Pašmērķis nav sodīt, galvenais — novērst

Krāpšana ir noziegums, kuru raksturo svešas mantas vai tiesību uz šādu mantu iegūšana, ļaunprātīgi izmantojot uzticēšanos vai ar viltu. Krāpnieki izmanto jebkādus līdzekļus, lai sazinātos ar saviem upuriem, — liek lietā tālruni, pastu, e-pastu un internetu. Viņi iegūst jūsu uzticību un, kad esat uzķēries(-usies) uz āķa, pazūd, atstājot pat tukšus kontus. Arvien biežāk dzirdam par dažādiem jauniem krāpšanas veidiem. Valsts policija regulāri brīdina un informē sabiedrību, tomēr joprojām cilvēki iekrīt slazdā un tiek apkrāpti. Šādās situācijās jāvēršas policijā.

Inga Randare norāda: — Ir daudz un dažādu krāpšanas veidu, tāpēc cilvēkiem šobrīd ir jābūt īpaši piesardzīgiem un vērīgiem, lai netiktu apkrāpti.

Valsts policijas Vidzemes reģiona pārvaldes Madonas apkalpojamajā teritorijā apkrāpšanas gadījumi nav retums. Par krāpniecību stāsta Vidzemes reģiona pārvaldes Madonas policijas iecirkņa Kriminālpolicijas nodaļas priekšniece **Inga Randare**.

— Šiem noziedzīgajiem nodarījumiem šobrīd ir novērojams neliels pieaugums. Ir palielinājies krāpšanas gadījumu skaits, un cilvēki biežāk vērsas policijā. Agrāk bija novērojama tendence, ka iedzīvotāji policijā vērsās, kad krāpniecība jau bija notikusi, šobrīd iesniegumus saņemam arī par krāpniecības mēģinājumiem. Lai arī kāpums ir neliels, tomēr neizskaidrojami ir, kāpēc tā notiek, ņemot vērā, ka sabiedrība daudz tiek brīdināta un informēta. Par krāpniecību runā presē, televīzijā, radio, sociālajos tīklos ir ļoti daudz informācijas, kā reaģēt, kādi ir krāpšanas gadījumi. Diemžēl kādā mirklī iedzīvotāji ir palaiduši šo informāciju garām un ir ļāvušies tikt apkrāpti.

Šobrīd cilvēki vairāk uzturas mājās, līdz ar to arī iepirkšanās notiek attālināti — internetā. Tas varētu būt viens no iemesliem, kāpēc apkrāpto cilvēku skaits ir audzis.

— Kādi ir izplatītākie krāpšanas veidi?

— Iepriekš vairāk tika runāts par datu iegūšanu un aizņēmumu noformēšanu uz citu personu vārda, tagad viens no populārākajiem veidiem joprojām ir telefonkrāpnieki, kad iedzīvotāji saņem zvanus it kā no bankas darbiniekiem, attiecīgi aicinot veikt kādas darbības — *Smart ID* paroļu ievadīšanu, datu apstiprināšanu, tādējādi piekļūstot bankas kontiem. Ja dati tiek ievadīti, nereti tiek aizskaitīta nauda vai noformēti aizdevumi. Šobrīd ļoti palielinājies gadījumu skaits, kad tiek saņemti zvani, kuru laikā cilvēks tiek informēts par it kā uz viņa vārdu atvērtu kriptovalūtas kontu. Stāsta, ka uz šī konta ir nauda un, lai to izņemtu vai kontu slēgtu, jāveic darbības, kādas pieprasa telefonkrāpnieki, kas zvana banku vārdā. Neraugoties uz to, ka šie cilvēki nekad šos *bitcoin* kontus nav atvēruši, viņi tomēr iekrīt. Vienubrīd bija standarta saruna, proti, ja cilvēks šo kontu neaizvērs, par šo kontu tiks atskaitīti četri simti eiro mēnesī. Pārliecinoši tika stāstīts, ka uz šī cilvēka vārda kāds ir šo kontu tomēr atvēris. Cilvēki tiek apvārdoti.

