Kuidas luua meeldejääv ja unikaalne salasõna ning seda turvaliselt hoida?

6 aastat tagasi - 20.01.2020 Autor: AM

Kasutaja tuvastamiseks on endiselt salasõnad veel enimlevinud viisiks. Samas on need ka küberkriminaalide lemmiksihtmärgiks, sest kontodega on mõnikord seotud ka pangakaardid või muud tähtsad isikuandmed, millega annab palju kurja teha. Elisa ärikliendiüksuse juht jagab mitu head nippi, mida tasub järgida salasõnade genereerimisel ja meeles pidamisel.

Turvaliste ja meeldejäävate salasõnade genereerimine on teinekord üsna vaevanõudev tegevus ning paraku ei jää need kõik hiljem meelde. Nii kiputakse minema kergemat teed ja kasutatakse lihtsaid paroole ning kasutatakse eri kohtades sama salasõna. Elisa ärikliendiüksuse juht Margus Vaino jagab mitu head nippi meeldejäävate salasõnade moodustamiseks ja turvaliseks hoiustamiseks. Kes teavad, nendel on hea seda kõike jälle meelde tuletada.

Turvaline parool on pikk parool

Hea parool ei tohi olla lihtne ega kergesti äraarvatav. Turvaline parool peaks olema võimalikult pikk ning sisaldama nii suuri ja väikseid tähti, numbreid, sümboleid ja olema vähemalt 12-14 tähemärki pikk. Internetis ja arvutites kasutatavad salasõnad peaksid alati olema võrdlemisi keerukad ja väga rasked äraarvamiseks.

Lühike parool on palju haavatavam nn “toore jõu” (inglise keeles *brute force*) rünnakuga, kus parooli üritatakse ära arvata lihtsalt erinevaid kombinatsioone järjest läbi proovides. Sellise rünnaku korral alustatakse kõigepealt populaarsemate paroolide proovimisega. Kui salasõna pole ükski nendest, siis hakatakse järjest proovima erinevaid tähekombinatsioone.

Moodusta paroole lause meetodiga

Üks meeldejäävamaid viise paroolide moodustamiseks on n-ö lause meetod. Selle meetodi järgi moodustatud parooli saab kohandada sõltuvalt veebilehest või rakendusest, kuhu kasutaja luuakse ja nii püsib see ka paremini meeles. Näiteks kui lood kasutajat sotsiaalmeediasse, siis mõtle endale välja lause, kus oleks sees antud veebilehe nimi, mõned numbrid ning vali, mis sõnad algavad suure

algustähega.

Näiteks *Minu üliSalajane SotsiaalMeedia faceBook parool 02.detsember*.

Sellest lausest võtame kõigi sõnade esimesed ja suured tähed ning saame kokku **MüSSMfBp02.d**, mis moodustabki üsna hea ning keerulise parooli, mis on 12 tähemärki pikk. Loomulikult võivad lause osad olla erinevad ning igaüks saab koostada nii parooli, mis on täiesti unikaalne, kergemini meelde tuletatav ja mis peamine – raskem ära arvata.

Näiteks võib luua Swedpanga jaoks parooli *Minu üliSalajane SwedPanga internetiPanga parool 02.detsember* ja Luminori panga jaoks *Minu üliSalajane Luminor Panga internatiPanga parool 02.detsember*, mis annavad erineva parooli, aga mida on lihtsam meeles pidada.

Ühe ettevõtte seminaril kõneledes tõin välja selle sama näite, kuid fraasiks oli Mina olen Väga Ilus tüdruk. Hiljem selgus, et arvestatav osa naistest võttis selle fraasi kasutusse, mis pole mõistagi kuigi turvaline ja seetõttu soovitangi igaühel moodustada endale unikaalne lause.

