OUCH! | Iulie 2015

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Informații cu caracter personal
- Securitate

Platformele de socializare online

Generalități

Platformele online de socializare, cum ar fi Facebook, Twitter, Instagram şi LinkedIn sunt resurse excepționale ce permit întâlnirea, interacțiunea și partajarea informațiilor cu oameni din întreaga lume. Cu toate astea, această versatilitate este însoțită de riscuri, nu numai pentru Dumneavoastră dar și pentru membrii familiei, prieteni sau angajator. În acest buletin informativ explicăm aceste pericole și cum se pot folosi aceste site-uri în siguranță și în mod securizat.

Editor Invitat

Tanya Baccam este consultant în securitatea informației cu o carieră îndelungată. A fost autor și instructor în cadrul SANS mai mult de o decadă, pentru cursuri ce includ SEC502, SEC542, SEC401, MGT414, AUD507 cât și alte cursuri. O puteți urmări pe Twitter la **@tbaccam**.

Informații cu caracter personal

O preocupare comună legată de platformele de socializare online este protecția datelor personale. Pericolele posibile pot fi:

- **Impactul asupra viitorului Dumneavoastră**: Unele organizații caută informații online pentru verificarea antecedentelor. Fotografiile sau comentariile jenante sau acuzatoare, indiferent de vechime, vă pot împiedica în obținerea unui post sau a unei promovări. Similar, multe universități fac verificări asemănătoare pentru candidaturile noilor studenți. Elementele de configurare a protecției datelor personale s-ar putea să nu ajute, deoarece aceste organizații pot să vă ceară să vă exprimați interesul pentru paginile lor prin butonul „Like“ sau să vă înregistrați pe aceste pagini, iar anumite comentarii online pot fi arhivate pe mai multe site-uri.
- **Atacuri îndreptate împotriva Dumneavoastră**: Răufăcătorii pot analiza comentariile pe care le faceți online și le pot utiliza pentru a obține accesul la datele Dumneavoastră sau ale companiei unde lucrați. De exemplu, ei pot folosi informațiile pe care le faceți publice pentru a ghici „întrebările secrete“ necesare reinițializării parolelor online, pot iniția atacuri cu destinație bine definită prin mesaje email ce vi se adresează — așa-zisele campanii *spearphishing*, sau pot suna pe cineva din companie pretinzând că sunteți Dumneavoastră. Mai mult, aceste atacuri se pot extinde către lumea reală, prin identificarea adreselor unde locuiți sau unde lucrați.
- **Atingerea adusă accidental imaginii angajatorului**: Infractorii sau competitorii pot folosi orice informații sensibile pe care le faceți publice despre companie pentru a face rău angajatorului Dumneavoastră. Asigurați-vă că verificați politicile companiei înainte să faceți publice informații despre serviciul Dumneavoastră și, în plus, aveți în vedere faptul că unele comentarii de pe platformele de socializare online pot fi monitorizate.

Cea mai bună protecție este să vă limitați în comentarii. Într-adevăr, elementele de configurare a protecției datelor personale ajută oarecum, dar cel mai adesea generează confuzie și se schimbă frecvent fără să știți. Ceea ce credeați că este secret poate deveni brusc public, din varii motive. În plus, caracterul privat al comentariilor Dumneavoastră se limitează și este

Platformele de socializare online

garantat de oamenii cu care partajați aceste informații. Cu cât audiența formată din prieteni și alte contacte este mai mare, cu-atât sunt mai mari șansele ca această informație să devină publică. Trebuie să acceptați că tot ceea ce scrieți poate sau chiar va deveni informație publică, o parte permanentă a Internetului.

În final, fiți conștienți de ce comentează prietenii despre Dumneavoastră. Dacă scriu ceva cu care nu sunteți de acord, cereți-le să șteargă. Dacă refuză sau vă ignoră, contactați site-ul de socializare și cereți-le să șteargă acele informații pentru Dumneavoastră. În același timp, dați dovadă de respect în comentariile pe care le faceți despre alții.



Site-urile de socializare online sunt distractive și puternice, dar fiți atenți la ce publicați și cui vă adresați.

Securitate

Pe lângă preocupările legate de securitatea datelor personale, iată câteva măsuri pentru a ajuta la protecția conturilor și activității pe care o aveți în mediile de socializare online.

