OUCH! | Decembrie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Datele personale**
- **Curățarea dispozitivului mobil**
- **SIM-ul și cartelele de memorie externă**

Casarea dispozitivelor mobile

Generalități

Dispozitivele mobile, cum ar fi telefoanele, ceasurile inteligente sau tabletele, continuă să avanseze tehnologic într-un ritm al inovației amețitor. Drept consecință unii oameni le schimbă frecvent, deseori anual. Din păcate prea mulți pur și simplu le aruncă, fără să se gândească câtuși de puțin la volumul de informații personale ce s-a acumulat pe acestea. În acest buletin informativ vom trece în revistă tipurile de informații personale ce pot fi stocate pe dispozitivul mobil și cum le puteți șterge în siguranță înainte să aruncați sau să returnați dispozitivul. Dacă acesta v-a fost pus la dispoziție de către angajator sau conține date ale companiei la care lucrați, consultați-vă superiorul ierarhic în privința procedurii corecte de efectuare a unor copii de siguranță a datelor și casarea efectivă a dispozitivului, înainte să parcurgeți pașii descriși mai jos.

Editor Invitat

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) este cercetător principal în domeniul criminalității digitale și coordonează eforturile de investigație criminalistică la ManTech CARD. Ea este coordonator și coautor al cursului SANS Analiza Criminalistică Avansată pentru Telefoanele Inteligente (FOR585) și instructor pentru cursul Analiza Criminalistică pe sisteme Windows (FOR408). Heather scrie pe blog-ul **smarterforensics.com**.

Datele personale

Dispozitivele mobile stochează mult mai multe date personale decât vă dați seama, poate chiar mai multe decât un calculator personal de birou. În mod uzual, informațiile stocate pe un dispozitiv mobil pot include:

- Unde locuiți, unde lucrați și care sunt locurile pe care le vizitați în mod frecvent.
- Datele de contact pentru toți cei din agendă, incluzând membrii familiei, prietenii și colegii de serviciu.
- Istoricul apelurilor telefonice, a celor primite sau inițiate cât și a celor pierdute.
- Mesaje text (SMS), audio sau multimedia.
- Conversațiile din aplicații cum ar fi cele de mesagerie instantanee securizată, jocurile sau cele de socializare online.
- Istoricul locurilor vizitate, în baza coordonatelor GPS sau a radio-antenelor celulelor de telefonie mobilă.
- Istoricul navigării pe Internet, cookies și copiile temporare a paginilor Web afișate.
- Fotografii, filme sau înregistrări audio personale și mesaje email.
- Parole salvate și date de acces la conturi personale, cum ar fi cele bancare sau email.
- Acces la fotografii, fișiere sau alte informații stocate în Cloud.
- Informații de monitorizare a stării de sănătate, ce pot include vârsta, ritmul cardiac, presiunea sanguină sau dieta urmată.

Curățarea dispozitivului mobil

După cum se poate vedea, cel mai probabil dispozitivul mobil conține o cantitate foarte mare de informații personale. Indiferent

Casarea dispozitivelor mobile

de modul în care alegeți să renunțați la dispozitivul mobil pe care-l aveți, fie prin donație, schimbându-l cu unul nou, fie făcându-l cadou unui alt membru al familiei, prin revânzare sau pur și simplu aruncându-l, trebuie să vă asigurați înainte de toate că ați șters informațiile delicate de pe acesta. Poate nu vă dați seama, dar simpla ștergere a acestor informații nu e suficientă, acestea putând fi recuperate cu ușurință folosind programe gratuite disponibile pe Internet. Prin urmare trebuie să ștergeți toate datele din dispozitiv într-o manieră ireversibilă, securizată. Această metodă suprascrie informația, garantând imposibilitatea recuperării ei. Rețineți că, înainte să faceți o ștergere securizată a datelor, veți vrea cel mai probabil să faceți o copie de siguranță a acestora, pentru a putea să le restaurați pe un nou dispozitiv.