Tāpat šogad izteikts krāpšanas veids ir fiktīvie precību piedāvājumi, kad tiek lūgts pārskaitīt naudu. Mērķauditorija ir sievietes, kuras izmanto iepazīšanās portālus. Ilgstoši norit sarakste, viss liekas skaisti un patiesi. Tad seko stāsts par problēmām, bēdīgu situāciju, kad nepieciešama nauda, vai — gluži pretēji — kad sola pārskaitīt naudu, bet, lai šo pārskaitījumu veiktu, nepieciešama iemaksa, lai šo naudu saņemtu, līdz ar to cilvēki šādi tiek apkrāpti.

Ļoti izplatīts krāpšanas veids ir mantojumi. Šis veids ir ļoti līdzīgs precinieku krāpšanas shēmām. Uzrodas it kā ārzemju radinieki, kuri ir miruši, ir atstāts mantojums, bet, lai to saņemtu, jāpārskaita kāda naudas summa. Visos šajos gadījumos, līdzko cilvēks ir pārskaitījis kādu naudas summu, viņš drīz vien saprot, ka ir apkrāpts, un griežas policijā.

— Krāpšanas veidi ir dažādi. Vai iespējams laikus pamanīt, ka tomēr cilvēks ir iekritis krāpšanas shēmās?

— Krāpnieki strādā ļoti ātri. Apjaušot, ka dati ir nodoti un cilvēks kļuvis par krāpšanas upuri, par to var pārliecināties internetbankā. Attiecīgi vai nu nauda ir rezervēta, kas ir variants, kad vēl iespējams apturēt naudas pārsūtīšanu, vai nauda jau ir pārsūtīta. Visas šīs shēmas tiek īstenotas ar bankas pārskaitījumiem, līdz ar to tas parādās internetbankā. Tiklīdz ir aizdomas par krāpniecību vai ja veikts kāds naudas pārskaitījums, nekavējoties ir jāgriežas policijā. Jo ātrāk tiek saņemta informācija, jo ātrāk var uz to reaģēt, un ir iespēja, ka cilvēks šo naudu atgūs.

Pat, ja ir tikai aizdomas par krāpšanas mēģinājumu, ir jāvēršas policijā. Tā tiek iegūts vairāk informācijas par krāpniekiem, viņu shēmām.

Joprojām turpinās dažādas krāpnieciskas darbības ar traktortehniku, kad zemniekiem piedāvā iegādāties traktortehniku. Cilvēks, īsti nepārliecinoties, uz kurieni tiek pārskaitīti naudas līdzekļi, tiek apkrāpts. Te liela vērība jāpievērš tam, uz kurieni tiek veikts pārskaitījums, — jāpārliecinās par uzņēmumu, jāpārbauda konta numurs, vai tas sakrīt. Nereti konta numurā tiek izmainīti vidējie skaitļi. Datiem jāpieiet ļoti vērīgi.

— Bieži nākas dzirdēt arī par gadījumiem, kad, izmantojot kurjerfirmu vārdu, tiek mēģināts apkrāpt cilvēkus.

— *DPD* un *Omniva* krāpniecībā tiek iesaistīta bieži. Mūsu apkalpojamajā teritorijā šādu gadījumu ir maz, tomēr tādi ir. Ar krāpniecību saistītās lietas ir grūtāk atklājamas un izmeklējamas. Process ir darbietilpīgs un laikietilpīgs. Šie ir citas kategorijas noziegumi, tomēr visam, kas notiek internetā, pēdas saglabājas. Protams, ne visos gadījumos, bet ir iespējams atklāt. Uzsākot kriminālprocesu, darām maksimālo, lai šos noziegumus atklātu.

— Arvien biežāk manīti jauni krāpšanas veidi, shēmas.

