VILNIUS TECH

Duomenų viliojimo atakos rezultatai

Dr. Justinas Rastenis

2023-11-16

Apie mane

16 metų dirbu VILNIUS TECH IT skyriuje
10 metus dirbu lektoriumi

IT sauga
Įgyvendinti IT infrastruktūros ir WIFI projektus

Problematika

- „Phishing“ (liet. k. duomenų viliojimas) yra vienas populiariausių kompiuterių užkrėtimo būdu organizacijose arba asmens duomenų išviliojimo;
- Dauguma techninių ir programinių priemonių sunkiai arba negali identifikuoti visų „phishing“ metodų ar technikų;
- Ne visi naudotojai, turi pakankamai žinių ir praktikos identifikuoti „phishing“ atakų.

Problematika

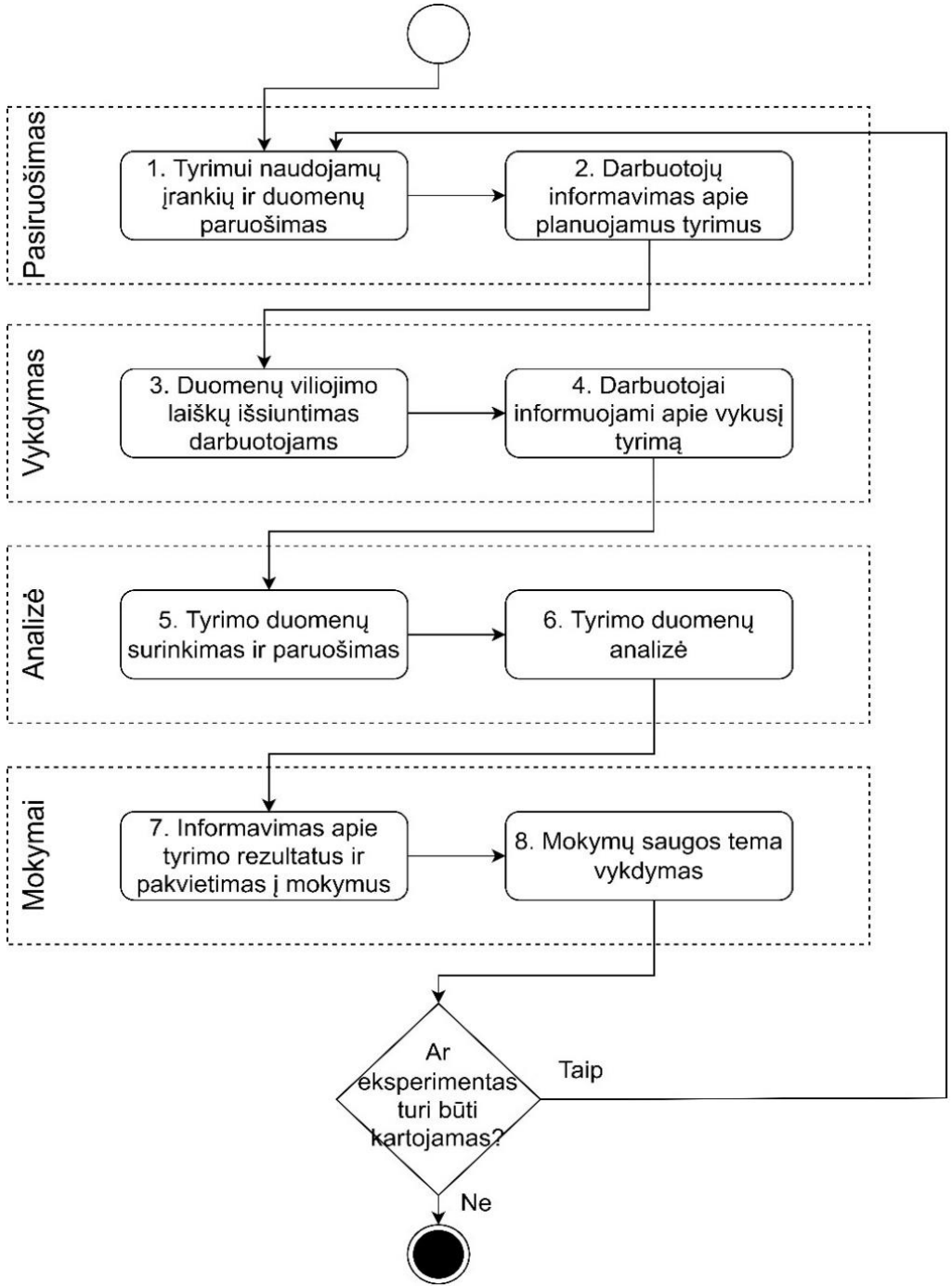
Tipinės antivirusinės priemonės atpažįsta tik po kelių valandų žalingą programinę kodą*.

