Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Apžvalga
- Privatumas
- Saugumas

Socialinė medija

Apžvalga

Tokios socialinės svetainės kaip Facebook, Twitter, Instagram ir LinkedIn yra laikomos nepaprastomis vietomis, kuriose galite susitikti, bendrauti ir dalintis informacija su žmonėmis iš viso pasaulio. Tačiau naudojantis visomis šiomis galimybėmis, pavojus kyla ne vien tik jums, bet ir jūsų šeimai, draugams ar darbdaviui. Šiame naujienlaiškyje paaiškinsime apie minėtuosius pavojus ir patarsime, kaip galėtumėte šiomis svetainėmis naudotis saugiai ir patikimai.

Kviestinis redaktorius

Tanya Baccam yra ilgametė konsultantė saugumo klausimais. Daugiau nei dešimtmetį ji buvo SANS instituto mokomosios programinės įrangos kūrėja ir dėstytoja, įskaitant SEC502, SEC542, SEC401, MGT414, AUD507 ir kitus kursus. Jos veiklą galite sekti Twitter, įvedę **@tbaccam**.

Privatumas

Dažniausias rūpimas klausimas, susijęs su socialinėmis svetainėmis, yra kaip apsaugoti savo asmeninę informaciją. Galimus pavojus apima:

- **Jūsų ateities įtakojimas**: kai kurių organizacijų darbuotojai po socialines svetaines naršo norėdami patikrinti biografinius faktus. Jūsų gali neįdarbinti arba nepaaukštinti dėl gėdingų ar kaltę įrodančių nuotraukų arba įrašų, neatsižvelgiant į jų senumą. Be to, daugumos universitetų administracija panašias patikras atlieka naujų stojančiųjų paraiškų nagrinėjimo metu. Privatumo parinktys gali jūsų neapsaugoti, kadangi šios organizacijos gali jūsų paprašyti paspausti mygtuką „Patinka“ arba prisijungti prie jų puslapių, o tam tikri įrašai gali būti saugomi daugybėje kitų svetainių.
- **Jūsų puolimas**: kibernetiniai užpuolikai gali išanalizuoti jūsų įrašus ir panaudoti juos, norėdami gauti prieigą prie jūsų arba organizacijos, kurioje dirbate, informacijos. Pavyzdžiui, jie gali panaudoti informaciją, kuria dalinatės, norėdami atspėti atsakymus į jūsų „slaptus klausimus“, kurie padėtų į pradinę būseną atstatyti jūsų internetinius slaptažodžius, sukurti prieš jus nukreiptus tikslinius el. pašto puolimus, bandydami jūsų vardu iš organizacijos išgauti konfidencialią informaciją, arba paskambinti kam nors iš jūsų organizacijos apsimetę jumis. Be to, šie puolimai gali būti fiziškai panaudoti realiame pasaulyje, pavyzdžiui, nustatant, kur dirbate ar gyvenate.
- **Atsitiktinis pakenkimas jūsų darbdaviui**: nusikaltėliai arba konkurentai prieš jūsų darbdavį gali panaudoti bet kokią konfidencialią informaciją, kurią skelbiate apie savo organizaciją. Be to, jūsų įrašai gali sugadinti jūsų organizacijos reputaciją. Taigi prieš skelbdami ką nors apie savo darbą, pirmiausiai įsitikinkite, kad esate susipažinę su savo organizacijos politika, kadangi kai kurie įrašai jūsų socialinėse svetainėse gali būti stebimi.

Socialinė medija

Geriausias būdas apsisaugoti yra riboti skelbiamų įrašų informaciją. Žinoma, privatumo parinktys gali kažkiek apsaugoti, tačiau dažnai jas sudėtinga suprasti ir neišmanant tinkamai pakeisti. Tai, ką laikėte privačia informacija, dėl daugumos priežasčių gali greitai tapti vieša. Be to, jūsų įrašų privatumas yra toks pat saugus, kaip ir žmonės, su kuriais jais dalinatės. Su kuo daugiau draugų ir kontaktinių asmenų pasidalinate, tuo didesnė tikimybė, kad ši informacija taps vieša. Turėtumėte suvokti, jog bet kas, ką skelbiate gali tapti arba taps vieša ir nuolatine interneto dalimi.

Galiausiai, atkreipkite dėmesį į tai, ką apie jus skelbia draugai. Jei jie skelbia ką nors, dėl ko nesijaučiate maloniai, paprašykite tai ištrinti. Jei jie tą padaryti atsisako arba jūsų prašymą ignoruoja, susisiekite su socialinės svetainės prižiūrėtojais ir paprašykite jų šį turinį dėl jūsų pašalinti. Tuo pat metu, atkreipkite dėmesį į tai, ką skelbiate apie kitus.



Socialinės medijos svetainės yra smagios ir veiksmingos, tačiau būkite atsargūs su kuo ir kokia informacija dalinatės.

