Üheksa soovitust, kuidas e-poest turvaliselt kaup kätte saada

10 aastat tagasi Autor: AM

Jah, alustame nagu naisteka nõuande lugu: üheksa soovitust, viis nippi... aga mis seal ikka, jõuluostud ongi natuke pea segi ajanud ja vaja on kainemat suhtumist, kasvõi punkt-punktilt turvaohud läbi käies. Seekordseks soovitajaks on turvatarkvara tootja ESET.

Kui eelistad külma kätte mitte minna ning teha oste pigem brauseriakna kaudu, ära unusta turvalisust! Just seetõttu on ESETi *online*-turbe guru Raphael Labaca Castro pannud viimase hetke jõuluostude tegijate jaoks kokku üheksa "Jõuluvana poolt heakskiidetud onlainis ostmise nõuannet".

1. Hoolitse, et sinu arvuti on valmis turvaliseks ostmiseks

Just niisamuti, nagu sa ei läheks teele sõidukõlbmatu autoga, ei peaks sa tegema oste arvutilt, mis on e-poodlemiseks sobivalt varustamata. Hoolitse, et sinu arvuti on parimas töökorras: värskenda võimalusel selle opsüsteemi, veebibrauserit ja muud tarkvara ning installeeri sellele turbelahendus. Paigad sulgevad teadaolevad nõrkused ning viirusetõrjetarkvara hoiab eemal sinu andmeid varastada püüdvad onlainohud. Proovi näiteks tasuta skannerit, et näha, kuidas sinu arvuti viirustega toime tuleb: www.eset.com/online-scanner.

2. Osta üksnes usaldusväärsetelt saitidelt

Usaldusväärsete onlainkaupmeeste kasutamine on äärmiselt tähtis. Müügiks pakutavatel kaupadel peaks olema korralikud kirjeldused ning neile peaks olema lisatud üksikasjalik tarneinfo koos prognoositavate kohalejõudmise kuupäevadega. Kui sa ei ole kindel veebisaidi reputatsioonis, siis guugelda – usaldusväärsetel veebisaitidel pole iial puudu neid onlainis kiitvatest klientidest.

3. Kindlusta oma turvalisus maksetehinguid tehes

Peaksid saidile logima turvalise ühenduse kaudu, et sinu andmed ei oleks kõigile näha. Saidid kasutavad turvalisuse tagamiseks tavaliselt HTTPS-ühendust, mida on lihtne ära tunda: kontrolli, et saidi aadress algab lühendiga 'https' ning et mobiilsetel seadmetel on kuvatud vastav lukusümbol. Sel juhul on ühendus krüpteeritud. See aitab vältida andmete lekkimist ning tagada andmevahetuse toimumist vaid sinu ja kaupluse vahel.

4. Ole ettevaatlik tasuta pakkumiste ja hämmastavate allahindluste suhtes

Hindade alandamine kiirel kauplemisperioodil klientide ligi meelitamiseks pole tavatu sel äärmiselt konkurentsirohkel ajal aastast, ent ole siiski ettevaatlik! Häkkerid võivad kasutada hämmastavate pakkumistega hüpikaknaid, mis on disainitud sarnanema usaldusväärsete kaupmeeste pakkumistele. Ole eriti skeptiline selliste hüpikakende suhtes, mis ütlevad sulle, et oled midagi võitnud, kui sa ei ole end vastavas kampaanias osalema registreerinud.

5. Kasuta turvalist juhtmeta ühendust

Kaugeltki kõik WiFi'd ei ole loodud võrdseks! Tasuta WiFi kuumkohad on oluliselt vähem turvalised ning neisse tuleks kahtlusega suhtuda alati, ent kahekordselt ettevaatlik tuleks olla siis, kui plaanid mõnd rahalist tehingut: kavatsed kasutada onlainpanka või Internetist oste teha. Kasuta selleks vaid turvalist ühendust, oma kodust või töökoha võrku, kus on vähem tõenäoline, et ringi nuhkivad küberkurjategijad sinu kommunikatsiooni pealt kuulavad.

6. Anna vaid hädavajalikku infot, mitte rohkem

Pole tavatu, et kinkide ostmiseks tuleb end veebisaidil registreerida, ent sul pole vaja jagada liiga palju infot enda kohta. Reeglina küsivad poed rohkem infot, kui vajavad – tärniga (*) märgistatud väljad on tavaliselt kohustuslikud ja neid ei saa vahele jätta, ent ära arva, et pead täitma ka kõik muud väljad. Kui nad olulisi välju esile ei tõsta, siis võib aidata selliste väljade täitmata jätmine muuta veebisaiti pisut läbipaistvamaks.

7. Kasuta krediitkaarti

Poed eelistavad tihti, et kasutad pigem oma deebetkaarti kui krediitkaarti, ent kui võimalik, siis maksa just krediitkaardiga. Miks? Krediitkaardid on tavaliselt kaitstud pettuse eest. Hoia oma kontodel alati silma peal, ent ole eriti tähelepanelik ostude tegemise perioodil, ning võta viivitamata ühendust oma pangaga, kui märkad mis tahes kahtlast tegevust (Eesti oludes on hea elektrooniline krediitkaart, mille saab luua vaid ühe ostu jaoks - toim).

8. Kasuta parooli kõikidel seadmetel

Kõik sinu seadmed peaks olema parooliga kaitstud. Telefoni on ahvatlev mugavusest lukustamata hoida, ent kui selles on palju salajasi andmeid, siis võib varas sulle palju kahju teha. Vali korralik parool, kasutades kaht või enamat sõna ning numbrite ja tähtede kombinatsiooni, ning seadista oma telefon automaatselt lukustuma, kui sellesse sisestatakse mitu korda järjest vale parool.

9. Varunda oma andmeid kord kuus

Andmete varundamine on oluline, kui peaksid kaotama juurdepääsu oma arvutile varguse või nakkuse tagajärjel. Liikvel on ka lunaraha nõudmise pahavara, millega ründaja püüab kaugkrüpteerida sinu failid ja nõuda raha nende uuesti dekrüpteerimise eest. Andmete sage varundamine võimaldab sul sellisele väljapressimisele mitte järele anda. Kord kuus varundamisest peaks tavaliselt piisama, ent kui vajad

sagedasemat ja korrapärasemat varundamisplaani, siis seadista see kindlasti.

Ja lõpuks - naudi poodlemishooaega oma diivanilt, kanna vaid hoolt selle eest, et teed seda turvaliselt. Ründajad teavad, et käes on kõige kiirem ja toimekam aeg: see on nii ka neil. Püsi neist seetõttu kindlasti meie nõuannete abil sammu võrra eespool ja säilita valvsus.

- Lahendused
- Turvalisus