

Esi #viedpircējs!



Pircēji Latvijā arvien biežāk iepērkas tiešsaistē.

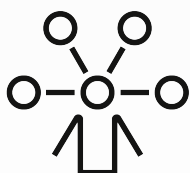


Taču svarīgi, lai, pieaugot iepirkumiem tiešsaistē, iedzīvotāji rīkojas kā viedpircēji — atpazīst uzticamus tiešsaistes veikalus un izvēlas drošus maksājumu veidus.



Ikdienas pirkumi tiešsaistē sniedz ērtību, drošību un tēriņu kontroli.

Kas ir #viedpircējs?



domā un rīkojas digitāli



bieži veic ikdienas pirkumus tiešsaistē



lieto dažādus maksājumu rīkus



spēj atpazīt uzticamus tiešsaistes veikalus

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Populārākie uzbrukumu veidi — no kā sevi pasargāt?

Ļaunprogrammatūra jeb ļaunatūra



Dažādu veidu kaitnieciskas programmas, kas tiek instalētas ierīcēs bez lietotāja ziņas. Šāda veida uzbrukums iespējo neatļautu darbību uzsākšanu datorā vai viedtālrunī, lai iegūtu vērtīgu informāciju, liegtu pieeju glabātajiem datiem vai apturētu ierīces darbību pavisam.



Ļaundari var izmantot jūsu ierīces, lai realizētu savus uzbrukumus citiem un slēptu savu darbību pēdas. Tas tiesībsargājošajām iestādēm liks jūs turēt aizdomās par šo noziegumu veikšanu.



Visbiežāk ļaunatūra tiek izplatīta e-pasta pielikumos, caur nelegālām vai inficētām tīmekļvietnēm, kā arī izmantojot reklāmas vai saites.

Pikšķerēšana



Veids, kā ļaundari, uzdodoties par banku, tirgotāju, policiju vai citu valsts iestādi, cenšas iegūt no interneta lietotāja personīgu, slepenu informāciju, tostarp kredītkaršu vai internetbankas datus, piekļuves lietotājevārdus, paroles u. c.



Visbiežāk ar e-pasta, telefona vai īsziņu starpniecību aicina atvērt saiti uz tīmekļvietni, kur jāievada privātie dati, vai arī, piemēram, tiek atsūtīta informācija, ka esi saņēmis paciņu un nepieciešams piemaksāt, lai to saņemtu.



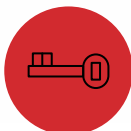
Atceries, ka banka vai citas iestādes nekad neprasīs sūtīt tavus identifikācijas datus pa e-pastu, ar īsziņu vai tālruņa starpniecību. Šādi dati nevienam nav jāizpauž.



Ja rodas aizdomas, vai sarunas laikā nenotiek krāpšana, nekavējoties pārtrauc sarunu un sazinies ar banku vai iestādi, no kuras it kā tiek zvanīts.



Paroļu uzlaušana vai piemeklēšana no uzlauztām datubāzēm



Vienkāršākais paroļu uzlaušanas veids ir tās atminēšana. Cilvēki bieži vien mēdz izvēlēties pārāk paredzamas paroles.



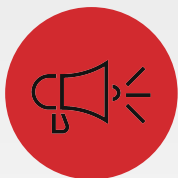
Ļaundari, lai piekļūtu parolēm, var ielauzties kādās tīmekļvietnes datubāzē un iegūt informāciju par lietotājiem, kas ietver arī paroļu šifrētās vērtības, ar šiem pašiem datiem piekļūt lietotāju kontiem vairākās vietnēs, jo nereti tiek izmantota viena parole.



Mūsdienās tikai parole nav uzskatāma par drošu autentifikācijas veidu. Lielākai drošībai nepieciešama vairākfaktoru autentifikācija. Mazāk sensitīvas informācijas aizsardzībai būtu vērts apsvērt iespēju autentificēties ar sociālo tīklu profilu.

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Populārākie krāpšanas veidi — no kā sevi pasargāt?



Reklāma internetā

Bieži izmantots krāpšanas veids ir reklāmu izvietošana internetā, piemēram, populāros sociālajos tīklos — Facebook un Instagram —, piedāvājot iegādāties produktus ar ievērojamu atlaidi, piemēram, par 80% lētāk. Parasti prece netiek piegādāta vispār, vai tiek piegādāta nepareiza prece.

Ziņas parādās no personai zināmiem cilvēkiem (draugiem), jo krāpnieki dažādos veidos var rast risinājumus, kā šīs ziņas ievietot draugu Facebook un Instagram profilos, tādēļ cilvēkiem rodas sajūta, ka atlaide ir īsta.

Krāpšana notiek pēc kāda laika, kad klienta kartes dati tiek izmantoti citiem nesaistītiem darījumiem, bet pirmais pirkums ir bijis domāts kartes datu zādzībai.