- **Autentificare**: Protejați-vă fiecare cont cu o parolă puternică, unică, și nu o faceți cunoscută nimănui. Suplimentar, multe site-uri oferă mecanisme puternice de autentificare, cum ar fi verificarea în doi pași. Activați întotdeauna aceste mecanisme puternice de autentificare, atunci când este posibil. În sfârșit, nu folosiți contul de socializare online pentru autentificarea pe alte site-uri, căci dacă este compromis toate celelalte conturi sunt vulnerabile.
- **Elemente de configurare a protecției datelor personale**: Dacă le folosiți, asigurați-vă că le verificați și le testați periodic. Site-urile de socializare modifică frecvent aceste elemente de configurare și este ușor să apară greșeli. În plus, multe aplicații și servicii permit atașarea de etichete cu coordonate (geolocație) la mesaje publicate. Verificați periodic aceste configurații dacă doriți să păstrați secretă localizarea Dumneavoastră fizică.
- **Criptarea**: Platformele de socializare online folosesc criptarea (HTTPS) pentru securizarea conexiunilor online cu site-ul. Unele site-uri, cum ar fi Twitter sau Google+, activează criptarea în mod implicit, în timp ce altele necesită activarea manuală a conexiunilor HTTPS. Verificați-vă configurația contului de socializare online și activați HTTPS ca mod de conectare implicit ori de câte ori e posibil.
- **Email**: Fiți precauți față de mesajele email ce pretind că sunt expediate de site-urile de socializare online, căci acestea pot fi contrafăcute cu ușurință de răufăcătorii ce lansează atacuri pe această cale. Cel mai sigur mod de a răspunde unor astfel de mesaje este să intrați direct în contul Dumneavoastră pe site-ul platformei de socializare, probabil folosit o adresă salvată în prealabil, să citiți și să răspundeți apoi oricărui mesaj sau notificări direct de pe site.
- **Adrese cu conținut înșelător / escrocherii online**: Fiți atenți la orice adresă suspectă sau potențiale escrocherii propagate prin intermediul site-urilor de socializare. Răufăcătorii folosesc platformele de socializare online pentru a distribui prin intermediul lor atacurile. Dacă un mesaj este transmis de un prieten nu înseamnă că mesajul este în mod cert scris de acesta, securitatea contului său poate fi compromisă. Dacă un membru al familie sau un prieten a publicat

Platformele de socializare online

un mesaj bizar pe care nu-l puteți verifica (bunăoară că au fost jefuiți și că au nevoie să le trimiteți bani), sunați-l pe telefonul mobil sau folosiți alt mijloc pentru a confirma că mesajul este într-adevăr trimis de el.

- **Aplicațiile de pe dispozitivele mobile**: Multe site-uri de socializare oferă aplicații pentru dispozitive mobile cu care să vă puteți accesa contul online. Asigurați-vă că descărcați aceste aplicații de pe site-uri de încredere și că vă protejați cu o parolă puternică dispozitivul mobil. Dacă acesta nu este protejat cu parolă atunci când îl pierdeți oricine vă poate accesa contul de socializare online prin intermediul dispozitivului mobil și poate pretindă că sunteți Dumneavoastră.

Site-urile de socializare online sunt o modalitate extraordinară de comunicare și pentru a păstra legătura cu lumea. Dacă urmați recomandările descrise aici, puteți să vă bucurați de o experiență online mai sigură. Pentru a învăța mai multe despre cum să folosiți în siguranță platformele de socializare online sau cum să raportați activitățile neautorizate, verificați pagina dedicată securității de pe site-urile corespunzătoare acestora.

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 http://www.securingthehuman.org

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Propoziții-parolă:	http://www.securingthehuman.org/ouch/2015#april2015
Verificarea în doi pași:	http://www.securingthehuman.org/ouch/2013#august2013
Utilizarea în siguranță a aplicațiilor de pe dispozitivele mobile:	http://www.securingthehuman.org/ouch/2015#january2015
Educarea copiilor cu privire la securitatea cibernetică:	http://www.securingthehuman.org/ouch/2015#june2015
Securitatea Facebook:	https://www.facebook.com/safety

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