Patarimai

Šie patarimai padės jums įgyti gerus saugaus darbo internete įpročius. Ši informacija parengta bendradarbiaujant su „Get Safe Online“ (JK) ir „Department of Homeland Security“ (JAV).

- Apsaugokite savo asmeninį kompiuterį (PC) ir nešiojamuosius įtaisus
- Apsaugokite asmeninę informaciją ir savo asmens tapatybės duomenis
- Apsaugokite verslo informaciją už savo organizacijos ribų
- Jungdamiesi kompiuteriu būkite atidūs
- Išmaniai naudokitės saitynu

Apsaugokite savo asmeninį kompiuterį (PC) ir nešiojamuosius įtaisus

PC

- Naudokite užkardą. Užkardos apsaugo tinklą nuo kai kurių virusų ir programišių.
- Įdiekite antivirusinę programą. Antivirusinė programa neleidžia virusiniam užkratui išplisti jūsų kompiuteryje.
- Įsigykite naujausias saugumo programas. Pasirūpinkite, kad programos ir operacinė sistema visuomet gerai veiktų, būtų nepažeistos ir atnaujintos.
- Užkirskite kelią šnipinėjimo programoms. Nepriimkite įtartinų elektroninių laiškų ir priedų, kad pašaliniai žmonės nepatektų į jūsų kompiuterį.
- Reguliariai darykite atsargines kopijas. Apsaugokite duomenis nuo avarinių įvykių.

Skreitiniai kompiuteriai

- Atjunkite bevielį ryšį, jei juo nesinaudojate ir jis jums nereikalingas.
- Reguliariai prijunkite savo skreitinį kompiuterį prie patikimo tinklo, kad atnaujintumėte saugumo mechanizmus.
- Darykite skreitiniame kompiuteryje saugomos informacijos atsargines kopijas.
- Nepalikite skreitinio kompiuterio be priežiūros.

Atmintukai

- Naudokite šifruotuosius atmintukus.
- Nustatykite nekeičiamąją atmintuko veikseną naudodami fizinį perjungiklį, kad nepersiduotų virusai. Kai kuriuose atmintukuose yra fiziniai perjungikliai, leidžiantys nustatyti nekeičiamąją veikseną, kad iš pagrindinio kompiuterio nebūtų galima į jį įrašyti duomenų arba juos keisti.
- Nusikopijavę rinkmenas iš nepatikimo ir (arba) neoficialaus šaltinio, peržiūrėkite atmintuką, kad neperneštumėte virusų.

- Prieš prijungdami atmintuką prie kito asmens kompiuterio, ištrinkite visas operacijai atlikti nereikalingas rinkmenas.
- Atmintuke darykite atsargines kopijas, kad avarinio įvykio atveju galėtumėte atkurti informaciją.
- Atmintuką pritvirtinkite prie raktų pakabuko (virvelės), kad nepamestumėte. Kadangi atmintukai maži, juos lengva pamesti ar pavogti. Be to, kuo didesnė atmintuko talpa, tuo didesniam duomenų kiekiui gresia pavojus patekti į nepageidautinas rankas. Paprastai atmintukai nešiojami rankinėse, kuprinėse, skreitinių kompiuterių dėkluose, švarkų ar kelnių kišenėse ar paliekami be priežiūros darbo vietose. Pastaruoju metu daugėja atvejų, kai atmintukai pametami, kažkur nudedami, be leidimo pasiskolinami ar pavagiami.

Mobilieji telefonai ir delniniai kompiuteriai

Delniniai kompiuteriai, kaip antai *Windows Mobile*, *Palm*, *iPhone*, *Android* ir *Blackberry* prietaisai, turi prieigą prie interneto, ir juose galima saugoti daugybę informacijos. Kadangi jie itin lengvai nešiojami, su jais reikia elgtis ypač atsargiai.