— Tā nu ir, ka noziedznieki kļūst arvien gudrāki. Izmeklētājiem, kuri izmeklē šos ekonomiskos noziegumus, ir „jāaug" līdzi noziedzībai un tā jāpārspēj. Šie ir tie noziegumi, kas regulāri mainās, attīstās. Līdz ar to krāpniecība ir izaicinājums Valsts policijai, galvenajai Kriminālpolicijas pārvaldei, kur tiek risināti jautājumi, kā palīdzēt atklāt šos noziedzīgos nodarījumus.

— Kā tad atpazīt krāpniecību?

— Gadījumos, kad tiek veikti pirkumi, rūpīgi jāpārliecinās, kam nauda tiek pārskaitīta. Savukārt, kas attiecas uz telefonkrāpniekiem, — uzmanīgi izturēties pret niansēm — piemēram, runātāja valodu. Noteikti nevajag ielaisties sarunās, jo šīs personas mēdz izmantot dažādas manipulatīvas metodes, piemēram, cilvēka apvārdošanu. Jāskatās, kam uztic savus personīgos datus. Tāpat, ja kāds sarunas laikā lūdz lejuplādēt *AnyDesk*, nekādā gadījumā to nedrīkst darīt. Tā ir programma, kas ļauj attālināti pieslēgties un ar datoru veikt dažādas darbības. Cilvēkiem jābūt ļoti uzmanīgiem un vērīgiem. Piemēram, kad zvana it kā banku darbinieki vai cilvēki, kas informē par kriptovalūtas kontiem, jāsaprot, ka neviens bankas darbinieks nerunās krievu valodā. Tāpat pa telefonu neprasīs nosaukt datus. Par to regulāri sabiedrība tiek brīdināta un informēta. Diemžēl cilvēki īsti to neievēro.

Nepavisam nav tā, ka šādā veidā tiek apkrāpti seniori, kā sākotnēji varētu šķist. Vecāka gadagājuma cilvēki patiesībā ir daudz piesardzīgāki. Tāpat ne visiem ir internetbanka, līdz ar to viņi nemaz nevar veikt šādas opcijas, apstiprinājumus ar *Smart ID*. Apkrāpto cilvēku kategorija lielākoties ir darbspējīgi, izglītoti cilvēki. Analizējot krāpšanas gadījumus, agrāk izteikti varēja manīt tendenci, kad apkrāpti tika nabadzīgi cilvēki, bezpajumtnieki, alkoholiķi, bezdarbnieki, bet šobrīd tie ir sociāli aktīvi, strādājoši cilvēki ar ienākumiem. Šī grupa ir ļoti plaša.

Pat, ja ir tikai aizdomas par krāpšanas mēģinājumu, ir jāvērsas policijā. Tā tiek iegūts vairāk informācijas par krāpniekiem, viņu shēmām. Katrs gadījums tiek izskatīts individuāli. Iespējas, kā informēt policiju, ir dažādas. Var rakstīt iesniegumu *latvija.lv*, zvanīt un informēt uz dežurdaļas tālruņa numuru. Iesniegumā jāapraksta situācija pēc iespējas plašāk. ■

EKSPERTA VIEDOKLIS

Krāpnieki kļuvuši aktīvāki

ARMĪNS PALMS, CERT.LV kiberdrošības eksperts:

— Kopš pandēmijas sākuma, kad vairums iedzīvotāju pārorientējās uz attālināto darbu, gan arī citu uzdevumu veikšanai sāka aktīvāk izmantot internetu (iepirkšanās, mācības, saziņa, izklaide), aktīvāki kļuva arī krāpnieki. Uzbrukumiem krāpnieki izmanto plašu arsenālu, sākot ar krāpniecisku e-pastu, kur uzdodas par banku vai e-pasta pakalpojumu sniedzēju, līdz telefona zvaniem, kuros tiek viltota zvanītāja identitāte (numurs) un zvanītāji izliekas par tiesībsargājošās vai finanšu iestādes pārstāvjiem, draud ar apjomīgiem finansiāliem zaudējumiem un sodiem.

Lai sevi pasargātu no krāpniecības, ņēmu vērā vairākas lietas.

