

Elektroniniai sukčiai nuolat kuria būdus išvilioti gyventojų pinigus: netikras interneto svetainės, melagingas SMS žinutės bei elektroninius laiškus, kurie imituoja tikrų finansų įstaigų ar institucijų pranešimus. Lietuvos bankų asociacija (LBA) atkreipia dėmesį, kad visą elektroniniais kanalais bei telefonu gaunamą informaciją svarbu kritiškai įvertinti atsakant sau į kelis klausimus.

„Provokacijų, kuriomis siekiama išvilioti asmeninius interneto banko prisijungimo duomenis bei pinigus, mobiliuoju telefonu bei elektroniniu paštu galima sulaukti bet kur ir bet kada. Nepamiršti šito – svarbiausia ir pirmiausia, bet ne vienintelė atsargumo priemonė“, – akcentuoja Mantas Zalatorius, LBA prezidentas.

M. Zalatorius siūlo kiekvienam sulaukusiam įtartino skambučio, žinutės ar paklausimo elektroninėje erdvėje užduoti sau kelis klausimus.

- **Su kuo aš bendrauju?** Griežtai nepasitikėkite gauta informacija, jei ši telefoną ar elektroninio pašto dėžutę pasiekė ne kaip atsakas į jūsų teiktą užklausą, pavyzdžiui, pateiktą oficialiu banko klientų aptarnavimo skyriaus adresu. Jeigu sulaukėte laiško su neįprastu pasiūlymu, prašymu iš nežinomo adresato, būkite ypač atsargūs. O jeigu šis prisistato žinomos įmonės, tarnybos ar kitokios institucijos atstovu, atsiprašę baikite pokalbį bei suradę nurodytos organizacijos reikalingus kontaktus internete, patys pasiskambinkite ir patikslinkite, ar ten dirba toks asmuo ir ar jo aprašytos aplinkybės, dėl kurių esą su jumis buvo susisiektas, yra tikros.
- **Ar mane bandoma paveikti emociškai?** Istorija apie giminaitį, pakliuvusį į bėdą, vadovu prisistatančio asmens reikalavimas pervesti įmonės pinigus, pasikartojantys investuoti kviečiančio „vadybininko“ skambučiai, naujo interneto bičiulio ar bičiulės prašymai padėti susitvarkyti laikinas finansines problemas... Visuose šiuose sukčiavimo scenarijuose pasitelkiamas emocinis spaudimas. Pastebėję jį, kelkite klausimą dėl visos situacijos tikrumo.
- **Ar naudojuosi oficialiu banko adresu?** Lankymasis sukčių sukurtose interneto svetainėse, imituojančiose oficialius finansų paslaugų teikėjų tinklalapius, gali pridaryti bėdų. Į jas viliojama žinutėmis ir laiškais su užuominomis į neva institucijų dokumentus ar dalykines situacijas. Nesinaudokite nuorodomis – patys įrašykite banko ar valstybės institucijos svetainės adresą naršyklėje. Specialistai taip pat rekomenduoja naudotis tik oficialiomis bankų mobiliosiomis programėlėmis – jose integruotas autentiškas el. bankininkystės svetainės adresas.
- **Ar tvirtinu operaciją, kurią noriu atlikti?** Vienas iš populiariausių išmaniųjų įrankių, skirtų prisijungti prie savo interneto banko paskyros – programėlė „Smart-ID“. Atsiskaityti ja yra paprasta ir greitai, tačiau taip pat būtina nepamiršti, kad tai – ne

žaidimas, o prieiga prie jūsų pinigų. Atlikdami mokėjimą, kaskart atidžiai perskaitykite, kokį veiksmą tvirtinate: ekrane parodomas tiek paslaugos pavadinimas, tiek trumpas operacijos aprašymas. Jei nesate tikri, kad jis teisingas, niekada neveskite savo PIN kodo. Taip pat visada patikrinkite, ar telefono ekrane rodomas kontrolinis kodas atitinka kodą, rodomą interneto svetainėje arba bankininkystės lange.

- **Ar pasiūlymas ne per geras, kad būtų tiesa?** Visus itin gerai skambančius pasiūlymus turėtume tikrinti dvigubai. Reklaminiai skydeliai, kviečiantys užsukti į negirdėtas e-parduotuves, siūlančias neva žinomų prekės ženklų gaminius pusvelčiui – vienas iš tokių pavyzdžių. Be to, interneto svetainės dabar labai aktyviai siekia komunikuoti su vartotoju – savo lankytojams siūlo leisti rodyti pranešimus. Tačiau pasitaiko nemažai atvejų, kai svetainės užvaldo ir per jas siųsti pranešimus mėgina sukčiai. Tad naršant internete reikia pasirūpinti antivirusinėmis programomis ir nepamiršti – jeigu pasiūlymas skamba įtartinais gerai, verčiau jį aplenkti.



Get real time update about this post category directly on your device, subscribe now.

[Subscribe](#)