Padomi un ieteikumi

Iegūstiet drošību tiešsaistē, ievērojot tālāk minētos padomus un ieteikumus. Šī sadaļa ir izstrādāta sadarbībā ar Apvienotās Karalistes kampaņu "Get Safe Online" un ASV Iekšzemes drošības departamentu.

- Personālā datora (*PC*) un pārnēsājamo ierīču aizsardzība
- Personiskās informācijas un identitātes aizsardzība
- Darba informācijas aizsardzība, atrodoties ārpus darba vietas
- Savienojuma piesardzīga izveidošana
- Droša tīmekļa lietošana

Personālā datora (*PC*) un pārnēsājamo ierīču aizsardzība

PC

- Izmantojiet ugunsmūri — ugunsmūris pasargā tīklu no dažiem vīrusiem un pretlikumīgas piekļūšanas.
- Instalējiet pretvīrusu programmatūru — pretvīrusu programmatūra nepieļauj vīrusu izplatību jūsu datorā.
- Saņemiet jaunākos drošības atjauninājumus — rūpējieties par lietojumprogrammu un operētājsistēmas atbilstību, funkcionalitāti un atjaunināšanu.
- Izvairieties no spiegprogrammatūras — izvairoties no aizdomīgiem e-pasta ziņojumiem un pielikumiem, neļaujiet svešiniekiem piekļūt informācijai jūsu datorā.
- Regulāri izveidojiet datu dublējumkopiju — aizsargājiet savus datus no iespējama zuduma.

Klēpjdatori

- Pārtrauciet bezvadu savienojumus, kad tie netiek lietoti vai nav nepieciešami.
- Regulāri izveidojiet savienojumu ar uzticamu tīklu, lai atjauninātu drošības mehānismus.
- Izveidojiet klēpjdatorā uzglabātās informācijas dublējumkopiju.
- Neatstājiet klēpjdatoru bez uzraudzības.

***USB* diski**

- Izmantojiet šifrētu *USB* disku.
- Lai nepieļautu vīrusu izplatību, ar fizisko slēdzi pārslēdziet *USB* zibatmiņas disku tikai lasāmajā režīmā — dažiem *USB* zibatmiņas diskiem ir fizisks slēdzis, ar ko pārslēgt disku tikai lasāmajā režīmā, lai neļautu resursdatoram ierakstīt vai izmainīt datus diskā.
- Pēc datņu kopēšanas no neuzticamas un/vai neatļautas iekārtas, skenējiet *USB* zibatmiņas ierīci, lai novērstu vīrusu izplatību.

- Pirms pievienojat *USB* zibatmiņas disku citas personas datoram, izdzēsiet visas datnes, kas nav nepieciešamas paredzētās darbības veikšanai.
- Izveidojiet *USB* diskā esošās informācijas dublējumkopiju, lai datu zuduma gadījumā tos varētu atgūt.
- Lai nenozaudētu *USB* datu nesēju, piestipriniet to pie atslēgu piekariņa vai aukliņas — tā kā *USB* zibatmiņas disks ir neliela izmēra, tas ir vieglāk nozaudējams vai nozogams. Turklāt lielāka atmiņas ietilpība palielina potenciālo datu skaitu, kam var mēģināt neatļauti piekļūt. *USB* zibatmiņas diski parasti tiek likti somās, mugursomās, klēpjdatoru somās, jakās, bikšu kabatās vai atstāti bez uzraudzības darbstacijās. Pēdējā laikā ir pieaudzis starpgadījumu skaits, jo *USB* zibatmiņas diski tiek nozaudēti, nolikti nevietā, tos aizņemas bez atļaujas vai nozog.

Mobilie tālruņi un plaukstdatori

Plaukstdatoros, piemēram, *Windows Mobile*, *Palm*, *iPhone*, *Android* un *Blackberry* ierīcēs var piekļūt interneta saitēm un uzglabāt lielus informācijas apjomus. Tā kā šie datori ir pārnēsājami, ar tiem ir jārīkojas īpaši uzmanīgi.