1. Ja esat uzrunāts e-pastā vai telefonsarunā un jūtat, ka tiekat steidzināts un uz jums tiek izdarīts spiediens — tiek norādīts, ka jārīkojas nekavējoties vai rīcībai ir ļoti maz laika (piemēram, 48 stundas), tiek draudēts, ka pazaudēsit visu savu naudu vai jums tiks piespriests sods, ja nerīkosities, — tā ir pazīme, ka jūs, visticamāk, mēģina apkrāpt. Pārtrauciet sarunu, neatbildiet uz e-pastu, ja jūs māc šaubas, sazinieties paši ar savu banku, piezvanot uz bankas mājaslapā norādīto telefona numuru, un pārliecinieties, ka ar jūsu kontu nav notikušas nevēlamas darbības, kā arī informējiet banku par krāpniecības mēģinājumu.

2. Ja kaut kas izskatās pārāk labi, lai būtu patiesi, tad tā tas, visticamāk, arī ir. Ja kādā interneta veikalā iespējams nopirkt zīmolu preces par cenu, kas ir būtiski zemāka nekā visur citur, tas ir signāls par krāpniecības mēģinājumu. Ja saņemat paziņojumu, ka esat laimējis loteriją, kaut arī neesat nopircis loterijas biļeti — atkal jau krāpniecība.

3. Ja tiekat aicināts pieslēgties savai bankai, sociālā tīkla profilam, e-pasta kontam, lai steidzami novērstu kādu problēmu, pirms sava lietotājvārda un paroles ievadīšanas saņemtajā vietnē pārliecinieties, vai šī vietne ir tā, par kuru uzdodas. Pārbaudiet vietnes adresi (adrese redzama adrešu laukā interneta pārlūka augšā un parasti sākas ar *https://…*), kurā esat aicināts ievadīt savus datus, vai adresei ir jelkāda saistība ar reālo vietni (piemēram, vai *banka.lv* vietā nav *baranka.lv*), adresē netrūkst kāda burta vai kāds nav lieks.

4. Atcerieties, ka ne bankas, ne tiesībsargājošās iestādes nekad jūs neaicinās atklāt personīgu informāciju vai bankas piekļuves datus. Tāpat arī jāatceras, ka maksājumu saņemšanai nav nepieciešams atklāt maksājumu kartes CVV kodu (trīs cipari kartes aizmugurē); šis kods nepieciešams tikai pirkumu izdarīšanai.

5. Katram kontam (sociālajos tīklos, e-pastam, interneta veikaliem u. c.) jāizmanto unikāla parole, lai gadījumā, ja uzbrucēji uzzina viena konta paroli, tie nevar ar to pašu paroli piekļūt arī citiem kontiem.

6. Papildu aizsardzībai katram kontam, kur tas vien ir iespējams, uzstādiet arī vairāku faktoru autentifikāciju. Tas nozīmē, ka gadījumos, kad uzbrucējam tomēr būs izdevies iegūt jūsu paroli, uzbrucēja piekļuve jūsu kontam būs apgrūtināta, jo tiks prasīts arī otrais faktors, piemēram, īsziņā atsūtīts vai īpašas lietotnes ģenerēts vienreizējs kods.

7. Ja tiek uzsākta romantiska sarakste un saruna biedrs lūdz materiālu palīdzību, vai tiekat uzrunāti ar izdevīgu investīciju piedāvājumu, vai pirms jebkuras citas darbības, kas no jums prasa materiālas vai juridiskas saistības, izstāstiet par notiekošo kādai uzticības personai — labākajam draugam, radiniekam, kolēģim — un palūdziet viņa viedokli. Tas palīdzēs uz situāciju palūkoties no malas un laikus atklāt krāpniecību.

Ja tomēr ir noticis tā, ka savus datus esat ievadījis un no jums ir izkrāpts maksājums, aicinām vispirms nekavējoties sazināties ar savu banku un pēc tam vērsties ar iesniegumu policijā.

