Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Slaptafrazės
- Kaip saugiai naudoti slaptafrazes?
- Šaltiniai

Slaptafrazės

Įvadas

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 vieta, kadangi, kam nors sužinojus jūsų slaptažodį, svetimas asmuo gali apsimesti jumis ir daryti pinigų pervedimus, skaityti el. paštą ar net pavogti jūsų asmens tapatybės duomenis. Todėl, norėdami apsisaugoti, turite susikurti patikimus slaptažodžius. Tai žmonėms įprastai kelia didelę sumaištį, nes juos sudėtinga prisiminti ir įvesti. Šiame naujienlaiškyje sužinosite, kaip susikurti patikimus, lengvai įsimenamus ir įvedamus slaptažodžius, vadinamus slaptafrazėmis.

Kviestinė redaktorė
My-Ngoc Nguyen (tariama Me-Nop Wynn) yra atestuota SANS instituto dėstytoja ir įmonės „Secured IT Solutions“ generalinė direktorė bei vyriausioji konsultantė. Ji turi profesinės patirties pagrindiniais saugos sertifikavimo klausimais ir yra sukaupusi daugiau nei 14 metų patirties įvairių pramonės šakų bei sektorių kibernetinės saugos programų kūrimo, plėtros ir valdymo srityse. Twitter paskyra: **@MenopN**; LinkedIn paskyra: My-Ngoc "Menop" Nguyen.

Slaptafrazės

Didžiausia problema, su kuria susiduriame, yra ta, kad kibernetiniai nusikaltėliai, 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. Įprastai tai yra atliekama nustatant sudėtingus slaptažodžius, tačiau jie gali sukelti daug painiavos, nes dažniausiai juos sunku prisiminti. Todėl rekomenduojame naudoti slaptafrazes, kuriomis laikoma atsitiktinių žodžių seka arba koks nors sakinys. Kuo daugiau spaudos ženklų turi jūsų slaptafrazė, tuo ji yra patikimesnė. Slaptafrazių privalumas yra tas, kad jas yra žymiai lengviau prisiminti ir įvesti, o kibernetiniams nusikaltėliams dėl jų vis dar yra ypač sunku įsilaužti. Štai pora skirtingų pavyzdžių.

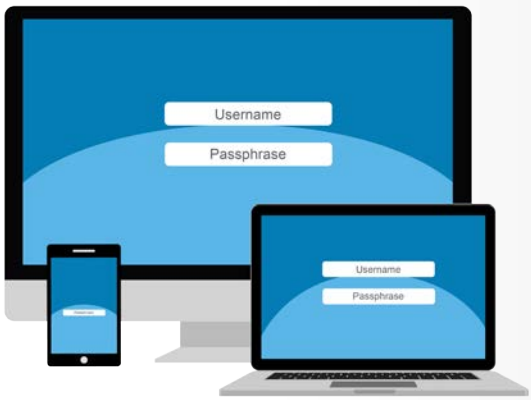
Išlaikyti-Lengvai-Įkalinti

Arbatos pertraukėlė 1:23

© SANS Institute 2017

Slaptafrazės

Šios slaptafrazės yra patikimos ne vien todėl, kad jos yra ilgos, bet ir todėl, jog jose naudojamos didžiosios raidės ir simboliai (prisiminkite, kad tarpai ir skyrybos ženklai yra laikomi simboliais). Tuo pačiu šias slaptafrazes lengva įsiminti ir įvesti. Raides pakeitus skaičiais arba 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 leistiną ženklų skaičių.



Slaptafrazės tai žymiai paprastesnis būdas susikurti ir prisiminti patikimus slaptažodžius.

Kaip saugiai naudoti slaptafrazes?

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

1. Kiekvienoje paskyroje arba naudojamame įrenginyje naudokite 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 prisimintumėte (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 ar kito įrenginio ir slaptažodžių tvarkytuvės.
2. Niekada niekam, įskaitant savo bendradarbius ar vadovą, neatskleiskite slaptafrazės arba jos kūrimo strategijos. Prisiminkite, kad slaptafrazė prilygsta paslapčiai, todėl kam nors ją sužinojus, jūsų slaptafrazė nebebus patikima. Jei slaptafrazę netyčia kam nors atskleidėte arba manote, jog ja kas nors gali pasinaudoti arba pavogti, nedelsdami ją pakeiskite. Vienintele išimtimi gali būti tai, kad savo asmeninėmis slaptafrazėmis norite pasidalinti su ypač patikimu šeimos nariu, kurias jis galėtų naudoti nelaimės atveju. Tokiu atveju, užrašykite savo pagrindines asmenines slaptafrazes (įsitikinkite, jog jos nėra susijusios su darbu), padėkite jas saugioje vietoje ir tą vietą nurodykite itin patikimam šeimos nariui. Taip, jums patekus į nelaimę ir prireikus pagalbos, jūsų artimieji galės prisijungti prie svarbiausių paskyrų.
3. Nenaudokite viešų kompiuterių, kuriuos galite rasti viešbučiuose ar interneto kavinėse. Kadangi šiais kompiuteriais gali naudotis bet kas, jie gali būti užkrėsti virusais arba sekti visus jūsų klavišų paspaudimus. Junkitės prie savo paskyrų naudodamiesi tik patikimais kompiuteriais arba mobiliais įrenginiais.

© SANS Institute 2017

Slaptafrazės

4. Saugokitės svetainių, kuriose prašoma jūsų atsakyti į asmeninius klausimus. Šie klausimai įprastai naudojami pamiršus slaptafrazę ir norint ją atkurti. Problema yra ta, kad atsakymus į šiuos klausimus neretai galima rasti 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. Jei negalite prisiminti visų sugalvotų atsakymų į saugumo klausimus, tuomet sugalvokite temą. Pavyzdžiui, „filmo veikėjas“ ir savo atsakymus susiekite su tuo veikėju. Kita išeitis yra naudoti slaptažodžių tvarkytuvę, kadangi daugumoje taip pat galėsite saugiai laikyti ir šią informaciją.
5. Daugumoje 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.
6. Mobiliuose įrenginiuose, dažnai prieš prisijungiant, prašoma įvesti apsauginį PIN kodą. Prisiminkite, kad PIN kodas – dar vienas slaptažodis. Kuo PIN kodas ilgesnis, tuo jis saugesnis. Daugumoje mobiliųjų įrenginių leidžiama PIN kodą pakeisti slaptafraze arba naudoti biometrinį atpažinimo būdą, pavyzdžiui, piršto antspaudą.
7. Galiausiai, jei daugiau paskyros nebenaudojate, įsitikinkite, kad ją uždarėte, ištrynėte arba išjungėte.

SUŽINOKITE DAUGIAU

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

Šaltiniai

Slaptažodžių tvarkytuvės: https://securingthehuman.sans.org/ouch/2015#october2015

Dviejų etapų tapatybės patvirtinimas: https://securingthehuman.sans.org/ouch/2015#september2015

Apsaugokite savo paskyrą: https://securingthehuman.sans.org/ouch/archives

SANS instituto „Penkių dienų kursas apie kibernetinio saugumo pradmenis“ (SEC301): https://sans.org/sec301

Licencija

OUCH! Yra leidžiamas SANS Securing The Human instituto ir platinamas pagal Creative Commons BY-NC-ND 3.0 licensiją. Jums leidžiama naudoti ir platinti šį naujienlaiškį su sąlyga, kad niekas nebus keičiama. Norėdami gauti daugiau informacijos susisiekite su mumis ouch@securingthehuman.org.

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.

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