

„Swedbank“: per dieną gyventojai praneša apie 400 sukčių atakų

Sukčiai nesiruošia vasaros atostogų ir nemažina atakų prieš gyventojus apsuks. „Swedbank“ duomenimis, per vieną dieną banko klientų konsultacijų centras gauna iki 400 gyventojų skambučių ir pranešimų apie sukčių bandymus išvilioti asmeninius interneto bankininkystės, mokėjimo kortelių duomenis ir reikalavimus patvirtinti mokėjimus, kurių gyventojai patys neinicijavo.

„Pastaraisiais mėnesiais sukčiai nesiliauja atakavę gyventojų klasikiniu būdu – pasitelkdami sukčiavimą telefonu. Šalies gyventojai sulaukia sukčių skambučių, kuomet skambinantys asmenys prisistato banko darbuotojais ir informuoja apie neva neteisėtas operacijas sąskaitoje, bandymą atlikti pavedimą iš kliento sąskaitos ar neva užpildytą paskolos paraišką“, – sako Žygeda Augonė, „Swedbank“ informacinės saugos vadovė.

Pasak jos, išskirtinis pastarojo meto telefoninių sukčių bruožas – jie dažniausiai į gyventojus iš karto kreipiasi ir bendrauja tik rusų kalba, nes absoliučia dauguma atvejų skambinama ne iš Lietuvos, tam pasitelkiamos įvairios nuotolinio bendravimo programėlės, pavyzdžiui, „Viber“.

„Sukčiai į gyventojus dažnai kreipiasi vardu, pasako daugiau asmeninių detalių, o pokalbio metu sumaniai išgavę kitą informaciją, sukčiai sudaro išpūdį, kad asmens duomenis gavo iš banko. Tačiau pokalbiui sukčiai būna pasiruošę iš anksto, o duomenis susirenka iš kitų šaltinių, įskaitant pačių gyventojų socialinių tinklų paskyras“, – teigia saugumo ekspertė. Pastebima tendencija, jog dėl sukčių nuostolių patyrusių gyventojų geografija apima tokius miestus, kaip Klaipėda, Vilnius, Visaginas, kuriuose gyvena nemaža dalis rusakalbių gyventojų.

„Paskambinus telefonu pirminis sukčių tikslas yra sukelti įtarimus, neva iškilo reali grėsmė prarasti pinigus arba susilaukti teisėtvarkos pareigūnų dėmesio dėl sąskaitoje atliekamų neteisėtų veiksmų. Jei gyventojai tuo patiki, sukčiai žengia antrą žingsnį – prisistatydami banko saugumo ekspertais jie pažada pagalbą ir siūlo išspręsti kilusias problemas“, – komentuoja Ž. Augonė.

Kaip pabrėžia saugumo ekspertė, tam sukčiai prašo suteikti savo asmeninius prisijungimo prie interneto bankininkystės ir/ar kortelių duomenis bei kliento autentifikacijai ar mokėjimo atšaukimui prašo patvirtinimo suvedant Smart-ID, mobiliojo parašo ar PIN generatoriaus kodus.

„Asmeninių duomenų atskleidimas yra kritinis momentas, nes tai atlikus iškyla reali grėsmė prarasti savo lėšas ir patirti finansinių nuostolių. Todėl gavus bet kokią prašymą iš kitų asmenų atskleisti duomenis ar patvirtinti mokėjimą, kai klientas pats nevykdo atsiskaitymo operacijos, būtina jį įvertinti kritiškai ir jokių būdu neskubėti atlikti tokių veiksmų“, – sako „Swedbank“ atstovė.

Ž. Augonė primena pagrindinį sukčių atpažinimo būdą – banko darbuotojai niekuomet patys neskambina gyventojams prašydami atskleisti prisijungimo duomenų, slaptažodžių, PIN kodų ar kitos slaptos informacijos. Svarbu žinoti, kad bankui nereikia klientų sutikimo tam,

„Swedbank“: per dieną gyventojai praneša apie 400 sukčių atakų

kad būtų atšaukta ar sustabdyta mokėjimo operacija.

„Saugokite savo prisijungimo priemones: kodus išiminkite, o ne užsirašykite, niekam jų neatskleiskite, apsaugokite savo išmaniuosius įrenginius ekrano užraktu ir niekuomet neskubėkite suvesti turimos tapatybės patvirtinimo priemonės duomenų bei perskaitykite įdėmiai, kam duodate sutikimą. Jei praradote prisijungimo priemonę ar išmanųjį telefoną arba pastebėjote įtartinas operacijas savo banko sąskaitoje, nedelsdami praneškite apie tai savo bankui“, – pabrėžia „Swedbank“ informacinės saugos vadovė Ž. Augonė.

