaj kundër spiunimit dhe e mbrojnë kompjuterin tuaj prej viruseve dhe programeve të spiunimit që të kenë qasje në fjalëkalimet, adresat që i përdorni dhe të dhënat tuaja personale. Pa këtë pajisjet tuaja janë të ekspozuara në rrezik të madhe se do të hakohen.