Antrą metų ketvirtį sukčiai taikėsi į 4,2 mln., išviliojo 2,5 mln. eurų

Finansiniai sukčiai iš Lietuvos gyventojų ir įmonių per antrąjį šių metų ketvirtį taikėsi išvilioti apie 4,2 mln. eurų, rodo Lietuvos bankų asociacijos (LBA) duomenys. Palyginti su tuo pačiu laikotarpiu pernai, sukčių padaryti nuostoliai buvo apie 1,4 mln. eurų mažesni. Per šių metų balandžio – birželio mėnesius nusikaltėlių padaryti nuostoliai siekė apie 2,5 mln. eurų, o finansų įstaigose sustabdytų bei iš sukčių sėkmingai atgautų lėšų suma sudarė apie 1,9 mln. eurų.

LBA reguliariai atnaujinama statistika rodo, kad šių metų antrąjį ketvirtį dar bankų sąskaitose sustabdytų ir į sukčių rankas nepatekusių lėšų suma sudarė net 1,7 mln. eurų. Apie 200 tūkst. eurų per šį laikotarpį pavyko atgauti iš nusikaltėlių.

Tačiau sukčių atakų mastas toliau auga – fiksuojama vis daugiau sukčiams sėkmingų incidentų. Iš viso per šių metų balandį – birželį finansų įstaigose užfiksuoti 2951 sukčiavimo atvejai, kai nusikaltėliams pavyko išvilioti gyventojų ar įmonių pinigus, tuo pat metu pernai jų įvykdyta 2454.

„Nors sukčiavimo atvejų nemažėja, viena po kitos ritasi naujos sukčiavimo bangos išnaudojant naujus metodus ir technikas, stebime tendencijas, kad rezultatus duoda finansų įstaigų ir kitų institucijų taikomos priemonės, siekiant apriboti sukčiavimo galimybes. Tad raginame gyventojus ir atostogų metu neatsipalaiduoti bei sukčiams neatiduoti savo prisijungimo duomenų“, – sako LBA prezidentė dr. Eivilė Čipkutė.

Vidutinė išviliota suma mažėjo

Lyginant šių metų antrąjį ketvirtį su atitinkamu laikotarpiu pernai, bendras sukčiavimo atvejų skaičius padidėjo nuo 2454 iki 2951, tačiau reikšmingai mažėjo vidutinė išviliota suma. Praėjusių metų balandį-birželį ji sudarė 1588 eurus, analogišku laikotarpiu šiemet – 856 eurus.

Populiariausias sukčių naudojamas apgaulės metodas ir toliau išlieka „fišingas“ (angl. phishing), kai gyventojams siunčiama suklastota SMS žinutė ar elektroninis laiškas, apgaulės būdu siekiant išvilioti asmens duomenis ir šitaip pavogti pinigus iš sąskaitos. Šių metų antrą ketvirtį užfiksuoti 1698 „fišingo“ atvejai, tuo pat metu pernai jų įvykdyta 1533.

„Sukčių taikomi metodai išlieka panašūs, tačiau jiems įgyvendinti nusikaltėliai naudoja vis išradingesnes technikas. Piktavaliai nuolat seka besikeičiančius gyventojų įpročius internete, atakas pritaiko pagal aktualijas, sezoniškumą, išbando naujas technologijas. Vienu metu išbandoma daugybė technikų, o atradę tą, kuri suveikė, nusikaltėliai ją pritaiko didesniam žmonių skaičiui. Todėl kiekvieną žmogaus žingsnį skaitmeninėje erdvėje privalo

lydėti atidumas ir kritinis mąstymas“, – teigia E. Čipkutė.

Per antrąjį 2023 metų ketvirtį taip pat dvigubai padaugėjo investicinio sukčiavimo – tokių atvejų fiksuota 440, palyginti su 204 atvejais atitinkamu laikotarpiu pernai. Tokių atakų metu sukčiai gyventojams siūlo investuoti į patrauklią grąžą generuojančius investicinius produktus. Specialistai nuolat primena – stebuklingų būdų greitai užsidirbti nėra, jei kažkas skamba pernelyg gerai – tai pirmas ženklas, kad galėjote tapti nusikaltėlių taikiniu.

Būtina atidžiai tvirtinti operacijas

Vertinamu laikotarpiu finansų įstaigoms pavyko iš sukčių atgauti apie 200 tūkst. eurų. Apie 1,7 mln. eurų buvo sustabdyti dar finansų įstaigose įtarus, kad lėšos galėjo tapti sukčių taikiniu.

Deja, ne visada teisėsauga ar bankas gali padėti išsigelbėti nuo neapdairaus elgesio. Bankai negali atšaukti ar pakeisti operacijų, kurios buvo inicijuotos mokėjimo kortelės duomenimis ir patvirtintos tik sąskaitos savininkui žinomais duomenimis.

Mokėjimo operacijų tvirtinimui naudojamos kvalifikuotos priemonės – „Smart-ID“, mobilus parašas – prilygsta rašytiniam parašui. Tvirtindami mokėjimo operacijas gyventojai pasirašo oficialų dokumentą, kurio pagal kai kurių mokėjimo kortelių paslaugų teikėjų taisykles atšaukti praktiškai neįmanoma.

Saugumo ekspertai primena, kad bankai, valstybės institucijos klientams nesiunčia žinučių su aktyviomis nuorodomis į e. bankininkystės skiltį ar sutrumpintų nuorodų, taip pat ragina įsidėmėti savo finansinių paslaugų teikėjo oficialios interneto svetainės adresą ir visada patikrinti naršyklėje, ar tikrai jungiamasi prie jos. Naudojantis „Smart-ID“ ar mobiliuoju parašu, kaskart reikia įsitikinti, kokią operaciją tvirtinate savo PIN kodais.