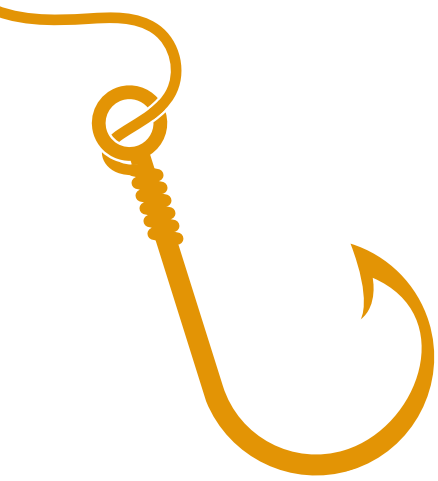
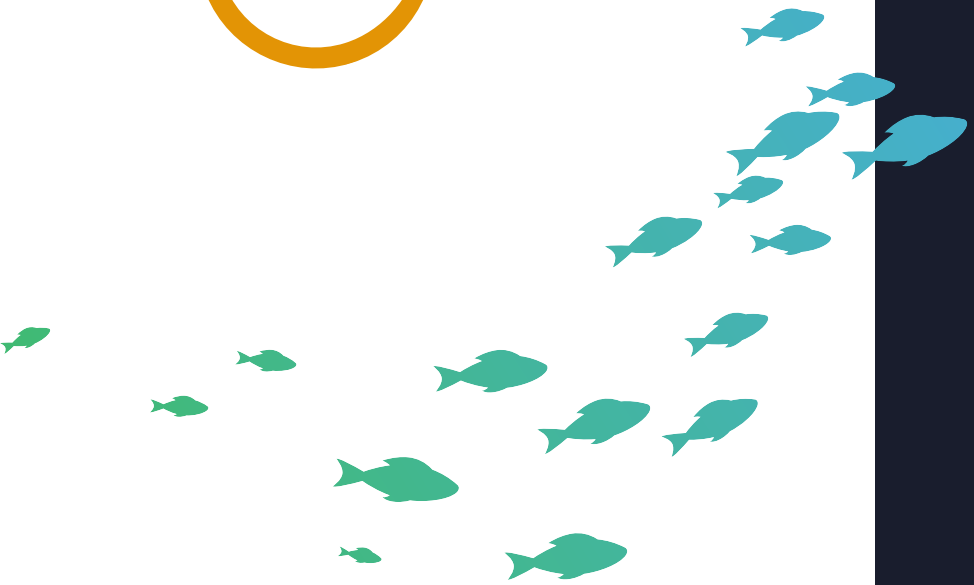
BENDROJI ATASKAITA 2022

Tiriamoji socialinės inžinerijos simuliacija





responsu

Apie projektą

Sukčiavimas el. paštu: atvejų daugėja ar mažėja dėl tinkamo darbuotojų pa(si)ruošimo?

responsu

Atlikti tyrimai rodo, jog net pusė Lietuvos gyventojų yra patyrę vienokių ar kitokių kibernetinių išpuolių, o dar labiau tobulėjančios socialinės inžinerijos principais paremtos atakos kelia vis didesnę grėsmę.

Sukčiavimas el. paštu, kitaip dar vadinamas fišingas, ir toliau išlieka aktuali problema. Pasaulyje vykstantys kariniai konfliktai, tebesitęsianti pandemija, ekonominiai pokyčiai ir prisitaikymas gyventi skaitmenizuotame pasaulyje lemia greitą kibernetinių atakų populiarėjimą.

Įmonių darbuotojai - vienas dažniausių šių kibernetinių atakų vektorių, tampantis tiesiausiu keliu pasiekti svarbiausius organizacijos duomenis. 2021 m. net **85%** kibernetinių incidentų įvyko dėl žmogiškosios klaidos.