Kasuta paroolihaldurit

Kui soovid, et paroolid oleksid turvalisemad ja elu lihtsam, tasub kasutada paroolihalduri tarkvara nagu LastPass, 1password või Dashlane. Paroolihaldurid on programmid, nutirakendused ja veebilehitseja lisad, mis genereerivad keerulisi salasõnu ning salvestavad need krüpteeritult turvalisse serverisse. Edaspidi pead meeles pidama ainult ühte salasõna, millega paroolihaldurisse siseneda ning kindlasti soovitame haldurisse sisenemiseks aktiveerida ka kahe astmelise autentimise.

Kui aga kommertstarkvara kasutada ei soovi, leidub ka vabavaral toimivaid lahendusi nagu näiteks Keepass. Seal saab kasutaja valida, kuhu tema salasõna salvestatakse ja seeläbi vähendada parooli lekkimise riski, sest paroolihaldurite keskkonnad on huvipakkuvad sihtmärgid küberpättidele.

Kasuta kaheastmelist autentimist

Veebilehtedel kasutatav parool võib olla väga pikk ja keeruline, kuid teinekord lekivad need kasutajast sõltumata. Juhul, kui sama parool on kasutusel ka mujal, siis võib pahalane su kasutajanime ja salasõnaga teistesse veebikeskkondadesse sisse logida. Täiendavaks kaitsemeetmeks oleks kaheastmeline autentimine.

Tegemist on protsessiga, mis käivitub pärast salasõna sisestamist ja tuvastab kas SMSi, e-maili, koodigeneraatoriga või muudmoodi, et veebilehele logib sisse õige inimene. Näiteks saadetakse registreerimisel märgitud telefoninumbrile või e-maili aadressile salajane kood, mis palutakse sisselogimisel veel lisaks sisestada.

Google ja Microsoft on teinud ka oma koodigeneraatori rakendused, mida on võimalik kasutada mitmetele veebilehtedele sisselogimiseks.

Veelgi turvalisem on turvavõti

Turvalisuse järgmine tase oleks turvavõti (inglise keeles *security key*). Tegemist on väikse vidinaga, mis on sisselogimisel vaja füüsiliselt arvutiga ühendada.

Kõige lihtsamad turvavõtmed näevad välja nagu õhukesed mälupulgad ja need ühendatakse USB-pesasse. Olemas on ka juhtmevaba ühendusega seadmeid, kuid need pole veel nii levinud. Tuntuimad turvavõtme tootjad on Yubico ja Google, mille toote nimed on vastavalt YubiKey ja Titan Security Key. Meil Eestis on võimalik kasutada ka ID-kaarti, mis täidab sama otstarvet, kuid kahjuks saab seda kasutada ainult Eesti e-teenustes.

Ära salvesta paroole veebilehitsejasse

Erinevalt paroolihaldurist, kus talletatakse paroolid krüpteeritult ja peaparooliga (master passwordiga) kaitstult, ei pruugi sama kehtida mõnedes veebilehitsejates. Kui kellelgi on juurdepääs arvutile, on tal võimalus ka saada ligi kõikidele paroolidele ja logida sisse erinevatesse rakendustesse või veebilehtedele. Selleks ohuks ei pea olema tingimata teine inimene, vaid tõenäoliselt on suuremaks riskiks arvutisse pääsenud pahavara.

Kas minu parooli on häkitud?

Microsofti turvaekspert Troy Hunt on teinud veebilehe aadressi haveibeenpwned.com, kus saab kontrollida, kas mõne e-posti aadressiga seotud konto on kuskilt lekkinud. Esilehel leiduvasse suurde lahtrisse tuleb sisestada ainult oma e-maili aadress ja süsteem ütlebki, kas mõnelt lehelt on sinu andmed lekkinud.

Kui pidev käsitsi kontrollimine tundub tüütu, siis on võimalik lehel seadistada ka automaatne teavitus juhul, kui mõned isikuandmed on lekkinud.

Uusaastalubaduseks sobib ka see, kui lubad, et tõstad oma turvalisuse taset ja kasutad ainult turvalisi paroole.

- Uudised

- Tarkvara
- Turvalisus

Pilt