Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Securizarea dispozitivului mobil personal

Generalități

Dispozitivele mobile personale sunt un mijloc uimitor de comunicare cu prietenii, pentru cumpărături și servicii bancare online, pentru vizionarea de filme, jocuri și pentru o multitudine de alte activități. Cum aceste dispozitive joacă un rol așa de important în viața dumneavoastră, iată câțiva pași simpli pentru a vă menține securitatea personală și a acestor dispozitive.

Securitatea dispozitivelor personale

S-ar putea să vă surprindă să aflați că cel mai mare risc pentru dispozitivul dumneavoastră mobil nu e activitatea hackerilor ci mai degrabă dumneavoastră înșivă. Sunt șanse mult mai mari să vă pierdeți sau să uitați mobilul decât să fiți victima unui atac informatic. Primul lucru pe care trebuie să-l faceți pentru a vă proteja dispozitivul este să activați blocarea automată a ecranului, deseori denumită „screenlock”. Aceasta înseamnă că de fiecare dată când doriți să utilizați dispozitivul, trebuie mai întâi să deblocați ecranul, cum ar fi folosind un cod de acces puternic sau o amprentă digitală. Acest lucru vă ajută să vă asigurați că, dacă dispozitivul este pierdut sau furat, nimeni nu îl poate accesa. În plus, iată câteva sfaturi pentru a vă ajuta să vă protejați dispozitivele.

Actualizarea

Activați actualizarea automată pe dispozitivele dumneavoastră, astfel încât să ruleze întotdeauna cea mai recentă versiune a sistemului de operare și a aplicațiilor. Atacatorii sunt mereu în căutare de noi vulnerabilități în software, iar producătorii lansează în mod constant noi actualizări pentru a le repara. Prin rularea întotdeauna a celui mai recent sistem de operare și a aplicațiilor mobile, faceți mult mai greu pentru oricine să acceseze fraudulos dispozitivele dumneavoastră.

Urmărirea

Instalați sau activați software pentru a urmări de la distanță dispozitivul mobil prin Internet. În acest fel, dacă dispozitivul este pierdut sau furat, vă puteți conecta la acesta prin Internet și găsi locul unde se află sau, în cel mai rău caz, puteți șterge de la distanță toate informațiile pe care le aveți pe el.

Aplicații de încredere

Descărcați numai aplicațiile de care aveți nevoie și din surse de încredere. Pentru iPad-uri sau iPhone-uri înseamnă descărcarea de aplicații de pe Apple App Store. Pentru aplicații Android descărcați numai de pe Google Play iar pentru tabletele Amazon limitați-vă la Amazon App Store. Deși este posibil să puteți descărca aplicații de pe alte site-uri, acestea nu sunt verificate și sunt mult mai susceptibile de a fi infectate. De asemenea, înainte de a descărca o aplicație,

asigurați-vă că are o mulțime de recenzii pozitive și că este actualizată activ de către producător. Feriți-vă de aplicațiile noi, aplicații cu câteva recenzii sau rareori actualizate. În cele din urmă, indiferent de locul de unde ați obținut aplicația, odată ce nu mai aveți nevoie de ea sau nu o folosiți în mod activ, vă recomandăm să o ștergeți de pe dispozitiv.

Opțiuni de confidențialitate

Când instalați o aplicație nouă, asigurați-vă că revizuiți opțiunile de confidențialitate. De exemplu, aplicația pe care tocmai ați descărcat-o trebuie într-adevăr să aibă acces la toate informațiile despre prieteni și contacte? De asemenea, vă recomandăm să dezactivați urmărirea locației, apoi să activați identificarea locației numai pentru aplicațiile pentru care considerați că e necesar. Dacă nu sunteți confortabil cu cerințele de acces ale unei aplicații, găsiți una diferită care să corespundă nevoilor dumneavoastră. În plus, verificați periodic permisiunile aplicațiilor, pentru a vă asigura că nu s-au schimbat.

Copiile de rezervă

Întotdeauna copiați-vă datele. Pentru dispozitivele mobile, multe informații sunt adesea salvate automat, cum ar fi fotografiile sau mesajele personale. Cu toate acestea, copiile de siguranță stochează, de asemenea, configurația, aplicațiile și alte informații despre dispozitiv, ceea ce face mult mai ușoară recuperarea datelor pentru un dispozitiv pierdut sau trecerea la unul nou.

La lucru

Când lucrați, fiți foarte atent și nu faceți niciodată poze sau videoclipuri care ar putea include în mod accidental informații confidențiale, cum ar fi imagini cu tablele din birouri sau ecrane de calculator.

Dispozitivele mobile sunt un instrument puternic, unul de care vrem să vă bucurați și să îl utilizați. Urmând acești câțiva pași simpli realizați un progres semnificativ în obținerea securității dispozitivelor proprii și a dumneavoastră.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse suplimentare

Propozițiile-parolă:	https://www.sans.org/u/A3E
Copiile de siguranță și recuperarea datelor:	https://www.sans.org/u/A3z
Casarea dispozitivelor mobile:	https://www.sans.org/u/A3u
Utilizarea în siguranță a aplicațiilor mobile:	https://www.sans.org/u/A3p
Recomandarea zilei de la SANS:	https://www.sans.org/tip_of_the_day.php

licență

OUCH! este publicat de SANS, Securing The Human și distribuit sub licența Creative Commons BY-NC-ND, versiunea 4. Sunteți liberi să distribuiți acest buletin informativ sau să-l folosiți în programele de instruire proprii atât timp cât nu-i modificați conținutul. Pentru traduceri sau informații suplimentare scrieți la www.sans.org/security-awareness/ouch-newsletter. Echipa editorială: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traducere: Cosmin Hănulescu