Saugumas

Kalbant apie privatumo problemas, pateikiame keletą veiksmų, kurie padės apsaugoti jūsų paskyras socialinėse svetainėse ir veiklą jose.

- **Prisijungimas**: apsaugokite kiekvieną iš savo paskyrų patikimu, unikaliu slaptažodžiu ir su niekuo jomis nesidalinkite. Be to, dauguma socialinių svetainių palaiko patikimą tapatybės nustatymą, tokį kaip patvirtinimas dviem etapais. Kai tik įmanoma, visada pasinaudokite šiais patikimesniais tapatybės nustatymo metodais. Galiausiai, nenaudokite savo socialinės paskyros, norėdami prisijungti prie kitų svetainių, nes jeigu ją užgrobs programišiai, tuomet visos jūsų paskyros taps pažeidžiamos.
- **Privatumo nustatymai**: jei visgi naudojate privatumo nustatymus, įsitikinkite, jog juos reguliariai peržiūrite ir išbandote. Socialinės svetainės dažnai keičia privatumo nustatymus, todėl paprasta suklysti. Be to, daugumoje programų ir paslaugų, skelbiamame įraše galite žymėti savo buvimo vietą (tai vadinama geografiniu žymėjimu). Jei norite, jog jūsų fizinė buvimo vieta liktų privati, šiuos nustatymus reguliariai tikrinkite.
- **Užšifravimas**: socialinėse svetainėse naudojamas užšifravimas vadinasi HTTPS (saugus HTTP protokolas). Jis skirtas apsaugoti jūsų internetinį prisijungimą prie svetainės. Kai kurios svetainės, tokios kaip Twitter ir Google+ tai įjungia automatiškai, tačiau kitose HTTPS gali tekti įjungti rankiniu būdu. Patikrinkite savo socialinės paskyros nustatymus ir, kai tik įmanoma, HTTPS nustatykite kaip numatytą jungtį.
- **El. paštas**: įtariai žiūrėkite į el. laiškus, kuriuose teigiama, jog yra rašoma iš socialinių svetainių, kadangi tai gali būti paprasčiausias kibernetinių nusikaltėlių puolimas, apsimetant kitais asmenimis. Saugiausias būdas atrašyti į

Socialinė medija

tokias žinutes yra prisijungti prie savo socialinės svetainės tiesiogiai (galbūt naudojant išsaugotą adresyno įrašą), o tuomet perskaityti ir atsakyti į bet kokias toje svetainėje gautas žinutes arba pranešimus.

- **Kenkėjiškos nuorodos/apgaulingi laiškai**: būkite atsargūs ir įtartinai žiūrėkite į nuorodas arba galimai apgaulingus laiškus, kurie yra skelbiami socialinėse svetainėse. Blogų tikslų turintys žmonės socialinę terpę naudoja norėdami skleisti savo išpuolius. Vien todėl, kad draugas paskelbė žinutę, nereiškia, jog ji iš tiesų yra nuo jo, kadangi jo paskyra gali būti užgrobta. Jei šeimos narys arba draugas paskelbė keistą žinutę, kurios negalite patikrinti (pavyzdžiui, tokią, kurioje teigiama, kad jis buvo apiplėštas ir reikia, kad jam atsiųstumėte pinigų), paskambinkite jiems mobiliuoju telefonu arba susisiekite kitomis priemonėmis, jog įsitikintumėte, kad žinutė tikrai buvo siųsta nuo jų.
- **Mobiliosios programos**: norint prisijungti prie savo internetinių paskyrų, daugumoje socialinių svetainių siūloma įsidiegti mobiliąsias programas. Įsitikinkite, kad šias mobiliąsias programas parsisiunčiate iš patikimos svetainės ir kad jūsų išmanusis telefonas yra apsaugotas patikimu slaptažodžiu. Jei jūsų išmanusis telefonas nėra užrakintas, tuomet jį praradus, bet kuris asmuo per šį išmanųjį telefoną galės prisijungti prie socialinių svetainių ir jūsų vardu skelbti įrašus.

Socialinės svetainės tai puikus būdas bendrauti ir palaikyti ryšį su pasauliu. Jei vadovausitės čia išdėstytais patarimais, galėsite mėgautis žymiai saugesne internetine patirtimi. Norėdami sužinoti daugiau, kaip galite saugiai naudotis savo socialinėmis svetainėmis, apsilankykite savo socialinės svetainės saugumo puslapyje.

SUŽINOKITE DAUGIAU

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

Šaltiniai

Slaptafrazės:	http://www.securingthehuman.org/ouch/2015#april2015
Dviejų žingsnių autentifikacija:	http://www.securingthehuman.org/ouch/2013#august2013
Saugus mobilių aplikacijų naudojimas:	http://www.securingthehuman.org/ouch/2015#january2015
Vaikų mokymas apie internetinį saugumą:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook'o sauga:	https://www.facebook.com/safety

Licencija

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