OUCH! | 2016m. birželio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Kas yra užšifravimas?
- Ką galite užšifruoti?
- Kaip tai padaryti teisingai?

Užšifravimas

Kas yra užšifravimas?

Tikriausiai esate girdėję žmones vartojant terminą „užšifravimas“ ir patarimus, kaip turėtumėte jį naudoti, siekdami apsaugoti tiek save, tiek savo informaciją. Tačiau užšifravimas gali atrodyti painus, todėl turėtumėte žinoti jo trūkumus. Šiame naujienlaiškyje paprastais žodžiais paaiškinsime, kas yra užšifravimas, kaip jis jus saugo ir kaip jį tinkamai naudoti.

Kviestinė redaktorė

Francesca Bosco (**@francibosco**) yra mokslininkė projektų, susijusių su internetinėje erdvėje vykdomais nusikaltimais, internetiniu saugumu ir netinkamu technologijų naudojimu, vykdytoja. Ji dirba Jungtinių Tautų tarpregioniniame nusikalstamumo ir teisingumo tyrimų institute bei yra įkūrusi Technologijų ir teisės centrą.

Jūsų įrenginiuose yra didžiulis kiekis slaptos informacijos, pavyzdžiui, asmeniniai dokumentai, nuotraukos ir elektroniniai laiškai. Jei prarastumėte arba iš jūsų būtų pavogtas bent vienas įrenginys, prie šios informacijos galėtų prisijungti bet kas, į kieno rankas jis patektų. Be to, internete tikriausiai atliekate ir tokias slaptas operacijas, kaip naudojimasis bankininkystės paslaugomis arba apsipirkinėjimas internetu. Jei kas nors šią veiklą stebėtų, jie galėtų pavogti tokią informaciją kaip jūsų finansinė paskyra arba kredito kortelių numeriai. Užšifravimas jus visose šiose situacijose apsaugo, užtikrindamas, kad pašaliniai asmenys negalės prisijungti ir keisti jūsų informacijos.

Užšifravimas egzistuoja jau tūkstančius metų. Šiais laikais šis procesas yra žymiai sudėtingesnis, tačiau jo paskirtis išlieka tokia pati – perduoti slaptą žinutę iš vienos vietos į kitą užtikrinant, kad ją galės perskaityti tik turintys šią teisę asmenys. Kai informacija nėra užšifruota, ji vadinama grynuoju tekstu. Tai reiškia, kad bet kas gali prie jos prieiti ir lengvai ją perskaityti. Užšifruojant ši informacija yra pakeičiama neįskaitomu formatu, vadinamu šifruotu tekstu. Šiais laikais užšifruojama naudojant sudėtingus matematinius veiksmus ir individualųjį raktą, kuriuo jūsų informacija paverčiama šifruotu tekstu. Šiuo raktu yra užrakinama ir atrakinama jūsų informacija. Daugeliu atvejų, jūsų raktu yra slaptažodis arba slaptas kodas.

Ką galite užšifruoti?

Iš viso yra dvi šifruojamų duomenų rūšys: nekintantys duomenys (pavyzdžiui, duomenys saugomi jūsų mobiliajame įrenginyje) ir kintantys duomenys (pavyzdžiui, draugui siunčiami elektroniniai laiškai arba žinutės).

Užšifravimas

Nekintančius duomenis būtina užšifruoti siekiant apsaugoti informaciją, jei būtų prarastas arba pavogtas jūsų kompiuteris arba mobilusis įrenginys. Šiais laikais įrenginiai yra itin galingi, juose galima talpinti didžiulį informacijos kiekį, kuris lygiai taip pat lengvai gali būti ir prarastas. Be to, slapta informacija gali būti laikoma ir tokiose nešiojamosiose laikmenose, kaip atmintukai ar išoriniai kietieji diskai. Viso disko užšifravimas (angl. Full Disk Encryption, trump. FDE) – tai plačiai naudojama šifravimo technologija, kuria galima užšifruoti visą jūsų sistemos diską. Tai reiškia, kad bus užšifruota viskas, kas bus laikoma sistemoje, todėl jums nebereikės spręsti, ką užšifruoti, o ko ne. Šiais laikais daugumoje kompiuterių yra įdiegta viso disko užšifravimo funkcija, tačiau ją reikia įjungti rankiniu būdu. Mac kompiuteriuose tai vadinama „FileVault“, tuo tarpu Windows kompiuteriuose, priklausomai nuo versijos, galite naudoti „Bitlocker“ arba „Device Encryption“. Dauguma nešiojamųjų įrenginių taip pat palaiko viso disko užšifravimo funkciją. iPhone ir iPad įrenginiuose esančioje iOS operacinėje sistemoje viso disko užšifravimo funkcija būna įjungiama automatiškai vos tik nustatomas slaptas kodas. Naudojant Android 6.0 (Marshmallow), Google reikalauja, kad viso disko užšifravimas būtų įjungtas pagal nutylėjimą, su sąlyga, kad aparatinė įranga atitiks tam tikrus minimalius standartus.