Užsikrėtus virusu pavagiama arba po “phishing” atakos (priklauso dar ir nuo versijos)*:

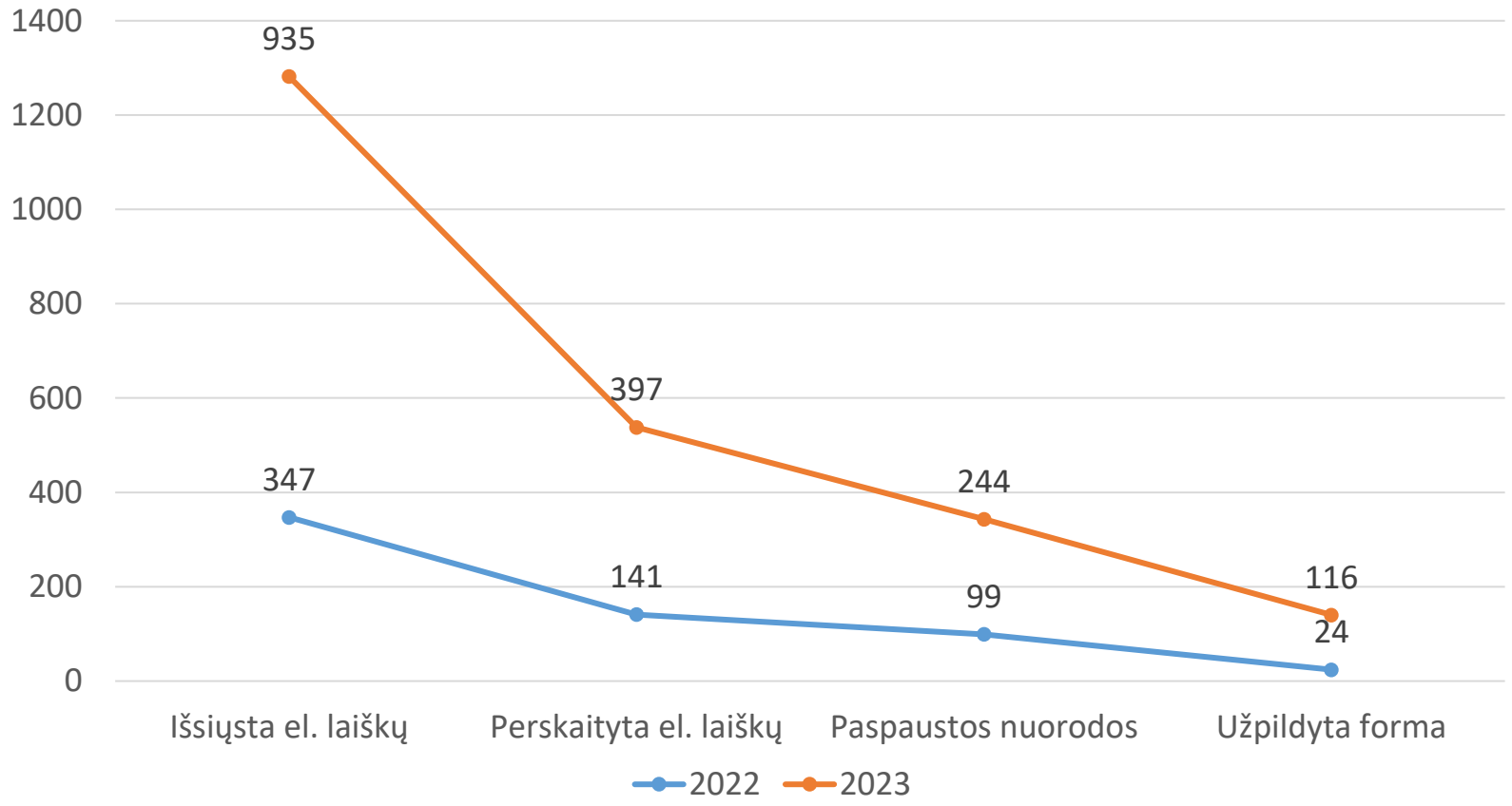
- El. pašto nustatymai;
- Prisijungimo vardas/slaptažodis;
- Adresatų sąrašas;
- Susirašinėjimo istorija;
- Interneto naršyklėse išsaugota prisijungimo informacija;
- Gali vykti vidinio tinklo skenavimai;
- Bruteforce atakos.

