Petturid ei maga: 10 lihtsalt nõuannet isikliku küberturvalisuse tagamiseks

3 aastat tagasi - 13.11.2022 Autor: AM

Hea küberhügieen on tänapäeval peaaegu sama tähtis kui kätepesu. Nii ongi hea kasutada mõnesid näpunäited, kuidas tagada enda kontode ja seadmete turvalisus ning kuidas märgata meid ümbritsevaid küberohte.

Petturid, kes veebis varitsevad võivad olla igas vanuses, tegutseda üksi või mitmekesi, nii Eestis kui välismaal, kuid sõltumata profiilist on igaühel neist tekkinud osavus inimesi pettuse õnge püüda. Ohvreid ei valita pikalt.

Mida saab teha tavaline inimene, et kaitsta end igapäevaselt küberohtude eest?

Elisa infoturbejuht **Mai Kraft** toob välja kümme lihtsat soovitust, mida järgides saab igaüks turvalisemalt küberruumis liigelda.

1. Kasuta erinevaid ja tugevaid salasõnu ning rakenda mitmetasemelist autentimist

Samade paroolide kasutamine erinevatel veebilehtedel või teenustes ei ole hea praktika. Teateid mõne foorumi, veebilehe või teenuse andmete lekkest laekub igakuiselt ning kui pahalaste kätte satuvad mitmete kasutajate e-mailid ning salasõnad, on võimalik nendega siseneda juba teistele veebilehtedele.

Samuti on oluline, et veebikeskkondades, kus võimalik, oleks rakendatud mitmetasemeline autentimine, mis tähendab, et lisaks kasutajatunnuse ja parooli sisestamisele on vajalik kinnitada sisselogimine, kas kasutades spetsiaalset rakendust (nt *Authenticator*), sisestades SMSiga tulnud kood või kasutades mõnda muud faktorit.

2. Muuda salasõnu tihti ja hoia neid ainult enda teada

Paroole tuleb uuendada regulaarselt mitmel põhjusel ja seda eriti, kui mitmes keskkonnas kasutatakse samu paroole. Salasõnade vahetamine piirab pahalaste ligipääsu kontodele ja ei luba kasutada mõnda teise arvutisse salvestatud salasõnu. Samuti võiks salasõnu vahetada siis, kui kahtlustad või avastad arvutist mõne pahavara.

3. Kontrolli hoolega kas veebileht, kuhu sisse logid, algab „https:“ tähekombinatsiooniga ning kas veebiaadress on korrektne

Turvalise ühenduse (https: algusega) puhul toimub andmevahetus kasutaja ja veebiserveri vahel kõrvaliste isikute jaoks loetamatul kujul ning ühendus on kaitstud erinevate rünnakute eest. Tihti püüavad aga petturid veebis kasutada ära inimeste tähelepanematust ja pealtnäha igapäevaselt külastatav veebileht on tegelikult libaleht, mille aadress ja ülesehitus näeb kohutavalt sarnane välja originaalile. Proovides sinna sisse logida, saavad pahalased sinu konto e-maili, kasutajanime ja parooli teada ning saavad juba seeläbi päris veebilehel sisse logida.

4. Avalikes või ühiskasutuses olevates seadmetes kasuta alati privaatset lehitsemist ehk inkognito režiimi ning kasutuse järgselt logi oma kontodest välja ja sulge brauseri aknad

Võimalusel hoidu üldse avalike seadmete kasutusest.

Tänapäeval tuleb iga interneti brauser privaatse lehitsemise funktsiooniga, mis ei salvesta sirvimisajalugu, küpsisefaile, lehtede andmeid ega vormidesse sisestatud teavet. Kunagi ei saa aga olla kindel, kes on ühiskasutatavaid seadmeid varem kasutanud, kui turvalised need on või kes neid haldab. Seetõttu peaks vältima ka antud seadmetesse sisselogimist, kui olukord seda just ei nõua.

5. Hoia oma isiklikud andmed ainult enda teada

Sotsiaalne häkkimine on üks enim levinumaid viise, kuidas kellegi andmete kaudu kontodele ligi saada. Inimeste vastu tuntakse huvi nii, et teine pool ei pruugi sellest arugi saada ja kui veebileht kasutab konto või parooli taastamiseks isikliku turvaküsimust, on võimalik seeläbi mõni kasutajakonto enda valdusesse võtta.

6. Hoidu kahtlaste või tundmatute manuste ja linkide avamisest

E-kirjade teel levib pahavara iga sekundis miljoneid. Enamasti on need täiesti tundmatutelt saatjatelt ja pakuvad tasuta lõunaid, mida pole olemas. Kavalamad petturid võivad saata aga e-kirja mõne sõbra või tuttava nimega, paludes näiteks vaadata, kas just sina oled manuses olevas videos. Alati tasub üle küsida, millega tegu ja vaadata täpselt üle, kas e-kiri tuli ikka sõbra aadressilt.

7. Kasuta oma nutiseadmetes viirusetõrjet

Viirusetõrje või pahavara otsiv tarkvara on alati hea abimees igas olukorras. Enamik arvuteid tuleb juba täna mõne tarkvaraga, mis otsib su arvutist kahtlasi või pahavarast nakatunud faile ning teavitab leidudest kasutajat. Viirusetõrje saab paigaldada ka nutitelefonile.