- Jei bevielis ryšys (t. y. *Bluetooth* ir WLAN) nereikalingas, išjunkite jį. *Bluetooth* technologija leidžia elektroniniams prietaisams susisiekti trumpojo nuotolio radijo ryšiu.
- Nepalikite mobiliojo telefono ar delninio kompiuterio be priežiūros, nes galite netekti duomenų.
- Naudokite slaptažodį, kad pašaliniai neįsilaužtų nuotoliniu būdu į jūsų išmanųjį telefoną.

Apsaugokite asmeninę informaciją ir savo asmens tapatybės duomenis

- **Naudokite sunkiai atspėjamą slaptažodį.** Jūsų slaptažodis – tai tas pat, kas jūsų namų internete spyna ir raktas. Slaptažodžiai – svarbiausia apsaugos priemonė, todėl geri slaptažodžio naudojimo įgūdžiai padės jums geriau apsaugoti svarbią asmeninę informaciją ir asmens tapatybės duomenis. Jūsų kompiuterio slaptažodis – raktas, leidžiantis prieiti prie visos jūsų – tiek asmeninės, tiek darbo – informacijos, kurią saugote kompiuteryje ir interneto paskyrose. Kad apsaugotumėte duomenis, naudokite sunkiai atspėjamą slaptažodį – sugalvokite sudėtingą raidžių (didžiųjų ir mažųjų), skaičių ir simbolių kombinaciją. Kuo ženklai įvairesni, tuo sunkiau atspėti slaptažodį. Nenaudokite asmeninės informacijos, kaip antai savo ar vaiko vardo, gimimo datų ir pan., kurią kas nors jau žino arba gali lengvai gauti. Stenkitės nenaudoti dažnai vartojamų žodžių, nes kai kurie programišiai naudoja programas, kurios slaptažodį tikrina pagal kiekvieną žodyne pateikiamą žodį.
- **Reguliariai keiskite slaptažodį**. Jei įtariate, kad sistema tapo nesaugi, keiskite slaptažodį nedelsdami.
- **Niekam nesakykite savo slaptažodžio**. Jūsų slaptažodis yra unikalus ir jo nereikia niekam sakyti. Stenkitės slaptažodžius kiek įmanoma atsiminti. Sugalvokite būdą, kaip juos geriau

įsiminti. Jei slaptažodžius užsirašote, tam pasirinkite tinkamą vietą. Nepalikite užrašytų slaptažodžių ten, kur nepaliktumėte jais saugomos informacijos.

- **Unikali paskyra, unikalus slaptažodis**. Kiekvienai interneto paskyrai naudokite skirtingus slaptažodžius (arba bent skirtingus slaptažodžių tipus). Jei naudosite tuos pačius slaptažodžius, programišius, įsilaužęs į vieną paskyrą, galės prieiti prie visų jūsų paskyrų.
- **Apsaugokite savo paskyras**. Prieš suteikdami galimybę atlikti operacijas paskyros svetainėje, daugelis paskyrų teikėjų siūlo papildomus būdus jūsų tapatybei patikrinti.
- **Valdykite savo interneto ryšius**. Esant galimybei, interneto svetainėse nusistatykite sau parankias keitimosi informacija privatumo ir saugumo nuostatas. Pageidautina riboti asmenų, su kuriais dalijatės informacija, skaičių.
- **Būkite apdairūs naudodamiesi socialinių tinklų svetainėmis**. Žinokite, kad socialinių tinklų svetainėse galima susidurti su daugeliu naršant internete kylančių pavojų, kaip antai bauginimu internete, privačios informacijos atskleidimu, persekiojimu elektroninėje erdvėje, prieiga prie amžiaus grupei netinkamo turinio ir kraštutiniais atvejais vaikų viliojimu ar seksualiniu išnaudojimu.