Arī nejauši var kļūt par krāpšanas upuri

Ikvienam no mums liekas, ka nekad nekļūsim par krāpšanas upuri — ar mani tas taču nenotiks. Tā domāja arī Anna (vārds mainīts). Tomēr notika citādāk.

— Lasot un dzirdot par dažādām krāpniecības shēmām, vienmēr biju pārliecināta, ka mani tas neskars. Arī ģimenes un draugu lokā nebiju dzirdējusi, ka kāds būtu ticis apkrāpts. Jau gadiem runā, ka zvana sveši numuri, īpaši ārzemju, vienmēr biju piesardzīga. Tomēr pienāca arī mana reize, kad *uzķēros*, — atzīst Anna.

Viss sākās, kad Anna saņēma īsziņu par it kā kāda piedāvājuma apstiprināšanu.

— Saņēmu ļoti savādu, nesaprotamu īsziņu, kuru ignorēju, to izdzēšot. Nezinu, vai tas ir saistīts, bet pēc tam sekoja trīs zvani. Zvanītājs stādījās priekšā kā *Swedbank* darbinieks. Teksts bija pavisam vienkāršs — ka no mana konta ir veikts aizdomīgs darījums un vai es to apstiprinu. Protams, saruna nebija valsts valodā. Man radās iespaids, ka tur teksts ir ierakstīts, pretī nav īsts cilvēks. Stāstīju latviski, uzdevu jautājumus, tomēr tās atbildes neviesa iespaidu, ka sarunājos ar reālu cilvēku, — atklāj Anna. — Visas trīs sarunas likās pilnīgi vienādas. Pēc tam man sāka zvanīt cilvēki. Protams, nesapratu, kas notiek, jo ikviens zvanītājs man teica, ka es esmu zvanījusi. Sākotnēji domāju, ka, iespējams, kāda vaina ir telefonam, ka tiek veikti zvani, man nezinot. Apskatot izejošo zvanu sarakstu, nekur neparādījās, ka būtu veikti kādi zvani. Sazinājos ar mobilo sakaru operatoru, lūdzu izdrukas, arī tajās neuzrādījās, ka šādiem numuriem es būtu zvanījusi. Telefons zvanīja vienā laidā. Ar daudziem cilvēkiem izdevās parunāties, paskaidrot situāciju, ka nesaprotu, kas notiek. Tomēr kādas sarunas laikā saņēmu arī draudus, ka ir izsekota mana atrašanās vieta, atbraukšot un pārmācīšot mani. Tā nepavisam nebija patīkama sajūta.

Nereti cilvēks tiek apkrāpts tieši telefonsarunas laikā.

Anna, lai vairs neturpinātos šādi zvani un situācijas, nolēma mainīt tālruņa numuru.

— Šobrīd patiesībā ir ļoti grūti izšķirties par tādu soli. Visās iestādēs, visur ir norādīts esošais tālruņa numurs. Doma, ka tas no jauna visur jāmaina, uzdzen bažas. Tāpat arī draugiem un radiem jāpaziņo jaunais numurs. Tas ir laikietilpīgi. Tomēr nolēmu, ka tā būs labāk. Sākotnēji nebiju plānojusi vērsties policijā, jo uzskatīju, ka viņi šādos gadījumos palīdzēt nevar. Tomēr, kad saņēmu draudus, sazinājos ar Madonas iecirkni un lūdzu padomu, kā pareizi rīkoties. Caur *latvija.lv* uzrakstīju iesniegumu, sīki un smalki aprakstot situāciju. Ieradās inspektors, sarakstījām nepieciešamos dokumentus. Šobrīd jāsaka — ļoti labi, ka neradās materiālie zaudējumi, jo varēja būt visādi un es būtu palikusi ar tukšu bankas kontu, — uzskata Anna. — Atskatoties uz notiekošo, saprotu, ka ir izstrādāta shēma, kad atbildot tiek nozagts mans tālruņa numurs un automātiski veikti zvani uz dažādiem reāliem Latvijas numuriem. Situācija gaužām nepatīkama, vairāk emocionāli, jo jāatbild uz šiem zvaniem, jāskaidrojas. Tāpat nezinu, kā šīs shēmas darbojas, ko ar šādu rīcību krāpnieki vēlas panākt. Aizdomājos, iespējams, šādā veidā tiek izkrāpti naudas līdzekļi no cilvēkiem, kuriem es it kā esmu zvanījusi. Šobrīd ir mācība ļoti izvērtēt zvanus, uz kuriem atbildēt. Daudziem šādas iespējas nav, jo zvani saistīti ar darbu. Pavisam negribot var kļūt par krāpšanas upuri. Tomēr, ja šādi tiek veiktas mahinācijas ar zvaniem, nav brīnums, ka kādā brīdī varētu pieslēgties arī bankas kontiem. Cilvēkiem jābūt ļoti piesardzīgiem.

