

viedpircējs

Digitālās drošības ABC – esi #viedpircējs



Kā atpazīt un izvairīties no krāpniecības tiešsaistē un telefonā?

Par virtuālās krāpniecības upuri var kļūt jebkurš — lai gan jaunākās Mastercard un Finanšu nozares asociācijas aptaujas dati liecina, ka 87 % Latvijas iedzīvotāju uzskata, ka viņi mācētu atpazīt, ja pa telefonu sazinātos krāpnieks ar mērķi izkrāpt naudu, taču Asociācijas dati rāda, ka kopumā četrās lielākajās Latvija bankās 2021. gadā konstatēti 3180 telefonkrāpšanas gadījumi, izkrāpjot 4 950 333 eiro. Turklāt konstatēts 1281 investīciju krāpšanas gadījums, izkrāpjot 4 459 278 eiro, un 785 cita veida krāpšanas gadījumi, izkrāpjot kopumā 1 654 550 eiro.

Valsts policijas apkopotie dati savukārt liecina, ka 2021. gada laikā uzsākti gandrīz 800 kriminālprocesi par telefonkrāpniecību. Krāpnieki pārsvarā izmanto jau pārbaudītas taktikas. Ja zināsi, kādas ir šīs metodes, būs vieglāk sevi pasargāt.



LŪDZU, ŅĒM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

Kā krāpnieki to dara?

ATPAZĪSTI UN IZVAIRIES NO KRĀPŠANAS PA TELEFONU!

- Telefonkrāpnieki visbiežāk uzdodas par banku, piegādes vai apdrošināšanas uzņēmumu pārstāvjiem; zvana no viltotiem numuriem — gan ārzemju, gan Latvijas.

Atceries!

Jebkuru zvanu no nezināma numura izvērtē ļoti kritiski!

Ja zvans no minēto organizāciju pārstāvjiem pienāk no mobilā tālruņa numura, ļoti iespējams, ka tā ir krāpšana. Tāpat, ja zvana no citas valsts. Arī oficiāla izskata numurs negarantē, ka zvans tiešām ir no bankas vai citas iestādes, jo zvanītāja numuru krāpnieki spēj mainīt.

- Krāpnieki mēģina iegūt konfidenciālu informāciju (personas kodu, PIN kodus, internetbankas pieejas datus u. c.).

Atceries!

Nekādā gadījumā neizpauž savus personīgos datus!

Telefonkrāpnieki sarunas laikā prot izvilināt informāciju, pārzinot cilvēka psiholoģiju — steidzina, rada spriedzi, mudina pieņemt nepārdomātus lēmumus. Banku darbinieki nekad neaicina klientus dalīties ar personas datiem vai nosaukt piekļuves paroles.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

vied pircējs

- Telefonkrāpnieki zvana laikā mudina veikt naudas pārskaitījumus, liek ievadīt stingrās autentifikācijas kodus, kā arī mēģina pārliecināt instalēt ierīcēs programmatūru, lai novērstu kādu problēmu. Līdzīgi uz šādām darbībām aicina, arī izsūtīt īsziņas, e-pastus vai privātas ziņas sociālajos tīklos.

VILTUS SMS PARAUGS



Avots: CERT.LV

Atceries!

Izvairies no internetbankas pieejas kodu izpaušanas, sev nezināmu vai nesaprotamu darījumu apstiprināšanas ar stingrās autentifikācijas līdzekļiem vai kodu kalkulatoru, kā arī jaunas programmatūras lejupielādēšanas.

Ja kāds sūta ziņu, prasot ievadīt stingro autentifikācijas līdzekļu vai kodu kalkulatora piekļuves kodus, tas ir skaidrs signāls par krāpšanu. Šādi apstiprinātu darbību nevar atcelt, tas tev nozīmēs pazaudētu naudu.