Atunci când renunțați la dispozitivul mobil asigurați-vă că ați făcut o resetare a acestuia la parametrii originali de fabrică și că ați scos SIM-ul și orice card de memorie SD, dacă era prevăzut cu vreunul.

Modalitatea cea mai simplă pentru a șterge ireversibil datele este folosind funcția de resetare la parametrii originali de fabrică. Această funcție aduce dispozitivul în starea inițială avută atunci când a fost cumpărat. Am constatat că resetarea la parametrii originali de fabrică oferă cea mai sigură și simplă metodă de a îndepărta datele din dispozitivul mobil. Această funcție diferă de la un producător la altul; mai jos sunt listați pașii pentru cele mai populare dispozitive:

- Dispozitive bazate pe Apple iOS: Settings | General | Reset | Erase All Content and Settings
- Dispozitive bazate pe Android: Settings | Privacy | Factory Data Reset

Din nefericire ștergerea datelor personale dintr-un dispozitiv bazat pe sistemul Windows Phone nu este așa de simplă precum reinițializarea parametrilor de fabrică. Se cercetează încă variantele care să ofere o metodă care să garanteze ștergerea ireversibilă a datelor de pe acest tip de dispozitive. Dacă mai aveți întrebări referitoare la cum se face resetarea la parametrii de fabrică, verificați manualul de utilizare primit sau consultați site-ul producătorului.

SIM-ul și cartelele de memorie externă

Pe lângă datele stocate pe dispozitiv trebuie să vă gândiți ce faceți cu SIM-ul (Subscriber Identity Module). SIM-ul este cartela folosită de dispozitiv pentru stabilirea de conexiuni telefonice și de date. Atunci când resetați dispozitivul la parametrii săi de fabrică, SIM-ul păstrează detalii despre contul dumneavoastră de client. Dacă păstrați numărul de telefon pentru a-l muta pe alt dispozitiv, luați legătura cu agentul de vânzări pentru efectuarea transferului SIM-ului. Dacă nu se poate, deoarece, de exemplu, noul telefon folosește un SIM de alte dimensiuni, păstrați vechiul SIM și distrugeți-l, pentru a preveni refolosirea lui de către altcineva.

Casarea dispozitivelor mobile

Unele dispozitive mobile folosesc o cartelă SD (Secure Digital) separată, pentru o capacitate suplimentară de stocare. Aceste cartele conțin de obicei fotografii, aplicații pentru telefoanele inteligente sau alte date personale. Nu uitați să scoateți aceste cartele din dispozitivul mobil atunci când renunțați la el (la unele dispozitive acestea se află ascunse în compartimentul bateriei, cel mai probabil sub ea). Aceste tipuri de cartele de stocare pot fi adesea refolosite pe noile dispozitive mobile sau pot fi atașate ca dispozitive generice de stocare de date pe un calculator personal prevăzut cu un adaptor USB. Dacă refolosirea unei cartele SD nu este posibilă atunci, la fel ca în cazul vechiului SIM, vă recomandăm distrugerea ei.

Dacă nu sunteți singur în privința pașilor descriși în acest articol, mergeți cu dispozitivul mobil la magazinul de unde l-ați cumpărat și cereți ajutorul unui tehnician instruit corespunzător. În final, dacă vă hotărâți să aruncați dispozitivul, vă rugăm să vă gândiți la posibilitatea donării lui. Sunt multe asociații caritabile excepționale care acceptă dispozitive mobile folosite.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS securingthehuman.sans.org/ouch/archives

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

Securizarea noii tablete:	https://securingthehuman.sans.org/ouch/2016#january2016
Copiile de siguranță și recuperarea datelor:	https://securingthehuman.sans.org/ouch/2015#august2015
Cursul de Analiză Criminalistică Avansată pentru Telefoane Inteligente:	https://sans.org/for585
Arhiva buletinelor informative OUCH:	https://securingthehuman.sans.org/ouch/archives

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducere: Cosmin Hănulescu