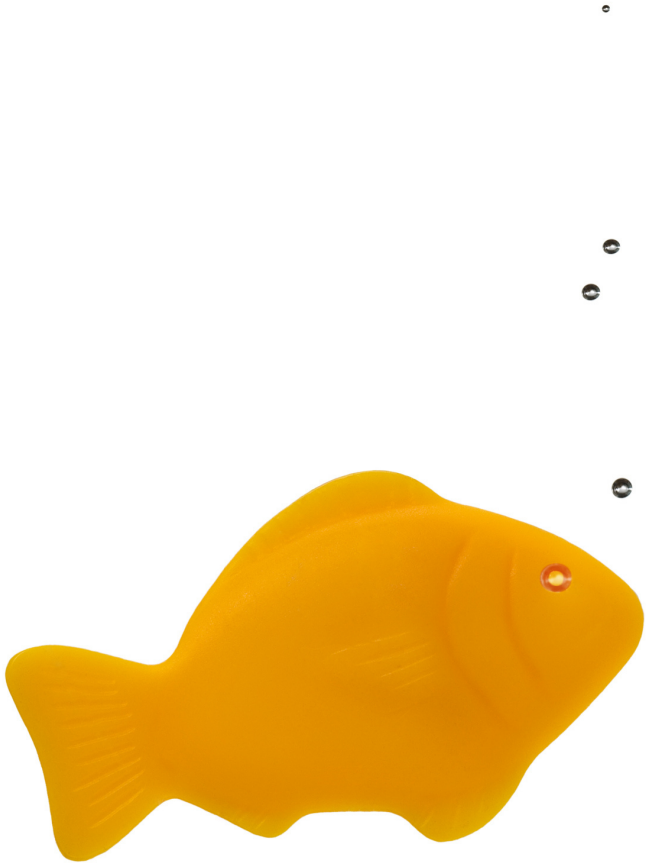
Birželis, 2021

BENDROJI ATASKAITA

Tiriamoji socialinės inžinerijos simuliacija



responsu

Apie projektą

Ar darbuotojai pasiruošę atremti šiandienos pavojus elektroninėje erdvėje?

Sukčiavimas el. paštu, dar kitaip vadinamas fišingas, nėra nauja problema IT saugos srityje. Tačiau pastarųjų metų įvykiai, tokie kaip neišvengiamas darbas iš namų ir sparti skaitmenizacija, šią problemą ypač paaštrino – per 2020 metus fišingo atakų skaičius išaugo 600%, o vartotojų, negalinčių atpažinti sudėtingo sukčiavimo laiško, pasiekė 97%.

Ši situacija baugina ir stambias organizacijas, ir valstybines įmones, ir smulkųjį verslą. Juk niekas nėra apsaugotas nuo sukčių. Kibernetiniams nusikaltėliams nėra svarbus įmonės dydis ar sektorius – dauguma atakų vykdomos automatizuotai. Net ir vienas neatsargus veiksmas, pvz. paspaudimas ant užkrėstos nuorodos, gali reikšti prarastą klientų pasitikėjimą, sutrikdytą veiklą ir finansinius nuostolius.

Organizacijas sunerimti verčia ir tai, kad įprastos priemonės darbuotojų IT saugumo suvokimui ugdyti, šiandien gali būti ne tokios veiksmingos. Juk atakų vektoriai sparčiai tobulėja, o išoriniai veiksniai ir toliau silpnina darbuotojų gebėjimą atpažinti grėsmės.

responsu

Siekiant padėti įmonėms įvertinti, ar jų IT saugumo suvokimo skatinimo politika veikia ir jų darbuotojai geba atpažinti sukčiavimą el. paštu, „Responsu“ inicijavo tiriamąją socialinės inžinerijos kampaniją. Projekto metu kartu su dalyvaujančiomis įmonėmis buvo vykdoma fišingo atakos simuliacija, išsiunčiant identiško turinio sukčiavimo el. laišką. Dalyvių paspaudimai ant tariamai žalingos nuorodos buvo fiksuojami, o gauti duomenys panaudoti analizei, kurioje paspaudimų rodikliai lyginami pagal įmonės sektorių ir dydį.

Šis tyrimas suteikia unikalią galimybę Lietuvos įmonėms pamatuoti tikrąjį darbuotojų gebėjimą atpažinti sukčiavimą ir atsakyti į klausimus – ar žmogiškasis faktorius yra silpnoji saugumo grandis organizacijoje ir ar turimos IT saugumo suvokimo skatinimo priemonės vis dar veiksmingos?

Situacijos apžvalga

Kaip viskas vyko?

