

**OUCH!**

Ikmēnešā informatīvais biļetens drošības izpratnes veicināšanai

Šis ir laiks, kad jābūt skeptiskiem – droša iepirkšanās internetā

Svētku piedāvājums, kas ir pārāk labs, lai būtu patiesība

Maija bija sajūsmā, kad atrada pazīstama zīmola bezvadu austiņas ar 70% atlaidi. Tīmekļa vietne izskatījās profesionāla, svētku akcija šķita neatliekama, un viņa pat saņēma apstiprinājuma e-pastu dažas minūtes pēc pasūtījuma veikšanas. Bet dienas pārtapa nedēļās, un nekas netika piegādāts. Viņas e-pasti un tālruņa zvani palika bez atbildes, un drīz pēc tam viņas kredītkarte tika izmantota neautorizētiem maksājumiem. Kas iesākās kā izdevīgs darījums, kļuva par dārgu mācību. Maija bija kļuvusi par upuri viltus tiešsaistes veikalam, kas bija izveidots, lai apkrāptu klientus svētku laikā.

Diemžēl, Maijas stāsts nav unikāls. Tā kā tiešsaistes iepirkšanās apjomi turpina pieaugt, īpaši svētku sezonā, kibernetizētie izmanto izdevību, lai pievilinātu upurus ar viltotām tīmekļa vietnēm, neeksistējošām akcijām un krāpnieciskiem veikaliem. Labās ziņas? Jūs varat iepirkties tiešsaistē droši, atpazīstot izplatītākās krāpniecības pazīmes un ievērojot dažus vienkāršus padomus.

Viltus tiešsaistes veikali

Kibernetizētie izveido viltus tīmekļa vietnes, kas imitē reālus mazumtirgotājus vai izmanto pazīstamu zīmolu nosaukumus. Meklējot labākos tiešsaistes piedāvājumus, jūs varat ienākt kādā no šīm viltus vietnēm. Noziedznieki bieži reklamē šīs vietnes sociālajos tīklos, piedāvājot preces ar milzīgām atlaidēm. Pērkot no šādām tīmekļa vietnēm, jūs varat zaudēt savu kredītkartes informāciju, saņemt viltotas vai nozagtas preces vai vispār nesaņemt neko. Aizsargājiet sevi, veicot šādas darbības:

- **Iepērcieties pie uzticamiem mazumtirgotājiem.** Iepērcieties tiešsaistes veikalos, kurus jau pazīstat un kuros esat veicis pirkumus. Pievienojiet tos grāmatzīmēm savā pārlūkprogrammā. Jūs varbūt neatradīsiet tik neticami izdevīgu piedāvājumu, bet jums būs daudz mazāka iespēja tikt apkrāptiem.
- **Ar aizdomām izturieties pret lielām atlaidēm.** Ja reklāmas vai akcijas cenas ir ievērojami zemākas nekā tās, ko redzat pazīstamos tiešsaistes veikalos, iespējams, tā ir krāpšana.
- **Pārbaudiet kontaktinformāciju.** Izvairieties no tīmekļa vietnēm, kurās nav kontaktinformācijas, nestrādā saziņas veidlapas vai ir norādītas personīgās e-pasta adreses. Fizisko adresi, tālruņa numuru, klientu apkalpošanas kontaktu un skaidru atgriešanas noteikumu trūkums bieži vien ir aizdomīgu tīmekļa vietņu pazīme.

