



Populārākie krāpšanas veidi

Publicēts: 12.10.2023.

Telefonkrāpnieki

Policija aicina iedzīvotājus būt piesardzīgiem, saņemot telefona zvanus no nezināmām personām, kuras sevi iepazīstina kā dažādu uzņēmumu finanšu brokerus vai arī dažādu citu arodu "finanšu speciālistus". Saziņas procesā, krāpnieki izmantojuši telefona numurus, kas reģistrēti dažādās valstīs (Latvijā, Lietuvā, Igaunijā, Portugālē, Itālijā, Austrijā, Francijā, Beļģijā, Anglijā, Vācijā, Rumānijā, Nīderlandē un citās valstīs) un visai uzstājīgā veidā aicina iedzīvotājus investēt finanšu līdzekļus dažādās brokeru/ ieguldījumu platformās, kuras nav tiesīgas darboties Latvijā. Potenciālajiem ieguldītājiem piekrirot aicinājumam, komunikācija turpmāk notiek, izmantojot tērzēšanas lietojumprogrammu "Skype" vai "Whatsapp". Jāuzsver, ka sarunvaloda starp ieguldītājiem un "finanšu speciālistiem" notiek krievu valodā, taču nedrīkst izslēgt arī iespēju, ka krāpnieki turpmāk var komunicēt citās valodās.

Šajos krāpšanas gadījumos arvien parādās jaunas platformas ar jaunajiem nosaukumiem, taču līdz šim krāpnieki piedāvājuši investēt platformās, kuru nosaukumā ir sekojoši vārdi:

gfbroker.;
alegramarkets.;
market-invest.;
maximarkets.;
mmglobal.;
everest.;
everest-trade;
gmoption.;
Capital Citadel FX;
Citadel Forex;
Go Capital FX;
CT – Trade;
Delloy Trade;
Glenmore Investment;

Trade.Rock-Finance;

Rock Capital Market;

Fx-dealer;

24option;

Fxnobels;

Fxgtrade;

Stock trade market;

Markets-invest;

alphacapital u.c.

Ar šo "finanšu speciālistu" palīdzību, uzticīgi iedzīvotāji izveido norēķina kontus virtuālās interneta platformās un tiek uzsākta investīciju ieguldīšana. Tādā veidā piesaistītās personas, kuras piekritušas iesaistīties apšaubāmajās finanšu operācijās tiešsaistē, sāk veikt dažādas finanšu darbības, kuru rezultātā vairākos maksājumos pārskaita dažādas naudas summas. Turpinot komunikāciju ar augstāk minētajiem "finanšu speciālistiem" – krāpniekiem, pēc viņu ieteikumiem ieguldītāji turpina veikt dažādas finanšu darbības – pērk un pārdod akcijas, veic citas finanšu aktivitātes, kas kopumā rada iespaidu, ka personas no šīm darbībām iegūst peļņu, taču patiesībā šo naudu zaudē.

Valsts policijai, veicot pārbaudi par šāda veida gadījumiem, ir pamatotas aizdomas, ka šādu naudas izkrāpšanas shēmu īsteno organizēta personu grupa no ārvalstīm, un noskaidrots, ka tie veikti ne tikai Latvijā, bet arī kaimiņvalstīs.

Lai sevi pasargātu no krāpšanas, policija aicina iedzīvotājus būt piesardzīgiem un nebūt pārļieku uzticīgiem, komunicējot ar nepazīstamiem cilvēkiem. Tāpat, pirms pieņemt lēmumu par finanšu līdzekļu ieguldīšanu, jāpārlicinās vai minētais uzņēmums (*uzņēmējdarbība*) ir reģistrēta Latvijā, kāds ir tā darbības veids, saņemtās licences un jebkāda cita veida informācija, kas liecina par uzņēmuma darbības tiesiskumu Latvijas teritorijā. Par to, vai attiecīgā investīciju platforma vai izvēlētais pakalpojuma sniedzējs ir tiesīgs savus pakalpojumus sniegt Latvijā, iedzīvotāji var pārlicināties FKTK mājas lapā (www.fktk.lv), kur ir atrodama informācija par licencētiem noguldījumu pakalpojumu sniedzējiem Latvijā. Ja tajā neatrodiet informāciju par izvēlēto investīciju platformu vai ieguldījumu brokera sabiedrību, tad to darbība nav atļauta vai ir aizliegta Latvijā.