- Krāpnieki nereti ir jau iepriekš izvilinājuši vai uzzinājuši upura personīgos datus (vārdu, uzvārdu, personas kodu, e-pastu, telefona numuru, kartes numuru u. c. informāciju), kas tiek aktīvi izmantoti upura pārliecināšanai un apkrāpšanai.

Atceries!

Personīgo datu piesaukšana nav pamats uzticēties. Iespējams, šāda informācija ir pieejama vai noziedzīgā ceļā iegūta internetā.

vied pircējs

- Krāpnieki sola mazu risku un lielu peļņu — vilina ar laimestiem loterijās, aicina piedalīties labdarības kampaņās, piedāvā īpaši izdevīgus aizdevumus u. c.

Atceries!

Liela peļņa vienmēr nozīmē arī lielu risku. Tiklīdz ir aizdomas par krāpniecisku piedāvājumu, nekavējoties jābeidz saruna.

- Krāpnieki bieži vien nemāk vai atsakās runāt valsts valodā, sarunās izmanto sarunvalodas izteicienus.

Atceries!

Bankas un citu iestāžu darbinieku pamatvaloda ir latviešu valoda, viņi nekad neatteiks saziņu valsts valodā.

- Telefonkrāpnieki saziņai ar saviem upuriem izmanto arī dažādas mobilās lietotnes, piemēram, *WhatsApp*, *Telegram*, *Viber* u. c., aicinot klikšķināt uz viltus saitēm.

Atceries!

Šādas ziņas ir jāignorē, tās nedrīkst pārsūtīt tālāk, turklāt ziņas sūtītājs ir jānobloķē.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

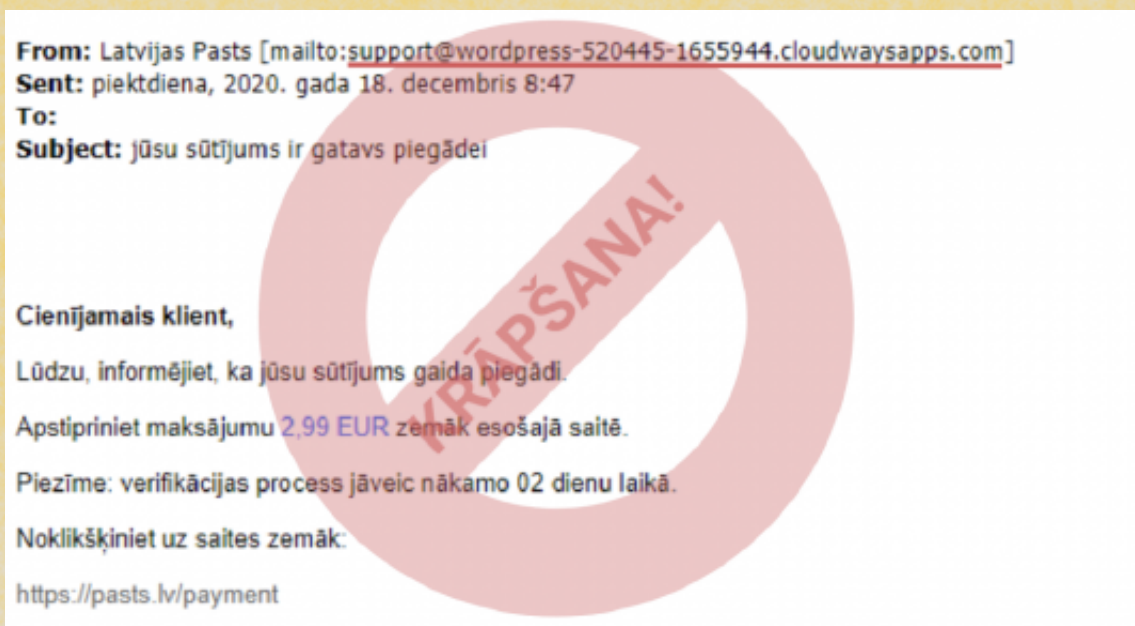
Kā krāpnieki to dara?

