Vienkārši padomi IT drošībai, kas noderēs ikvienam

FOTO: Publicitātes foto

Digitālā drošība ir aktuāls jautājums kopš internets ir kļuvis par mūsu ikdienas sastāvdaļu. Vieniem tās ir pašsaprotamas darbības, taču citiem to iegaumēšana un ieviešana ikdienā padodas grūtāk. Jebkurā gadījumā mūsdienu mainīgajā vidē zināšanas par IT drošību ir ieteicams atsvaidzināt ikvienam, neatkarīgi no vecuma, profesijas vai digitālajām iemaņām. Šajā rakstā IT tehnoloģiju uzņēmums "Capital" iesaka vienkāršus padomus, kā parūpēties par sevi interneta vidē.

Pārbaudiet savus privātuma iestatījumus

Mūsdienās visām sociālo tīklu platformām ir pienākums piedāvāt iespēju ierobežot trešo pušu piekļuvi personīgajai informācijai, piemēram, fotoattēliem, dzimšanas datumam, atrašanās vietai. Iepazīstoties ar privātuma iestatījumiem sociālajos tīklos, varat kontrolēt, kādus datus un kurām lietotnēm vēlaties tos atklāt.

Regulāri pārskatiet paroles

Laba interneta drošības prakse ir vismaz reizi trīs mēnešos pārskatīt savas paroles un pārliecināties, vai tās ir pietiekami drošas. Ir svarīgi katram resursam veidot savu unikālo paroli, kas sastāv no pēc iespējas vairāk simboliem. Tāpat vajadzētu izvairīties no jau kādreiz izmantotu paroļu lietošanas.

Lielākai drošībai ieteicams izmantot divu faktoru autenti kāciju, kas sastāv no diviem posmiem: paroles ievadīšanas un papildu soļa veikšanas, piemēram, uz viedtālruni nosūtītā koda ierakstīšanas.

Tāpat arī pirms ievadīt svarīgus datus (paroles, norēķinu kartes informāciju un tamlīdzīgi), noteikti nepieciešams pārliecināties, vai tīmekļa vietne ir īstā – vai adresē nav parādījušies lieki burti, simboli, atvasinājumi un tamlīdzīgi.

