Teadlane soovitab: 10 käsku küberohtude ennetamiseks

7 aastat tagasi - 21.01.2019 Autor: AM

Küberkurjategijad on huvitatud igaühest, kelle kohta leidub veebis andmeid ja kes kasutavad nutiseadmeid. TalTechi küberjulgeoleku nooremteadur ning kutsekoolinoorte digiprogrammi Samsung Digi Pass koolitaja Tiia Sõmer reastas küberturvalisuse kümme käsku, mis aitavad end pahatahtlike huviliste eest paremini kaitsta.

Maailmapanga andmetel on internetivõrguga ülemaailmselt seotud umbes 12,5 miljardit seadet – eelkõige arvutid ja telefonid, kuid ka muud „vidinad" nagu külmkapid, kohvimasinad või nutipirnid.

Riigi infosüsteemi ameti kinnitusel toimib Eestis üle 90% pangandusest internetis ja üle 90% tuludeklaratsioonidest täidetakse veebis. Allkirjastamiseks ja krüpteerimiseks kasutatakse ID-kaarti. Kui räägime internetimaailma kaitsmisest, siis räägime tegelikult enda e-eluviisi kaitsmisest.

Kübermaailm on igapäevaeluga tihedalt läbi põimunud. Kasutame arvutit ja nutiseadet pangatehinguteks, suhtleme ametiasutustega, säilitame veebis fotosid-dokumente, käime e-valimas. Me ise paneme kõik andmed enda kohta veebi üles: piltlikult öeldes koduvõtmed, rahakoti, dokumendid ja päevakava.

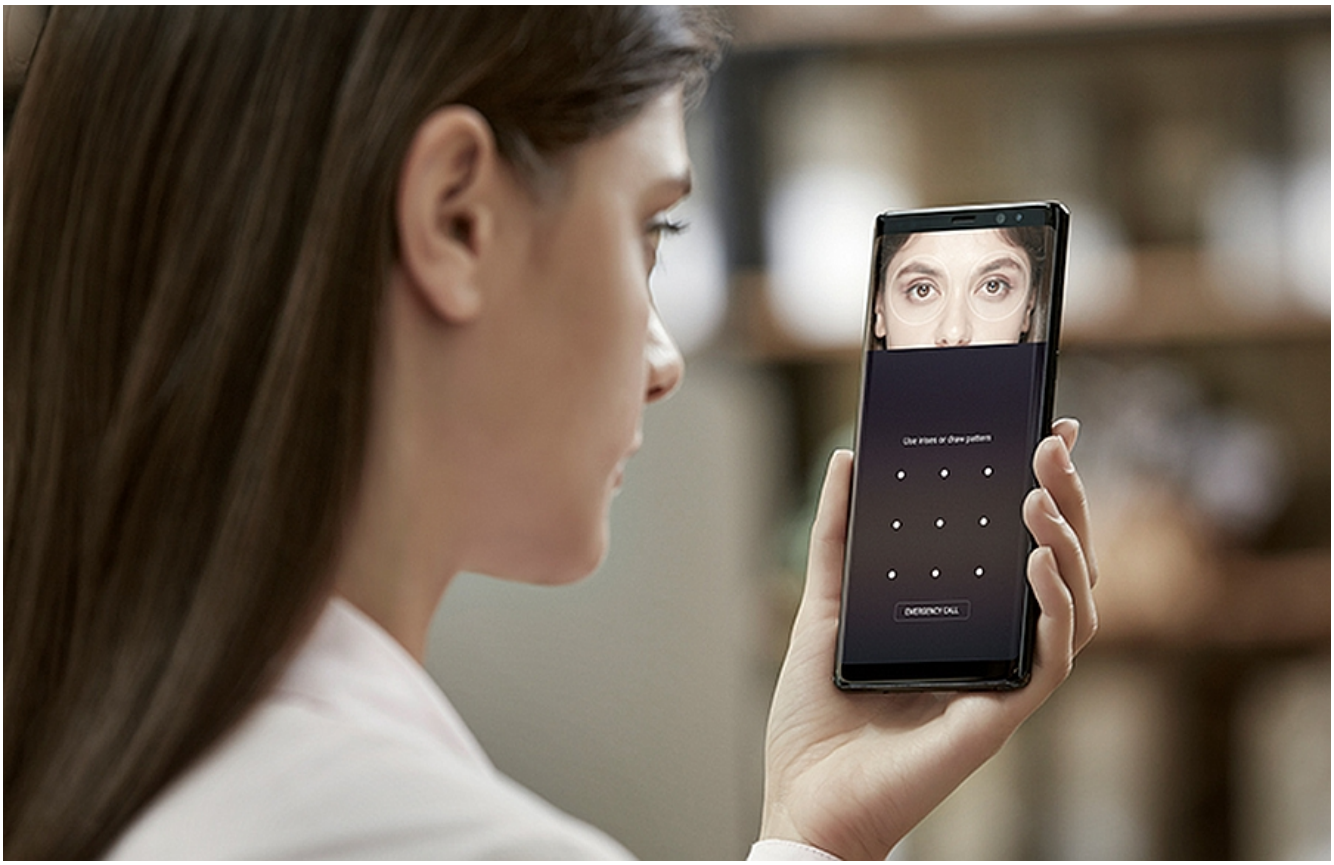
Kõik selle võib kurjategija enda kasuks pöörata, rõhutab kutsekoolinoorte digioskuste programmi Samsung Digi Pass koolitaja, TalTechi küberjulgeoleku nooremteadur Tiia Sõmer. Seepärast on teadlase sõnul oluline kinni pidada elementaarsetest küberhügieeni reeglitest: uuendused peavad olema tehtud ning salasõnad turvalised ja eri kontodel erinevad.