Kaip parodė praėjusiais metais „Responsu" atlikta tiriamosios socialinės inžinerijos simuliacija, kas antras darbuotojas, perskaitęs sukčiavimo laišką, „pakibtų ant kabliuko". Šiemet projektas buvo pakartotas. Šiais metais situacija geresnė, tačiau rezultatai rodo, jog Lietuvos įmonėms vis dar trūksta žinių ir skaitmeninės higienos kibernetinio saugumo srityje.

Siekiant padėti įmonėms įsivertinti, kaip veikia jų kibernetinio saugumo suvokimo skatinimo politika ir pamatyti, ar darbuotojai geba atpažinti sukčiavimą el. paštu bei tinkamai reaguoti, „Responsu" jau antrus metus iš eilės inicijavo tiriamąją socialinės inžinerijos kampaniją.

Incenizuojant ataką, buvo siunčiamas el. laiškas, panašus į realios organizacijos siunčiamą informaciją, naudojant netikrą siuntėjo adresą. El. laiško tekste buvo pateikiamas įtikinamas tekstas, skatinantis paspausti ant suklastotos nuorodos. Rezultatai, palyginus su praėjusiais metais atliktu tyrimu, rodo, kad yra padidėjęs perskaitymo procentas, o tai parodo, jog buvo pasirinktas šiai dienai aktualus el. laiško formatas.

Tokio tyrimo nauda - ugdyti darbuotojus kibernetinio saugumo srityje, kad šie netaptų pagrindine rizika sukčiams lengvai ir greitai gauti reikiamus duomenis. Pasitelkus mokymus ir neinvestuojant daug išteklių užtikrinama įmonės technologinė branda ir saugumas.

Situacijos apžvalga

Kaip viskas vyko?

Tiriamoji socialinės inžinerijos simuliacija vyko keturis mėnesius: 2022 m. kovo – birželio mėn. Projekte dalyvavo **9989 darbuotojai** iš **78 skirtingų organizacijų** ir **13 sektorių**. Iš viso išsiųsta virš **10000 el. laiškų**. Tai beveik dvigubai daugiau nei pernai. Kelių įmonių rezultatai nebuvo įtraukti, kadangi neatitiko tyrimui keliamų reikalavimų.

Projekto metu atakai inscenizuoti buvo pasirinktas *Sophos Phish Threat* socialinės inžinerijos simuliacijų įrankis, kuris leido dalyvaujančiomis įmonėmis išsiųsti identiško turinio el. laiškus lietuvių ir anglų kalbomis su tariamai užkrėsta nuoroda bei fiksuoti gavėjų veiksmus – el. laiško atidarymą (perskaitymą), paspaudimą ant nuorodos, laiką, naudojamą įrenginį.

Rezultatai

Gauti rezultatai parodė, jog el. laišką perskaitė kiek daugiau darbuotojų nei 2021 m. - **41% (2021 m. 35%). 37%** iš jų perskaitė ir paspaudė nuorodą. Šis rodiklis mažesnis nei pernai metų (**54%**). Projekte dalyvavo kelios įmonės, kurios į tyrimą buvo įtrauktos ir praėjusiais metais ir yra žinoma, jog šiose įmonėse buvo imtasi atitinkamų priemonių darbuotojų informavimui ir ugdymui kibernetinio saugumo srityje.

9989
Darbuotojai

78
Įmonės

13
Sektorių

Sektoriai

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

16%
Bendrai paspaudė
(nuo visų išsiųstų)

