OUCH! | Octombrie 2017

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Introducere**
- **Cinci pași simpli**
- **Securitatea copiilor aflați în vizită**

Ajutându-i pe ceilalți să se protejeze

Introducere

Mulți dintre noi se simt în largul lor cu tehnologia, incluzând aici și utilizarea ei în siguranță și securizată. Cu toate astea, unii prieteni sau membri de familie s-ar putea să nu fie la fel de confortabili. În realitate, aceștia ar putea fi derutați, intimidați sau chiar speriați de tehnologie. Acest lucru îi face foarte vulnerabili față de atacurile cibernetice din zilele noastre. Securitatea cibernetică nu trebuie să fie înfricoșătoare, ci e chiar ceva simplu atunci când îi înțelegi elementele de bază. Ei au nevoie, așadar, de un ghid ca dumneavoastră, pentru a-i ajuta să înțeleagă chestiunile fundamentale.

Editor Invitat

Randy Marchany (Twitter: **@randymarchany**) este CISO la Virginia Tech și instructor certificat SANS.

Cinci pași simpli

Iată cinci pași simpli pe care-i puteți parcurge pentru a-i ajuta pe ceilalți să-și depășească temerile și să folosească eficient tehnologia actuală. Pentru mai multe detalii legate de fiecare punct, consultați secțiunea referințe, la sfârșitul acestui buletin informativ.

1. **Ingineria socială**: Ingineria socială este o tehnică obișnuită folosită de răufăcători pentru a păcăli oamenii să facă ceva ce nu ar trebui, cum ar fi să le faceți cunoscută parola, să infectați calculatorul sau să dezvăluiți date confidențiale. Acest lucru nu e ceva nou, înșelătoriile și escrocii există de când lumea. Singura diferență este că acum răufăcătorii aplică aceleași tehnici în mediul online, pe Internet. Îi puteți ajuta pe ceilalți explicându-le cele mai frecvente indicii ale atacurilor de inginerie socială, cum ar fi atunci când cineva induce un sentiment puternic de urgență, când ceva pare să fie prea bun ca să fie adevărat, sau când atacatorul pretinde să fie cineva cunoscut dar mesajele sale nu sună ca fiind ale prietenului dumneavoastră. Arătați exemple ale atacurilor de inginerie socială frecvent întâlnite, cum ar fi mesajele de phishing sau faimosul apel telefonic de la serviciul tehnic Microsoft. Dacă nu altceva, măcar asigurați-vă că membrii familiei înțeleg să nu dea parola personală nimănui sau să permită accesul la distanță pe calculatorul propriu.
2. **Parolele**: Parolele puternice sunt cruciale pentru protejarea dispozitivelor și a oricărui cont online. Recomandăm propozițiile-parolă, deoarece sunt mai ușor atât de scris cât și de memorat. Propozițiile-parolă nu sunt altceva decât parole formate din mai multe cuvinte. În plus, ajutați-i să instaleze și să folosească un program de gestiune a parolelor. Este important să aveți o parolă unică pentru fiecare dintre conturile și dispozitivele dumneavoastră. Dacă un manager de parole este prea mult pentru ei, învățați-i, poate, să-și scrie parolele undeva, apoi să le depoziteze într-un loc securizat. În final, pentru conturile importante, ajutați-i să activeze verificarea în doi pași (deseori cunoscută ca autentificare cu doi

Ajutându-i pe ceilalți să se protejeze

factori). Verificarea în doi pași este unul dintre cei mai eficace pași pe care-i puteți face pentru securizarea oricărui cont.