„Kübermaailm, milles elame ja töötame, on pidevas muutumises. Meie tegevus on väga suures sõltuvuses infotehnoloogiast ning igapäevane küberhügieen on sama oluline kui lihtsalt hügieen – oluline on probleeme ennetada," selgitas Sõmer.

Küberjulgeoleku nooremteaduri kinnitusel on kõige nõrgem lüli kahtlemata kasutaja, mitte seade. Meil võib olla kõige uuem tehnoloogia, tulemüürid või viirustõrjed, kuid lõpuks on pahatihti inimene see, kes kusagile klikib ja probleemid majja toob. Üle 90% rünnakutest toimub inimeste, mitte tehnoloogia

vastu.

Sõmer soovitab igaühel koostada kümnele punktile mõeldes oma tegevuse „küberaudit” mõistmaks, kui palju meie tegevustest toimub veebis, kui turvaliselt käitume ja millised ohud kus varitsevad. Selleks on vaja läbi mõelda, missugust infot me kuskil hoiame, mis on selle väärtus, kui palju aega või muid ressursse kulub nende kadumisel taastamisele, või mis juhtub kui see info kuskile kaob. Kui mitmete asjade kohta saab arvutada varalist kahju, siis on palju ka sellist, mille kadumisel on suur emotsionaalne väärtus.



1. Ole tähelepanelik

Pööra tähelepanu e-kirjade manuste laienditele, saatja aadressile, linkide ja veebilehtede aadressidele. Mõtle hetkeks ja alles siis kliki!

2. Uuendused, uuendused, uuendused

Süsteemi uuendused on nii arvutile kui nutiseadmele tegelikult kõige lihtsam, kuid üliolulinе kaitsemehhanism, mida igaüks saab oma turvalisuse tagamiseks teha. Need ei maksa mitte midagi ning nende tegemine on ühe kliki kaugusel. Uuendused võimaldavad ära hoida suure osa süsteemidevastaseid ründeid, mille käigus võib kaotada oma seadmes leiduvat.

3. Kasuta erinevaid ja tugevaid salafraase

Salasõnadest ja -fraasidest räägitakse söögi alla ja söögi peale, kuid siiski murtakse maailmas sadu tuhandeid salasõnu iga päev. Statistiliselt on enimkasutatavad paroolid ikka veel 123456, password, admin või qwerty. Lisaks sellele, et turvaline salasõna peaks koosnema suurtest ja väikestest tähtedest koos kirjavahemärkide ja numbritega, on veel mõned olulised nipid.