41%
Perskaitė

37%
Perskaitė ir paspaudė

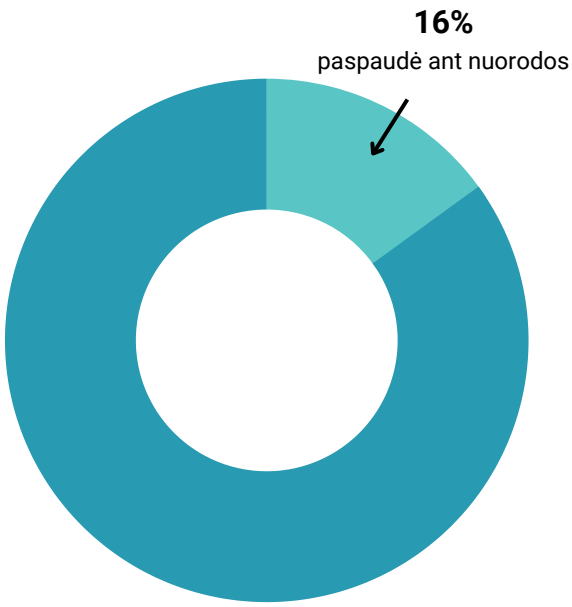
Detali apžvalga

Bendrai paspaudė

Iš visų dalyvavusių darbuotojų, ant tariamai žalingos nuorodos paspaudė **16%**. Džiugu, kad tokių paspaudimų sumažėjo, palyginus su praėjusiais metais (**19%**).

Tam įtakos galėjo turėti darbuotojų turimos ir įgytos žinios ar išklausyti mokymai kibernetinio saugumo srityje.

Svarbu pamatuoti ne tik bendrą paspaudimų rodiklį (paspaudimai/visi išsiųsti el. laiškai), bet ir **perskaitytų el. laiškų** (paspaudimai/perskaityti el. laiškai) statistiką.



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

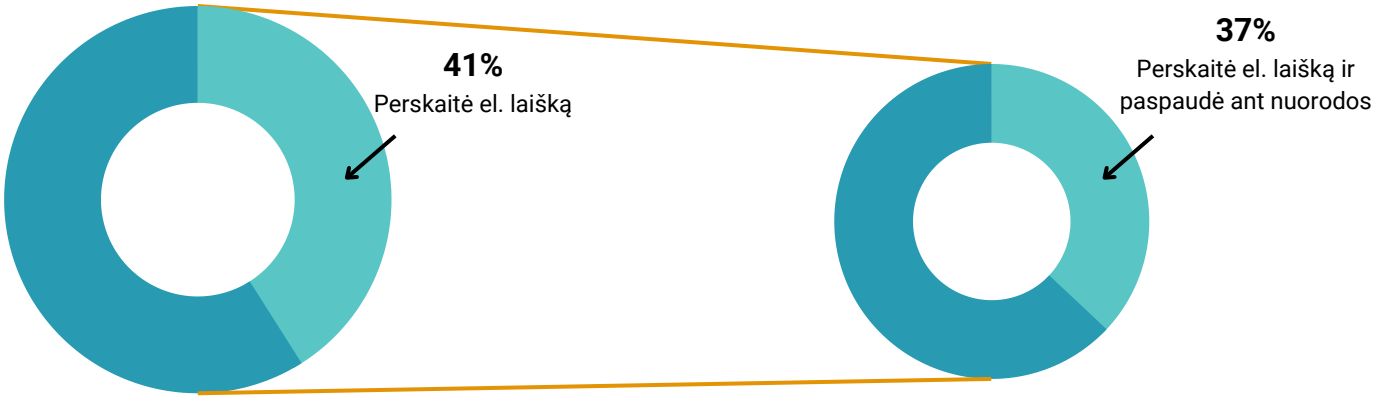
Perskaitė el. laišką

41% dalyvių laišką perskaitė. Šis skaičius padidėjo palyginus su praėjusio tyrimo rezultatais ir tai rodo, kad tinkamai parinkta sukčiavimo laiško forma, gali padinti tikimybę, jog darbuotojas apsigaus.

Perskaitė el. laišką ir paspaudė

37% laišką perskaičiusių asmenų, paspaudė ant nuorodos. Tai gerokai mažiau nei parodė pirmoji socialinės inžinerijos simuliacija, alikta 2021 m. (**54%**). Tokiam rezultatui ženklią įtaką turėjo ir antrą kartą dalyvavusių įmonių atlikti „namų darbai" kibernetinio saugumo srityje.

