Turvaline aasta küberruumis: kuidas võrgus ilusasti osta ja oma andmeid kaitsta

10 aastat tagasi Autor: AM

Et järgmisel aastal skimmeriga raha pihta ei pandaks ega küberruumis arvet pahalased ei tühjendaks, selleks polegi palju vaja, et end esmatasandil turvata. Siin on mõned nõuanded ja vahendid, et end ise aidata. Kui aga mõni suur valitsusasutus tahab piiluda isiklikku telefoni või arvutisse, siis ei pruugigi muud väga head rohtu olla, kui käituda viisakalt ja/või netist loobuda. Nõuanded on kasperskylt, Briti valitsuselt, AM arhiivist ja Arvutikaitse.ee-st.

Mida teha, et meid pealt ei kuulataks?

Esiteks, hea kodanik – suhtle oma rahvasaadikuga, küsi sellel teemal tulevikuplaanide kohta! Facebooki, Gmaili ja muid sarnaseid teenuseid kasutades arvesta, et kõik, mis liigub läbi Ameerika serverite, jääb sealse jurisdiktsiooni alla ja Ameerika valitsusel pole meie kui välismaalaste suhtes palju kohustusi. Kuna Eesti on väike ja sigadused kipuvad kiiresti välja tulema, siis tasub kohalikke teenusepakkujaid ning võrke usaldada rohkem kui ookeanitaguseid. Avatud lähtekoodiga tarkvara on ka üldiselt nuhkimiskindlam, sest nende koodi saab vajadusel ise kontrollida või lasta kontrollida.

Kuidas näha, kes meid kuulab?

Ega kõigi nuhkijate kohta ei saagi teada, aga seda, kuhu mingit veebi külastades andmed saadetakse, saab mingil määral kindlaks teha küll (ja vajadusel ära keelata). Üks hea tööriist on Disconnect.me, mis analüüsib lisaks reklaamidele ka sotsiaalvõrke, analüütikat, kahltaseid lehekülgi ja ebasoovitavat sisu. Otsida saab jälgi jätmata ning veebide külastamine läheb peaaegu kolmandiku võrra kiiremaks, kuna koduleht ei korja ja ei saa da igale poole kasutajainfot, nagu tavaliselt.

Kontrolli, kellelt ostad

Internetipoe koduleht võib osutuda võltsituks: seda võivad kasutada kurjategijad, et saada infot ostja pangakaartide kohta. Ostes veebist, tuleb kontrollida tarnija kontaktinfot ja füüsilist aadressi juhuks, kui peaks tekkima probleem raha ülekandmise või pangakontoga.

Hüpikakende teateid tuleks ignoreerida, eriti juhul, kui nende kaudu päritakse pangakaardiandmeid. Ainult petturite lehed küsivad infot otsesuhtluse või e-posti vahendusel.

Kasuta turvalisi salasõnu

Lihtne salasõna on häkkerile kerge saak, selle lahtimuukimine ei maksa neile midagi. Selleks, et mitte lasta kurjategijaid oma veebikontodele ligi, peab kasutama eri allikates erinevaid salasõnu. Juba on hulk juhtumeid, kui mõne tuntud teenusepakkuja (nt Adobe) salasõnad on pahategijatele lekkinud ning varem või hiljem hakatakse neid katsetama ka teistes veebides, sest pahatihti on kasutajatel harjumus logida sama salasõnaga sisse kõikidesse teenustesse.

Mõned lihtsad nõuanded, kuidas salasõna valida

- Ära kasuta salasõnana oma sünnikuupäeva, kodulooma nime vms – seda infot on lihtne välja uurida või ära arvata.
- Ära vali parooliks sõnu, mida saab leida igast sõnaraamatust. Selliseid salasõnu on lihtne tarkvara abil lahti muukida.
- Tuleta keeruline salasõna mnemoonilise lause või fraasi põhjal. Selline sõnajada jääb paremini meelde kui suvalistest sümbolitest parool ja tänu sellele ei pea seda üles kirjutama. Salasõna moodustamiseks vali välja tuntud lause ja kasuta näiteks selle iga sõna esimest tähte. Näiteks lausest „Päkapikk, päkapikk, küll sa oled imelik!" saab moodustada sõna „ppksoi" (nüüd ei maksaks muidugi hakata massiliselt seda näidet kasutama, vaid ikka midagi muud).

- Kasuta salasõnas nii suuri kui ka väikeseid tähti.
- Kombineeri tähti, numbreid ja märke.

Veendu, et tehing on krüpteeritud ja isiklikud andmed kaitstud

Paljud kodulehed kasutavad info krüpteerimiseks infoturbeprotokolli SSL (ingl *secure sockets layer* – turvasoklite kiht). Kontrolli, et veebiaadressi rea alguses oleks märgijada ″https://" (mitte lihtsalt "http://") ning et seal oleks ka kinnise tabaluku ikoon (veebiaadressi real paremal või vasakul või siis lehitseja akna alumises osas).

Enne, kui sisestada netipoe lehele isiklikku või finantsinfot, võiks võtta aega, et tutvuda lehe konfidentsiaalsuspoliitikaga ning aru saada, kuidas isiklikku infot säilitatakse ja kasutatakse.

Kasuta veebis ostlemiseks eraldi pangakaarti

Veebioste tasub teha eraldi pangakaardiga, mille krediidilimiit on väike. See teeb ostja petturite ees vähem haavatavaks ja aitab raha säilitada.

Uuenda regulaarselt oma arvuti tarkvara

Kindlasti paigalda viirusetõrje, mille signatuuride andmebaas on uuendatav. See aitab kaitsta arvutit viiruste ja troojalaste eest, mis varastavad olulist finantsinfot. Paigalda aegsasti ka kõik süsteemi paigad ja uuendused kõikidele lehitsejatele ning tihti kasutatavatele lisarakendustele. See puudutab kõiki rakendusi – alustades Adobe Flash Playerist ja PDF Readerist ning lõpetades Java ja iTunesiga.

Paljud operatsioonisüsteemid ja rakendused pakuvad ka automaatset uuendamist. Kui niisugune võimalus on olemas, tuleks see aktiveerida.

Jälgi oma pangakonto jääki, et vastuolusid aegsasti märgata

Pea arvestust oma ostude üle, säilita tellimuste kinnitused ja võrdle neid oma pangakonto väljavõtetega. Vastuoludest teavita viivitamatult oma panka.

Head aastavahetust ja turvalist uut aastat!

FOTO: ISTOCKPHOTO

- Lahendused
- Turvalisus