*2021 01 26 organizuoto Kibernetinio saugumo subjektų ir NKSC susitikimo demonstruotų skaidrių informacija

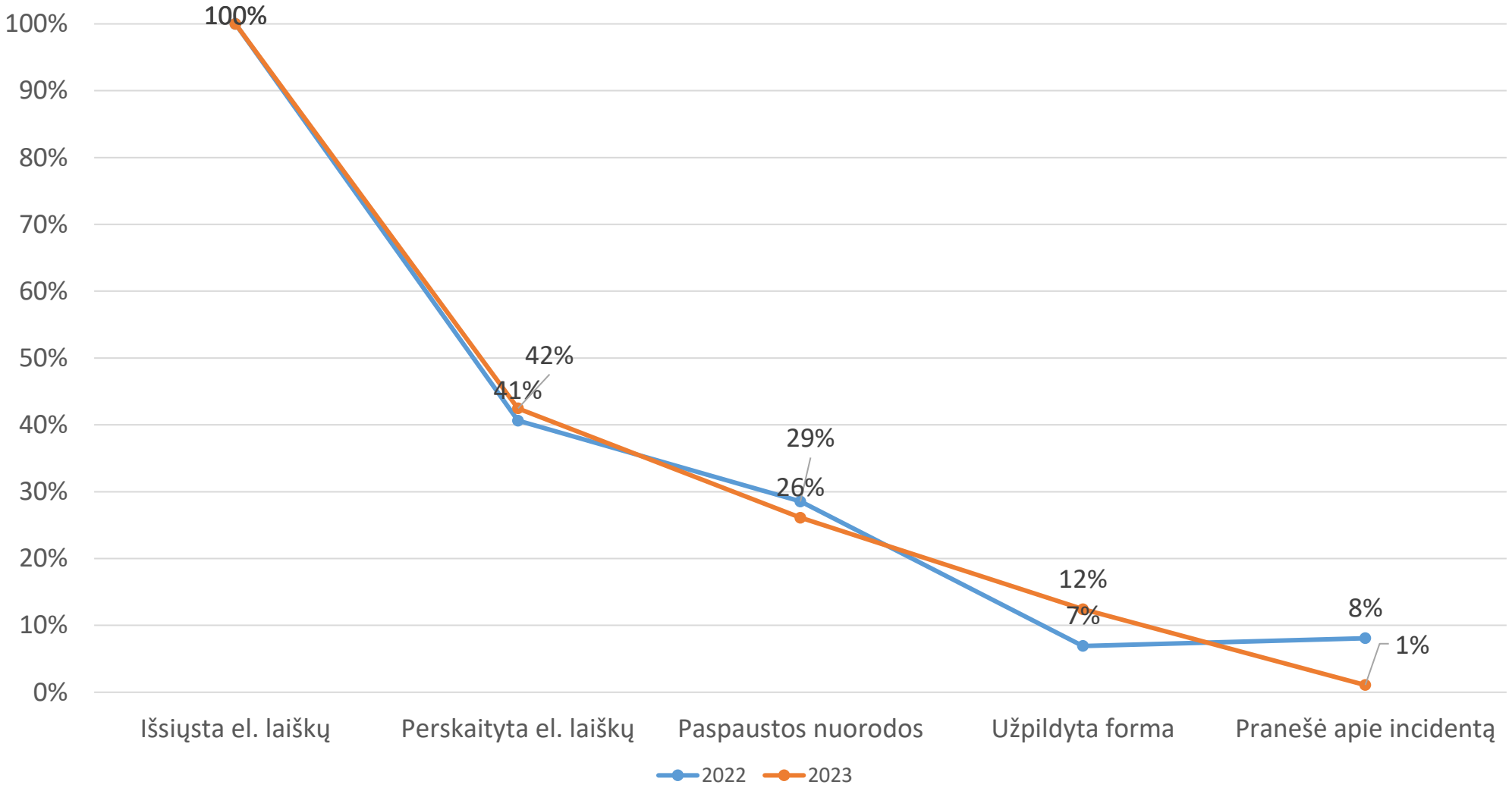
Eksperimentas



Rezultatai


1400
1200
1000
800
600
400
200
0
935
397
347
244
141
99
116
24
Išsiųsta el. laiškų
Perskaityta el. laiškų
Paspaustos nuorodos
Užpildyta forma
2022
2023

