OUCH! | 2015 m. balandžio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Slaptafrazės
- Saugus slaptafrazių naudojimas
- Šaltiniai

Slaptafrazės

Faktai

Slaptažodžius naudojate beveik kasdien, jungdamiesi prie savo el. pašto ar internetinės banko sistemos, pirkdami prekes ar jungdamiesi prie savo išmaniojo telefono. Tačiau slaptažodžiai taip pat yra silpniausia jūsų vieta, kadangi kam nors sužinojus jūsų slaptažodį, gali būti pasinaudota jūsų tapatybe, pervedami pinigai arba prisijungta prie jūsų asmeninės informacijos. Todėl norėdami apsisaugoti turite susikurti patikimus slaptažodžius. Šiame naujienlaiškyje sužinosite, kaip susikurti patikimus ir lengvai įsimenamus slaptažodžius, naudojant slaptafrazes.

Kviestinis redaktorius

Guy Bruneau yra vyresnysis įmonės IPSS Inc. konsultantas saugumo klausimais, SANS instituto dėstytojas ir ISC (Internet Storm Center) prižiūrėtojas. Guy SANS institute įgijo Pasaulinės informacijos patikimumo sertifikavimo saugumo specialisto (GSE) išsilavinimą ir tame pačiame institute baigė Kibernetinės apsaugos programą. Daugiau informacijos apie Guy galite rasti Twitter, įvedę **@GuyBruneau** arba apsilankę šioje svetainėje **handlers.sans.org/gbruneau**.

Slaptafrazės

Didžiausia problema, su kuria susiduriame yra ta, kad kibernetiniai įsilaužėliai, norėdami atspėti arba „nulaužti“ slaptažodžius, naudoja profesionalius metodus, kurie vis tobulėja. Tai reiškia, jog kuo jūsų slaptažodžiai yra paprastesni arba kuo juos lengviau atspėti, tuo didesnis pavojus jiems kyla. Norint nuo to apsisaugoti, labai svarbu naudoti patikimus slaptažodžius. Kuo daugiau ženklų sudaro slaptažodį, tuo jis patikimesnis ir tuo sunkiau jį atspėti įsilaužėliui. Tačiau ilgus ir sudėtingus slaptažodžius gali būti sunku prisiminti. Todėl rekomenduojame naudoti slaptafrazes, kuriomis laikomos paprastos frazės arba lengvai įsimenami, tačiau sunkiai atspėjami sakiniai. Pavyzdžiui:

Kur yra karalius Džulianas?

Ši slaptafrazė yra patikima ne vien todėl, kad ją sudaro 27 ženklai, bet ir todėl, kad joje naudojamos didžiosios raidės ir simboliai (prisiminkite, jog tarpai ir skyrybos ženklai taip pat yra simboliai). Raides pakeitus simboliais, jūsų slaptafrazė taps dar patikimesnė, pavyzdžiui raidę „a“ galite pakeisti simboliu „@“, o raidę „o“ galite pakeisti nuliu. Jei svetainėje arba programoje slaptažodžio ženklų skaičius yra ribojamas, naudokite didžiausią leistinų ženklų skaičių.

Slaptafrazės

Saugus slaptafrazių naudojimas

Naudodami slaptafrazes, būkite atsargūs. Slaptafrazės bus nenaudingos, jei kas nors galės jas lengvai pavogti arba nukopijuoti.

Slaptafrazių naudojimas tai vienas iš veiksmingiausių būdų, kuriuo galite apsaugoti ne tik savo tapatybę, bet ir informaciją.