VALSTS POLICIJAS VIDZEMES REĢIONA PĀRVALDĒ

Statistikas dati 9 mēnešu periodā

Uzsākti 84 kriminālprocesi, kuros reģistrēti 90 noziedzīgi nodarījumi.

Krāpšana, uzdodoties par bankas darbinieku — kopā 9 notikumi, t. sk. uzsākti 27 kriminālprocesi. Kopējie materiālie zaudējumi — 71 404,08 eiro.

DPD krāpšana — kopā 22 notikumi. Kopējie materiālie zaudējumi — 2784,32 eiro.

***Omniva* krāpšana** — kopā 11 notikumi, t. sk. uzsākti 2 kriminālprocesi. Kopējie materiālie zaudējumi — 2671,33 eiro.

Viltus bankas saites (linki) — kopā 12 notikumi, t. sk. uzsākti 10 kriminālprocesi. Kopējie materiālie zaudējumi — 11 911,69 eiro.

Viltus finanšu brokeri (platformas, kurās iegulda naudu) — kopā 41 notikums, t. sk. uzsākti 26 kriminālprocesi. Kopējie materiālie zaudējumi — 7 529 065,80 eiro un 22 632 USD.

Telefonkrāpniekiem jauna metode

IKT pakalpojumu sniedzējs „Bite" aicina iedzīvotājus būt uzmanīgiem, jo pēdējo nedēļu laikā telefonkrāpnieki masveidā sākuši jaunu krāpšanas metodi, kopējot un izmantojot eksistējošus Latvijas mobilo telefonu numurus. Zvani visbiežāk tiek veikti caur ārvalstu tīklu, dublicējot Latvijas numuru, krāpniekiem uzdodoties par banku darbiniekiem un runājot krievu valodā. Par vēl viltīgāku šo metodi padara tas, ka, atzvanot uz šiem mobilo telefonu numuriem, atbildēs nevis krāpnieki, bet gan reāli cilvēki Latvijā, kuru mobilā telefona numuri diemžēl tiek izmantoti krāpnieciskiem mērķiem.

„Bite" korporatīvo un sabiedrisko attiecību vadītāja **Una Ahuna-Ozola** stāsta: — Būtiski, ka, saņemot zvanu, uzrādās eksistējošs un reālam klientam piederošs Latvijas mobilā telefona numurs ar kodu +371, bet patiesībā krāpnieki šo telefona numuru ir dublicējuši tikai uz zvana laiku, izmantojot IP telefoniju un viltojot to īpašā un sarežģītā šifrēšanas sistēmā. Visbiežāk šādi zvani tiek pārraidīti uz Latviju caur ārvalstu mobilo sakaru tīkliem. Visu šo apstākļu dēļ mobilo sakaru operatoriem ir ļoti sarežģīti bloķēt šādus zvanus.

Šobrīd skaidri novērojams, ka telefonkrāpnieku izmantotās metodes strauji evolucionē. Tāpēc ļoti būtiski preventīvi informēt un izglītot sabiedrību, tā palīdzot cilvēkiem jau pēc pirmajiem aizdomīgiem signāliem būt uzmanīgiem un izvairīties no nokļūšanas krāpnieku nagos.