Ieguldījumu krāpšana

Populārs krāpšanas veids, kad agresīvā veidā (parasti pa telefonu) klients tiek pārliecināts investēt naudu, solot pasakainu un drošu peļņu.

Klients notic krāpnieka piedāvājumam, veic naudas pārskaitījumus, neiepazīstoties ar faktiskajiem darījuma un servisa noteikumiem, tādējādi pats dodot piekrišanu.

Diemžēl izplatīta prakse, kad krāpnieki izvilina karšu datus, solot, ka investēs un būs liela peļņa īsā laikā posmā. Kad krāpnieki ir ieguvuši kartes datus, tad izmanto tos dažādu preču iegādei — krāpšanai. Investīciju krāpšanā parasti ir vislielākie naudas apjomi.

Vienmēr izturies ar aizdomām, ja tiek solīti droši ieguldījumi ar ātru un neticami labu peļņu.



Viltus aizdevumu krāpšana

Cilvēkiem, kas meklē aizdevumu (sludinājumos vai citādi), tiek zvanīts un iestādīts, ka nepieciešamas pārbaudes Valsts ieņēmumu dienesta datubāzēs vai, piemēram, kredītreģistros, un tam nepieciešams nosaukt internetbankas pieejas kodus, apstiprināt darbības mobilaajā lietotnē vai nosaukt karšu datus.

Pie pirmajām aizdomām, ka sarunas laikā notiek krāpšana, **nekavējoties pārtrauc sarunu** un pats sazinies ar iestādi, no kuras it kā saņem zvanu.



Viltus loterijas

Ļoti izplatīts krāpšanas veids, kurā cilvēkam piedāvā piedalīties populāru viedtālrunu vai citu iekārojamo zīmolu izlozē sociālajos tīklos vai citur. Bieži vien šādās viltus loterijās tiek pieprasīti lietotāja maksājumu karšu dati.

Atceries, savas paroles un bankas **dati nevienam nav jāizpauž!**

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Kā atpazīt drošu interneta veikalu?



Pārbaudi vietnes nosaukumu un saiti

Vai tajā nav lieku rakstzīmju vai simbolu, kas paņemti no cita alfabēta, piemēram, "e", bet viltus vietnē atpazīstamais nosaukums uzrakstīts ar "ē". Tieši viltus mājaslapas, kas izskatās pēc oficiālās organizācijas vietnes, ir viens no biežākajiem veidiem, kā krāpnieki cenšas apmānīt pircējus, lai iegūtu pieejas datus vai citu vērtīgu informāciju, ko tālāk pārdot melnajā tirgū.



Pārlicinies, ka izmanto drošu interneta savienojumu

Par to liecina saites priekšā esošais apzīmējums HTTPS, kā arī atslēdziņas vai vairoga ikoniņa adreses logā. Tomēr tas nav vienīgais aspekts, kuram būtu jāpievērš uzmanība, jo uzbrucēji kļūst attapīgāki un arī bīstamas mājaslapas var tikt apzīmētas ar šo savienojuma veidu. Drošs savienojums vēl neliecina par vietnes drošību.



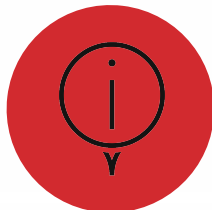
Pārbaudi uzņēmuma reputāciju un citu pircēju atsauksmes pirms pirkuma veikšanas

Droša interneta veikalā būs viegli pieejama un skaidri saprotama informācija par uzņēmumu, tostarp kontaktinformācija jautājumu gadījumā, un skaidrojums par tiesībām atdot precī atpakaļ. Jāpievērš uzmanība arī tam, cik senas ir norādītās atsauksmes, vai tās nav pārāk vienādas, jo nereti viltus uzņēmumi paši nodrošina šāda veida saturu par sevi. Drošāk izvēlēties plaši pazīstamus vietējos un Eiropas Savienībā reģistrētus veikalus.



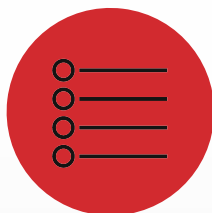
Neuzķeries uz pārāk vilinošiem piedāvājumiem, kas šķiet nesamērīgi izdevīgi

Krāpnieki zina, ka cilvēki labprāt izmanto iespēju iegādāties preces, jo īpaši pazīstamu zīmolu, par izdevīgāku cenu, tāpēc piesardzīgi būtu jāizturas, ja reklāma vēsta par piedāvājumu ar, piemēram, 90 % atlaidi.



Pārlicinies,

vai norādīti apmaksas un piegādes noteikumi, atteikuma tiesības, sniegta preces apraksts, kā arī nodrošināta saziņa ar klientu.



