Häkitud? Kolmandikul juhtudest oli selle põhjuseks liiga nõrk parool

4 aastat tagasi Autor: AM

Väljapressimistarkvara on ennustuste järgi 2020. aasta kõige levinuim küber-oht. Selle põhjuseks, miks aga häkkimise ohvriks langetakse, on PreciseSecurity.com´i uuringu järgi liiga nõrgad salasõnad. 30% väljapressimisrünnakutest 2019. aastal õnnestusid liiga nõrga salasõna pärast.

Pahavararünnakutest 67% olid aga põhjustatud mitmesugustest õngitsuskirjadest või õngitsusnippidest. 36% vastanutest arvasid, et nad sattusid rünnaku ohvriks liiga väheste teadmiste tõttu sellest, kuidas end küberrünnakute eest kaitsta.

2019. aastal tehtud Google´i uuringu põhjal aga selgus, et kaks kolmest kasutajast tarvitab samu paroole mitmete kontode juures. 50% tunnistas, et kasutavad lemmikparooli enamuse kontode juures. Vaid kolmandik teadsid, mis on *Password Manager* ehk paroolihaldusprogramm.

Statista 2019. aastal tehtud uuringu tulemusena selgus, et USA kasutajatest pidas 64% varastatud paroole kõige suuremaks ohuks oma privaatsusele. 43% vastanutest ütlesid, et kindlaim viis oma paroole hallata on need kuhugi üles kirjutada. 45% üritasid aga paroole pähe õppida.

Kõige olulisem samm oma salasõna turvalisena hoidmisel on sellise keerulise parooli kasutamine, mida on raske ära arvata. Suurbritannia National Cyber Security Centre´i 2019. aasta uuringu järgi on maailmas 23,2 miljonit kasutajakontot, mille parooliks on 123456. Veel 7,8 miljonit kontot kasutavad paroolina 12345678. 3,5 miljonit aga "kaitsevad" oma andmeid salasõnaga "password". Seega on üsna lihtne kammida internetti ja leida kohe ilma eriti vaeva nähgemata kümneid miljoneid kasutajakontosid, kuhu sissehäkkimine ei nõua mingit pingutust.

- Uudised
- Turvalisus