Šobrīd krāpnieki izmanto aizvien komplicētākas un rafinētākas metodes, shēmās iesaistot jau reālu personu Latvijas mobilo telefonu numurus, saglabājot vienu kopīgu iezīmi — zvans no bankas un saruna krievu valodā. Brīdinot un informējot sabiedrību, mums ir jāpanāk, ka līdz ar šādas sarunas uzsākšanu cilvēki to uztver kā brīdinājumu par to, ka saruna nav ikdienišķa un tās nodoms ir izkrāpt naudu. Jebkurā gadījumā, saņemot šādu zvanu, tas tūlītēji ir jāpārtrauc.

Sākotnēji tie bija neeksistējoši, bet tagad — reālu cilvēku mobilo telefonu numuri. Esam saskārušies ar situācijām, kad, atzvanot uz šādu krāpnieku izmantotu numuru, cilvēks izsaka draudus numura īpašniekam. Aicinām cilvēkus būt ļoti uzmanīgiem, atbildot uz zvaniem, saņemot ziņas no nepazīstamiem telefona numuriem, un noteikti neatklāt zvanītājam personas datus vai bankas pieejas. „Zelta padoms", saņemot zvanu no krāpnieka, ir vienkārši nedarīt neko no viņa pieprasītā un vērsties policijā ar iesniegumu, informējot par radušos situāciju.

Jau šobrīd operatori regulāri sadarbojas ar atbildīgajām iestādēm Latvijā, ārvalstu, starptautiskajiem mobilo sakaru operatoriem, kā arī Valsts policiju.

Izkrāpj naudas līdzekļus

Krāpniecības veidu ir ļoti daudz. Neraugoties uz to, tiem visiem ir viens mērķis — piekļūt bankas kontiem, lai gūtu finansiālos līdzekļus. Kā sevi pasargāt, atbildes sniedz Anrijs Šmits, *Luminor* krāpšanas novēršanas eksperts.

— Šāgada laikā vērojama pastiprināta krāpnieku aktivitāte, un krāpniecības veidi mēdz būt dažādi. Visbiežāk ir sastopami gadījumi, kad krāpnieki uzdodas par bankas darbiniekiem un zvana klientiem ar mērķi izkrāpt internetbankas pieejas vai privātos datus. Krāpnieki visbiežāk sarunājas krievu valodā un zvana no ārvalstu tālruņa numuriem, taču nereti izmanto arī viltus numurus.

Pieaugot iedzīvotāju ieguldījumu aktivitātei, aktivizējušies arī investīciju krāpnieki jeb viltus finanšu brokeri, kas piedāvā cilvēkiem ātru peļņu, investējot līdzekļus neeksistējošās ieguldījumu shēmās.

Luminor novērojumi liecina, ka pandēmija veicinājusi iepirkšanos internetā, līdz ar to ir krasi pieaugušas dažādas ar tirdzniecību saistītas krāpšanas. Visbiežāk tie ir krāpnieciski gadījumi, kur, izmantojot viltus interneta vietni, kas šķietami atgādina zināmus kurjerdienestus, krāpnieki aicina iedzīvotājus sniegt norēķinu karšu u. c. personīgus datus par pirkuma starpniecību internetā.

Pastāv arī viltus interneta veikali, tāpēc pirms iepirkšanās nezināmā veikalā ir ļoti svarīgi pēc iespējas vairāk izpētīt pieejamo informāciju un kritiski izvērtēt, vai veikalam var uzticēties. Lai samazinātu iespējamos riskus, ieteicams izmantot Latvijas interneta veikalus, par kuru autentiskumu ir iespējams vieglāk pārliecināties.

Lai neiekristu krāpnieku lamatās, svarīgākais ir būt piesardzīgam un neatklāt savus personīgos datus, tostarp bankas pieejas un *Smart-ID* PIN kodus. Būtiski ir atcerēties, ka banka nekad nezvanīs un nesūtīs klientiem e-pasta vēstules ar lūgumu izpaust klientu privātos datus (konta numuru, *Smart-ID* PIN kodus, maksājumu kartes datus — kartes numuru un CVC kodu, kas atrodas kartes aizmugurē, kartes PIN kodu, internetbankas pieejas paroles u. c.), nelūgs autorizēties internetbankā vai apstiprināt maksājumus.