Tiriamoji socialinės inžinerijos simuliacija vyko penkias savaites 2021 metų gegužės – birželio mėnesiais. Projekte dalyvavo 5510 asmenų iš 70 skirtingų organizacijų ir 13 sektorių.

Fišingo atakai inscenizuoti buvo pasitelktas Sophos Phish Threat socialinės inžinerijos simuliacijų įrankis, kuris leido išsiųsti identiško turinio el. laiškus su tariamai užkrėsta nuoroda bei fiksuoti gavėjų veiksmus – el. laiško atidarymą, paspaudimą ant nuorodos, laiką ir naudojamą įrenginį.

Rezultatai

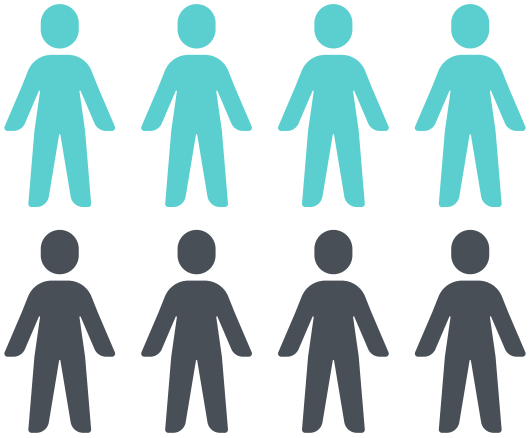
Tiriamoji socialinės inžinerijos simuliacija atskleidė, kad vis dar didelė dalis įmonių stokoja praktinio pasiruošimo atpažinti sukčiavimą el. paštu – laišką perskaitė 35% darbuotojų, iš kurių 54% neatpažino klastos ir paspaudė ant nuorodos. Pagal pasaulinę statistiką, 31% paspaudimų jau signalizuoja apie itin prastą situaciją.

Taip pat pastebimas neapdairus ir skubotas darbuotojų elgesys – gavus laišką 31% dalyvių ant nuorodos paspaudė nepraėjus nei minutei. Tai įspėja, kad šie asmenys neturi pakankamai informacijos ir teorinių žinių, kad galėtų kritiškai įvertinti gaunamus laiškus.

13 Sektorių

70 Įmonių

5510 Darbuotojų



Sektoriai

- Didmeninė ir mažmeninė prekyba
- Dujų ir vandens tiekimas, energetika
- Finansinės paslaugos
- Gamyba
- Informacinės technologijos
- Konsultavimas
- Nekilnojamasis turtas, nuoma
- Sveikatos priežiūra
- Švietimas
- Transportas, sandėliavimas ir ryšiai
- Turizmo paslaugos
- Viešasis valdymas
- Viešbučiai ir restoranai

19%
Bendrai paspaudė
(nuo visų išsiųstų)

35%
Perskaitė el. laišką

54%
Perskaitė ir paspaudė

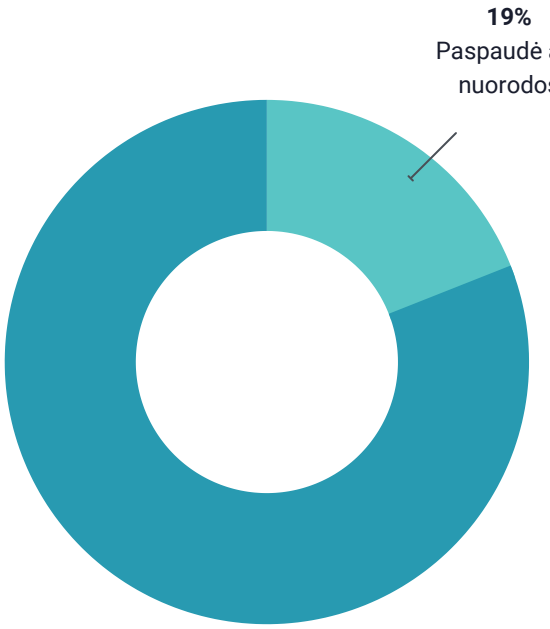
Detali apžvalga

Bendras paspaudimų rodiklis

Iš visų dalyvavusių įmonių darbuotojų, ant tariamai žalingos nuorodos paspaudė 19%. Svarbu suprasti, kad ir vienas neapdairus paspaudimas gali sukelti nesugrąžinamus nuostolius.

81% ant kabliuko nepakibo. Tai dažnai sąlygoja ne tik darbuotojų budrumas, bet ir techninės IT saugos priemonės ir skirtingi nustatymai, kurie neleidžia patekti įtartiniems laiškams į el. pašto dėžutę arba įspėja apie pavojų. Pastaruoju atveju, asmuo neperskaitys laiško ir niekada nesužinos apie įvykusią ataką.