- **Pārbaudiet tīmekļa adresi.** Pievērsiet uzmanību, ja tīmekļa vietne izskatās tāpat kā tā, ko izmantojāt iepriekš, bet domēna vārda nosaukums vai veikala nosaukums ir atšķirīgs. Piemēram, jūs, iespējams, esat pieradis iepirkties vietnē “Amazon”, kuras tīmekļa vietnes adrese ir www.amazon.com, taču nokļūstat viltus vietnē, kas izskatās līdzīgi, bet kuras adrese ir www.aamazon.deals.
- **Meklējiet atsauksmes.** Ierakstiet veikala nosaukumu vai URL meklētājprogrammā, lai redzētu, ko citi par to ir teikuši. Meklējiet tādus jēdzienus kā “krāpšana”, “vairs nekad” un “viltota”.
- **Esiet uzmanīgi ar maksājumu metodēm.** Vietnes, kas pieņem tikai bankas pārskaitījumus, dāvanu kartes vai kriptovalūtu, bieži izmanto krāpnieki.
- **Aizsargājiet savus kontus.** Aizsargājiet savus tiešsaistes kontus, izmantojot unikālas un drošas paroles. Ja tās ir grūti atcerēties, apsveriet iespēju tās saglabāt paroļu pārvaldniekā. Izmantojiet papildu drošības funkcijas, piemēram, daudzfaktoru autentifikāciju (MFA) un piekļuves atslēgas, ja tās ir pieejamas.

Krāpnieki reālās iepirkšanās vietnēs

Daži tiešsaistes veikali piedāvā produktus, ko pārdod privātpersonas vai mazie uzņēmumi, un krāpnieki var slēpties starp tiem. Pirms pasūtījuma veikšanas pārbaudiet katra pārdevēja reputāciju, izlasot atsauksmes. Esiet piesardzīgs attiecībā uz pārdevējiem, kuri tiešsaistes veikalā ir nesen, kuriem trūkst atsauksmju vai kuri pārdod preces par neparasti zemām cenām.

Tiešsaistes maksājumi par pirkumiem

Vēl viens veids, kā sevi aizsargāt, ir regulāri pārskatīt savus kredītkartes izrakstus, lai identificētu aizdomīgus maksājumus. Ja iespējams, savā kredītkartes kontā izmantojiet iespēju saņemt paziņojumus e-pastā, SMS vai lietotnē, kad tiek veikts maksājums ar jūsu kredītkarti. Ja redzat aizdomīgas darbības, nekavējoties ziņojiet par to kredītkartes izsniedzējam. Maksājumiem tiešsaistē izmantojiet kredītkartes, nevis debetkartes. Debetkartes ņem naudu tieši no jūsu bankas konta; ja notiek krāpšana, jums būs daudz grūtāk atgūt naudu. Elektroniskie maksājumu pakalpojumi vai e-maki, piemēram, “PayPal”, ir drošāka iespēja arī pirkumiem tiešsaistē, jo tie neprasa atklāt kredītkartes numuru.

Viesredaktore

Triša Makmahona (Tricia McMahon), organizācijas Women in Cybersecurity (WiCyS) Sandjego filiāles prezidente un WiCyS izglītības un apmācības pārvaldniece, ir apņēmusies īstenot WiCyS galveno misiju – piesaistīt, noturēt un veicināt sieviešu karjeru kibernetikas jomā. Viņai ir maģistra grāds kibernetikā, un viņa ir aizrautīga mūžizglītības un profesionālās attīstības piekritēja. [linkedin.com/in/triciaamcmahon](https://www.linkedin.com/in/triciaamcmahon)



Resursi

Kā kibernetikas nozogs jūsu paroles: <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/>
 Kā kibernetikas nozogs jūsu emocijas: <https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/>
 Paroļu pārvaldnieku spēks: <https://www.sans.org/newsletters/ouch/power-password-managers/>
 Paroļu frāžu spēks: <https://www.sans.org/newsletters/ouch/power-passphrase/>

Kopienai tulkoja: CERT.LV

OUCH! Izdevējs: SANS Security Awareness, izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licenci](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt to, ja vien jūs to nepārdodat vai nepārveidojat. Redakcijas kolēģija: Fils Hofmans, Leslijs Ridouts, Princese Janga.

Vairāk informācijas par Ouch! Varat atrast šajā saitē: <https://www.sans.org/newsletters/ouch>