Droša iepirkšanās tiešsaistē

Svētku laiks jau tuvojas. Drīz miljoniem cilvēku meklēs ideālas dāvanas saviem tuvajiem, un daudzi no mums iepirksies tiešsaistē. Diemžēl arī kibernoziedznieki būs diez gan aktīvi, veidojot viltotas iepirkšanās vietnes un citus krāpnieciskus tiešsaistes iepirkšanās rīkus, lai nozagtu jūsu datus vai naudu. Uzziniet, kā atrast labus piedāvājumus, nekļūstot par kibernoziedznieku upuri.

Viltoti tiešsaistes veikali

Noziedznieki izveido viltotus tiešsaistes veikalus, kas atdarina reālu vietņu izskatu vai izmanto pazīstamu veikalu vai zīmolu nosaukumus. Meklējot labākos tiešsaistes piedāvājumus, jūs varat ienākt kādā no šīm viltotajām vietnēm. Iepērkoties šādās vietnēs, jūs varat nejauši iegādāties viltotas vai nozagtas lietas, vai arī jūsu pirkumi var netikt piegādāti vispār. Lai pasargātu sevi, veiciet turpmāk norādītās darbības:

- Ja iespējams, iepērcieties tajos tiešsaistes veikalos, kurus jūs jau zināt, kuriem uzticaties un ar kuriem iepriekš esat veicis darījumus. Atzīmējiet (bookmark) šos tiešsaistes veikalus.
- Esiet piesardzīgāks ar reklāmām vai piedāvājumiem meklētājprogrammās vai sociālajos medijos, kas ir ievērojami sliktāki par tiem, ko redzat izveidotajos tiešsaistes veikalos. Ja darījums izklausās pārāk labi, lai būtu patiesība, tā varētu būt krāpšana.
- Esiet piesardzīgs ar vietnēm, ar kurām nav iespējams sazināties, kļūdaināms kontaktformām vai personīgā e-pasta izmantošanu.
- Esiet piesardzīgs, ja vietne izskatās tāpat kā tā, kuru jūs izmantojāt jau agrāk, taču vietnes nosaukums (domēna vārds) vai veikala nosaukums atšķiras. Piemēram, jūs, iespējams, esat pieradis iepirkties vietnē "Amazon", kuras tīmekļa vietnes adrese ir www.amazon.com, bet galu galā atrodaties viltus vietnē, kas izskatās līdzīgi, bet kuras adrese ir www.amazonshoppers.com.
- Ievadiet tiešsaistes veikala nosaukumu vai tā tīmekļa adresi meklētājprogrammā, lai redzētu, ko citi par to ir teikuši. Meklējiet tādus terminus kā “krāpšana”, “vairs nekad” un “viltota”.
- Aizsargājiet savus tiešsaistes kontus, katram kontam izmantojot unikālu, spēcīgu paroli. Vai nevarat atcerēties visas savas paroles? Apsveriet iespēju tās visas saglabāt paroļu pārvaldniekā.

Krāpnieki likumīgās vietnēs

Esiet piesardzīgs, iepērkoties pat uzticamās vietnēs. Interneta veikalos bieži tiek piedāvāti produkti, ko pārdod trešās puses – dažādas personas vai uzņēmumi – un tiem var būt krāpnieciski nodomi. Šādi tiešsaistes galamērķi ir kā reālās pasaules tirgi, kur daži pārdevēji ir uzticamāki nekā citi.

- Pirms pasūtījuma veikšanas pārbaudiet katra pārdevēja reputāciju, izlasot atsauksmes.
- Esiet piesardzīgs pret pārdevējiem, kuri ir jauni tiešsaistes veikalā, kuriem trūkst atsauksmju vai kuri pārdod preces par neparasti zemām cenām.
- Pārskatiet tiešsaistes veikala politiku attiecībā uz pirkumiem no šādām trešajām pusēm.
- Ja rodas šaubas, iegādājieties preces, ko pārdod tieši tiešsaistes veikals, nevis trešo pušu pārdevēji, kas piedalās tā tiešsaistes tirgū.
- Pat ar likumīgiem pārdevējiem, pirms pirkuma veikšanas pārliecinieties, ka saprotat pārdevēja garantijas un atgriešanas politiku.

Tiešsaistes maksājumi par pirkumiem

Regulāri izskatiet kredītkartes pārskatus, lai noteiktu vai ir kādas aizdomīgas izmaksas. Ja varat, iespējojiet opciju paziņot jums pa e-pastu, īsziņu vai lietotni, kad tiek iekasēta maksa. 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 tiek veikta 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. Izvairieties no vietnēm, kurās tiek pieņemti maksājumi tikai kriptovalūtā vai ir jāizmanto neskaidras maksājumu metodes.

Tas, ka tiešsaistes veikalam ir profesionāls izskats, nenozīmē, ka tas ir likumīgs. Ja vietne rada jums neērtības, neizmantojiet to. Tā vietā dodieties uz labi zināmu vietni, kurai varat uzticēties vai kuru esat iepriekš droši izmantojis. Jūs, iespējams, neatradīsiet to pašu neticamo preci vai pakalpojumu, taču jūs, visticamāk, izvairīsities no krāpšanas.

Viesredaktors

Marks Orlando (Mark Orlando) ir drošības vadītājs, kurš bijis atbildīgs par tīklu drošību Pentagonā, Baltajā namā un daudzu privātā sektora klientu tīklu drošību. Šobrīd viņš ir kiberdrošības uzņēmuma "Bionic" izpilddirektors un līdzdibinātājs, kā arī pasniedzējs un kursu autors "SANS" institūtā. [Twitter: @markaorlando]

Resursi

Vienkāršu paroļu izveidošana: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Krāpšana ziņojumapmaiņā: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Krāpšana, izmantojot sociālos medijus: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Tulkojums: CERT.LV