

Jei savo istorija apsaugojau bent vieną žmogų – tai buvo verta paviešinti, nors ir nukentėjo mano EGO – sako nuo sukčių nukentėjusi Asta

„Mane išdūrė. Praradau palyginus nedaug, internetiniai sukčiai išviliojo 184 Eur“, taip savo pasakojimą pradeda verslininkė Asta. Moteris pripažįsta, kad ilgai teko dvejoti dėl istorijos viešinimo, kadangi reakcijų galima sulaukti įvairių, vieni pagiria, kad žmogus išdrįsta dalintis patirtimi, ir galbūt sužinojus apie sukčių naudojamas technikas ir būdus, kitiems žmonėms pavyks išvengti panašių sukčiavimo atvejų. Tačiau juk yra dalis ir tokių, kurie pikdžiugiškai pasijuokia bei pagalvoja „na, kaipgi galima taip žioplai pasielgti, aš tai niekada taip nepakliūčiau...“.

Pastaruoju metu įvairiuose interneto portaluose dažnai matome straipsnių su didelėmis antraštėmis „Siautėja internetiniai sukčiai! Būkite atsargūs“, „Tūkstančių eurų netekęs vyras perspėja: taip gali nutikti kiekvienam iš mūsų“ ir pan. Antraštes perskaitome ir galbūt atidarome publikaciją detaliau peržiūrėti, jeigu antraštėje yra geras kabliukas, arba norime sužinoti daugiau pikantiškų aplinkybių, ar kiek auka prarado pinigų. Dauguma iš mūsų žinome apie sukčių naudojamas taktikas, suprantame, kad negalima spausti nežinomų nuorodų iš nežinomų siuntėjų, reikia ignoruoti įtartinas SMS žinutes, nepasiduoti sukčiavimui telefonu, tačiau **internetinių sukčių aukų ne tik nemažėja, bet ir pastebima tokių sukčiavimo atvejų augimo tendencija.**

Sakoma, kad vienas iš kovos su sukčiais būdų yra žmonių švietimas ir sąmoningumo didinimas. Tačiau turime suvokti, kad prie tos pačios informacijos prieina ir sukčiai, jie sugalvoja vis naujesnių būdų, kaip užmesti masalą ir užkibus aukai stengtis kuo greičiau išvilioti pinigų, asmeninę informaciją, kreditinės kortelės duomenis, užkrėsti aukos įrenginį ir pan. **Nė vienas sukčius nesako tiesiai šviesiai – atiduok pinigus! Jie tai daro subtiliai, panaudoja psichologinį spaudimą, dažniausiai pateikiami nurodymai atlikti tam tikrus veiksmus kuo skubiau, siūlomos įvairios nuolaidos ar kitos naudos.**

Asta nusprendė parduoti panaudotus daiktus gerai žinomoje internetinėje svetainėje

Asta pasakoja, kad vienoje gerai žinomoje internetinėje platformoje nusprendė parduoti kelis brangesnius nebenaudojamus daiktus. Moteris dalijasi patirtimi, kad internetinė svetainė, kurioje ji užsiregistravo, nebuvo labai intuityvi, sistema šiek tiek strigo. Praėjus kelioms dienoms po skelbimo paviešinimo, viena potenciali pirkėja susidomėjo jos parduodamais daiktais ir pasiūlė tęsti bendravimą per Viber programėlę. Toks pasiūlymas Astai neatrodė įtartinas, kadangi tokiu būdu bendravimas vyksta daug greičiau ir paprasčiau.

Bendraudama per Viber pirkėja pareiškė, kad ji nori įsigyti Astos prekes ir atsiuntė nuorodą apie atliktą pavedimą. Asta norėdama įsitikinti ar pavedimas atliktas, prisijungė prie internetinės platformos, kadangi ten nebuvo jokios informacijos apie pavedimą, ji nusprendė šiek tiek palaukti.



CyberPhish

„Jei savo istorija apsaugojau bent vieną žmogų - tai buvo verta paviešinti, nors ir nukentėjo mano EGO“

sako nuo sukčių nukentėjusi Asta

CyberPhish kursas www.cyberphish.eu/learn
Daugiau informacijos www.cyberphish.eu

Funded by the Erasmus+ Programme of the European Union

Pirkėja „susirūpino“ dėl atlikto pavidimo

Po kelių dienų pirkėja „susirūpinusi“ klausė, ar Asta gavo pinigus ir pradėjo skubinti, kad viskas greičiau vyktų. Asta suabejojo dėl pinigų pervedimo, tačiau buvo girdėjusi, kad tokios platformos pinigus už prekes ne iš karto pveda pardavėjui, todėl grįžo prie pirkėjos atsiųstos nuorodos.

