Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

Mobiliųjų prietaisų apsauga

Apžvalga

Mobilieji prietaisai yra puiki ir paprasta priemonė, skirta bendrauti su draugais, apsipirkinėti, naudotis internetinės bankininkystės paslaugomis, žiūrėti filmus, žaisti žaidimus bei užsiimti kita veikla. Kadangi jūsų prietaisai yra laikomi tokia svarbia gyvenimo dalimi, pateikiame keletą paprastų patarimų, kurie padės juos apsaugoti.

Mobiliųjų prietaisų apsauga

Galite nustebti sužinoję, kad didžiausią pavojų jūsų mobiliesiems prietaisams kelia ne programišiai, o jūs patys. Didesnė tikimybė yra ta, jog savo mobilųjį prietaisą pamesite ar pamiršite, negu į jį kas nors įsilauš. Taigi pirmiausias dalykas, kurį turėtumėte padaryti, yra įjungti automatinį ekrano užrakinimą, dar vadinamą ekrano užraktu. Tai reiškia, kad kaskart jums panorus pasinaudoti savo prietaisu, pirmiausiai turėsite atrakinti ekraną, įvesdami patikimą skaičių kodą arba nuskaitydami piršto antspaudą. Taip užtikrinsite, jog pametus ar pavogus jūsų prietaisą, niekas prie jo negalės prisijungti. Be to, pateikiame dar kelis patarimus, kaip galite apsaugoti savo prietaisus:

Atnaujinimas

Įjunkite automatinį prietaiso operacinės sistemos ir programų atnaujinimą, kad jame visada būtų naujausios jų versijos. Programišiai programinėje įrangoje pastoviai ieško pažeidžiamų vietų, todėl programų leidėjai, norėdami jas pataisyti, nuolat išleidinėja programų naujinius arba pataisas. Visada naudojant naujausias operacinės sistemos ir mobiliųjų programų versijas, programišiams bus žymiai sudėtingiau įsilaužti į jūsų prietaisus.

Stebėjimas

Įdiekite ir įjunkite programinę įrangą, kurią naudodami, galėsite internetu stebėti savo mobiliojo prietaiso buvimo vietą. Tokiu būdu, pametus ar pavogus jūsų prietaisą, jūs galėsite internetu prie jos prisijungti ir nustatyti jo buvimo vietą, o blogiausiu atveju, nuotoliniu būdu ištrinti visą jame esančią informaciją.

Patikimos programos

Reikiamas programas parsisiųskite tik iš patikimų šaltinių. „iPad“ arba „iPhone“ įrenginių programas parsisiųskite iš „Apple“ „App Store“ programos. „Android“ įrenginių programas parsisiųskite iš „Google Play“ programos, o

„Amazon“ planšetinių kompiuterių programas parsisiųskite iš „Amazon“ „App Store“. Nors programas galite parsisiųsti ir iš kitų vietų, jos nėra tikrinamos, todėl yra žymiai didesnė tikimybė, jog prietaisas bus užkrėstas virusais. Taip pat, prieš parsisiųsdami programą, patikrinkite, ar ji turi daug teigiamų vartotojų atsiliepimų ir ar jos kūrėjas pastoviai ją atnaujina. Venkite neseniai išleistų naujų programų, kurios turi mažai vartotojų atsiliepimų arba kurios yra retai atnaujinamos. Galiausiai, nepriklausomai nuo to, iš kur gavote savo programą, kai tik jos nebereikės arba aktyviai nebenaudosite, rekomenduojame ją iš savo prietaiso ištrinti.

Privatumo parinktys

Įdiegdami naują programą, įsitikinkite, kad peržiūrėjote privatumo parinktis. Pavyzdžiui, ar ką tik parsisiųstai programai išties reikia prieigos prie visų jūsų draugų sąrašo ir jų kontaktinės informacijos? Taip pat, rekomenduojame visose programose išjungti vietos nustatymą ir įjungti jį tik toms programoms, kurioms išties to reikia. Jei nesate tikri dėl programos leidimų prašymo, susiraskite kitą programą, kuri atitiktų jūsų poreikius. Be to, reguliariai peržiūrėkite, ar suteikti leidimai nepasikeitė.

Atsarginės kopijos

Visada darykite savo duomenų atsargines kopijas. Mobiliuosiuose prietaisuose didelės jūsų informacijos dalies (nuotraukų ar žinučių) atsarginės kopijos yra daromos automatiškai. Tačiau atsarginėse kopijose taip pat yra saugoma jūsų prietaiso konfigūracija, programos ir kita informacija, todėl ją yra žymiai lengviau atkurti iš pamesto įrenginio ar perkelti į naują.

Darbas

Būdami darbe, būkite itin atsargūs ir niekada nieko nefotografuokite bei nefilmuokite, kadangi interaktyvių lentų ar kompiuterių ekranų nuotraukose galima išvysti konfidencialią informaciją.

Jūsų mobilieji prietaisai yra galinga priemonė, todėl norime, kad ja naudodamiesi mėgautumėtės. Todėl, laikydamiesi šių kelių paprastų patarimų, galite apsaugoti ne tik save, bet ir savo prietaisus.

Resources

Slaptafrazės:	https://www.sans.org/u/A3E
Atsarginių kopijų darymas ir atkūrimas:	https://www.sans.org/u/A3z
Kaip saugiai pakeisti mobilųjį prietaisą nauju?:	https://www.sans.org/u/A3u
Kaip saugiai naudotis mobiliosiomis programomis?:	https://www.sans.org/u/A3p
SANS instituto dienos patarimas apie saugą:	https://www.sans.org/tip_of_the_day.php

License