Apsaugokite verslo informaciją už savo organizacijos ribų

- **Laikykite neskelbtiną informaciją saugioje vietoje.** Kai esate ne darbo vietoje, neskelbtiną informaciją ir įrangą visuomet laikykite saugioje vietoje, kad jos niekas nepavogtų ar jos neprarastumėte. Su informacija ypač atsargiai elkitės viešose vietose.
- **Užtikrinkite verslo informacijos konfidencialumą.** Nepamirškite, kad jūsų pokalbių gali būti klausomasi. Neleiskite, kad jūsų organizacijos konfidenciali informacija taptų prieinama visiems.
- **Saugokitės jums už nugaros žvilgčiojančių informaciją nuskaityti norinčių asmenų.** Keliaudami ar dirbdami nuotoliniu būdu, saugokitės jums už nugaros žvilgčiojančių informaciją nuskaityti norinčių žmonių.
- **Naudokitės saityno paštu išmintingai.** Naudojantis interneto naršykle elektroniniams laiškams skaityti reikia laikytis tų pačių atsargumo taisyklių kaip ir naudojantis stalinio kompiuterio pašto sistema. Be to, kyla ir kitų saityno paštui būdingų saugumo pavojų.

Jungdamiesi būkite atidūs

- **Jei bevieliu ryšiu nesinaudojate ar jis jums nereikalingas, atjunkite jį.**
- **Atsargiai naudokitės internetu viešosios interneto prieigos vietose.** Viešosios interneto prieigos vietose ribokite veiklą ir kompiuteryje nustatykite saugumo parametrus, kurie ribotų prieigą prie jūsų kompiuterio.
- **Saugokite pinigus.** Atlikdami banko operacijas ir pirkdami internetu, įsitikinkite, kad interneto svetainė yra saugi. Žiūrėkite, kad saityno adresas būtų su raidėmis „https://“ arba „shttp://“. Šios raidės rodo, kad svetainė imasi papildomų priemonių jūsų informacijai apsaugoti. „Http://“ nėra saugu.

- **Stabdykite nepageidautinus elektroninius laiškus**. Brukami elektroniniai laiškai kelia grėsmę saugumui. Neatidarykite nepažįstamų elektroninių laiškų ir jų priedų.
- **Jei abejojate, išmeskite**. Jei nuorodos elektroniniuose laiškuose, „Twitter“ tinklo žinutėse, forumų ar diskusijų žinutėse ir interneto reklamose atrodo įtartinos, geriau jas ištrinkite, nors ir žinote, kas jas atsiuntė, arba jei manote, kad tai tikslinga, pažymėkite jas kaip brukalą.
- **Persiųskite elektroninius laiškus tik tais atvejais, kai tai tikslinga**. Prieš persiųsdami elektroninį laišką, pagalvokite, ar nevertėtų ištrinti laiško ankstesnio turinio.
- **Naršydami po internetą būkite atsargūs.**
- **Neatsisiųskite dokumentų ir medžiagos iš nepatikimų šaltinių.**
- **Naudodamiesi viešaisiais kompiuteriais, būkite atsargūs.** Junkitės prie viešojo kompiuterio tik tuo atveju, jei ryšys yra šifruotas (šifruotą ryšį rodo spyna jūsų naršyklės lango apatiniame dešiniajame kampe ir tinklalapio adreso pirmosios raidės https://).
- **Naudokitės tik gerai žinomų ir patikimų įmonių teikiamomis saityno pašto paslaugomis.**

Išmaniai naudokitės saitynu

- **Sekite naujienas.** Domėkitės naujausia informacija apie saugą internete. Patikimose svetainėse ieškokite naujausios informacijos ir ja dalykitės su savo šeima, draugais bei kolegomis ir skatinkite juos išmaniai naudotis saitynu. Pasirūpinkite savo naršyklės saugumu.
- **Prieš imdamiesi veiksmų, gerai pagalvokite.** Atsargiai elkitės su žinutėmis, kuriose raginama nedelsiant imtis kokių nors veiksmų, siūloma kas nors neįtikėtinai naudinga ar prašoma asmens duomenų.
- **Darykite atsargines kopijas.** Apsaugokite savo darbus, muziką, fotografijas ir kitokią skaitmeninę informaciją darydami elektronines kopijas ir jas laikydami saugioje vietoje.