G Data press release 2012

Cumparaturi online: Detalii de care trebuie sa tinem cont

24 zile – 24 sfaturi – 24 sanse de castig

Bucuresti (Romania) 04.12.2012 – Sunt cateva motive pentru care cumparaturile online au devenit foarte populare in ultimul timp: nu trebuie sa cautam locuri de parcare, nu trebuie sa stam la cozi sau sa ne agitam in cautarea cadourilor. Aceasta perioada este cea mai aglomerata din intreg anul pentru comerciantii de pe Internet, dar nu numai pentru ei: G Data se asteapta ca infractorii cibernetici sa ii vizeze si in acest an pe cumparatorii online. Peste doar cateva saptamani probabil ca va creste volumul de spam anuntand oferte aparent atragatoare, notificari false de livrari sau de transport maritim de la presupusi comercianti, ce vor sa-i atraga pe destinatari in capcane malware sau de phishing. G Data prezinta 3 dintre pericolele de top intalnite in timpul cumpararii de cadouri online si explica ce pot face utilizatorii pentru a se pazi de pericole. In plus, prin campania de constientizare "Safe Christmas 2012 – no chance for online fraudsters" va oferi zilnic sfaturi utilizatorilor de Internet incepand de sambata, 8 decembrie.

24 zile – 24 sfaturi – 24 sanse de a iesi castigator

De sambata, G Data va incepe o campanie pentru cumparaturi online si navigare pe Internet sigure sub motto-ul "Safe Christmas 2012 – no chance for online fraudsters" . In fiecare zi, calendarul G Data Christmas va deschide o noua fereastra, cu un nou sfat de securitate. Cu aceasta campanie, G Data vrea sa atraga atentia asupra tacticilor folosite de infractorii online si de distribuitorii de malware, deoarece acestia tind sa devina foarte activi in perioada sarbatorilor de iarna. In plus, oameni de toate varstele sunt incurajati sa-i convinga pe apropiati sa constientizeze aceasta problema. Astfel, G Data va solicita tuturor utilizatorilor de Internet sa trimita pe adresa de e-mail xmas@gdatasoftware.com propriile sfaturi de securitate. Cel mai bun sfat dintr-o zi va fi publicat pe website-ul G Data (www.gdatasoftware.com/safe_christmas) si pe pagina de Facebook. In semn de multumire, fiecare castigator va primi un premiu special; cadourile includ versiuni complete ale solutiilor G Data, cadouri de securitate adecvate sarbatorilor de iarna si un brad de Craciun G Data original.

Notificari de transport false

Cadourile de Craciun sunt livrate, de obicei, prin servicii de coletarie. Infractorii exploateaza asta si trimit e-mail-uri cu notificari de transport sau facturi false. Aceste mesaje sugereaza, de exemplu, ca un anumit pachet nu a putut fi livrat sau ca o noua factura este disponibila in centrul de comenzi. Cand utilizatorul acceseaza ink-urile integrate, programe malware se pot instala singure, fara stirea acestuia. Acest gen de e-mail-uri contin deseori si un fisier atasat care este, deasemenea, infectat cu malware. Daca utilizatorul deschide atasamentul, malware-ul ar putea descarca un program spyware, care va inregistra toate cheile intrarilor viitoare, de exemplu, datele de logare pentru serviciile de plata sau pentru online banking.

Oferte irezistibile

Infractorii ofera produse renumite, de genul ceasurilor luxoase sau branduri ale designerilor cunoscuti la preturi foarte mici. Link-urile integrate directioneaza utilizatorii spre website-uri infectate cu malware sau spre magazine online false de unde datele bancare si nu numai, sunt sustrase pe perioada procesarii comenzii. Acest tip de e-mail-uri sunt adesea usor de identificat dupa subiect: "Christmas Sale, Thousands of luxury goods for under $100".

Carduri de felicitari de Craciun

O alta strategie intalnita in aceasta perioada este trimiterea de felicitari electronice false. Acestea pot contine fisiere atasate infectate cu o varietate de tulpini de malware sau link-uri ce duc spre website-uri infectate.

5 sfaturi de securitate pentru siguranta cumparaturilor online:

1. Aruncati o privire: Inainte de a cumpara, cercetati magazinul online si verificati reputatia acestuia. Aceasta include si citirea termenilor si conditiilor generale, a notitelor legale, verificarea conditiile de livrare si costurile suplimentare. Utilizatorii pot face o scurta cercetare pentru a vedea daca magazinul online are un renume prost.
2. Plata online: Pe perioada procesului de plata, utilizatorul va verifica foarte atent notificarile din browser pentru a se asigura ca datele sunt transferate criptat. Un lucru important este sa verificati daca exista lacatelul din bara, abreviatia "https" inaintea adresei introduse, background de culoare verde si domeniul desfasurat in partea dreapta.
3. Direct la cos: In mod ideal, tot spamul ar trebui sters inainte de a fi citit. Utilizatorii ar trebui sa evite deschiderea link-urilor integrate sau a fisierelor atasate. Link-urile ce conduc spre site-uri de online banking, magazine online sau servicii de plati ar trebui introduse manual in browser. In acest sens, ar trebui acordata o mare atentie erorilor de scriere, deoarece infractorii folosesc asta pentru a directiona cumparatorii spre website-uri false.
4. Inchideti bresele de securitate: Trebuie sa folositi update-uri pentru a va asigura ca sistemele de operare, programele instalate si aplicatiile sunt complet actualizate. Aceasta conditie nu se aplica doar utilizatorilor de computere, ci si utilizatorilor de telefoane inteligente si tablete.
5. Banking securizat: cand folositi serviciul de online banking, ar trebui sa folositi o procedura dubla de autentificare, daca este posibil. G Data BankGuard – singura protectie impotriva troienilor bancari cunoscuti si necunoscuti – ofera protectie suplimentara pe parcursul tranzactiilor de plati online. Cumparatorii care apeleaza la un provider de servicii de plata pentru a plati facturi, ar trebui sa apeleze la un provider care ii ofera protectie adecvata.

-###-