Soovitused ja nõuanded

Interneti turvaliseks kasutamiseks püüa täita järgmisi soovitusi ja nõuandeid. Jaotis on välja töötatud koos Ühendkuningriigi juhtiva internetiturbe veebikohaga Get Safe Online ja USA sisejulgeoleku ministeeriumiga.

- Kuidas kaitsta arvuteid ja nutiseadmeid?
- Kuidas kaitsta teavet ja isikuandmeid?
- Kuidas kaitsta äriteavet väljaspool ettevõtet?
- Kuidas luua turvalist ühendust?
- Ole internetis tark

Kuidas kaitsta arvuteid ja nutiseadmeid?

Lauaarvutid

- Kasuta tulemüüri: see kaitseb teatud viiruste ja häkkerite eest.
- Kasuta viirusetõrjet: see kaitseb arvutit viiruste eest.
- Kasuta alati uusimaid turberakendusi: jälgi, et rakendused ja operatsioonisüsteem oleksid korras ning ajakohased, ning kasuta alati viimaseid turbeuuendusi.
- Väldi nuhkvara: ära ava kahtlasi e-kirju ega manuseid.
- Varunda korrapäraselt: nii saab arvutist hävinud andmeid taastada.

Sülearvutid

- Lülita välja wifi, kui sa seda ei kasuta või ei vaja.
- Laadi turbeuuendusi alla ainult usaldusväärsete võrkude kaudu.
- Varunda arvutis olevad failid.
- Ära jäta arvutit järelevalveta.

Mälupulgad

- Kasuta ainult krüptitud mälupulki.
- Viirustega nakatumise vältimiseks ühenda mälupulk arvutiga nii, et mälupulk on kirjutuskaitstud. Osadel mälupulkadel on spetsiaalne kirjutuskaitse nupp. Nii ei saa arvuti, kuhu mälupulk ühendatakse, sellele midagi kirjutada ega seal olevaid faile muuta.
- Kui oled mälupulgale kopeerinud faile arvutist, mille turvalisus ei ole teada, kontrolli mälupulka kohe seejärel viirustõrjega.
- Enne kui ühendad mälupulga kellegi teise arvutiga, kustuta mälupulgalt kõik failid, mida tal vaja ei ole.
- Varunda korrapäraselt ka mälupulga faile, et neid saaks vajaduse korral taastada.

- Hoia mälupulka võtmehoidja või kaelapaela küljes: mälupulgad on väikesed ja neid on lihtne kaotada ja varastada. Mida suurem on mälupulga maht, seda rohkem andmeid võib sattuda võõrastesse kätesse. Mälupulki kantakse sageli hoolimatult käekotis, seljakotis ja taskus või unustatakse arvuti kõrvale. Mälupulkade kaotamine, unustamine, loata laenamine ja varastamine on viimasel ajal sagenenud.

Mobiiltelefonid ja pihuarvutid

Mobiiltelefonidel ja pihuarvutitel on internetiühendus ning nende mälumaht võib olla väga suur. Nendega tuleb eriti ettevaatlik olla juba sellepärast, et nad on väikesed ja mahuvad kergesti taskusse.

- Lülita välja wifi ja Bluetooth, kui neid ei ole vaja. Bluetoothi kaudu saavad elektroonikaseadmed ühenduda ka vahetult, võrku vajamata.
- Ära jäta mobiiltelefoni ega pihuarvutit järelevalveta. Nendes sisaldub palju andmeid ja teavet.
- Häkkerite tõrjumiseks kaitse nutitelefoni salasõnaga.

Kuidas kaitsta teavet ja isikuandmeid?

- **Kasuta tugevat salasõna**: salasõna toimib internetis samamoodi nagu lukk koduuksel. Salasõna pakub head kaitset nii failidele kui ka üldse teabele ja isikuandmetele. Arvuti salasõna kaitseb kõike sinu arvutis ja selle kaudu internetikontodel olevat teavet, nii sinu enda kui ka ettevõtte oma. Kasuta tugevat salasõna, milles on läbisegi eri märke – suur- ja väiketähti, numbreid ja sümboleid. Mida rohkem on salasõnas eri märke, seda raskem on seda muukida. Ära kasuta salasõnas isikuandmeid, näiteks enda või lapse nime või sünniaega: neid võib teada või teada saada ka keegi muu. Väldi ka keeles olemasolevaid sõnu: häkkerid võivad kasutada salasõnade muukimiseks programme, mis proovivad läbi sõnaraamatu kõik sõnad.
- **Muuda salasõna korrapäraselt**: kui arvad, et sinu arvutisse on sisse tungitud, muuda salasõna kohe.
- **Hoia salasõna salajas**: sinu salasõna kuulub ainult sulle ja seda ei tohi öelda kellelegi. Kui vähegi võimalik, jäta salasõnad meelde, mõeldes selleks välja mingi süsteemi. Kui kirjutad salasõna üles, siis ole ettevaatlik: ära hoia üleskirjutatud salasõna sellega kaitstava teabe lähedal.
- **Igal kontol olgu oma salasõna**: igal sinu internetikontol olgu oma salasõna või vähemalt kasuta mitut. Kui mitmel kontol on sama salasõna, võib juhtuda, et ühe salasõna äraarvamisel saab sissetungija kohe juurdepääsu ka kõigile teistele kontodele.
- **Turva kontosid ka teistmoodi**: veebilehtedel võib olla peale salasõna ka muid viise, kuidas tõendada, et sina oled sina. Kasuta neid.