- Pārtrauciet bezvadu savienojumus (piemēram, *Bluetooth* un *WLAN*), kad tie netiek izmantoti. Tehnoloģija *Bluetooth* elektroniskām ierīcēm ļauj izveidot savstarpēju savienojumu, izmantojot maza darbības rādiusa radiolīniju.
- Neatstājiet savu mobilo tālruni un plaukstdatoru bez uzraudzības. Pretējā gadījumā varat zaudēt datus.
- Lai nepieļautu attālu nelikumīgu ielaušanos jūsu viedtālrunī, izmantojiet paroles funkciju.

Personiskās informācijas un identitātes aizsardzība

- **Lietojiet drošu paroli.** Internetā parole ir ekvivalents jūsu mājas slēdzenei un atslēgai. Paroles nodrošina ievērojamu aizsardzību, un atbilstošu paroļu lietošana aizsargā konfidenciālu personisko informāciju un identitāti. Ar jūsu datora paroli var piekļūt visai informācijai — gan darbavietas, gan personiskajai —, ko glabājat datorā un tiešsaistes kontos. Lai aizsargātu savus datus, lietojiet drošu paroli — izmantojiet sarežģītu rakstzīmju kopumu; kombinējiet lielos un mazos burtus, ciparus un simbolus. Jo lielāka rakstzīmju dažādība ir parolē, jo grūtāk ir to uzminēt. Neizmantojiet personisko informāciju — savu vārdu, bērna vārdu, dzimšanas datumus utt. —, ko kāds jau zina vai var viegli uzzināt, un mēģiniet neizmantot vienkāršus vārdus — daži hekeri izmanto programmas, kas paroles uzminēšanai izmanto visus vārdnīcā esošos vārdus.
- **Regulāri mainiet paroli.** Ja rodas aizdomas, ka ir noticis sistēmas drošības politikas pārkāpums, nekavējoties nomainiet paroles.
- **Neizpaudiet nevienam savu paroli.** Jūsu parole ir unikāla, un jūs nedrīkstat to izpaust citiem. Kad vien tas ir iespējams, mēģiniet atcerēties savas paroles. Izdomājiet iegaumēšanas stratēģiju. Ja paroles pierakstāt, uzmanīgi izvēlieties, kur tās glabāsiet.

Neatstājiet pierakstītās paroles vietās, kur jūs neatstātu informāciju, kas ar šīm parolēm ir aizsargāta.

- **Unikāls konts, unikāla parole.** Katram tiešsaistes kontam, kam piekļūstat, izmantojiet atšķirīgu paroli (vai vismaz dažādas paroles). Ja vairākos kontos izmantojat vienu paroli, uzbrucējs, kas ir ieguvis piekļuvi vienam kontam, varēs piekļūt visiem jūsu kontiem.
- **Aizsargājiet savus kontus.** Daudzi kontu nodrošinātāji piedāvā papildu veidus, ar kuriem pārbaudīt jūsu identitāti, pirms attiecīgajā vietnē varat sākt darbu.
- **Pārvaldiet savus tiešsaistes datus.** Ja vietnē šāda opcija ir pieejama, iestatiet konfidencialitātes un drošības iestatījumus tādā informācijas koplietošanas līmenī, kas jums ir pieņemams. Vēlams noteikt informācijas koplietošanas ierobežojumus.
- **Sabiedrisko sakaru veidošanas vietnes izmantojiet piesardzīgi.** Ņemiet vērā, ka sociālo sakaru veidošanas vietnēs vienlaicīgi var pastāvēt daudzi riski, kas saistīti ar atrašanos tiešsaistē, — personas aizskaršana tiešsaistē, privātas informācijas izpaušana, kiberizsekošana, piekļuve vecumam nepiemērotam saturam un sliktākajos gadījumos arī uzmākšanās tiešsaistē un vardarbīga izturēšanās pret bērniem.

