G Data press release 2011

Nu oferiti cadouri de Craciun infractorilor cibernetici

G Data a identificat cele mai populare tipuri de escrocherii si ofera sfaturi pentru cumparaturi online sigure

Bucuresti (Romania), 7 decembrie 2011 – In perioada sarbatorilor de Craciun creste numarul cumparaturilor online cu mai mult de 50%, ceea ce face ca infractorii sa targeteze utilizatorii ce cauta cadoul potrivit. Ei isi ademenesc victimele prin e-mail-uri cu oferte de bunuri de lux sau chilipiruri sau prin notificari de livrare false. Infractorii incerca de obicei sa obtina date personale, precum detaliile de logare la un site de online banking sau informatii de pe cardurile de credit. G Data a identificat Top 5 pericole de care ar trebui sa se fereasca utilizatorii atunci cand cumpara online si ofera sfaturi de prevenire a acestor pericole.

Top 5 pericole ale cumparaturilor online de Craciun

1. E-mail-uri cu reclame-capcana

In aceste e-mail-uri, cei care fraudeaza promit produse brand, gen ceasuri de lux sau incaltaminte de firma scumpe, la un pret foarte mic. Link-urile integrate ademenesc utilizatorii catre site-uri infectate cu malware sau catre magazine online false de unde datele bancare sunt sustrase in timpul procesarii comenzii. Aceste tipuri de e-mail sunt usor de identificat dupa titluri gen: „De Craciun, mii de produse de lux la preturi incepand de la 100 lei."

2. Frauda prin online banking

Operatiunile de online banking sunt foarte populare printre persoanele care doresc sa cumpere cadouri online, datorita rapiditatii si usurintei cu care se fac transferurile bancare. Troienii bancari au inregistrat deasemenea o crestere a popularitatii printre infractori, care ii folosesc pentru a interveni in tranzactii de plati si a devia banii catre conturile proprii. Utilizatorii de computere se pot infecta cu malware prin mai multe cai: de exemplu, pot primi un mesaj contrafacut de la o banca ce reclama faptul ca o plata online nu a putut fi tranzactionata. In cazul in care utilizatorul incerca sa acceseze link-ul indicat este condus pe un site infectat cu un troian bancar.

3. E-mail-uri despre presupuse servicii de livrare

Cadourile de Craciun comandate sunt livrate de regula prin servicii de coletare. Infractorii exploateaza asta si trimit e-mail-uri pretinse cu confirmari de transport sau cu facturi. Aceste mesaje anunta ca un colet nu a fost livrat sau, asa cum a fost in cazul unui pretins e-mail de la UPS, ca o noua factura este disponibila in centrul de facturare. Acest e-mail contine deasemenea un fisier atasat care ascunde un key logger. Daca un utilizator da click pe fisierul

atasat, malware-ul se descarca si spioneaza toate intrarile viitoare, ca de exemplu datele de logare la online banking.

4. E-mail-uri de la implementatorii de sisteme de plata

Infractorii trimit e-mail-uri pretinse a fi de la providerii sistemelor de plata care atesta ca un cont a fost blocat datorita unor presupuse nereguli si ca tranzactia nu s-a efectuat. Destinatarul ar trebui astfel sa repete operatiunea de plata sau sa deblocheze contul dand click pe un link integrat care il conduce pe utilizator catre un site conceput pentru a fura datele sau care este infectat cu malware.

5. Felicitari de Craciun contrafacute

Aceasta este o alta strategie preferata de infractori de sarbatori. E-card-urile pot contine fisiere atasate cu o varietate de programe malware sau cu link-uri ce conduc catre site-uri infectate.

8 sfaturi pentru cumparaturi de Craciun desfasurate in siguranta

1. Utilizatorii ar trebui sa foloseasca solutii de securitate cuprinzatoare care sa contina un scanner de virusi, firewall, filtru antispam si sa asigure protectie in timp real. Aceste solutii trebuie sa fie actualizate cu regularitate atat cu cele mai recente versiuni, cat si cu cele mai noi baze de semnaturi de virusi. Recomandam scanarea intregului sistem inainte de a incepe operatiunile de cumparare.

2. Cand utilizeaza instrumentele de online banking, utilizatorii trebuie sa se asigure ca solutia pe care o detin ofera protectie impotriva troienilor bancari cunoscuti sau necunoscuti.

3. Utilizatorii ar trebui sa se asigure ca sistemele de operare si programele software instalate sunt complet actualizate.

4. Ar fi ideal ca toate e-mail-urile spam sa fie sterse fara a fi citite. Utilizatorii nu ar trebui sa acceseze link-uri integrate sau fisiere atasate suspecte. Link-urile catre site-uri de online banking, magazine online sau servicii de plata ar trebui sa fie introduse manual in browser.

5. Utilizatorii ar trebui sa inspecteze magazinele online inainte de a face cumparaturi. Aceasta include citirea termenilor si conditiilor, avizele juridice, sa verifice modalitatea de trimitere a coletelor si alte costuri aditionale. Mai trebuie verificat si daca respectivul magazin are un renume negativ.

6. Cumparaturile nu se vor face de pe computere publice si insuficient protejate. Retelele WiFi publice ar trebui deasemenea evitate deoarece infractorii pot intercepta traficul de date din acestea.

7. Pe timpul procesului de plata, utilizatorii ar trebui sa acorde atentie notificarilor de securitate din browser pentru a se asigura ca datele sunt transferate in forma criptata. Este important ca anumite aspecte sa fie respectate: lacatul din bara de status sau din campul adresei, abrevierea HTTPS inaintea adresei introduse, fundalul verde in campul adresei in majoritatea browserelor moderne si domeniul afisat in partea din dreapta sus.

8. Sa fie folosite parole considerate puternice, in special pentru conturile sistemelor de plata, online banking-urilor si magazinelor online. De regula, acestea sunt generate aleatoriu si contin doar 8 caractere. Aceste parole ar trebui sa constituie o combinatie formata din litere mici, majuscule si caractere speciale.