Naudas drošība paša rokās.

Kā atpazīt krāpnieciskus mēģinājumus un kā rīkoties, ar tiem saskaroties? Zini, atpazīsti un neuzķeries!

Krāpnieki visbiežāk zvana!

Ja iepriekš krāpnieciski piedāvājumi visbiežāk parādījās e-pastā, tagad populārākas kluvušas telefonsarunas.

Nekādā gadījumā neizpaudiet datus par sevi! Neievadiet un nenosauciet pieejas kodus savai internetbankai un neapstipriniet ar Smart-ID/ kodu kalkulatoru darbības, ko neesat ierosinājis. Ja tomēr esat izpaudis datus, nekavējoties sazinieties ar savu banku, lai pēc iespējas ātrāk blofiētu pieejas un pasargāt savu naudu.

Telefona numurs nav atpazīšanas zīme!

Krāpnieki var zvanīt gan no ārzemju numura, gan viltota Latvijas numura. Var uzrādīties, ka zvana banka.

Jo ātrāk beigsiet šādu sarunu, jo mazāks risks izpaust kādus svarīgus datus. Krāpnieki lieliski prot izvilināt informāciju sarunas laikā.

Personīgo datu piesaukšana nav pamats uzticēties!

Steidzināšana, jūsu datu piesaukšana un apvārdošana ir krāpnieku stiprā puse. Krāpnieks no internetā pieejamās vai noziedzīgā celā iegūtās informācijas var zināt jūsu vārdu, uzvārdu, telefona numuru un pat personas kodu vai maksājumu kartes numuru.

Ja pastāv kaut mazākās šaubas par zvanītāja identitāti, nolieciet klausuli un personīgi sazinieties ar savu banku vai kādu citu uzņēmumu, ko zvanītājs uzdodas pārstāvam, lai pārliecinātos par patieso situāciju.

Smart-ID kods ir pielīdzināms e-parakstam!

Ar Smart-ID vai kodu kalkulatoru apstiprināts darījums ir pielīdzināms e-parakstam – jebkurš darījums, kas apstiprināts ar Smart-ID vai kodu kalkulatoru teju izslēdz iespējas to labot.

Smart-ID lietotnē pirms darījuma apstiprināšanas ir redzama informācija, kas tieši tiek apstiprināts. Nekad neapstipriniet darījumus, par kuru mērfii neesat pārliecināts! Labāk pārbaudīt vairākkārt, nekā apstiprināt neskatoties.

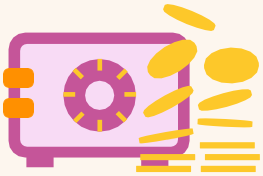
Sargājiet datus!

Ļoti rūpīgi jāizturas pret datu ievadīšanu gan mazāk pazīstamās, gan lielās un plaši zināmās platformās, piemēram, sociālajos tīklos. Nereti dati par cilvēku pieejami publiski, kā arī tos iespējams iegūt no pakalpojumu sniedzējiem ar vāju datu aizsardzību. Iespējams, ka datus nozog arī no paša lietotāja.

Iepērcieties tikai zināmos interneta veikalos, rūpīgi pievērsiet uzmanību, kādās vietnēs reģistrējaties un kādus datus tajās prasa ievadīt. Vai tie vienmēr nepieciešami pakalpojuma nodrošināšanai? Lai sargātu savas ierīces un datu nesējus, uzstādiet drošas paroles un neveriet vaļā aizdomīgus dokumentus/ pielikumus.

Lūdz atjaunot datus?

Zem aicinājuma apstiprināt savu identitāti un atjaunot pieejas datus var slēpties krāpnieku shēma, kuras mērķis ir pārliecināt dalīties ar vērtīgu informāciju, piemēram, bankas kartes datiem. Šādi e-pasti parasti tiek veidoti līdzīgi oficiāliem paziņojumiem no bankas vai citām iestādēm.
Pārbaudiet, vai sūtītāja e-pasta adresē ir iekļauta pareiza mājaslapas adrese, vai tajā nav iesprucis kāds lieks cipars vai burts. Ja e-pasts šķiiet aizdomīgs, izdzēsiet to un ziņojiet par krāpšanas mēģinājumu. Izvairieties atvērt aizdomīgus pielikumus - pat antivīrusa programmas bieži vien nespēj identificēt uzbrukumus.



Ātra un garantēta peļņa = zaudēta nauda!

Solījums par ātru un lielu peļņu visbiežāk rezultējas prāvā izkrāptās naudas summā.
Peļņas iespējas iet roku rokā ar risku – jo lielāks risks zaudēt naudu, jo augstāka iespējamā peļņa. Jo zemāks risks, jo zemāka peļņa. Šīs tirgus sakarības ir nemainīgas. Ja kāds mēģina pārliecināt, ka ieguldījums būs ātrs un lielu peļņu nesošs, visticamāk tā ir krāpšana!

Neklūstiet par naudas mūli!

Ja kāds piedāvā samaksāt par jūsu bankas konta izmantošanu naudas pārskaitījumiem, tad šī persona jūs lūdz kļūt par "naudas mūli". Tā ir naudas atmazgāšana, kas ir prettiesiska darbība un paredz smagas sekas - ne tikai nonākšanu policijas redzeslokā, bet arī krietni pabojātas izredzes darba tirgū, piemēram, nespējot atvērt bankā kontu.
Nekad neļaujiet rīkoties ar savu bankas kontu citai personai, neatklājiet savas internetbankas piekļuves datus vai kartes informāciju. Ja jums kādā brīdī rodas aizdomas, ka esat iesaistīts krāpšanas shēmā "naudas mūļa" lomā, nekavējoties pārtrauciet naudas pārskaitījumu veikšanu. Informējiet savu banku vai maksājumu pakalpojumu sniedzēju un Valsts policiju.

Jaunas programmatūras instalēšana – ar rūpīgu piesardzību!

Uzmanieties no pakalpojumu sniedzējiem, kuri jūs aicina uzstādīt savā datorā vai telefonā kādu jaunu programmatūru.
Instalējot jaunu programmatūru, pilnībā jāpārliecinās par tās reputāciju un to, kādam mērķiim programmatūra nepieciešama. Krāpnieki šādā veidā var iegūt kontroli pār ierīci un kopēt informāciju, ko lietotājs tajā ievada – piemēram, internetbankas lietotājvārdu, personas kodu, maksājumu karšu informāciju, paroles u.tml.

Spēle ar jūtām

Šobrīd aktuāla ir t.s. romantiskā krāpšana. Cilvēks internetā sāk saraksti, ar laiku atzīstas jūtās, bet, lai pirmo reizi satiktos, lūdz atsūtīt naudu biletēm vai sniegt palīdzību tuviniekiem. Izredzētais tā arī nekad neatbrauc, bet nauda par biletēm pazūd uz neatgriešanos.
Šajā gadījumā emocijas jāatliek otrajā plānā. Komunicējot internetā, informācija un rīcība jāizsver maksimāli racionāli.