G Data press release 2015

Sezonul sarbatorilor de iarna: trei saptamani de promotii pentru infractorii online

G DATA atrage atentia asupra perioadei in care efectuam cumparaturi online in cautare de cadouri si ofera sfaturi despre cum sa ne ferim de pericole.

Bucuresti (Romania) 10.12.2015

De pe telefon, tableta sau computer, cumparaturile online de cadouri sunt in plina expansiune. Anul trecut, numai in Germania, 37 de milioane de cumparatori au decis sa cumpere cadouri online, pentru a evita magazinele aglomerate si cozile de la casele de marcat (Sursa: Bitkom). Aceasta perioada nu este doar sezonul cu cele mai mari vanzari pentru comercianti - este, de asemenea, sezonul de varf pentru infractorii online care sustrag date personale, precum si sume mari de bani. Acestia ruleaza campanii dedicate de Craciun: trimit e-mailuri cu oferte dubioase ce fac referire la anumite cadouri sau avize de expeditie false pentru a colecta date cu caracter personal de la utilizatorii de Internet. Succesul este garantat mai ales in timpul sezonului de iarna, cand oamenii sunt in asteptarea comenzilor si a notificarilor de transport pentru bunurile pe care le-au cumparat online. O alta inselatorie des intalnita este manipularea tranzactiilor financiare, atunci cand cumparatorii sunt gata sa plateasca prin transfer bancar. G DATA avertizeaza asupra campaniilor online sofisticate de dinainte de Craciun si arata cum se pot face cumparaturi in conditii de siguranta.

„In fiecare an, in jurul sarbatorilor de Craciun, casele de marcat din supermarket-uri si magazinele online sunt solicitate din plin. Acesta este, de asemenea, varf de sezon pentru infractorii online “, explica Ralf Benzmuller, Head of G DATA SecurityLabs. „Atacatorii sunt in cautare de date de acces pe carduri de credit si date ale conturilor de email, precum si credentialele pentru serviciile de

plata online. Instrumentele lor principale sunt mesajele cu URL-uri de phishing incluse si atasamente de e-mail infectate. Utilizatorii ar trebui sa acorde o atentie sporita pentru a se proteja impotriva acestora.“

Cele mai populare scheme utilizate de catre infractorii online in timpul sezonului:
Escrocheria #1: Afaceri dubioase oferite prin e-mail
In special in timpul sezonului de sarbatori de iarna, utilizatorii de Internet sunt bombardati cu mesaje cu oferte de smartphone-uri, tablete, bijuterii sau produse de firma la preturi foarte mici. Aceste oferte sunt prea frumoase sa fie adevarate – de cele mai multe ori se dovedeste ca asa este. Link-urile din e-mailuri conduc utilizatorul catre un site infectat cu programe malware sau un magazin web fals. In acest fel, utilizatorii isi servesc datele lor personale - adresa de email, adresa postala, date de acces pentru serviciile de plata - pe tava. Atunci cand este utilizata plata in avans, cumparatorii isi pierd banii si astepta transportul care nu mai ajunge niciodata.

Escrocheria #2: Notificari de transport false primite in inbox
Atunci cand comandati bunuri online, un curier vi le va livra la adresa. Prin urmare, clientii asteapta primirea unui mesaj care ii informeaza ca articolul comandat a fost livrat. Acesta este motivul pentru care, infractorii trimit prin e-mail notificari de expediere trucate. Link-uri catre pagini web de "online tracking ", duc, de multe ori, direct intr-o capcana malware si sustrag informatii cu caracter personal.

Escrocheria #3: “ Felicitari de sezon" prin e-mail, mesaje text sau aplicatii mobile
In prezent, din comoditate sau lipsa de timp, oamenii trimit felicitari electronice. Infractorii fac uz de acest lucru prin trimiterea de mesaje SMS, mesaje e-mail sau aplicatii mobile, ce contin link-uri catre site-uri infectate cu malware. E-mailurile pot contine, de asemenea, un atasament infectat cu malware.

Escrocheria #4: Manipularea de tranzactii bancare online
Multe cadouri achizitionate online sunt platite in avans, prin intermediul online banking. Pentru a pacali utilizatorii sa viziteze un site web manipulat sau pentru a deschide un atasament infectat, infractorii trimit remindere de plata falsificate sau note de comanda. Site-urile infectate contin adesea un troian bancar specializat - daca infectia este de succes, platile efectuate de catre victima sunt redirectionate catre un alt cont bancar.

Sfaturi G Data pentru cumparaturi de Craciun si online banking in siguranta:
■ Protejati-va pe Internet: o solutie completa de securitate ar trebui sa fie parte din fiecare calculator, smartphone sau tableta. Suita de securitate ar trebui sa aiba o protectie puternica în timp real impotriva amenintarilor online curente.
■ Ramaneti permanent actualizati: Orice software, aplicatie, precum si sistemul de operare pe un computer sau un dispozitiv mobil ar trebui sa fie actualizate si toate update-urile

disponibile ar trebui sa fie instalate cat mai repede posibil. In acest fel, utilizatorii vor acoperi vulnerabilitatile, care altfel ar fi exploatate de infractori.

■ Efectuati operatiunile de online banking in siguranta: Cand efectuati transferuri de bani sau alte tranzactii bancare, ar trebui sa va asigurati ca utilizati o solutie cu doua cai de autentificare. Protectia poate fi imbunatatita prin utilizarea tehnologiei G DATA BankGuard care este inclusa in toate solutiile desktop.

■ Cumparati numai de la magazine web cunoscute: Cumparatorii sunt sfatuiti sa verifice cu atentie magazinele online inainte de a cumpara ceva; un bun indicator sunt termenii si conditiile, precum si informatii despre costurile de transport. Verificarea reputatiei site-ului are cu siguranta sens pentru a vedea daca operatorul site-ului nu este cunoscut ca o "oaie neagra".

■ Stergeti e-mailurile spam: Mesaje cu oferte de cadouri dubioase, precum si alte mesaje spam necesita a fi sterse imediat. Utilizatorii ar trebui sa nu deschida fisierele atasate si sa nu dea clic pe link-urile incluse. Dupa toate probabilitatile vor conduce utilizatorul direct intr-o capcana malware.

■ Efectuati plati online in conditii de siguranta: In timpul procesului de plata, trebuie sa se acorde o atenție deosebita la orice mesaj de securitate al browser-ului. Un simbol verde in forma de lacat si prefixul https: // in bara de adrese sunt un bun indicator ca utilizatorul este pe un site web securizat. Nicio plata nu ar trebui sa fie efectuata in cazul in care unul dintre cele doua lipsesc.

-###-