FINANŠU NOZARES ASOCIĀCIJA

Doma laukums 8A-6, Rīga, LV-1050
Reģ. Nr. 40008002175
Tālrunis: 67284528
info@financelatvia.eu
www.financelatvia.eu

RĪGĀ

2021. gada 7. aprīlī

## Ko darīt, ja uzķērāties uz finanšu krāpnieku āķa?

**Krāpšanas mēģinājumiem atsaucas katrs desmitais uzrunātais, liecina Finanšu nozares asociācijas īstenotā eksperimenta rezultāti*. Galvenais iemesls, kāpēc cilvēki uzķeras ir ziņkārība, kam seko vēlme saņemt solītos labumus, nereti arī steiga. Diemžēl ik nedēļu šādā veidā iedzīvotājiem tiek izkrāpti no dažiem desmitiem līdz pat vairākiem tūkstošiem eiro. Finanšu nozares asociācija ir apkopojusi būtiskākos padomus, kā rīkoties, ja ir gadījies uzķerties uz finanšu krāpnieka āķa.**

**Ja sarunā krāpniekam atklājāt bankas piekļuvi un personas datus,** nekavējoties sazinieties ar savu banku un informējiet par situāciju, lai bloķētu piekļuvi kontam vai iespēju izmantot maksājuma kartes datus.

"*Ja ir aizdomas, ka notikusi krāpšana, piemēram, nauda ir pārskaitīta krāpniekam vai maksājumu kartes, internetbankas dati ir nopludināti, pēc iespējas ātrāk par to jāziņo bankai. Arī, ja karte ir pazaudēta vai nonākusi nepareizajās rokās, tā nekavējoties ir jābloķē savā internetbankā vai jāzvana bankai. Iedzīvotājiem jābūt piesardzīgiem un jāatceras, ka nekad nevar izpaust informāciju par internetbankas pieeju vai maksājumu kartes datiem trešajām personām. Tāpat aicinu iedzīvotājus parūpēties par saviem tuviniekiem, īpaši senioriem, iesakot neatbildēt uz šiem krāpnieciskajiem zvaniem vai e-pastiem*," uzsver **Luminor informācijas drošības eksperts Pāvels Mickevičs.**

**Ja uzspiedāt uz saites e-pastā, īsziņā vai sociālo tīklu ziņojumā vai lejupielādējāt krāpniecisku pielikumu:**

- uzreiz izslēdziet ierīcei Wi-Fi un/vai atvienojiet to no tīkla vada. Ja izdarīsiet to pietiekami ātri, iespējams, apturēsiet krāpnieku no ļaunprātīgas programmatūras instalēšanas vai liegsiet attālinātu piekļuvi ierīcei.
- skenējiet ierīci uz kaitniecisko programmatūru un vīrusu esamību. Pretvīrusu programmatūra pārbaudīs ierīci, brīdinot par visiem failiem, kas varētu būt inficēti.
- informējiet par šo gadījumu uzņēmumu, kura vārdā tika saņemts krāpnieciskais ziņojums.

"*Nereti krāpnieki izmanto dažādus izklaidējošus testus, kuros iedzīvotājus mudina noskaidrot, kādam dzīvniekam vai filmas tēlam esat līdzīgi, taču tie izveidoti, lai iegūtu jūsu datus un vēlāk tos izmantotu turpmākās krāpšanas shēmās. Tāpat bieži cilvēki tiek maldināti ar dažādiem pēkšņiem laimestiem loterijās, lai tikai panāktu, ka šīs ziņas saņēmējs atver atsūtīto saiti vai pielikumu. Taču jāatceras, ka krāpnieki izmanto dažādus psiholoģiskus paņēmienus, lai atrastu cilvēka vājās vietas, kā arī paļaujas uz cilvēku vājajām digitālajām prasmēm un vēlmi iegūt ātru "laimestu". Savukārt, iegūstot savā rīcībā pieeju lietotāju e-pastiem, krāpnieki var sūtīt ziņojumus personas draugiem, kuros mudina atvērt kādu saiti vai pielikumu, kas tomēr izrādās vīruss, un attiecīgi arī jūsu e-pasts ar visu tā saturu nonāk krāpnieku rīcībā. Parasti tie ir īsi un*

* Finanšu nozares asociācijas eksperiments tika īstenots 2021. gada februārī, izsūtot viltotu krāpniecisko e-pastu internetā brīvi atlasītiem 500 adresātiem visā Latvijā.

