

NEUZĶERIES!

ESI GUDRĀKS PAR KRĀPNIEKIEM!



KRĀPŠANAS VEIDI

Kā atpazīt finanšu krāpnieku āķus?
Kā pasargāt savus personas datus un naudu?



Tālrūņa zvani

Krāpnieki bieži uzdodas par bankas pārstāvjiem. Viņi rada spriedzi, ka no konta tiek veikts aizdomīgs pārskaitījums, nauda ir apdraudēta.

Bieži jau ir sagatavojuši krāpniecisko darbību un liek ievadīt Smart-ID kodu, kas to oficiāli apstiprina.

Krāpnieki var melot par laimestiem loterijā vai sociālo tīklu konkursā, aicināt atvērt sirdi labdarības kampaņām, reklamēt dažādus brīnumlīdzekļus, piedāvāt darbu vai izsniegt īpaši izdevīgus aizdevumus.

Kā atpazīt telefonkrāpniekus?

- ✓ Uzstājīgi pieprasa bankas piekļuvi, Smart-ID vai eParaksta rīku piekļuves datus.
- ✓ Agresīvi biedē un steidzina, izmanto psiholoģiskus paņēmienus, meklējot cilvēka vājās vietas.
- ✓ Izsaka aizdomīgus piedāvājumus.
- ✓ Viltoti tālrūņa numurus, lai izskatās, ka zvana no bankas.
- ✓ Visbiežāk runā krievu valodā, bet ir sākuši apgūt latviešu.



E-pasti, izsiņas

Krāpnieki uzdodas par labi atpazīstamu banku un citu pakalpojumu sniedzēju pārstāvjiem. Paziņojumi parasti satur lūgumus atvērt interneta saites, atjaunot datus un apliecināt savu identitāti.

Var informēt par it kā laimētu balvu sociālo tīklu konkursos. Izplatīta arī pieeja atsūtīt rēķinu par populāru pakalpojumu, ar atpazīstamu logo vai ļoti līdzīgu uzņēmuma nosaukumu, kurā maksājumu ir jāveic uz krāpnieku kontu.

Kā atpazīt krāpnieciskus e-pastus, izsiņas?

- ✓ Viltota adrese. Īsto adresi var ieraudzīt, ja uzvirza kursoru uz adreses.
- ✓ Neuzticama interneta saite. Pirms uz tās klikšķini, uzvirzi kursoru un apskati īsto nosaukumu.
- ✓ Uzstājīgi pieprasa bankas piekļuvi un Smart-ID kodus.
- ✓ Neveikla, bieži kļūdaina valoda.
- ✓ Izsaka aizdomīgus piedāvājumus.



Investīciju piedāvājumi

Krāpnieki uzdodas par investīciju brokeriem vai bankas darbiniekiem un piedāvā veikt īpaši izdevīgus ieguldījumu akcijās, obligācijās, kriptovalūtā un citur.

Viņi aicina instalēt programmatūru, lai veiktu ieguldījumus. Var arī vienkārši likt pārskaitīt naudu uz krāpnieku kontiem. Krāpnieki bieži rada tīmekļa vietnes, kurās upuris var sekot līdz "augošajai peļņai", jo maldinošie panākumi mudina investēt vēl un vēl. Turklāt viltvārži steidzina potenciālos investorus, norādot, ka izdevīgais piedāvājums būs spēkā tikai noteiktu laiku.

Kā atpazīt investīciju krāpniekus?

- ✓ Pieprasa bankas paroli, Smart-ID kodus vai citus personas datus.
- ✓ Liek instalēt programmatūru, ar kuru iegūst piekļuvi tavai ierīcei.
- ✓ Sola 0 risku un milzu peļņu.
- ✓ Agresīvi biedē un steidzina, izmanto psiholoģiskus paņēmienus, meklējot cilvēka vājās vietas.
- ✓ Darbojas nelegāli. Valsts aizsargā tikai tos klientus, kuri investē licencētu tirgus dalībnieku pakalpojumos. Pārbaudi potenciālo sadarbības partneri Latvijas Bankas mājaslapā!
- ✓ Visbiežāk runā krievu valodā, bet ir krāpšanas gadījumi arī latviski.

10 PADOMI, KĀ NEUZĶERTIES UZ KRĀPNIEKIEM:

1. Nedalies ar informāciju par bankas pieejām, parolēm un eParaksta piekļuves datiem ne telefonsarunās, ne sarakstēs internetā! Neievadi šos datus atsūtītajās interneta saitēs! Banka nekad nezvanīs vai nerakstīs klientiem, lai lūgtu dalīties ar parolēm vai citiem personas datiem.
2. Neglabā informāciju par bankas pieejām, parolēm, kodiem un eParaksta piekļuves datiem vietās, kur tai var piekļūt citi cilvēki piemēram, makā!
3. Nekādā gadījumā nesūti citām personām attēlus vai video ar bankas kartēm vai personu apliecināšiem dokumentiem!
4. Regulāri pārbaudi konta izejošos maksājumus! Uzstādi ienākošus paziņojumus par izmaiņām kontā vai pārbaudi konta pārskatu pēc iespējas bieži, lai ātrāk pamanītu aizdomīgus darījumus.
5. Regulāri atjaunini bankā kontaktinformāciju! Ja darījums šķiet aizdomīgs, bankas darbinieki sazinās ar klientu, lai pārliecinātos, vai to tiešām veic klients.
6. Neievadi informāciju uz nirstošajos logos un neklikšķini uz saitēm tajos!
7. Beidzot darbu, vienmēr atvienojies no internetbankas (poga – Iziet) un tikai pēc tam aizver pārlūkprogrammu!
8. Veic elektroniskos maksājumus tikai drošās interneta vietnēs! Pie interneta adreses pārlūkā ir jābūt atslēgas simbolam vai tai jāsākas ar https://.
9. Nepakļaujies krāpnieku prasībām viedierīcēs instalēt attālinātas piekļuves programmatūru! Nepieļauj, ka svešs cilvēks var rīkoties ar tavu ierīci un identitāti.
10. Neklikšķini uz e-pasta vēstulē un sociālo tīklu ziņojumā norādītās saites, ja neesi pārliecinājies, ka saite ved uz vietni, kas saistīta ar uzticamu vēstules sūtītāju!



Ko darīt, ja tev ir radušās aizdomas, ka esi ticis apkrāpts?

Ja tev ir aizdomas, ka esi kļuvis par krāpnieku upuri un esi pazaudējis naudu, aicinām pēc iespējas ātrāk ziņot savai bankai un vērsties ar iesniegumu tuvākajā Valsts policijas iecirknī.