SANS SECURITY AWARENESS

cegeka

OUCH! | Noiembrie 2017

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Magazine online frauduloase**
- **Calculatorul personal / Dispozitivul mobil**
- **Cardul de credit**

Cumpărături online în siguranță

Generalități

Perioada sărbătorilor se apropie pentru mulți dintre noi și, în curând, milioane de oameni în jurul lumii vor fi în căutare pentru a cumpăra cadourile perfecte. Mulți dintre noi vor alege să cumpere online, fiind în căutare de promoții speciale și pentru evitarea cozilor și a mulțimilor nerăbdătoare. Din nefericire, aceasta e perioada în care răufăcătorii creează site-uri frauduloase pentru cumpărături online, pentru a escroca și a fura de la alții. Mai jos explicăm riscurile cumpărăturilor online și cum să obținem acea ofertă specială în siguranță.

Editor Invitat

Lenny Zeltser realizează produse de securitate la Minerva Labs și ține cursuri de combaterea programelor malware la SANS Institute. Lenny este activ pe Twitter la **@lennyzeltser** și scrie pe blogul său despre securitatea informației la **zeltser.com**.

Magazine online frauduloase

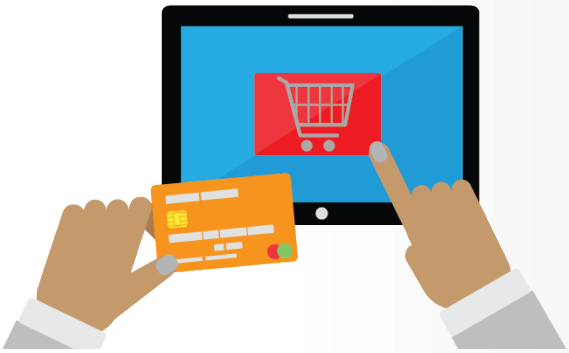
Deși multe magazine online sunt legitime, există unele site-uri false create de infractori. Aceștia concep site-urile frauduloase copiind aspectul unor site-uri reale sau folosind denumirile unor magazine sau mărci bine-cunoscute. Ei folosesc apoi aceste site-uri false pentru jefuirea oamenilor care sunt în căutarea celor mai bune oferte. Atunci când căutați online cele mai mici prețuri cu putință v-ați putea trezi direcționați către un astfel de site fraudulos. Atunci când alegeți un site pentru a face cumpărături, fiți rezervați față de acele site-uri care promovează prețuri semnificativ mai mici decât oriunde altundeva sau site-uri ce ofertă produse ce nu mai sunt disponibile nicăieri în țară. Explicația pentru faptul că produsele lor sunt mai ieftine sau disponibile este aceea că ce primiți nu este legitim, ar putea fi contrafăcut sau furat sau, în multe cazuri, nu vi se livrează nimic. Protejați-vă după cum urmează:

- Atunci când e posibil, cumpărați de pe site-urile pe care le cunoașteți deja, în care aveți încredere și cu care ați avut relații de afaceri anterior.
- Verificați că site-ul are o adresă de email legitimă și un număr de telefon pentru vânzări și întrebări legate de asistență. Dacă site-ul pare suspect, sunați și vorbiți cu o persoană. Dacă nu reușiți să luați legătura cu nimeni este un semn că aveți de-a face cu un site fraudulos.
- Căutați semnalmente evidente cum ar fi ocazii prea bune ca să fie adevărate sau gramatică și ortografie slabe.
- Fiți foarte rezervați dacă un site pare să fie o copie fidelă a unui site bine cunoscut pe care l-ați folosit în trecut, dar numele acestuia sau al domeniului Internet este puțin diferit. De exemplu, puteți fi obișnuiți să cumpărați online

Cumpărături online în siguranță

de pe Amazon.com, al căror site este https://www.amazon.com. În schimb, fiți foarte suspicioși dacă vă treziți pe un site care pretinde că e Amazon, cum ar fi http://store-amazoncom.com.