Iepazīsties

ar Patērētāju tiesību aizsardzības centra (PTAC) Melno sarakstu un Aizdomīgo interneta vietņu sarakstu.

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Spēcīgas paroles datu drošībai

Visvienkāršākais veids, kā pasargāt savus datus, ir izvēlēties **drošas un unikālas paroles** katrai vietai.



Papildu drošībai ieteicams izmantot arī **divu faktoru jeb stingro autentifikāciju**, kas pieprasa apstiprināt pieeju vēl kādā veidā, piemēram, nosūtot īsziņu ar unikālu pieslēgšanās kodu vai izmantojot autentifikācijas lietotni.

Droša parole ir gara — vismaz 14–16 simbolu, kas ietver burtus, ciparus, citas zīmes. Lai būtu vieglāk atcerēties, var izmantot tā sauktās paroļu frāzes, kas ietver, piemēram, tev zināmas dziesmas vai dzejoļa vārdus, ciparus un simbolus.



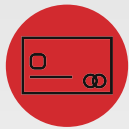
Ja garu paroli ir grūti izdomāt un atcerēties, eksperti iesaka lietot **automātiski ģenerētas paroles**. Paroļu pārvaldnieks ir lietotnes veids, kas pieejams viedierīcēs, kurā var uzglabāt dažādas paroles šifrētā veidā, lai tās netiktu aizmirstas.

Jāatceras, ka nepieciešams parūpēties par uzglabāto paroļu drošu aizsardzību, uzstādot atbilstošu **autentifikāciju/šifrēšanu** aizsargājamajām parolēm, kā arī ierīcei.



LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Drošas maksājumu metodes internetā



Vienmēr **lieto drošus maksāšanas līdzekļus**, piemēram, bankas karti vai savienojumu ar internetbanku.



Iepērcies interneta veikalos, kas maksājumiem izmanto drošu jeb **divu faktoru autentifikāciju**. Tas liecina, ka tirgotājs augstu vērtē maksājumu drošību.



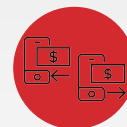
Ja par preci jānorēķinās, veicot rēķina **apmaksu pirms preces saņemšanas, padomā divreiz**. Šajā gadījumā, ja būs notikusi krāpšana, naudu atgūt ar bankas palīdzību nevarēs.



Maksā tikai tad, kad esi pieslēgts **drošam interneta savienojumam** — izvairies izmantot atvērtu, publisku Wi-Fi.



Maksāšanai izmanto **drošu ierīci**, kam programmatūras atjauninājumi veikti vismaz pēdējo 3 mēnešu laikā.



Seko līdzi naudas plūsmai savā kontā — papildu kontrolei ieslēdz paziņojumus mobilajā lietotnē. Pēc vajadzības maini maksājumu limitu.



Karšu maksājumi

- Karšu maksājumi ir viena no klientu iecienītām maksājumu metodēm internetā, kas ir drošs un pārbaudīts maksājumu veids. Mastercard ir populārākās maksājumu kartes Latvijā. Vairāk nekā 80 % no visām izsniegtajām kartēm ir tieši Mastercard.
- Par karšu maksājumu drošību rūpējas gan karšu izsniedzēji, gan bankas un tirgotāji. Tāpat par savas kartes drošību jāgādā arī katram kartes lietotājam.
- Bankas piedāvā internetbankā ērti ieslēgt un atslēgt tiešsaistes maksājumus kartei. Pirms pirkuma veikšanas ieslēdz drošu e-pirkumu funkcionalitāti, bet pēc tam — atslēdz.
- Uz pirkumiem ar maksājumu karti attiecas karšu maksājumu garantija, kas klientam sniedz iespēju vērsties bankā neautorizētu un krāpniecisku maksājumu gadījumā.
- No maksājumu viedokļa tiešsaistē visdrošākie ir tie interneta veikali, kas karšu maksājumiem atbalsta drošu jeb divu faktoru autentifikāciju, piemēram, paroli un vēl kādu papildu attālās atpazīšanas veidu. Tas apliecina, ka tirgotājs augstu vērtē maksājumu drošību un, visticamāk, būs parūpējies arī par citiem savu IT sistēmu drošības aspektiem.
- E-komercijā maksājumiem divu faktoru autentifikācija, piemēram, parole un E-Mobile vai SmartID, ir garantijas zīme, ka veikals ir drošs. Divu faktoru jeb stingrā autentifikācija ir kā drošības slānis, kas palīdz novērst neatļautus tiešsaistes karšu norēķinus un pasargā no krāpšanas. Mastercard karšu lietotājiem svarīgi pievērst uzmanību, vai ir Mastercard Identity Check logotips.