Todėl svarbu pamatuoti ne tik bendrą paspaudimų rodiklį (paspaudimai/visi išsiųsti laiškai), tačiau ir **perskaitytų el. laiškų** (paspaudimai/ perskaityti laiškai).



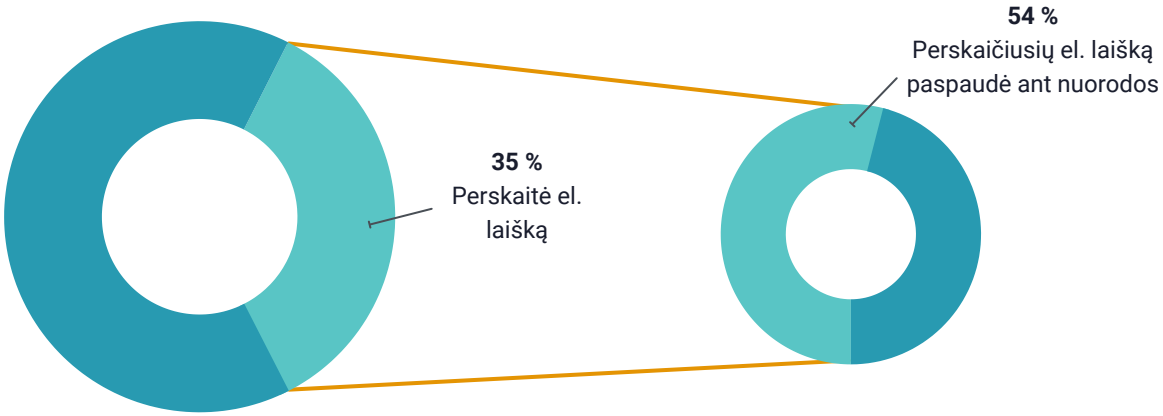
Ant tariamai žalingos nuorodos paspaudusių darbuotojų bendra dalis % (nuo visų išsiųstų laiškų)

Perskaitė laišką

35% dalyvių laišką perskaitė. Nemaža dalis (65%) neperskaitytų laiškų rodo, kad darbuotojai įtariai vertina nelauktus laiškus ir jų net neatidaro.

Perskaitė ir paspaudė

Net 54% laišką perskaičiusių asmenų, paspaudė ant nuorodos. Pagal pasaulinę statistiką 31% paspaudimų jau signalizuoja apie itin prastą situaciją.

