

„Luminor“ bankas perspėja klientus: sukčiai ragina patvirtinti mokėjimo operacijas, kurių nebuvo

Paskutinį 2021 m. sausio savaitgalį dalis „Luminor“ banko klientų, turinčių mokėjimo korteles, gavo Smart-ID arba mobiliojo parašo pranešimus, siūlančius patvirtinti mokėjimo operacijas, nors tokių neinicijavo. Bankas informuoja, jog tai buvo sukčiavimo ataka, nukreipta prieš mokėjimo kortelių turėtojus.

Nors sukčiavimui elektroninėje erdvėje valdyti bankas „Luminor“ naudoja daugiapakopės saugumo sistemas, leidžiančias tiek veikti prevenciškai, tiek valdyti situaciją incidentui įvykus, norime dar kartą atkreipti klientų dėmesį į tai, jog PIN kodus ar slaptažodžius (tiek Smart ID, tiek mobilaus parašo) įvesti reikia tik toms operacijoms, kurias klientas pats inicijuoja, o ne paprašyti bet kuriuo metu.

Greičiausias būdas įsitikinti, ar netapote sukčiavimo auka, yra prisijungimas prie elektroninės bankininkystės ir sąskaitos likučio, atliktų operacijų bei rezervuotų sumų jūsų sąskaitoje patikrinimas. Kuo anksčiau pastebėsite sukčiavimą, tuo lengviau bus jį išaiškinti, todėl rekomenduojame periodiškai tikrinti minėtus duomenis. Jei visgi klientai įtaria, jog kortelės duomenys buvo pavogti, tapo žinomi tretiesiems asmenims, prašome nedelsiant užblokuoti mokėjimo kortelę interneto ar mobiliajame banke, arba susisiekti telefonu su „Luminor“ klientų aptarnavimo centru.

Tais atvejais, kai „Luminor“ banko saugumo sistemos identifikuoja apgaulingą elgesį naudojantis mokėjimo kortele, bankas nedelsdamas informuoja paveiktus klientus. Priklausomai nuo banko kortelės saugumo pažeidimo, bankas konkrečiai nurodo, kokių veiksmų ėmėsi, siekdamas užkirsti kelią galimai nusikalstamai veikai vykdyti (kortelė apribota pilnai, apribota tik internetiniams mokėjimams ir pan.). Taip pat informuojama, kokių veiksmų klientui imtis: įvertinti atliktų operacijų netipiškumą, atsinaujinti mokėjimo kortelę ar kreiptis į banką bendruoju telefonu 1608.

Nepaisant priminimų, pasitaiko ir tokių sukčiavimo atvejų, kuomet klientai, norėdami sutaupyti daugiau pinigų, bando apsipirkti netikrose (nors ir labai įtikinamai atrodančiose) internetinėse parduotuvėse. Norintiems sutaupyti ir nepatekti į sukčių pinkles, bet ketinantiems pirkti internete ypač žemomis kainomis rekomenduojame neskubėti atlikti transakcijos ar įvesti mokėjimo kortelės duomenų. Pirmiausia reikėtų įsitikinti, jog internetinė svetainė ar jos parinktys veikia sklandžiai, nėra gramatinių bei loginių klaidų, svetainėje randate visą jums reikalingą informaciją: pardavėjo duomenis (įskaitant telefono numerį, elektroninio pašto adresą, įmonės pavadinimą, kodą bei buveinės adresą), pristatymo ir prekių grąžinimo sąlygas. Nepamirškite pasitikrinti viešojoje erdvėje atsiliepimų apie įmonę, ir, žinoma, prekės kainą palyginkite su kitais prekę siūlančiais, seniai rinkoje veikiančiais pardavėjais.

„Luminor“ bankas perspėja klientus: sukčiai ragina patvirtinti
mokėjimo operacijas, kurių nebuvo