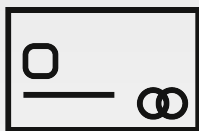


Savienojums ar internetbanku (BankLink)

- Drošs savienojums ar internetbanku ir viena no klientu visieciņākajām maksājumu metodēm internetā, liecina Latvijas iedzīvotāju aptauja. Klients pēc preces vai pakalpojuma izvēlēšanās tiek novirzīts uz jau aizpildītu maksājuma uzdevumu savā internetbankā vai mobilajā lietotnē.
- BankLink nodrošina, ka tirgotājs var sagatavot maksājumu uzdevumu tieši pircēja internetbankā un klients var nekavējoties to apstiprināt.
- Jāņem vērā, ka BankLink pārskaitījums negarantē naudas atskaitīšanu atpakaļ krāpšanas gadījumā. Ja prece vai pakalpojums netiks piegādāts, naudu atgūt ar bankas palīdzību nevarēs.

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Kā rīkoties, ja prece nav piegādāta?



Izmantojot maksājumu kartes, **iespējas atgūt naudu** krāpšanas vai nekvalitatīvi piegādātas preces gadījumā ir **lielākas**.



Ja prece nav piegādāta, sākumā **sazinies ar tirgotāju**. Iespējams, ir kāds objektīvs iemesls, kāpēc preces piegāde ir aizkavējusies.



Ja nav atbildes un neizdodas vienoties par risinājumu, sazinies ar savu banku, rakstot iesniegumu un iesniedzot dokumentētus pierādījumus par pirkuma veikšanu un saziņu ar tirgotāju.



Ja noticis neautorizēts maksājums, proti, maksājumu kartes lietotājs nav devis piekrišanu tā izpildei, **bankai nauda jāatmaksā vienas dienas laikā**. Savukārt, ja iepērkoties internetā, pakalpojums vai **prece nav piegādāta vai ir bojāta, klientam sākumā būtu jāvērsas pie tirgotāja**. Ja ar tirgotāju neizdodas vienoties par naudas atmaksu, klientam jāvērsas savā bankā. Banka katru gadījumu izvērtēs individuāli — ja pirkums veikts ar maksājumu karti, klients naudu atgūs, naudas atmaksa var ilgt līdz 90 dienām.



Ja ir aizdomas par krāpšanu, ziņo policijai. Parasti, izvērtējot individuālo gadījumu, banka iesaka vai pat lūdz sazināties ar policiju.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.

Padomi drošiem tiešsaistes pirkumiem



#1

Esi vērīgs, izvēloties interneta veikalu. Pārlicinies, vai norādīts: uzņēmuma nosaukums, reģistrācijas numurs, juridiskā adrese, kontakttālrunis, e-pasta adrese ātrai saziņai. Apskaties, kādas ir citu pircēju atsauksmes, un izvērtē, vai sniegta skaidra un saprotama informācija par preci.

Uzmanies no reklāmām, kas sola brīnumproduktus vai neticami mazas produktu vai pakalpojumu cenas.



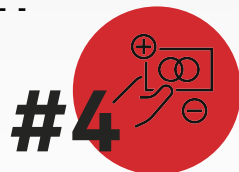
#2



#3

Iepērcies interneta veikalos, kas izmanto drošo jeb divu faktoru autentifikāciju. Tas liecina, ka tirgotājs augstu vērtē maksājumu drošību.

Seko līdz naudas plūsmai savā kontā — papildu kontrolei ieslēdz paziņojumus mobilajā lietotnē. Pēc vajadzības maini maksājumu limitu.



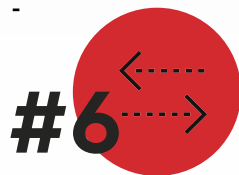
#4



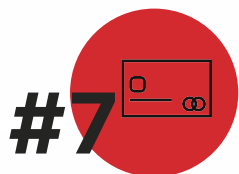
#5

Pārlicinies, ka savienojums ir drošs (http un https). Neizmanto ierīci, kurai programmatūras atjauninājumi nav veikti ilgāk nekā 3 mēnešus.

Noskaidro, kādi ir preču atpakaļ nosūtīšanas noteikumi.



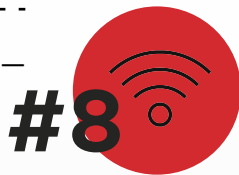
#6



#7

Vienmēr lieto drošus maksāšanas līdzekļus, piemēram, bankas karti vai savienojumu ar internetbanku (BankLink).

Maksā tikai tad, kad esi pieslēgts drošam interneta savienojumam — izvairies izmantot atvērtu, publisku Wi-Fi.



#8

LŪDZU, ŅEM VĒRĀ, KA ŠIS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS. PIRMS PĀSŪTI PRECI INTERNETĀ, TEV PATSTĀVĪGI JĀNOVĒRTĒ TIEŠSAISTES VEIKALI, KURUS IZVĒLIES.