Paspaudimų ant tariamai žalingos nuorodos dalis % (tik nuo perskaitytų laiškų)



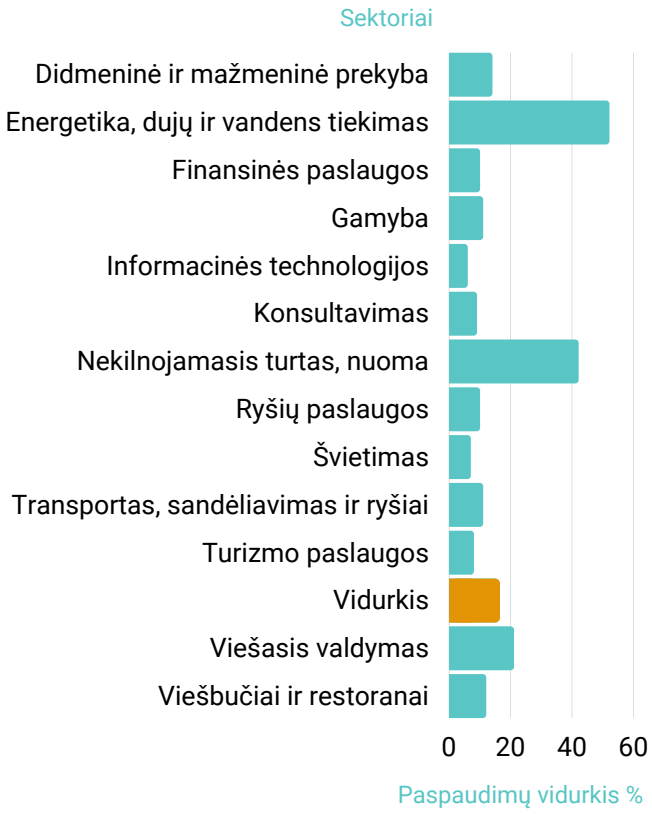
Detali apžvalga

Paspaudimai pagal sektorių

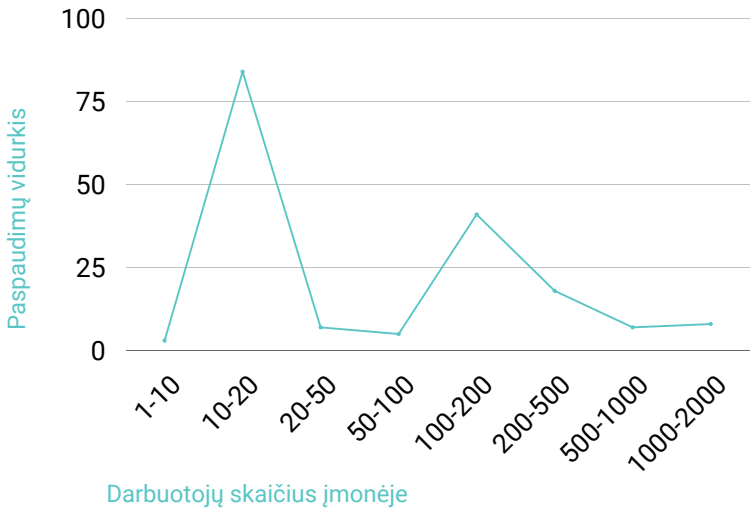
Šiemet žymiai didesnis nei vidutinis paspaudimų vidurkis fiksuojamas trijuose sektoriuose – energetikos (**52%**), nekilnojamo turto ir nuomos (**42%**), bei viešojo valdymo (**21%**). Džiugu, kad šiemet yra daugiau sektorių, kur paspaudimų ant nuorodos yra daug mažiau už vidurkį: informacinės technologijos **6%**, švietimas **7%**, turizmo paslaugos **8%**, konsultavimas **9%**.

Tiek mūsų tyrimas, tiek pasauliniai rezultatai rodo, kad darbuotojų informavimas bei ugdymas kibernetinio saugumo srityje yra naudingas, nes gali sumažinti paspaudimų skaičių vidutiniškai **85%**. Įvertinus įmonių, kurios dalyvavo mūsų tyrime šiais bei praėjusiais metais rezultatus, po mokymų jose sumažėjo galimų sėkmingų sukčiavimo atvejų: nuo maždaug **32%** iki **11%** (draudimas/finansinės paslaugos), nuo **39%** iki **7%** (turizmas), nuo **27%** iki **7%** (švietimas).