Darba informācijas aizsardzība, atrodoties ārpus darba vietas

- **Nodrošiniet konfidenciālās informācijas aizsardzību.** Kad atrodaties ārpus darba vietas, pārliecinieties, ka jūsu konfidenciālā informācija un aprīkojums nepārtraukti ir drošībā, lai nepieļautu to zādzību vai nozaudēšanu. Rīkojieties ar informāciju piesardzīgi, jo īpaši tad, ja atrodaties publiskā vietā.
- **Rūpējieties par darba informācijas konfidencialitāti.** Ņemiet vērā, ka citas personas var dzirdēt jūsu sarunas. Nepadariet savu konfidenciālo darba informāciju pieejamu citiem.
- **Ņemiet vērā, ka citas personas var iegūt informāciju, skatoties jums pār plecu.** Pasargājiet sevi no skatīšanās pār plecu, kad ceļojat vai strādājat attālināti.
- **Izmantojiet tīmekļa e-pastu piesardzīgi.** Izmantojot interneta pārlūkprogrammu e-pasta ziņojumu lasīšanai, nepieciešams ievērot tos pašus drošības pasākumus, ko ievērojat, izmantojot darbvirsmas pasta sistēmu; turklāt pastāv vēl citi papildu riski.

Savienojuma piesardzīga izveidošana

- **Pārtrauciet bezvadu savienojumus, kad tie netiek lietoti vai nav nepieciešami.**
- **Ievērojiet piesardzību, izmantojot bezvadu tīklājus.** Izmantojot bezvadu tīklājus, ierobežojiet ar darbu saistīto darbību izpildi un pielāgojiet savas ierīces drošības iestatījumus, lai ierobežotu citu personu piekļuvi jūsu ierīcei.
- **Aizsargājiet savu naudu.** Veicot bankas darījumus un iepērkoties tiešsaistē, pārliecinieties, vai vietnēs ir iespējota drošība. Izmantojiet tīmekļa adreses, kas sākas ar “https://” vai “shttp://” — tas norāda, ka vietnes veidotāji veic papildu pasākumus, lai nodrošinātu jūsu informācijas aizsardzību. Adreses, kas sākas ar “http://”, nav drošas.
- **Izvairieties no nevēlamiem e-pasta ziņojumiem.** Surogātpasts ir drošības apdraudējums. Neatveriet no nezināmas e-pasta adreses sūtītus ziņojumus un pielikumus.

- **Ja rodas šaubas, izmetiet ziņojumus atkritnē.** Ja saites e-pasta ziņojumos, sīkziņās, ziņās un tiešsaistes reklāmās šķiet aizdomīgas — pat ja zināt to avotu —, vēlams tās dzēst vai atzīmēt kā surogātpastu.
- **Pārsūtiet atbilstošus e-pasta ziņojumus.** Pirms ziņojuma pārsūtīšanas apsveriet iespēju dzēst tā vēsturi.
- **Izmantojiet internetu piesardzīgi.**
- **Nelejupielādējiet dokumentus un materiālus no neuzticamām personām.**
- **Publiski pieejamus datorus izmantojiet uzmanīgi.** Savienojumu ar publiski pieejamu datoru veidojiet tikai tad, ja jūsu ierīce var izveidot šifrētu savienojumu (to apzīmē slēdzene pārlūkprogrammas loga augšējā labajā stūrī un burti "https://" tīmekļa adreses sākumā).
- **Izmantojiet tīmekļa e-pasta pakalpojumus, ko nodrošina labi zināmi un uzticami uzņēmumi.**

Droša tīmekļa lietošana

- **Sekojiet aktualitātēm.** Iegūstiet informāciju par jauniem veidiem, kā tiešsaistē saglabāt drošību — meklējiet jaunāko informāciju uzticamās tīmekļa vietnēs, kopīgojiet to ar ģimeni, draugiem un kolēģiem un aiciniet viņus ievērot drošību tīmeklī. Padariet savu pārlūkprogrammu drošu.
- **Rīkojieties apdomīgi.** Izturieties piesardzīgi pret paziņojumiem, kuros jūs aicina rīkoties nekavējoties, izsaka neticami labus piedāvājumus, vai arī lūdz sniegt personisko informāciju.
- **Veidojiet dublējumkopijas.** Aizsargājiet savas darba, mūzikas, fotoattēlu datnes un citu digitālo informāciju, izveidojot tās elektronisko kopiju un droši to uzglabājot.