Pardavėjo autorizacijos procesas, siekiant įsitikinti, kad pardavėjas yra ne „sukčius“

Paspaudus pirkėjos atsiųstą nuorodą, atsidarė svetainė, kurios adresas nė kiek neatrodė įtartinas, svetainės aplinka atrodė originali. Norint sužinoti apie pavidimo detales, svetainėje buvo prašoma užpildyti specialią formą ir patvirtinti savo tapatybę. Formoje reikėjo suvesti banko kortelės duomenis, kadangi pavidimas turės būti atliekamas į tos kortelės sąskaitą. Astai nesukėlė įtarimo ir tai, kad siekiant atlikti pardavėjo autorizaciją bei įsitikinti, kad pardavėjas yra ne „sukčius“, formoje reikia nurodyti kortelėje esančių lėšų likutį. Kadangi kortelėje buvo mažiau nei 100 Eur, užpildžius formą, Asta gavo pranešimą, kad kortelėje privalo būti ne mažiau, kaip 150 Eur, kuriuos sistema nuskaito ir iš karto grąžina. Sistemoje nuolatos pabrėžiama, kad tai daroma dėl pardavėjo tapatybės nustatymo ir „dėl pastaruoju metu padažnėjusių sukčiavimo atvejų“. Norėdama kuo greičiau pabaigti registraciją, Asta nieko nelaukdama papildė savo banko sąskaitą dar 100 Eur. Atlikus visus prašomus registracijos veiksmus, buvo pateiktas pranešimas, kad pavidimas buvo „anuliuotas“, o tuo tarpu pirkėja nenustojo klausinėjusi, ar Asta gavo pinigus už prekes.

Kitą dieną Asta patikrinusi savo sąskaitą pamatė 0,00 Eur sąskaitos likutį – sąskaita buvo ištuštinta. Tada pasidarė aišku, kad Asta papuolė ant sukčių kabliuko, ir ji skubiai ėmėsi veiksmų: susisiekė su banku, užblokavo banko kortelę bei informavo policiją.

Istorijos viešinimo kitiems poveikis

Tik atsigavusi po patirtos situacijos, Asta pastebėjo, kad formą pildė visgi ne originalioje panaudotų prekių svetainėje, svetainės adresas buvo kitoks, nei originalios svetainės: adrese buvo pridėtos papildomos raidės „-lt.lt“, kurios įtarimo nesukėlė. Taip pat Asta susimąstė ir dėl nuolatinio spaudimo, ar „gavai pinigus“ ir „kur mano prekės“, o galiausiai įtarimą turėjo sukelti asmeninių ir finansinių duomenų suvedimas svetainės formoje.

Savo patirtimi moteris pasidalijo socialiniame tinkle perspėdama, kad draugai būtų atidūs ir nepapultų į panašias situacijas. Po šios istorijos paviešinimo Asta sulaukė labai daug įvairių draugų bei pažįstamų istorijų, taip pat ir apie prarastus tūkstančius eurų.

Asta galiausiai pripažįsta, kad jos istorija sukėlė nemažą diskusiją, ir kad tai prisideda prie žmonių švietimo apie internetinius sukčius. Moteris sako „jei savo istorija apsaugojau bent vieną žmogų nuo internetinių sukčių – tai buvo verta paviešinti, nors ir nukentėjo mano EGO“.

Kaip apsisaugoti nuo sukčių ir nepapulti ant jų kabliuko?

Norėdami nepapulti į panašias situacijas, turime ne tik dalintis istorijomis, išmokti atpažinti sukčiavimo atvejus, bei žinoti, kaip elgtis, kad išvengtume nemalonių situacijų, kadangi sukčių atakos gali būti įvykdytos ne tik parduodant prekes internetu, bet ir el. paštu, SMS žinutėmis, telefono skambučiais, naršant internete. Taip pat turime žinoti, kokių veiksmų imtis, jei sukčiai pasiekė savo tikslą.

Pastebėję internetinių sukčių suaktyvėjimo tendencijas, kelios organizacijos iš Lietuvos, Latvijos, Estijos, Maltos ir Kipro nusprendė sukurti mokymo medžiagą apie internetinį sukčiavimą (angl. phishing). Projekto partneriai Lietuvoje: VU Kauno fakultetas ir VšĮ „Informacinių technologijų institutas“.

Prisijungę prie nuotolinės mokymo aplinkos www.cyberphish.eu/learn galėsite ne tik sužinoti apie sukčiavimą, bet ir patikrinti žinias, bei išspręsti atsparumo sukčiavimui scenarijus. Baigusiems internetinį kursą, išduodamas pažymėjimas.

Dr. Renata Daniėlienė, VšĮ „Informacinių technologijų institutas“