Šifravimas yra galingas būdas padėti apsaugoti jūsų informaciją, bet tai tik tokia stipri, kaip ir Jūsų raktu.

Informacija taip pat tampa pažeidžiama ją perduodant. Jei duomenys nėra užšifruojami, jie gali būti stebimi, keičiami ir pasisavinami internete. Štai kodėl turite įsitikinti, kad bet kokios internete vykdomos slaptos operacijos ir siunčiami pranešimai yra užšifruojami. Dažniausias internetinio užšifravimo ženklas yra HTTPS. Tai reiškia, jog visas duomenų srautas tarp jūsų naršyklės ir tinklalapio yra šifruojamas. Atkreipkite dėmesį, ar internetinės svetainės adresas prasideda trumpiniu https://, ar ant naršyklės matosi užrakintos spynelės piktograma ir ar jūsų internetinės svetainės adreso juosta nusidažo žalia spalva. Kitu pavyzdžiu gali būti akimirka, kai siunčiate ir gaunate elektroninius laiškus. Dauguma elektroninio pašto programų siūlo užšifravimo galimybes, kurias jums tereikia įsijungti. Trečiuoju pavyzdžiu gali būti siunčiamos informacijos užšifravimas tarp dviejų tarpusavy susirašinėjančių vartotojų tokiomis programomis, kaip iMessage, Wickr, Signal, WhatsApp arba Telegram. Tokios programos užšifruoja pranešimus, kurie yra siunčiami tik tarp konkrečių galutinių vartotojų (angl. end-to-end encryption), todėl juos siunčiant iš vienos sistemos ar įrenginio į kitą, prie jų negali prieiti jokie kiti pašaliniai asmenys. Tai reiškia, kad tai, kas yra siunčiama, galite perskaityti tik jūs ir asmuo, su kuriuo susirašinėjate.

Užšifravimas

Kaip tai padaryti teisingai?

Norėdami įsitikinti, kad būsite apsaugoti naudodami užšifravimą, pirmiausiai turite įsitikinti, jog jį naudosite teisingai.

- Jūsų informacijos užšifravimo patikimumas priklausys nuo jūsų nustatyto apsaugos kodo. Jei kas nors atspės arba gaus prieigą prie jūsų kodo, tai jie gaus prieigą ir prie jūsų duomenų. Apsaugokite savo kodą. Jei naudojate slaptą kodą arba slaptažodį, įsitikinkite, kad tai yra patikimas ir unikalus slaptažodis. Kuo jūsų slaptažodis ilgesnis, tuo sudėtingiau programišiui jį atspėti arba nulaužti. Nepamirškite savo slaptažodžio, nes be jo nebegalėsite iššifruoti savo informacijos. Jei nesugebate prisiminti visų savo slaptažodžių, rekomenduojame naudoti slaptažodžių tvarkytuvę.
- Jūsų informacijos užšifravimo patikimumas priklausys nuo jūsų įrenginių saugumo. Jei jūsų įrenginiui kils pavojus arba jį užkrės kenkimo programa, tada kibernetiniai nusikaltėliai jūsų užšifravimą galės apeiti. Štai kodėl yra svarbu imtis papildomų veiksmų, siekiant apsaugoti savo įrenginį, įskaitant antivirusinės programos ir patikimų slaptažodžių naudojimą bei reguliarų programos atnaujinimą.
- Šiuo metu dauguma mobiliųjų programėlių ir kompiuterinių programų siūlo patikimą užšifravimą, siekiant apsaugoti jūsų duomenis ir siunčiamus pranešimus. Jei jūsų ketinama naudoti kompiuterinė programa arba mobilioji programėlė nepalaiko užšifravimo, tada apsvarstykite galimybę naudoti alternatyvią programą.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Užšifravimo paaiškinimas:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Slaptafrazės:	https://securingthehuman.sans.org/ouch/2015#october2015
Slaptažodžių tvarkytuvės:	https://securingthehuman.sans.org/ouch/2016#january2016
Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#february2016
Jūsų naujos planšetės apsauga:	https://securingthehuman.sans.org/ouch/2016#january2016

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.

