2025. gada 14. novembrī

Avots: Citadele

Neuzmanība izmaksā dārgi. Krāpnieki izmanto uzņēmumu digitālo ievainojamību

Finanšu krāpniecības metodes bieži mainās sezonāli – noteiktos periodos atsevišķas krāpnieku shēmas kļūst īpaši aktīvas. Bankas Citadeles dati liecina, ka uzņēmumu krāpšanas gadījumos visbiežāk sastopama telefonkrāpniecība, taču arvien biežāk noziedznieki izmanto arī e-pastus un citus digitālos kanālus, kas ļauj nemanāmi piekļūt sarakstei un piesavināties naudas līdzekļus.

„Bankas Citadele dati rāda, ka fiksēto krāpšanas gadījumu skaits kopumā ir samazinājies, savukārt to kopējā summa — nedaudz pieaugusi. Ja runājam par krāpšanu uzņēmumu pusē, īpaši satraucoši ir gadījumi, kuros noziedznieki pārtver uzņēmumu saraksti ar kolēģiem vai sadarbības partneriem un nomaina kontu rekvizītus, radot būtiskus finanšu zaudējumus," skaidro Citadeles Krāpšanas novēršanas daļas vadītāja **Līga Everte**.

Finanšu krāpšanu uzņēmumos bieži ir grūti pamanīt – noziedznieki iesaistās reālā uzņēmumu sarakstē. Parasti krāpnieki sāk ar piekļuves iegūšanu uzņēmuma vai tā partnera e-pastam, izmantojot vājas paroles un to atkārtotu izmantošanu. Kad pienāk krāpšanai piemērots brīdis, piemēram, notiek aktīva rēķinu apmaksas veikšana – krāpnieki nemanāmi iejaucas sarakstē, atbildot partnera vārdā vai nosūtot identisku rēķinu ar nomainītiem rekvizītiem. Tā kā ziņojumi izskatās autentiski un nāk no ierasta e-pasta, darbinieki bieži nepamana izmaiņas un pārskaita līdzekļus uz noziedznieku kontiem. Dažos gadījumos krāpnieki pat turpina saraksti vairākas dienas, lai radītu iespaidu, ka viss ir kārtībā, un tikai pēc tam pazūd.

Cilvēka modrība — izšķirošs faktors

Pieaugot kiberdraudu mērogam, uzņēmumi arvien vairāk iegulda drošības risinājumos, tomēr pat modernākās tehnoloģijas nespēj pilnībā aizsargāt no cilvēciskas neuzmanības. Krāpnieki arvien biežāk mērķē nevis uz sistēmām, bet uz cilvēkiem – mēģinot

izprovocēt steidzīgus lēmumus vai izmantot kolēģu un partneru uzticību.

„Tehniskie drošības pasākumi ir nepieciešami, taču ar tiem vien nepietiek. Gadījumi visbiežāk notiek cilvēku neuzmanības dēļ – kad e-pasti netiek rūpīgi pārbaudīti vai steigā tiek pieņemti lēmumi. Drošība ilgtermiņā nav tikai tehnoloģiju jautājums – tā balstās uz darbinieku izpratni par riskiem un finanšu drošību, ko stiprina regulāra darbinieku izglītošana un risku apzināšanās kultūras veicināšana," uzsver **L. Everte**.

Lai mazinātu riskus, eksperte iesaka ieviest skaidras iekšējās procedūras un regulāri izglītot darbiniekus:

- Vienmēr rūpīgi pārbaudīt e-pastos saņemto rēķinu rekvizītus;
- Izmantot dubulto maksājumu apstiprināšanu, īpaši lieliem maksājumiem, un ieviest automātiskus brīdinājumus, ja maksājums tiek veikts jaunam saņēmējam;
- Ieviest daudzfaktoru autentifikāciju pieslēgšanās brīžos e-pastam, internetbankai un citām būtiskām sistēmām;
- Pievērst uzmanību, vai norādītie konta dati atbilst saņēmēja vārdam un uzņēmuma nosaukumam;
- Nedalīties ar piekļuves datiem, nespiest uz aizdomīgām saitēm un vienmēr izmantot manuāli ievadītas internetbankas adreses;
- Regulāri rīkot darbinieku apmācības un kiberuzbrukumu simulācijas, lai laicīgi spētu atpazīt potenciālos riskus.

Par Citadeles Grupu

Citadele ir vienīgā Baltijas valstu banka, kuras mātes uzņēmums atrodas Latvijā, nodrošinot proporcionāli lielāku ieguldījumu Latvijas ekonomikā. Meitasuzņēmumi un filiāles darbojas Latvijā, Lietuvā un Igaunijā.

Citadeles misija ir modernizēt finanšu nozari, līdztekus klasiskajiem bankas pakalpojumiem piedāvājot virkni jaunākās paaudzes

finanšu tehnoloģijās bāzētu pakalpojumu gan privātpersonām, gan uzņēmējiem visā Baltijā. 2025. gada pirmajos deviņos mēnešos Citadele jaunos aizdevumos izsniedza 1,2 miljardus eiro, kopējam kredītportfelim sasniedzot 3,67 miljardus eiro un depozītu apjomam pieaugot līdz 4,1 miljardam eiro.