- Scrieți numele magazinului sau adresa URL într-un portal de căutare online și vedeți ce păreri au avut alții. Căutați termeni ca „fraudă", „escrocherie", „niciodată" sau „fals". O lipsă de recenzii poate de asemenea fi un indiciu că site-ul este foarte nou și ar putea fi lipsit de credibilitate.
- Înainte să cumpărați orice, asigurați-vă că aveți o conexiune securizată cu site-ul. Majoritatea programelor de navigare online evidențiază conexiunile securizate afișând un lacăt și / sau prefixul HTTPS scris cu verde exact înaintea numelui site-ului.



Protejați-vă online făcând cumpărăturile numai pe site-uri de încredere, cu reputație recunoscută.

Rețineți: doar pentru că site-ul are un aspect profesional asta nu înseamnă că e legitim. Dacă nu sunteți confortabili cu site-ul, nu-l folosiți. Căutați, în schimb, un site bine-cunoscut, de încredere, pe care l-ați mai folosit în siguranță în trecut. Poate că nu mai găsiți acea ofertă excepțională, dar sunteți mult mai probabil în situația de a obține un produs legitim, evitând să vă fie furate datele personale și financiare.

Calculatorul personal / Dispozitivul mobil

În plus față de cumpărături făcute pe site-uri legitime, veți dori să vă asigurați că dispozitivul mobil și calculatorul personal sunt securizate. Răufăcătorii vor încerca să vă infecteze echipamentele ca să poată extrage conturi bancare, date despre cardurile de credit sau parole. Urmați pașii de mai jos pentru a vă păstra dispozitivele securizate:

- Dacă aveți copii, luați în calcul deținerea a două dispozitive, unul pentru copii și unul pentru adulți. Copiii sunt curioși și interacționează cu tehnologia, și în consecință e mult mai probabil ca să infecteze dispozitivul personal. Folosind un calculator sau o tabletă separat, doar pentru tranzacții online, cum ar fi serviciile bancare sau cumpărături, reduceți riscul de a fi infectați.
- Instalați întotdeauna cele mai recente actualizări și folosiți programe antivirus permanent aduse la zi. Acest lucru face mult mai dificil pentru răufăcători să vă infecteze dispozitivul.

Cardul de credit

Verificați periodic extrasul de cont al cardului de credit pentru a identifica orice activitate suspectă, mai ales dacă folosiți cardul pentru a face cumpărături online sau dacă ați folosit un site nou. Unii ofertanți de carduri de credit vă pun la dispoziție

Cumpărături online în siguranță

posibilitatea alertării prin email sau mesaj text de fiecare dată când este înregistrată o tranzacție pe card, sau atunci când este depășită o limită prestabilită pentru suma retrasă. O altă opțiune este să aveți un card de credit doar pentru tranzacțiile online, în felul acest dacă este compromis puteți să schimbați cardul cu ușurință fără să afectați oricare alta dintre plățile personale. Dacă aveți credința că s-a comis o fraudă, sunați compania de credit imediat. Acesta este de asemenea un motiv pentru care veți vrea să folosiți carduri de credit pentru cumpărăturile online; evitați pe cât posibil folosirea cardurilor de debit. Cardurile de debit iau bani direct din contul bancar personal, dacă s-a comis o fraudă va fi mult mai dificilă recuperarea banilor. În final, aveți în vedere cardurile de credit care generează un număr de card unic pentru fiecare plată online, carduri pentru cadouri sau folosiți servicii de plată populare, cum ar fi PayPal, ce nu necesită să dezvăluiți numărul cardului de credit furnizorului.

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
Patru pași în păstrarea securității:	https://securingthehuman.sans.org/ouch/2016#october2016
Securizarea rețelei personale, domestice:	https://securingthehuman.sans.org/ouch/2016#february2016
Recomandarea zilei de la SANS:	https://www.sans.org/tip_of_the_day.php

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

