10 näpunäidet IT-vaatlik olemiseks

1

Uuenda seadmeid ja rakendusi

Kui nutiseade või arvuti pakub võimalust uuenduseks, tee seda esimesel võimalusel. Usaldusväärsed teenusepakkujad arendavad enda riist- ja tarkvara kasutajamugavuse või turvalisuse parendamiseks pidevalt. Uuenduste edasilükkamine jätab küberkurjategijatele avatuks turvaaugud, mis muudavad sind küberrünnakutele haavatavaks.

2

Kasuta erinevaid paroole

Tugevate paroolide kasutamine muudab sinu parooli varastamise küberkurjategijale keeruliseks, kuid paraku pole parooli lekkimine kunagi täielikult välistatud. Erinevate paroolide kasutamine tagab, et küberkurjategija ei pääse kerge vaevaga sisse sinu erinevatele kontodele.

3

Veendu, et sinu paroolid on tugevad

Hea parool on pikk (vähemalt 15 tähemärki), kerge meelde jätta, kuid raske ära arvata. See peaks sisaldama suur- ja väiketähti, numbreid ning mõnda erisümbolit (näiteks &, % või ?).

4

Ära jaga enda paroole ega sisesta neid kahtlastel veebilehekülgedel

Sinu parool jäägu vaid sulle teadmiseks. Avalikult jagatud parool võib sinu teadmata hakata elama oma elu ja tekitada suuri kahjusid. Parooli sisestamine kahtlastel veebilehekülgedel võib olla küberkurjategija lõks, millega sinu parool välja petta, et seda erinevates keskkondades sisselogimiseks testida.

5

Rakenda e-posti kontodel mitmeastmelist autentimist

Mitmeastmeline autentimine teeb küberkurjategijale sinu kontodele ja seeläbi andmetele ligipääsemise oluliselt keerulisemaks, sest sunnib kurjategijat korduvalt tõestama, et tegemist on sinuga. Mitmeastmelise autentimise seadistamine on lihtne ja selle kasutamine aitab ennetada suurt osa küberrünnakutest.

6

Väldi tundmatuid manuseid ja linke

Tundmatute failide ja linkidega levib sageli pahavara, millega krüpteeritakse ära seadme sisu selliselt, et ligipääs olulistele kaustadele või andmetele peatub. Enne failide avamist või linkidele klikkimist veendu nende turvalisuses otsingumootoreid kasutades või IT-spetsialistiga nõu pidades.

7

Kontrolli tähelepanelikult kirja saatja aadressi

E-posti saatja nime võltsimine on lihtne, aadressi võltsimine veidi keerukam. Enne postkasti saabunud kirjale vastamist kontrolli tähelepanelikult, kas kirja saatja aadress on korrektne ega sisalda kummalisi laiendusi. Kahtluse korral küsi nõu IT-spetsialistilt või teenusepakkujalt.

8

Tee regulaarselt andmetest ja failidest koopiaid

Keegi meist pole lõpuni kaitstud arvuti katki minemise, varguse, tarkvara rikke või lunavara ohvriks langemise eest. Loo endale välisest kõvakettast või mälupulgast arhiiviketas, kuhu tõstad regulaarselt kõige olulisemaid andmeid ja faile. Selliselt toimides saad olla kindel, et ligipääs tähtsale teabele säilib ka ootamatuste ilmnemisel.

9

Tutvu levinumate küberrünnakutega

Levinumad küberintsidendid on IT-vaatliku inimese jaoks üldiselt tuvastatavad. Nende tundmine aitab ennetada oluliste andmete lekkimist, kaustadele ligipääsu blokeerimist ja meilikontode üle võtmist, mis halvab nii era- kui ka tööelu. Levinumate küberrünnakutega saad tutvuda veebilehekülje[l www.itvaatlik.ee](http://www.itvaatlik.ee)

10

Selgita välja, kelle poole pöörduda küberrünnaku korral

Küberrünnakute lahendamise tõhusus sõltub neile reageerimise kiirusest. Uuri, keda kolleegidest küberjuhtumitest koheselt teavitada. Selgete protseduurireeglite olemasolu aitab küberrünnakuid ennetada ja neile vajadusel efektiivselt reageerida.

itvaatlik.ee

Euroopa Liit
Euroopa Regionaalarengu Fond

Eesti tuleviku heaks