8. Aktiveeri nii arvutis kui nutiseadmes automaatne tagavarakoopiate tegemine

Tagavarakoopiad aitavad pahavara või krüptoviirusesse nakatumise korral ja võimaldavad andmeid kaotamata taastada arvuti või nutitelefoni nakatamata seisu. Lisaks kaitseb see ka andmeid juhul, kui nutitelefon peaks kaduma või õnnetuses hävima.

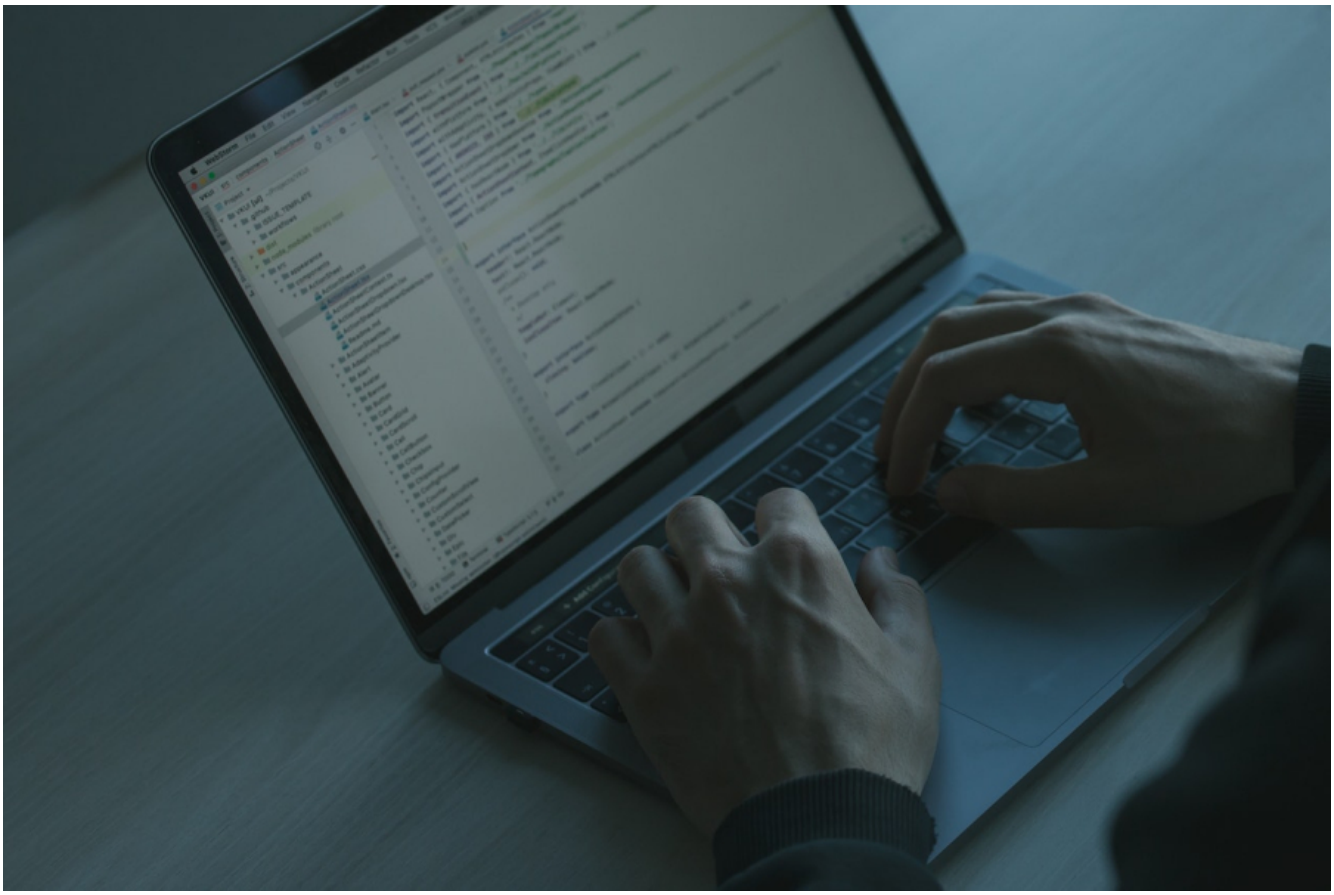
9. Ära lükka uuendusi edasi ja hoia seadmed ajakohasena

Regulaarsete tarkvarauuendustega tõuseb iga seadme turvalisus. Seadmete tarkvaranõrkuste leidmine on järjepidev protsess ja seeläbi parendab tootja oma tarkvara turvalisust. See võib tunduda küll jube tüütu, aga võib kaitsta sind võimalike riskide eest.

10. Kasuta uute rakenduste allalaadimiseks ainult ametlike poode

Ametlike partnerite tarkvarapoodidel on üldjoontes ette määratud protsess läbi mille saab tarkvara seal kasutajatele kättesaadavaks. See tähendab, et igal petturil pole võimalik oma pahavara sinna ülesse riputada. Loomulikult leidub erandeid, mida aeg-ajalt ka avastatakse, kuid alati peaks jälgima ka soovitud rakenduse hinnangut ja varasemat allalaadimiste arvu.

- Uudised
- Lahendused

- Turvalisus

Pilt