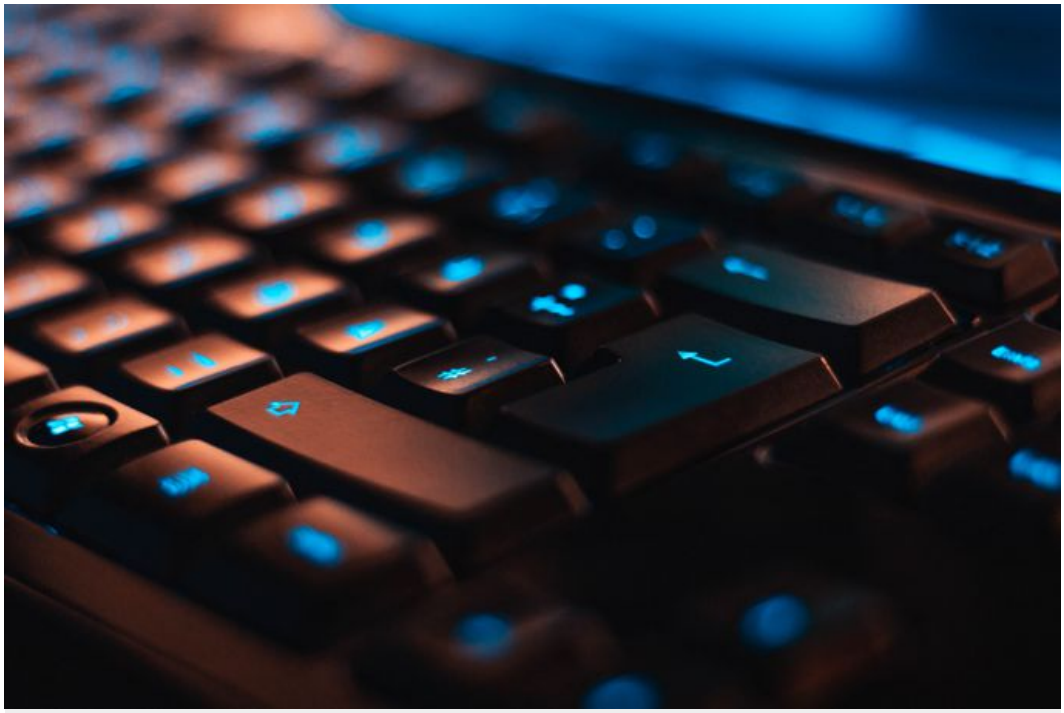

FOTO: Publicitātes foto

Neklikšķiniet uz aizdomīgām saitēm vai pielikumiem

Lai arī vairums īpaši aizdomīgo e-pastu nu jau paši krīt mēstuļu kastītē, tomēr jāatceras, ka tāpat nav jāver vaļā e-pasti no cilvēkiem, kas nav jūsu kontaktu sarakstā un kam ir nesaprotams sūtītāja vārds vai kliedzošs ziņas virsraksts. Protams, katrs gadījums ir jāizvērtē atsevišķi, bet piesardzība interneta vidē noteikti nāks tikai par labu.

Ja tomēr esat atvēris e-pastu, kas saņemts no nedroša avota, galvenais ir nespiest uz saitēm. Ja neesat drošs, vai e-pasts ir patiess vai nē, sazinieties ar IT atbalstu, ja tāds ir pieejams, vai vismaz pajautājiet kādam, kam uzticaties, izteikt savu viedokli.

Veiciet regulāru lietotņu atjaunināšanu viedierīcē

Regulāra lietotņu un operētājsistēmas atjaunināšana nepieciešama, lai pārliecinātos, ka nav beidzies ražotāja atbalsts, kas garantē drošu darbību. Veicot lietotņu atjauninājumus, nepieciešams pārliecināties, ka tās tiek lejupielādētas tikai no uzticamiem avotiem, piemēram, Google Play vai App Store.

Izpētiet viedierīces lietotņu atļaujas

Visbiežak, lejupielādējot viedierīcēs jaunas lietotnes, laika trūkuma dēļ mēs nemaz neizpētām noteikumus, kam piekrītam. Par laimi, viedierīču iestatījumos lielākoties iespējams pārskatīt, kādas atļaujas un pieejas lejupielādētajām lietotnēm ir dotas. Piemēram, pārbaudiet, vai tām ir piekļuve jūsu kamerai, mikrofonam un atrašanās vietai, kā arī liedziet šīs informācijas piekļuvi tām lietotnēm, kurām tāda acīmredzami nav nepieciešama.

Nomainiet rūpnīcās iestatīto paroli savā Wi-Fi rūterī

Lai arī rūpnīcu izgatavotās ierīces tiek uzskatītas par drošām, vienmēr pastāv iespēja, ka tīkla piekļuves oriģinālo paroli iespējams atklāt un tādējādi ielauzties jūsu mājās vai darbā esošā Wi-Fi rūterī, kam pieslēgtas visas izmantotās ierīces. Personīgā Wi-Fi tīkla nosaukuma un paroles maiņa aizņem dažas minūtes, taču rezultāts var sniegt ievērojami augstāku drošības līmeni.

Tāpat gadījumos, kad nepieciešams pieslēgties publiskam Wi-Fi tīklam, bet tas nešķiet drošs, labā prakse ir izmantot VPN (virtuālo privāto tīklu) vai mobilos datus.

Bloķējiet piekļuvi savām ierīcēm

Aktivizējiet automātisku ekrāna bloķēšanu pēc iespējami īsa dīkstāves perioda, aizsargājot to ar drošu PIN kodu, paroli, biometriju vai citu autenti kācijas veidu. Nenobloķēta ierīce vienmēr ir pakļauta lielākam riskam, ka trešā persona var iegūt sensitīvu informāciju jums par to nemaz nenojaušot.

Neizmantojiet personīgo profilu svešās ierīces

Sociālo tīklu profils vai e-pasts ir gana privāta informācija, ko nevajadzētu lietot svešās ierīcēs. Ja tomēr nepieciešams pierakstīties savā profilā, vienmēr atcerieties pārbaudīt, vai esat tiešām no tā izgājis, nevis vienkārši aizvēris interneta pārlūku.