OUCH! | Noiembrie 2015

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Magazine online frauduloase**
- **Calculatorul personal / Dispozitivele mobile**
- **Cardul de credit**

Cumpărăturile online în siguranță

E sezonul precauției

Perioada sărbătorilor e aproape, curând milioane de oameni în jurul lumii vor fi în căutarea cadoului perfect. Mulți dintre noi vor alege să facă cumpărături online, în căutarea unui chilipir și pentru a scăpa de cozile mari și aglomerațiile nervoase. Din păcate aceasta este de asemenea perioada favorită a răufăcătorilor, pentru fraudă online și escrocherii financiare. Luna aceasta explicăm pericolele cumpărăturilor online și căile prin care vă puteți proteja.

Editor Invitat

Jonathan Homer (**@JonathanLHomer**) este lider recunoscut în domeniul instruirii asupra securității cibernetice, fiind activ atât în sectorul guvernamental cât și cel privat. Jon se specializează pe implicarea audienței și tehnici de ultimă oră în cursurile de instruire.

Magazine online frauduloase

Deși majoritatea magazinelor online sunt legitime, unele nu sunt, fiind site-uri falsificate, puse la punct de răufăcători. Aceștia creează astfel de site-uri false copiind aspectul vizual sau folosind numele unor magazine bine cunoscute. Apoi, ei folosesc aceste site-uri pentru a-i jefui pe cei care caută cea mai bună ofertă posibilă. Atunci când căutați online cele mai scăzute prețuri posibile veți fi probabil redirectați către unul dintre aceste site-uri frauduloase.

Atunci când alegeți un site pentru a cumpăra un produs, fiți rezervați față de site-urile care se laudă cu prețuri cu mult mai mici decât în oricare altă parte sau care oferă produse ce nu mai sunt în stoc nicăieri altundeva. Motivul pentru care produsele lor au prețurile atât de mici sau sunt disponibile este că ceea ce veți primi nu este original, ci un produs contrafăcut sau furat sau, în unele cazuri, pentru că nu veți primi nimic de fapt. Protejați-vă așadar în felul următor:

- Verificați dacă site-ul are o adresă poștală legitimă și un număr de telefon pentru vânzări și întrebări legate de asistența clienților. Dacă site-ul arată suspect, sunați și vorbiți cu un reprezentant.
- Căutați semne evidente de atenționare, cum ar fi o gramatică și ortografie precare.
- Fiți foarte circumspecți dacă un site pare să fie o copie fidelă a unuia bine-cunoscut pe care l-ați mai folosit în trecut, dar numele și adresa domeniului Internet sunt puțin diferite. De exemplu, sunteți obișnuiți să mergeți pe site-ul https://amazon.com pentru toate cumpărăturile pe care le faceți de la Amazon. Însă, trebuie să fiți foarte suspicioși dacă ajungeți pe un site care pretinde să fie Amazon, având adresa http://store-amazon.com.
- Scrieți manual numele magazinului sau adresa URL într-un motor de căutare online și vedeți ce-au avut de spus alții despre acel site în trecut. Căutați termeni precum „înșelătorie [scam]“, „niciodată [never again]“ sau „făcătură

Cumpărăturile online în siguranță

[fake]“. Lipsa comentariilor și impresiilor altora este de asemenea un semnal negativ, deoarece arată că site-ul este foarte nou.

Rețineți, doar pentru că site-ul arată profesional făcut nu înseamnă că este legitim. Dacă ceva ce ține de site ridică semne de întrebare, luați-vă puțin timp să investigați. Dacă nu vă simțiți siguri pe site-ul respectiv, nu-l folosiți. Căutați în schimb un site popular în care puteți avea încredere sau pe care l-ați mai folosit în trecut. Poate că nu mai găsiți o ofertă atât de tentantă sau acel lucru extrem de căutat, dar e mult mai probabil să sfârșiți cu un produs autentic și un raport curat pe cardul de credit.

Protejați-vă online făcând cumpărături numai pe site-uri de încredere, cu o reputație solidă.

Calculatorul personal / Dispozitivele mobile

Pe lângă cumpărăturile făcute pe site-uri legitime, trebuie să vă asigurați că propriul calculator sau dispozitiv mobil este securizat. Răufăcătorii vor încerca să vă infecteze echipamentele cu programe ce colectează date despre conturile bancare, informații despre credite și parole. Urmați pașii de mai jos pentru a vă păstra dispozitivele securizate:

- Dacă sunt copii în casă, luați în calcul folosirea a două dispozitive, unul pentru copii și unul pentru adulți. Copiii sunt animați de curiozitate și interacțiunea cu tehnologia și, drept consecință, sunt mult mai predispuși să infecteze propriul dispozitiv. Folosind un calculator sau o tabletă separat, numai pentru tranzacții online, cum ar fi serviciile bancare sau cumpărăturile, reduceți șansele de a fi infectați. Dacă un dispozitiv separat nu e o soluție viabilă, atunci folosiți conturi diferite pe același calculator și asigurați-vă că copiii nu au drepturi de administrator pe acesta.
- Conectați-vă numai la rețele fără fir pe care le controlați, cum ar fi rețeaua de acasă sau rețelele cunoscute, în care puteți avea încredere atunci când faceți tranzacții financiare. Folosirea rețelelor WiFi publice, cum sunt cele din cafenele, poate fi convenabilă pentru citirea știrilor dar nu pentru accesarea contului bancar personal.
- Întotdeauna instalați cele mai recente actualizări și folosiți un program antivirus ce este permanent menținut la zi. Aceasta face mult mai dificil pentru răufăcători să vă infecteze calculatorul.

Cardul de credit

Fiți atenți la extrasele cardului de credit pentru a identifica tranzacții suspecte. Verificați extrasele de cont regulat, cel puțin o dată pe lună. Unii ofertanți de carduri de credit vă pun la dispoziție opțiunea de a fi notificați prin email sau mesaj SMS de fiecare dată când se face o plată de pe card sau când suma reținută depășește o anumită valoare prestabilită. O altă opțiune

Cumpărăturile online în siguranță

este să aveți un card doar pentru tranzacțiile online, astfel încât, dacă acesta este compromis, să-l puteți schimba cu ușurință, fără impact asupra niciuneia dintre celelalte plăți pe care le faceți. Dacă aveți credința că s-a comis o fraudă, sunați imediat furnizorul cardului de credit și explicați situația. Acesta este de asemenea un motiv pentru care este mai bine să folosiți un card de credit pentru cumpărăturile online în locul unui card de debit. Cardurile de debit iau banii direct din contul bancar și, dacă s-a comis o fraudă, poate fi mult mai dificil să vă recuperați banii.

În final, există tehnologii noi care vă oferă posibilitatea plăților fără a dezvălui numărul cardului de credit. Aveți în vedere folosirea cardurilor care generează un număr de card unic pentru fiecare plată făcută online, sau folosiți servicii de plăți foarte cunoscute, cum ar fi PayPal, care nu vă impun să faceți cunoscut numărul de card vânzătorului.

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

Cinci elemente de bază pentru păstrarea securității:	https://www.securingthehuman.org/ouch/2014#october2014
Securizarea rețelei de acasă:	https://www.securingthehuman.org/ouch/2014#january2014
Despre securitatea tabletelor:	https://www.securingthehuman.org/ouch/2013#december2013
Recomandarea zilei:	https://www.sans.org/tip_of_the_day.php

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