Ära kasuta kergesti äraarvatavaid sõnu, endaga seotud infot (telefoninumbrid, isikukoodid, nimed) ega klaviatuuril järjestikku asuvaid sümboleid. Kõige tüüpilisem turvarisk on see, et kasutatakse sama salasõna erinevatel kontodel. Kui aga keegi saab ligi juba ühele kontole, katsetab ta võimalikke muid kontosid ja sama parooliga on neile sisse häkkimine juba väga lihtne. Hea uudisena on uuematel nutitelefonidel juba olemas turvalisemad lahendused nagu sõrmejäljelugeja, näotuvastus ja iiriseskanner.

4. Kasuta erinevaid e-posti kontosid

Soovitatav on teha endale mitu e-posti aadressi – ühega ajad igapäevaseid asju, teisega suhtled sõpradega, kolmandaga registreerid end eri keskkondadesse. Rusikareegel on see, et töö- ja kooliasju ajada ametliku e-posti aadressiga ning isiklikke asju isiklikult kontolt. Kui isikliku kontoga midagi juhtub, ei laiene see automaatselt töö- või kooli süsteemidesse.

5. Varunda oma andmed (*backup*)

Mõtle, mis juhtub, kui sinu arvutis või muus seadmes olev info jäädavalt kaob. Infokao või küberrünnakute ja lunavaranõuete vältimiseks on oluline omada varukoopiaid oma andmetest. Seejuures on soovituslik omada vähemalt ühte failide koopiat, mis asub füüsiliselt sinu seadmest eemal ning mida regulaarselt uuendad. Kui lunavara rünnakute puhul seade krüpteeritakse ja küsitakse selle avamiseks raha, siis võib oma andmed kätte saada, aga ei pruugi (ka selle kohta on näiteid).

6. Ära jaga isiklikke andmeid kergekäeliselt

Kõik, mida näiteks sotsiaalmeedias enda kohta jagada, on avalik info, ning lihtsa guugeldamisega võib igaühe identiteedist tervikpildi kokku saada. Isiklike andmete kergekäelise jagamisega kaasnevaks ohuks on aga identiteedivargus. Enda kaitsmiseks kasuta „minimaalsuse põhimõtet” ehk jaga nii vähe infot, kui võimalik ja vajalik. Tutvuda tasub ka isikuandmete kaitse seadusega.

7. Kontrolli, kes ja kus su andmeid kasutavad

Hoia oma seadmetel silm peal – mõtle läbi, kuhu salvestad oma andmed ning kellel on neile ligipääs. Samuti tasub eri keskkondadesse registreerimisel kontrollida, milliseid andmeid üldse soovid jagada. Mobiilirakenduste installeerimisel vaata, millele rakendus ligipääsu soovib, ning küsi endalt, milleks seda vaja on. Mõtle, kas taskulambil on tõesti vaja ligipääsu sinu kontaktidele, sotsiaalmeediale või muule?

8. Kasuta viirustõrjet

Viirustõrje eesmärk on kaitsta süsteemi pahavarasse nakatumise eest ning hea viirustõrje peab kinni enamiku ohtudest. Siiski, kunagi ei tasu kasutada mitut viirustõrjetarkvara korraga, kuna need võivad hakata üksteist segama.

9. Krüpteeri oma andmeid

Krüpteerimist on vaja turvalisuse tagamiseks ning krüpteerida võiks nii olulisi isikuandmeid kui kõike muud, mida pead tähtsaks. Krüpteerima peaks sealhulgas sensitiivseid andmeid e-kirjavahetuses, lihtsaim ja kättesaadavaim viis selleks on kasutada ID-kaarti.

10. Hari ennast

Palju harivat infot küberturvalisusest leiab ka eestikeelsena. Näiteks on head infoallikad riigi infosüsteemi ameti blogi ja andmekaitse inspektsiooni koduleht. Igapäevaseid uudiseid edastavad portaalidki kajastavad küberhügieeniga seonduvat ning aitavad kiirelt muutuva teemaga kursis olla.

Kokkuvõtteks on oluline saada aru riskidest ning mõelda, mis võivad olla tagajärjed ning mida saame ise ette võtta nende maandamiseks.

- Uudised
- Turvalisus

Pilt