ATPAZĪSTI UN IZVAIRIES NO KRĀPŠANAS TIEŠSAISTĒ!

VILTUS E-PASTI

- Krāpnieki uzdodas par dažādu banku, organizāciju un uzņēmumu pārstāvjiem, izsūta e-pastus ar lūgumiem apstiprināt savu identitāti, atvērt pielikumus un viltus saites, kurās tālāk jāievada privāta informācija.

VILTUS E-PASTA PARAUGS



Avots: CERT.LV

Atceries!

Never vaļā aizdomīgus e-pastus un neklikšķini uz saitēm tajos. Pievērs uzmanību ziņas sūtītāja adresei un e-pasta saturam — pareizrakstības un loģikas kļūdas signalizē par krāpšanu.

VILTUS RĒĶINI

- Krāpnieki imitē e-pastus no dažādiem uzņēmumiem, piemēram, piegādes pakalpojumu nodrošinātājiem, aicinot noklikšķināt uz saites un apmaksāt rēķinu par nepienākušu sūtījumu.

Atceries!

Ja esi saņēmis rēķinu par nepasūtītu preci vai neizmantotu pakalpojumu, tā visticamāk ir krāpšana. Neievadi personīgos datus un neveic maksājumus par neeksistējošu preci vai pakalpojumu!

VILTUS TĪMEKĻA VIETNES

- Krāpnieki izmanto viltus interneta vietnes, kas šķietami atgādina internetbankas un interneta veikalus, lai izvilinātu no iedzīvotājiem bankas datus un citu privātu informāciju, kā arī mudina veikt viltus pirkumu.

Atceries!

Vienmēr rūpīgi apskati tīmekļa vietnes adresi — iespējams, tajā ir kāds lieks vai trūkstošs simbols.

Tāpat vēlams pārbaudīt atsauksmes par interneta veikalu, ja tajā iepērcies pirmo reizi. Drošāki ir tie internetveikali, kuriem adrese sākas ar "https://" un tās priekšā atrodas "lock" jeb atslēdzīņas simbols. Tāpat drošāki ir tie internetveikali, kuros tiek izmantota 3D Secure sistēma jeb Stingrā klientu autentifikācija, kas nozīmē, ka papildus maksājumu kartes datu ievadīšanai darījums jāapstiprina, pieslēdzoties internetbankai.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

VILTUS REKLĀMA INTERNETĀ

- Vēl viens no krāpšanas paņēmieniem ir reklāmas, kas stāsta par neticami izdevīgiem piedāvājumiem. Šīs reklāmas bieži vien bez viņu pašu ziņas izmanto sabiedrībā zināmas personas, atsaucas uz fiktīviem ziņu sižetiem un viltus pozitīvo

Atceries!

Ja piedāvātās cenas ir aizdomīgi izdevīgas un atlaides neticami lielas, ļoti iespējams, ka tas ir krāpšanas mēģinājums.

VILTUS INVESTĪCIJU PIEDĀVĀJUMI

- Krāpnieki internetā piedāvā arī ieguldīšanas iespējas, kas sniedz iespēju neticami labi nopelnīt — aicina investēt naudu virtuālajās valūtās vai dažādās ieguldījumu platformās. Ļaundari uzdodas par brokeriem vai bankas darbiniekiem un piedāvā ielādēt lietotnes vai pārskaitīt naudu, lai izdevīgi investētu. Solīto investīciju un peļņas vietā nauda nonāk krāpnieku rokās.

Atceries!

Ja kāds tev piedāvā ātru un lielu peļņu, tā, visticamāk, ir krāpšana.