Tāpat Valsts policija atgādina iedzīvotājiem būt īpaši piesardzīgiem, rīkojoties ar saviem personas datiem, elektronisko maksāšanas līdzekļu (kreditkaršu) datiem un citu personisku informāciju. Lai nepakļautu sevi krāpšanas riskam, nekādā gadījumā tos nedrīkst izpaust citām personām.

Kā tas notiek?

Sākotnēji kibernetizētie veic uzņēmumu mājaslapu analīzi, ievāc informāciju par darbiniekiem un izmantotajām e-pasta adresēm. Kādam uzņēmuma darbiniekam tiek nosūtīts e-pasts ar inficētu saturu. Ar maldi panākot inficētā e-pasta atvēršanu, kibernetizētie inficē darbinieka darba staciju ar spiegošanas ļaunatūru, kā rezultātā iegūst piekļuvi e-pasta sarakstei. Tiek izvēlēts kāds no apdraudētā uzņēmuma sadarbības partneriem, un brīdī, kad tas atsūta kārtējo rēķinu apmaksai, rēķins tiek viltots un tajā tiek norādīts kibernetizētie konts citā bankā (Lielbritānijā, Čehijā, Vācijā, Ķīnā). Parasti par iegāsti bankas konta maiņai tiek minētas dažādu raksturu problēmas ar tiesībsargājošām iestādēm – uzņēmuma nodokļu pārbaude, konta arests, konta bloķēšana un tamlīdzīgi.

Kā pasargāt uzņēmuma e – pastu?

Veidojot darījuma attiecības ar partneriem, drošības nolūkos ieteicams izmantot dažādus saziņas kanālus, piemēram, telefona sakarus, faksu vai kriptēto saraksti;

pirms pārskaitīt naudu sadarbības partneriem, vajadzētu pārliecināties, ka rēķinā norādītais bankas nosaukums, bankas konts un uzņēmuma nosaukums atbilst sadarbības partnera norādītajai informācijai;

ja tiek novērotas izmaiņas sadarbības partnera bankas nosaukumā vai bankas kontā, nepieciešams sazināties ar sadarbības partneri, izmantojot alternatīvo saziņas veidu, lai pārliecinātos par informācijas precizitāti;

ieteicams izmantot antivīrusu programmas un datorprogrammas ar atjauninātām versijām.

Krāpnieki izveido viltus interneta veikalus, lai ļaunprātīgi iegūtu pircēju naudu. Pircējs noskata kāroto preci, veic tās pirkumu, pārskaitot naudu, taču pasūtītā prece kaut kur pazūd jeb ilgstoši vai nemaz netiek saņemta. Tādās situācijās naudas saņēmējs tišuprāt neizsūta preci, kā rezultātā pasūtītājs kļūst par interneta krāpšanas upuri.

Kā nekļūt par ārzemju interneta veikalu krāpšanas upuri?

Kritiski jāizvērtē izvēlētais interneta veikals – ja izvēlētā prece tiek noskatīta kādā no populārajiem interneta veikaliem, par pirkuma drošību nevajadzētu uztraukties. Svarīgi pirms pasūtījuma veikšanas internetā ievākt ziņas par konkrēto pārdevēju – atsauksmes, citu pircēju iepriekšējo pieredzi;

vienmēr rūpīgi jāizlasa pirkuma nosacījumi un noteikumi – šī sadaļa satur ļoti svarīgu informāciju gan par preces izsūtīšanas laiku, gan izsekošanu, gan iespējām to atgriezt utt.;

jāizmanto atsevišķa norēķinu karte – ja pirkuma apmaksai tiek izmantota kredītkarte, iesakām iegādāties atsevišķu norēķinu karti, ar kuru tiks veikti iepirkumi interneta veikalā un uz kuru tiks pārskaitīta tikai konkrēta pirkuma naudas summa. Tādējādi, ja būs notikusi krāpniecība, naudas saņēmēji iegūs tikai to naudu, kas bija paredzēta attiecīgajam pirkumam;

ja ir iespēja, jāmaksā pēc pirkuma saņemšanas – lai nepazaudētu naudu, par preci ir iespējams maksāt arī pēc tās saņemšanas;

nevajadzētu izpaust personīgo informāciju – nekādā gadījumā nevajadzētu atklāt savas norēķinu kartes un pases vai cita apliecinošā dokumenta numuru. Krāpnieki var lūgt ne tikai norādīt norēķinu kartes numuru, bet arī telefona numuru, personīgos datus, norēķinu kartes drošības kodu un pat internetbankas paroli;

jāpieprasa preces dokuments – pircējs var droši pieprasīt preces, piemēram, sadzīves tehnikas vai elektropreces dokumentu.