1. Įsitikinkite, jog kiekvienoje paskyroje arba naudojamame įrenginyje nustatėte skirtingą slaptafrazę. Pavyzdžiui, niekada nenaudokite tokios pačios slaptafrazės savo darbo paskyroje arba banko sąskaitoje, kokią naudojate savo privačiose paskyrose, tokiose kaip Facebook, YouTube ar Twitter. Tokiu būdu, įsilaužus į vieną iš jūsų paskyrų, kitos paskyros liks saugios. Jei sukūrėte pernelyg daug slaptafrazių, kad jas visas galėtumėte prisiminti (o taip nutinka gana dažnai), apsvarstykite galimybę naudoti slaptažodžių tvarkytuvę. Tai speciali programa, patikimai sauganti visas jūsų slaptafrazes. Tokiu būdu, vienintelės slaptafrazės, kurias turėsite prisiminti bus jūsų kompiuterio ir slaptažodžių tvarkytuvės.

2. Niekada niekam, įskaitant savo bendradarbius, neatskleiskite slaptafrazės arba jos kūrimo strategijos. Prisiminkite, jog slaptafrazė prilygsta paslapčiai, todėl kam nors ją sužinojus, jūsų slaptafrazė nebebus patikima. Jei slaptafrazę netyčia kam nors atskleidėte arba manote, kad ja kas nors gali pasinaudoti arba pavogti, nedelsdami ją pakeiskite.

3. Kaip ir su slaptažodžiais, venkite kurti lengvai atspėjamas arba dažnai naudojamas slaptafrazes. Pavyzdžiui, slaptafrazė „Prieš keturis kart dvidešimt ir septynerius metus“ (angl. Four score and seven years ago) nėra gera, kadangi šis posakis yra gerai žinomas.

4. Norėdami prisijungti prie darbo paskyros arba banko sąskaitos, nenaudokite viešų kompiuterių, kuriuos galite rasti viešbučiuose ar bibliotekose. Kadangi šiais kompiuteriais gali naudotis bet kas, juose gali būti įdiegtas kenkėjiškas kodas, sekantis visus jūsų klavišų paspaudimus. Junkitės prie savo darbo paskyros arba banko sąskaitų, naudodamiesi tik patikimais kompiuteriais arba mobiliais įrenginiais.

5. Saugokitės svetainių, kuriose prašoma jūsų atsakyti į asmeninius klausimus. Šie klausimai įprastai naudojami pamiršus slaptafrazę ir norint ją atkurti. Problema yra ta, jog atsakymus į šiuos klausimus neretai galima rasti

Slaptafrazės

internete arba net apsilankius jūsų Facebook puslapyje. Įsitikinkite, jog atsakydami į asmeninius klausimus naudojate tik tokią informaciją, kuri nėra viešai prieinama arba tokią, kuri yra išgalvota. Šioje situacijoje, slaptažodžių tvarkytuvės padės jums įsiminti papildomą informaciją.

6. Dauguma internetinių paskyrų siūloma naudoti du skirtingus prisijungimo būdus, kurie dar vadinami dviejų etapų patvirtinimu. Čia be slaptafrazės dar reikia įvesti ir į išmanųjį telefoną atsiųstą slaptą kodą. Ši parinktis yra žymiai saugesnė už pavienę slaptafrazę. Todėl, kai tik įmanoma, visada naudokite šiuos patikimesnius patvirtinimo būdus.

7. Mobiliuose įrenginiuose dažnai prieš prisijungiant prašoma įvesti apsauginį PIN kodą. Prisiminkite, jog PIN kodas tai dar vienas slaptažodis. Kuo PIN kodas ilgesnis, tuo jis saugesnis. Daugumoje mobiliųjų įrenginių leidžiama PIN kodą pakeisti slaptafraze.

8. Galiausiai, jei daugiau paskyros nebenaudojate, įsitikinkite, jog ją uždarėte, ištrynėte arba išjungėte.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę http://www.securingthehuman.org.

Šaltiniai

Dviejų etapų patvirtinimas:	http://www.securingthehuman.org/ouch/2013#august2013
Slaptažodžių tvarkytuvės:	http://www.securingthehuman.org/ouch/2013#october2013
Socialinė inžinerija:	http://www.securingthehuman.org/ouch/2014#november2014
Dažniausiai naudojami saugumo terminai:	http://www.securingthehuman.org/resources/security-terms

Licencija

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus