

Pasirodžius incidentams apie naujų būdų apgauti patiklius žmones radusius internetinius sukčius, Finansinių paslaugų įmonių asociacija FINCO dalinasi patarimais kaip apsisaugoti.

Asociacijos vadovo Šarūno Frolenko teigimu, užfiksavę atvejų, kai žmonės patys atidavė savo asmens duomenis internetiniams sukčiams, vartojimo kreditų bendrovės ėmėsi papildomų saugumo priemonių. “Bet ir patys žmonės turi būti itin atsargūs, nes sukčiai atranda vis naujų būdų apgauti” – pabrėžė Š. Frolenko.

Koks Jūsų juridinio asmens kodas?

Gavus viliojantį darbo pasiūlymą arba pasiūlymą investuoti, pirmiausia reikia patikrinti, ar tokia įmonė apskritai egzistuoja. Internetiniai sukčiai, gavę tokį klausimą, greičiausiai nurodys kokią nors įmonę, kuri su jų siūlomomis “paslaugomis” neturi nieko bendro. Taigi, gavę atsakymą pasakykite, kad pasižiūrėsite informaciją internete ir jiems perskambinsite.

Jei nurodyta įmonė tikrai egzistuoja, susiradę jos kontaktus tokiuose puslapiuose kaip rekvizitai.lt, paskambinkite ir pasiteiraukite, ar tikrai jie Jums skambino. Greičiausiai įmonė, su kuria susisieksite, neturės jokio supratimo, apie ką kalbate – tuomet paskambinkite telefonu 112 ir užfiksukite įvykį policijoje.

Nesidiegti įtartinų programėlių

Asmens duomenų vagys neretai ant jų kabliuko užkibusių prašo įsidiegti programėles, kurios jiems leidžia stebėti viską, ką savo telefone arba kompiuteryje daro įsidiegęs asmuo. Paprastai jokios verslo įmonės taip nedaro, todėl išgirdus prašymą įsidiegti tokias programėles kaip “TeamViewer” reiktų sunerinti ir paklausti prašančių, kam to reikia.

Netvirtinti jokių operacijų mobiliuoju parašu

Vartojimo kreditų sutartis apgautų žmonių vardu sudarinėjantys sukčiai neretai prašo patvirtinti įvairias operacijas nuotoliniu būdu.

Asociacija FINCO įspėja nenaudoti savo mobiliojo parašo ar kitų programėlių (“Smart ID”), kai to esate prašomi nepažįstamų žmonių. Gali būti, kad prašydami “ką nors patvirtinti mobiliuoju parašu” sukčiai arba sudarinėja paskolų sutartis už Jus, arba, jau žinodami Jūsų banko prisijungimus, daro pinigų pervedimo operacijas iš Jūsų banko sąskaitos.

Nemokamų pietų nebūna

Neretai žmonės praranda savisaugos jausmą tada, kai pasiūlymas jiems pasirodo pernelyg geras, kad nebūtų verta surizikuoti.

“Mūsų duomenimis, žmonės susivilioja, pavyzdžiui, apgavikų paskelbtu itin pelningu darbo pasiūlymu ir galvoja – kodėl nesumokėjus tų kelių šimtų eurų už mokymus, kurie padės man gauti darbo vietą” – sakė FINCO vadovas Š. Frolenko.

Asociacijos atstovas pabrėžia, kad jokie patikimi darbdaviai neprašo žmonių dalyvauti brangiuose mokymuose tam, kad suteiktų darbo vietą.

Naujausi apgaulės būdai

Asociacijos FINCO turimais duomenimis, tarp naujausių sukčių pasitelkiamų būdų išgauti žmonių asmens duomenis – fiktyvių investicijų ar investavimo paslaugų siūlymai, taip pat – fiktyvios įdarbinimo paslaugos.

Dalis sukčių žmonėms siūlo investuoti pinigus į akcijų biržą per investicijų paslaugas nelegaliai siūlančios bendrovės „Vet-trade“ puslapį. Galimybę susivilioję žmonės telefoninio pokalbio metu atlieka visus sukčių prašomus veiksmus – atsisiunčia programėles (pavyzdžiui, „TeamViewer“), patvirtina savo tapatybę mobiliojo parašo pagalba, suveda savo asmens duomenis, prisijungia prie elektroninės bankininkystės paskyrų ir net pateikia savo asmens dokumentų kopijas.

“Visus šiuos duomenis gavę sukčiai sudaro paskolos sutartis, o to nesuprasdami žmonės į savo asmenines sąskaitas iš vartojimo kreditų bendrovių gautus pinigus vėliau dar ir perveda į sukčių sąskaitas”, – sakė asociacijos FINCO vadovas.

Kiti sukčiai, asociacijos duomenimis, darbo skelbimų portaluose skelbė fiktyvius darbo skelbimus, kurių viena sąlygų – prieš įsidarbinant dalyvauti mokymuose, už kuriuos prašydavo susimokėti. “Vėlgi, darbo pasiūlymais susivilioję žmonės sukčiams pervesdavo ne tik pinigus už taip ir neįvykusius mokymus, bet dar ir pateikdavo savo asmens duomenis bei dokumentus”, – pabrėžė Š. Frolenko.

FINCO asociacijos teigimu, vieni iš jų narių jau kreipėsi į Lietuvos banką dėl puslapių, kurių pagalba buvo vykdoma apgaulė, blokavimo. „Lietuvos bankas turi galimybę inicijuoti neteisėtų puslapių blokavimą, tačiau kol kas minėtas puslapis užblokuotas nėra“, – sakė asociacijos FINCO vadovas.