Neeksistējoša lauksaimniecības tehnikas tirgošana, pieprasot avansa maksājumu



Kā tas notiek?

Krāpnieki ievieto sludinājumu portālos fotogrāfijas ar attiecīgo lauksaimniecības tehniku un tās tehnisko aprakstu, piedāvājot to iegādāties par izdevīgāku cenu, kas bieži ir zemāka par tirgus cenu. Piesaistot potenciālos pircējus, krāpnieki darījuma laikā ar viņiem sazinās telefoniski vai sarakstoties e-pastā. Savstarpējā komunikācija turpinās līdz brīdim, kad krāpnieki potenciālajam klientam nosūta sagatavotu rēķinu par pirmās iemaksas veikšanu, lai organizētu tālāku preces pārdošanu. Brīdī, kad persona attiecīgo samaksu veikusi, komunikācija beidzas un no krāpnieka un pirktās preces vairs nav ne vēsts.

Kā nekļūt par neeksistējošas lauksaimniecības tehnikas tirgošanas upuri?

Ja ir uzsākta komunikācija ar kādas eksistējošas vai zināmas firmas dīleri elektroniski, jāpārliciecinās, kā ir uzrakstīts firmas nosaukums un darbinieka e-pasta adrese, jo visbiežāk tiek veidoti līdzīgi nosaukumi, vien pamainot kādu burtu vai variējot ar pieturzīmēm e-pasta adresē;

nevajadzētu iegādāties tehniku, kura nav redzēta dzīvē, bet tikai fotogrāfijās;

nevajadzētu pārskaitīt avansa maksājumu, ja nav pārlicības, ka prece tiešām atrodas darījuma partnera – pārdevēja īpašumā vai valdījumā un var tikt pārdota.

Viltus loterijas



Kā tas notiek?

Loterijas būtība – dažādās interneta vietnēs un pārlūkos tiek rīkotas viltus akcijas, kurās interneta lietotāji aicināti piedalīties neeksistējošās loterijās, tādējādi laimējot vērtīgas balvas. Atbildot pareizi uz dažiem jautājumiem, tiek izlozēti vairāki pareizo atbilžu autori, kuri savā īpašumā it kā saņems kādu vērtīgu balvu. Tomēr, lai laimestu saņemtu, personām ir jāsniedz savi personīgie un bankas kartes dati. Šāds aicinājums rada aizdomas, ka tādā veidā tiek izkrāpti fizisko personu dati.

Kā nekļūt par krāpnieku upuri?

Kritiski jāizvērtē interneta vietnes piedāvātais saturs un valoda, kā arī iespējamās loterijas nosacījumus;

jāizvērtē nepieciešamība trešajām personām sniegt savus personīgos datus.

Kā tas notiek?

Krāpnieks uzdodas par AS "Latvijas gāze" darbinieku, kura mērķis, iegūstot uzticību, iekļūt privātīpašumā, lai izdarītu zādzību vai laupīšanu. Kā iemesls iekļūšanai privātīpašumā var būt vēlme pārbaudīt skaitītāja rādījumus, kā arī jebkurš cits ticams iemesls.

Kā nekļūt par viltus AS "Latvijas gāze" darbinieka upuri?

Šaubu gadījumā jāpieprasa apsekotājus uzrādīt "GASO" darbinieku apliecības*;

lai pārliecinātos, ka Jūsu īpašumā darbus veic "GASO" darbinieks, jāzvana: darba dienās no pulksten 8.00 līdz 17.00 – pa tālruņa numuru 155, pēc pulksten 17.00 un brīvdienās – pa tālruņa numuru 114;

GASO" darbinieka apliecības paraugu un formastērpus var apskatīt GASO mājaslapas sadaļā "Atpazīsti GASO"

- <https://www.gaso.lv/atpazisti-gaso> ;

ja tiek konstatēts, ka notikusi krāpniecība, nekavējoties jāvērsas tuvākajā Valsts policijas iecirknī vai jāzvana pa tālruni 112.

*Saskaņā ar likumā noteikto AS "Latvijas Gāze" reorganizāciju, ar 2017. gada 1. decembri vienīgā komercsabiedrība Latvijā, kas ir tiesīga veikt dabasgāzes sadales sistēmu apsekojumus mājāsaimniecībās ir akciju sabiedrība "GASO".