Ja tomēr ir aizdomas, ka notikusi krāpšana, nauda ir pārskaitīta krāpniekam vai maksājumu kartes, internetbankas dati ir nopludināti, pēc iespējas ātrāk par to jāziņo bankai un policijai.

Jaunas shēmas krāpšanā

Bieži nākas saskarties ar situācijām, kad dažādu uzņēmumu vārdā uzdarbojas krāpnieki, kuri šādā veidā mēģina izkrāpt iedzīvotāju norēķinu karšu datus. Krāpnieki uzrunā iedzīvotājus, kas dažādās interneta tirdzniecības platformās ir izvietojuši preces pārdošanai, ar mērķi it kā iegādāties konkrēto preci, izmantojot kurjera pakalpojumus. Šādās krāpšanas shēmās nereti tiek izmantots uzņēmums „DPD Latvija".

„DPD Latvija" pārdošanas un mārketinga vadītāja **Dita Mirbaha** skaidro: — Krāpnieki darbojas pēc shēmas, kad iedzīvotājiem tiek nosūtīta viltus interneta vietnes saite, kas vizuāli šķietami atgādina „DPD Latvija" mājaslapu, aicinot iedzīvotājus ievadīt norēķinu kartes datus, lai saņemtu apmaksu par preci attālināti. Tādējādi krāpniekiem ir iespēja piekļūt personu norēķinu karšu datiem un finanšu līdzekļiem. Krāpnieki ļoti drosmīgi turpina darboties jau mēnešiem ilgi. Diemžēl neviens nevar viņus apturēt.

Krāpnieki visaktīvāk uzdarbojas *ss.com* portālā, bet pēdējos mēnešus izmanto pirkt un pārdot grupas *facebook.com*. Komunikācija primāri norit caur *WhatsApp* kanālu, izveidojot profilu ļoti uzticamu. Uzticamību rada fakts, ka tiek izmantoti arī numuri ar Latvijas valsts kodu +371. Tomēr krāpniecību ir viegli atpazīt, jo šīs personas saziņai izmanto tulkošanas programmas. Līdz ar to teikumi ir gramatiski nepareizi.

Jāvērš uzmanība, ka šie krāpnieki neņem vērā summas, par kādām prece tiek tirgota. Summas var būt arī 5 eiro, jo viņu galvenais mērķis ir iegūt norēķinu kartes datus, bankas kontus.

Iedzīvotājiem jāņem vērā, ka „DPD Latvija" nenodrošina attālinātu pirkuma starpniecības pakalpojumu interneta vidē, kā arī aicina drošības nolūkos vienmēr pārbaudīt interneta vietnes adresi, kas tiek atvērta. Konkrētajā krāpniecības shēmā tiek izmantotas vairākas viltus adreses, piemēram, *lv-expresssafe.xyz*, *lvdpd-safe.xyz*, kurām nav nekādas saistības ar „DPD Latvija".

Dzīvē situācijas ir dažādas, nereti cilvēki uzķeras uz šīm shēmām. Ja ir nodoti bankas konta numuri un savi dati, nekavējoties ir jāblokē konts. Jāziņo arī Valsts policijai. Pat gadījumos, kad ir tikai saņemts šāds paziņojums.

Savukārt, ja iedzīvotājus māc šaubas, vienmēr var sazināties ar „DPD Latvija".

Atvērumu sagatavoja AGRITA NUSBAUMA-KOVAĻEVSKA
Izmantoti AGRA VECKALNIŅA foto

Vides aizsardzības un reģionālās attīstības ministrija

MAF Mediju atbalsta fonds

Projektu finansē Mediju atbalsta fonds no Latvijas valsts budžeta līdzekļiem