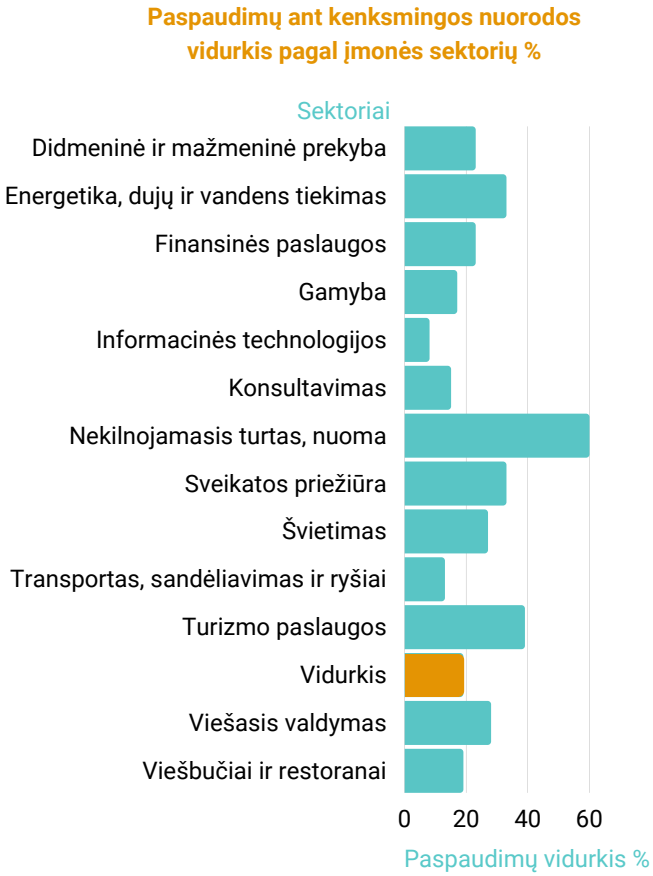


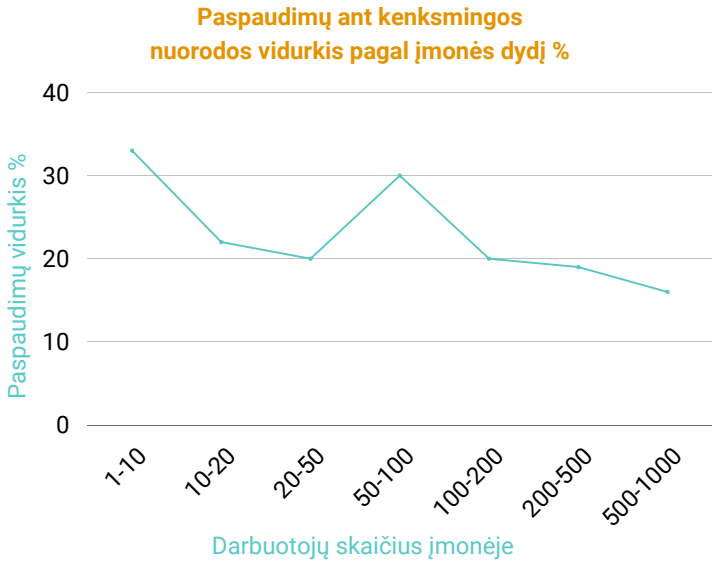
Detali apžvalga

Paspaudimai ant nuorodos pagal sektorių

Žymiai didesnis nei vidutinis paspaudimų vidurkis fiksuojamas keturiuose sektoriuose – turizmo paslaugų (39%), sveikatos priežiūros (33%), nekilnojamo turto ir nuomos (60%), bei energetikos, dujų ir vandens tiekimo srityse (33%). Dvigubai mažesnis nei vidutinis paspaudimų ant nuorodos vidurkis išryškėja informacinių technologijų srityje (8%).

Vertinant organizacijas pagal sektorių, būtina atkreipti dėmesį, kad kiekvienas sektorius susiduria su skirtingais iššūkiais, kurie turi įtakos paspaudimų ant nuorodos skaičiui. Pagrindinė priežastis, lemianti pastebimai didesnį rodiklį tam tikruose sektoriuose, gali būti paaiškinama sparčia kasdienių operacijų skaitmenizacija, kai siekiant sukurti didesnę vertę ir geresnę patirtį klientui, nepakankamai dėmesio skiriama darbuotojų IT saugumo suvokimo skatinimui.





Paspaudimai pagal įmonės dydį

Smulkiausio verslo segmente paspaudimų vidurkis didžiausias (33%). Tai rodo, kad itin mažose įmonėse (iki 5 asmenų) vis dar skiriama nepakankamai žmogiškųjų ir techninių išteklių IT saugai užtikrinti. Kai tuo tarpu stambiose organizacijose darbuotojai linkę spausti ant nuorodos dvigubai rečiau (16%). Tai lemia, jog įprastai didesnėse organizacijose skiriama daugiau dėmesio saugumo politikos formavimui ir įgyvendinimui, bei atitikties reikalavimų užtikrinimui.

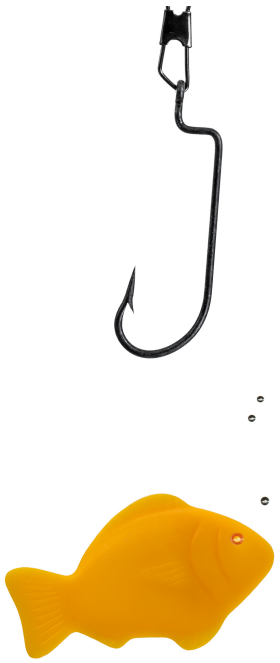
Kitos įžvalgos:

- **IT saugumo suvokimo ugdymo programos veiksmingos**: daugiau nei pusė įmonių pranešė (57%), kad bent vienas darbuotojas informavo atsakingus asmenis apie gautą įtartiną laišką.
- **Globalūs skaičiai sutampa**: pagal pasaulinę statistiką, 20% darbuotojų neatpažintų sukčiavimo laiško ir paspaustų ant žalingos nuorodos, o Lietuvoje – 19%.
- **Mobilieji įrenginiai nėra didesnė grėsmė**: daugiausiai greičiausių paspaudimų užfiksuota darbuotojams naudojant kompiuterį, o ne mobilųjį telefoną.

responsu

31%

Perskaičiusių laišką ant nuorodos paspaudė per pirmąją minutę



Rekomendacijos

- Peržiūrėti įmonės IT saugos politiką ir priemones.
- Ugdyti darbuotojų kritinį mastymą, pasitelkiant teorines ir praktines užduotis.
- Reguliariai priminti apie sukčiavimo el. laiškus ir kitus pavojus, slypinčius elektroninėje erdvėje.
- Užtikrinti tinkamas technines priemones el. pašto apsaugai.

Norite dalyvauti kitoje tiriamojoje socialinės inžinerijos simuliacijoje?

Susisiekite!
info@responsu.com,
+370 688 81450