- **Ole internetis iseenda peremees**: internetti ühendudes ja seal suheldes kasuta sulle sobivaid privaatsus- ja turbeseadeid. Soovitatav on piirata nende inimeste arvu, kellega teavet vahetad.
- **Ole sotsiaalvõrgustikes ettevaatlik**: nendes on korraga koos paljud internetiohud – kiusamine, isikliku teabe avaldamine, jälitamine, lastele sobimatu teave ning äärmuslikel juhtudel ka lastega seksuaalse kontakti otsimine ja nende ahistamine.

Kuidas kaitsta äriteavet väljaspool ettevõtet?

- **Jälgi, et tundlikud andmed oleksid kaitstud**: väljaspool ettevõtet viibides jälgi, et tundlik teave ja sellega seadmed oleksid varguse või kaotuse ärahoidmiseks alati kaitstud. Ole eriti ettevaatlik, kui käsitled teavet avalikes kohtades.
- **Hoia äriteave konfidentsiaalne**: jälgi, et keegi pealt ei kuulaks. Jälgi, et ettevõtte konfidentsiaalne teave ei tuleks avalikuks.
- **Hoidu pealtvaatajate eest**: reisil või avalikus kohas töötades pea silmas, et keegi sind ei jälgiks.
- **Veebimeili kasutades ole ettevaatlik**: veebimeiliga tuleb olla sama ettevaatlik kui tavalise e-posti programmiga. Lisaks on veebimeilil omad turvariskid.

Kuidas luua turvalist ühendust?

- **Lülita välja wifi, kui sa seda ei kasuta või ei vaja**
- **Ole avaliku wifiga ettevaatlik**: tee turvamata wifi-võrgus ainult hädapäraseid toiminguid ja kasuta seadme kaitsmiseks rangeid turvapiiranguid.
- **Kaitse oma raha**: internetipangas ja internetipoes kontrolli, kas selle veebileht on turvaline. Kui veebiaadressi alguses on „https://" või „shttp://", kasutab veebileht täiendavaid turbemeetmeid. Kui aadressi alguses on „http://", on veebileht ebaturvaline.
- **Kaitse end soovimatute e-kirjade eest**: rämpspost võib olla ohtlik. Tundmatutelt aadressidelt tulnud e-kirju ja nende manuseid ära ava.
- **Kahtluse korral kustuta**: kui e-kirjas, sõnumis ja postituses olev link või veebilehel olev reklaam tundub kahtlane, kustuta see otsekohe, kui võimalik, või märgista rämpspostina, isegi kui saatja on sulle teada.
- **Saada saabunud e-kirju edasi ainult siis, kui seda on tingimata vaja**. Kui uus saaja ei pea teadma, kellelt e-kirja said, kustuta varasemate saatjate andmed.
- **Ole internetti kasutades ettevaatlik.**
- **Ära laadi alla dokumente ega faile kahtlastelt veebilehtedelt.**
- **Avalikke arvuteid kasutades ole ettevaatlik:** avalikus arvutis mine internetti ainult juhul, kui ühendus on krüptitud – seda näitab tabalukusümbol brauseriakna servas ja „https://" veebiaadressi alguses.
- **Kasuta ainult tuntud ja usaldusväärsete pakkujate veebimeili.**

Ole internetis tark

- **Hoia end kursis:** loe internetiturvalisuse uudiseid, mida avaldavad usaldusväärsed veebilehed. Jaga loetut pereliikmete, sõprade ja töökaaslastega ning julgusta ka neid kasutama internetti targasti. Muuda brauser turvaliseks.
- **Enne tegutsemist mõtle**: mõtle hoolikalt järele, enne kui reageerid teadetele, mis käsivad tegutseda kohe, pakuvad midagi uskumatut või küsivad isikuandmeid.
- **Varunda**: failide, muusika, fotode jt kaitsmiseks varunda neid korrapäraselt ning hoia varukoopiaid turvalises kohas.