Paspaudimų ant kenksmingos nuorodos vidurkis pagal įmonės sektorių %



Paspaudimų ant kenksmingos nuorodos vidurkis pagal įmonės dydį %



Paspaudimai pagal įmonės dydį

Kaip ir praėjusiais metais, labai mažose ir mažose įmonėse paspaudimų vidurkis išlieka didžiausias (**84%**). Didelėse įmonėse darbuotojai linkę spausti ant nuorodos gerokai rečiau (**vos 5%**). Sukčiai toli gražu ne visuomet taikosi tik į didelius verslus, nes žino, jog mažesnėse įmonėse dažnu atveju galima atrasti daugiau spragų. Užkirsti kelią virtualiems nusikaltėliams įmanoma iš anksto tam ruošiantis ir laikantis svarbiausių saugumo taisyklių.

Kitos įžvalgos

- **Kibernetinio saugumo suvokimo ugdymo programos veiksmingos:** beveik visos dalyvavusios organizacijos informavo (**87%**), kad bent vienas jų darbuotojas pranešė atsakingiems asmenims įmonėje apie gautą įtartiną el. laišką.

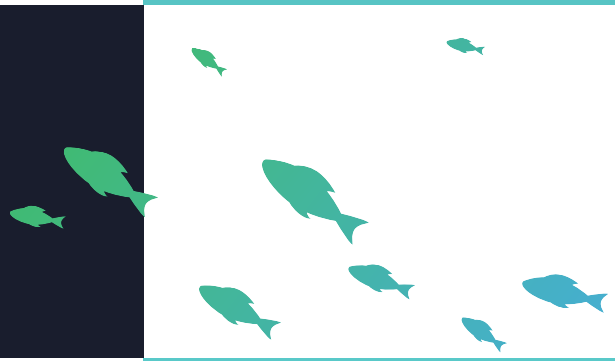
- **Nedžiugina skubotas darbuotojų elgesys**: gavus el. laišką **30%** dalyvių ant nuorodos paspaudė nepraėjus nė minutei. Šią situaciją sąlygoja ne tik neapgalvoti ir skuboti asmenų veiksmai bei teorinių žinių trūkumas. Rezultatas labai panašus į praėjusių metų (**31%**).

- **Mobilieji įrenginiai tampa vis populiaresni**: skirtingai nei praėjusias metais, daugiau greičiausių paspaudimų užfiksuota darbuotojams naudojant mobilųjį telefoną (**55%**), o ne kompiuterį. Tai paskatinti galėjo įmonių mobiliuosiuose telefonuose diegiami sprendimai patogesniam darbui. Vis dėlto, juose sunkiau pastebėti sukčiavimo atvejus.

30%

Perskaičiusių el. laišką paspaudė ant nuorodos per pirmąją minutę

Rekomendacijos



- Įvertinti įmonės kibernetinio saugumo rizikas ir paruošti rekomendacijas siekiant jų išvengti ar atlikti tinkamus veiksmus joms įvykus.

- Stiprinti darbuotojų suvokimą ir informuoti apie kibernetines grėsmes bei jų poveikį organizacijai.

- Reikia suvokti, jog el. laiškus, kuriais siekiama išvilioti duomenis, neabejotinai gausite ir ateityje, todėl itin svarbu reguliariai vykdyti darbuotojų teorinių žinių bei praktinių užduočių kibernetinio saugumo mokymus.

- Užtikrinti technines priemones el. pašto ir kitų kibernetinių grėsmių apsaugai: įdiegti tinkamas kibernetinio saugumo priemones bei laikytis kibernetinio saugumo higienos.

responsu

Norite dalyvauti kitoje tiriamojoje socialinės inžinerijos simuliacijoje ar išbandyti mūsų mokymus?

Susisiekime!
info@responsu.com
+370 6 888 1450