Swedbank

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 kļuvušas 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 bloķētu 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.

Uzņēmumi mēdz saņemt viltotus sadarbības partneru e-pastus!

Krāpnieki mēdz izmantot viltotus e-pastus, kas it kā tiek sūtīti no sadarbības partneriem vai nu lai izvilinātu informāciju (nospiežot uz e-pastā iekļautām interneta vietnēm), vai nu lai izkrāptu naudu caur viltotiem rēķiniem. Uzņēmumi arī mēdz saņemt e-pastus it kā darbinieka vārdā par jauno norēķina konta numuru uz kuru jāveic algas pārskaitījums.

Pievērs uzmanību no kāda e-pasta sūtīta vēstule. Tāpat kā pārbaudi kāda adrese slēpjas zem tekstā iekļautajām interneta vietnēm. Nekādā gadījumā neļauj instalēt programmatūru no šādām vietnēm un neievadi tajās personīgos datus.

Personīgo datu piesaukšana nav pamats uzticēties!

Steidzināšana, jūsu datu piesaukšana un apvārdošana ir krāpnieku stiprā puse. Krāpnieks no internetā pieejamās vai noziedzīgā ceļā 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.

Aizdomīga komunikācija no uzņēmuma vadītāja!

Krāpnieki mēdz sūtīt viltotus e-pastus, izliekoties par uzņēmuma vadītāju vai kādu citu vadības komandas locekli, aicinot veikt pārskaitījumus vai izpaust informāciju. Šobrīd jau aicinām arī uzņēmumus būt uzmanīgus, ņemot vērā tehnoloģiju attīstību – krāpnieki var arī pārveidot balsi vai pat attēlu video zvana laikā.

Ja tiek saņemts netipisks vadītāja lūgums vai arī tas paredz naudas pārskaitījumus vai konfidenciālas informācijas izpaušanu, labāk lieku reizi pārliecinieties, ka vadītājs tiešām šādu e-pastu sūtījis. Pievērsiet uzmanību arī sūtītāja e-pasta pareizrakstībai un lietotās valodas stilam/gramatikai.

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 mērķi 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.

Izspiešanas draudi!

Krāpnieki mēdz iebiedēt ar datu noplūdi, liekot darbiniekam pieņemt neracionālus lēmumus. Iebiedējot, ka nepubliskojama informācija tiks nopludināta cenšas izspiest naudu vai pierunāt uzstādīt krāpnieku programmatūru. Šādā veidā krāpnieki tik tiešām iegūst pieeju datiem, kurus nošifrē vai padara nepieejamus, pieprasot par to atbloķēšanu samaksu.

Neļaujies iebiedēšanai, pat, ja draudi šķiet īsti, pārbaudi to patiesumu. Ja krāpnieki imitē kādu kolēģi, nekautrējies sazināties ar šo kolēģi un noskaidrot patiesību. Tāpat informē drošības kolēģus (ja uzņēmumā tādi ir)

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 šķiet aizdomīgs, izdzēsiet to un ziņojiet par krāpšanas mēģinājumu. Izvairieties atvērt aizdomīgus pielikumus - pat antivīrusa programmas bieži vien nespēj identificēt uzbrukumus.

Daži ieteikumi:

- Nesteidzies, pārliecinies par minēto faktu patiesumu
- Saņemtiem rēķiniem pārbaudi rekvizītus, krāpnieki mēdz izmantot reālus rekvizītus, kuros ievada savu bankas konta numuru
- Never vaļa interneta vietnes, kuras prasa ievadīt datus vai uzstādīt programmatūras
- Starptautiski piedāvājumi e-pastā parasti ir krāpšanas mēģinājums
- Neizmanto pirātiskas programmatūras, tās bieži vien kalpo par pamatu šantāžai un izspiešanai
- Nosakiet sava uzņēmuma saimnieciskajai darbībai atbilstošus dienas un mēneša pārskaitījumu limitus