*lakoniski teksti: "Atver šo, te tu izskaties smieklīgs!" vai "Skat, kādu tavu bildi atradu internetā!". Tie visi ir krāpšanas mēģinājumi, tāpēc ir jābūt ļoti modriem un kritiskiem, izvērtējot jebkuru saņemto informāciju, arī no tuviem cilvēkiem*," norāda **Pāvels Mickevičs**.

**Ja ievadījāt datus krāpnieciskā vietnē:**

- Nomainiet paroli reālajā vietnē (e-pasta pakalpojums vai sociālā medija konts), kuru krāpnieki atdarināja. Ja izmantojat to pašu paroli vairākiem kontiem, nomainiet arī tās. Drošības eksperti neiesaka izmantot vienu paroli vairākkārt. Tāpat vēlams izmantot divu faktoru autentifikāciju, kad tiek izmantota gan parole, gan vēl viens faktors jeb papildu solis, atsūtot, piemēram, kodu uz lietotāja viedtālruni. Divu faktoru autentifikācija šobrīd tiek uzskatīta par vienu no drošākajām pieejām savas informācijas aizsargāšanai tiešsaistē.
- Ja ievadījāt norēķinu kartes informāciju, nekavējoties sazinieties ar banku, lai karti bloķētu.
- Pārliecinieties, vai neesat kļuvis par identitātes zādzības upuri. Vispirms uzstādiet ienākošos paziņojumus par izmaiņām kontā vai pārbaudiet konta pārskatu pēc iespējas biežāk, lai ātrāk pamanītu aizdomīgus darījumus. Informējiet par incidentu kredītinformācijas birojus, brīdinot, ka jūsu datus kāds varētu ļaunprātīgi izmantot un palūdzot informēt par izmaiņām jūsu kredītvēsturē.

Liela daļa pašreiz izplatīto kibernoziegumu ir starptautiski, un Valsts policija sadarbojas ar citu valstu tiesībsargājošām iestādēm, sniedzot atbalstu izmeklēšanā. Lai gan izmeklēšana starptautiskos kriminālprocesos ir sarežģīta un ilgstoša, ir gadījumi, kad, pateicoties ātrai ziņošanai attiecīgajām iestādēm, cietušie savu naudu ir atguvuši.

*"Naudas atgūšanas iespējas ir proporcionālas laikam, cik ātri cietušais ir vērsies bankā, un tam, cik ātri uzrakstījis iesniegumu policijā. Svarīgi nekavējoties ziņot bankai, nākamais solis – vērsties ar iesniegumu policijā. Mēs aktīvi saņemam iesniegumus ne tikai no cietušajiem par jau izkrāptu naudu, bet arī no iedzīvotājiem, kas ziņo par aizdomīgām darbībām interneta vidē. Tas palīdz laikus novērtēt situāciju kiberdrošības jomā un veikt preventīvas darbības,"* norāda **Valsts policijas Ekonomisko noziegumu apkarošanas pārvaldes priekšnieka vietnieks Dmitrijs Homenko.**

Iesniegumu Valsts policijai iespējams nosūtīt elektroniski portālā Latvija.lv, apstiprinātu ar elektronisko parakstu, sūtīt uz e-pastu pasts@vp.gov.lv, iesniegt klātienē vai nosūtīt pa pastu uz tuvāko Valsts policijas iecirkni. Brīdinājumu par dažādām aizdomīgām darbībām interneta vidē sūtiet izskatīšanai policijai mobilajā lietotnē Mana Drošība.

**Papildu informācija:**
Sabīne Spurķe
E-pasts: sabine.spurke@financelatvia.eu
T. +371 20604166
Komunikācijas vadītāja Finanšu nozares asociācija