

Sparčiai tobulėjant technologijoms, progresuoja ir sukčiai, jų sukčiavimo schemas vis išradingesnės ir išmanesnės. Elektroninis sukčiavimas tapo viena iš dažniausiai pasitaikančių problemų elektroninėje erdvėje. Sukčiams pavyksta apgauti ne tik naivius senolius, į jų sumaniai suregztas pinkles papuola ir įmonės. Pastaruoju metu apgavikai taikosi į įmonių susirašinėjimą ir taip išvilioja solidžias pinigų sumas.

Panevėžio apskrities vyriausiasis policijos komisariatas kovo 12 d. sulaukė pranešimo, kad į Panevėžyje veikiančios bendrovės elektroninį paštą buvo gauta klaidinanti informacija ir apgaulės būdu išviloti 35 000 eurų. Pirminiais duomenimis, elektroniniai sukčiai pasinaudojo nuolatinų įmonės verslo partnerių užsienyje vardu ir atsiuntė neva pakeistą savo sąskaitos numerį, į kurį nieko blogo neįtariant ir buvo pervesti pinigai. Tik vėliau paaiškėjo, kad verslo partneriai mokėjimo negavo, o 35000 eurų nuplaukė į sukčių sąskaitą.

Tam, kad išvengtumėte elektroninėje erdvėje vykdomų apgavysčių, būtina **pasirūpinti įmonėje naudojamų informacinių sistemų, įskaitant el. paštą, saugumu, naudoti tik legalias kompiuterines programas.**

Svarbu gaunamus elektroninius laiškus skaityti itin atidžiai!

Atkreipkite dėmesį ir kritiškai įvertinkite gautą informaciją, jeigu gavote elektroninį laišką, kuriame pranešama apie **pasikeitusią nuolatinio Jūsų verslo paslaugų/prekių tiekėjo banko sąskaitą**. Net jei paaiškinimas atrodo įtikinamas, neskubėkite atlikti mokėjimo. Kilus abejonėms, visada skambinkite atsakingam asmeniui, su kuriuo bendravote ir išsiaiškinkite, ar tikrai buvo atlikti tokie pakeitimai, ar duomenys tikslūs. Taip pat pasitaiko atveju, kai suklastoti el. laiškai siunčiami įmonės finansininkui nuo neva įmonės vadovo, kuris prašo skubiai pervesti pinigų į konkrečią sąskaitą.

Gavę įtarimų sukėlusį elektroninį laišką, **atidžiai patikrinkite elektroninio pašto adresą**, nes dažnai sukčiai įsilaužia į kompiuterį ir jį ilgą laiką seka: stebi susirašinėjimus elektroniniais laiškais. Jie sukuria elektroninio pašto adresą, labai panašų į žmogaus, su kuriuo susirašinėjate ir sulaukę tinkamo momento atsiunčia laišką su prašymu pervesti pinigų. Iš pirmo žvilgsnio jis gali niekuo nesiskirti, tačiau geriau išsižiūrėję, galite pamatyti, kad **pakeista ar pridėta viena raidė ar simbolis.**

Pasirūpinkite savo naudojamų IT įrenginių saugumu: **reguliariai atnaujinkite programinę įrangą**, keiskite slaptažodžius, naudokite telefono/kompiuterio užraktą.

Niekada **neskubėkite paspausti įtartinuose laiškuose esančių nuorodų, atsisiųsti laiške esančių priedų** ar atlikti siūlomų veiksmų.

Nors sukčių atakos būna kruopščiai suplanuotos, išvengti jų galima laikantis saugumo taisyklių.