Visām Latvijā licencētajām ieguldījumu platformām jābūt reģistrētām, pārliecinies par to īstumu Finanšu un kapitāla tirgus komisijas (FKTK) mājas lapā.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

VILTUS DARBA PIEDĀVĀJUMI

- Krāpnieki mēdz izveidot un izvietot internetā fiktīvus darba piedāvājumus. Izsludinot viltus vakanci kāda zināma uzņēmuma vārdā, ļaundari aicina kandidātus reģistrēt savus pieteikumus, izmantojot internetbankas datus, atsūtīt bankas konta un pases datus vai iemaksāt noteiktu naudas summu darba devējam.

Atceries!

Lai iesniegtu pieteikumu vakancei vai stātos darbā, darba devējam nav nepieciešami tavi bankas konta dati vai pārskaitījums uz viņa kontu.

VIEGLAS PEĻŅAS PIEDĀVĀJUMI JEB KĻŪŠANA PAR "NAUDAS MŪLI"

- Krāpnieki, izmantojot sociālos medijos, e-pastus vai dažādas saziņas lietotnes, piedāvā iegūt vieglu peļņu — par atlīdzību lūdz izmantot tavu bankas kontu, lai veiktu naudas pārskaitījumus, nereti tos formulējot kā darba piedāvājumus naudas pārskaitīšanas aģenta vakancei. Tādā veidā upuris kļūsti par "naudas mūli", kas palīdz noziedzniekiem anonīmi veikt noziedzīgi iegūtas naudas pārskaitījumus uz dažādam valstīm.

Atceries!

Šāda veida darbības ir naudas atmazgāšana, kas ir aizliegta ar likumu, un upurim nozīmē nonākšanu policijas redzeslokā. Ja rodas aizdomas, ka esi iesaistīts krāpšanas shēmā kā naudas mūlis, nekavējoties pārtrauc naudas pārskaitījumu veikšanu.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

Kā rīkoties, ja notikusi krāpšana vai tās mēģinājums?



Nekavējoties informē savu banku!



Ja dati ievadīti krāpnieciskā vietnē, nomaini paroli īstajā vietnē, kuru krāpnieki atdarināja! Ja izmanto to pašu paroli vairākiem kontiem, nomaini arī tās!



Pievērs īpašu uzmanību savam bankas konta pārskatam, lai laicīgi pamanītu aizdomīgus darījumus! Ja pamani maksājumu, kuru neesi veicis, nekavējoties sazinieties ar banku, lai bloķētu karti vai kontu!



Vienmēr ziņo policijai par aizdomīgiem gadījumiem, arī tad, ja tevi vēl nepaguva apkrāpt!



Iesniedz iesniegumu valsts policijas iecirknī, elektroniski — portālā latvija.lv vai, apstiprinātu ar elektronisko parakstu, sūti to uz e-pasta adresi pasts@vp.gov.lv!



Informāciju par aizdomīgiem gadījumiem interneta vidē iespējams nosūtīt policijai arī mobilajā lietotnē "Mana drošība".



Par aizdomīgām saitēm un pikšķerēšanas vietnēm raksti uz cert@cert.lv, lai saites pēc iespējas ātrāk varētu bloķēt!



Par krāpšanas shēmām brīdini arī savus radus, draugus un paziņas!

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS!

Esi #viedpircējs ikdienā!



DOMĀ UN RĪKOJIES DIGITĀLI!



LIETO DAŽĀDUS MAKSĀJUMU RĪKUS!



BIEŽI VEIC IKDIENAS PIRKUMUS TIEŠSAISTĒ!



IEPĒRCIES UN RĪKOJIES DROŠI UN GUDRI!

Papildu resursi

Izglītojošā kampaņa "Neuzķeries" 

Ziņo par drošības pārkāpumiem internetā! 

Latvijas kibertelpa skaitļos 

Krāpniecība maksājumos 

Kā pasargāt sevi no krāpniekiem internetā? 

Drošības kļūdas 

Kā neuzķerties uz finanšu krāpnieku ēsmām? 

Dažādas krāpšanas shēmas 