3. **Actualizarea**: Menținerea sistemelor la zi și complet actualizate este un pas cheie pe care oricine îl poate face pentru securizarea dispozitivelor personale. Acest lucru nu este aplicabil doar calculatoarelor și dispozitivelor mobile, ci oricăror altora conectate la Internet, cum ar fi consolelor de jocuri, termometrelor sau chiar a iluminatului sau boxelor audio. Cel mai simplu mod pentru a vă asigura că toate dispozitivele sunt la zi este să activați actualizarea automată, oricând este posibil.
4. **Programe antivirus**: Oamenii fac greșeli, uneori dăm clic pe sau instalăm lucruri care probabil că n-ar trebui, ce pot infecta sistemele proprii. Programele antivirus sunt concepute să ne protejeze de aceste greșeli. Deși antivirusul nu poate opri orice tip de malware, ajută, totuși, la detectarea și prevenirea celor mai frecvente atacuri. Ca atare, asigurați-vă că orice calculator domestic personal are antivirus instalat și că acesta este actualizat și activ. Suplimentar, multe dintre soluțiile antivirus actuale includ și alte tehnologii de securitate, cum ar fi protecția programului de navigare online sau un firewall.
5. **Copiile de siguranță**: când orice alt altceva eșuează, copiile de siguranță sunt singura modalitate în care vă puteți recupera de pe urma unei greșeli, cum ar fi ștergerea fișierelor greșite sau atacurile cibernetice, ca programele Ransomware. Fiți siguri că familia și prietenii au un sistem automat de realizare a copiilor de siguranță pus la punct. Deseori cele mai simple soluții sunt bazate pe tehnologie Cloud, care creează copiile de siguranță pentru dispozitivele proprii în fiecare oră sau ori de câte ori modificați un fișier. Aceste soluții ușurează nu numai crearea copiilor de siguranță ci și recuperarea datelor.

Ajutați-i pe ceilalți să profite la maxim de tehnologie în siguranță făcându-le cunoscuți acești cinci pași simpli.

Securitatea copiilor aflați în vizită

Dacă sunteți familiarizați cu tehnologia atunci cel mai probabil că nu v-ați securizat doar personal ci și copiii. Cu toate astea, atunci când copiii vizitează o rudă ce nu e obișnuită cu tehnologia, cum ar fi bunicii, acești apropiați s-ar putea să nu știe cum e cel mai bine să protejezi copiii online sau care sunt așteptările dumneavoastră legate de asta. Mai jos aveți câțiva pași pe care-i puteți urma pentru a ajuta la protecția copiilor atunci când sunt în vizită la alții, în special în familie.

- **Reguli**. Asigurați-vă ca, dacă aveți o seamă de reguli și așteptări legate de securitatea copiilor, ceilalți le cunosc. De exemplu, există vreo regulă pentru cât timp își petrec copiii online, cu cine pot vorbi și ce fel de jocuri pot folosi online sau nu? Credeți-ne, nu vă bazați pe copii să le explice regulile celorlalți membri de familie. O idee ar fi să concepeți o „listă” de reguli pe care s-o faceți cunoscută rudelor pe care copiii le frecventează des.

Ajutându-i pe ceilalți să se protejeze

- **Controlul**: dacă un copil înțelege tehnologia mai bine decât tutorele său, poate profita de acest lucru. De exemplu, copiii pot cere sau obține cumva drepturi de administrator pe calculatorul bunicilor pentru ca apoi să facă orice își doresc, cum ar fi să instaleze un joc pe care n-ați vrea să-l joace. Asigurați-vă că rudele înțeleg că nu trebuie să dea copiilor vreun drept de acces suplimentar față de ceea ce s-a stabilit în prealabil.

În final sugerați-le celorlalți să se aboneze la buletinul informativ OUCH!, pentru a continua să învețe pe cont propriu. Acest buletin informativ este publicat cu frecvență lunară în mai mult de 20 de limbi. Abonați-vă la https://securingthehuman.sans.org/ouch.

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

Ingineria socială:	https://securingthehuman.sans.org/ouch/2017#january2017
Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2017#april2017
Programe de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2017#september2017
Verificarea în doi pași:	https://securingthehuman.sans.org/ouch/2015#september2015
Copiile de siguranță și recuperarea datelor:	https://securingthehuman.sans.org/ouch/2017#august2017
Securizarea activității online a copiilor astăzi:	https://securingthehuman.sans.org/ouch/2017#may2017

Echipa editorială: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducere: Cosmin Hănulescu