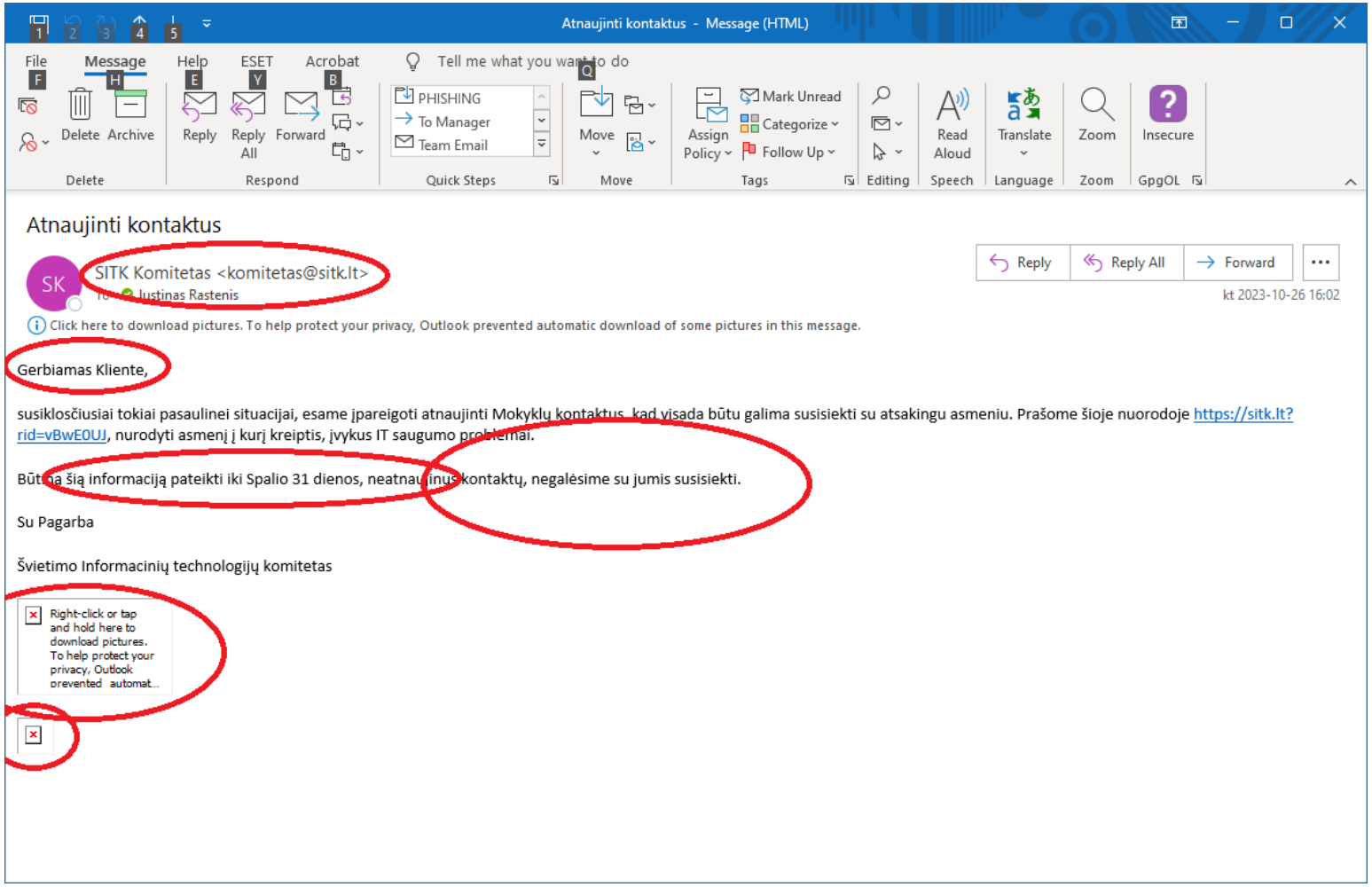
Rezultatai


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
100%
42%
41%
29%
26%
12%
7%
8%
1%
Išsiųsta el. laiškų
Perskaityta el. laiškų
Paspaustos nuorodos
Užpildyta forma
Pranešė apie incidentą
2022
2023

Atsparumo duomenų viliojimo atakos rezultatai

Metai	2018		2019		2022		LitNET 2022		LitNET 2023	
	Kiekis	% nuo visų laiškų	Kiekis	% nuo visų laiškų	Kiekis	% nuo visų laiškų	Kiekis	% nuo visų laiškų	Kiekis	% nuo visų laiškų
Išsiųstų laiškų	1648	100	1618	100	1785	100	347	100	935	100
Perskaitytų laiškų	708	**43**	931	**58**	679	**38**	141	**40**	**397**	**42**
Apsilankymų interneto portale	410	**25**	355	**22**	413	**23**	99	**28**	**244**	**26**
Užpildė netikrą formą	214	**13**	21	**1**	61	**3**	24	**6**	**116**	**12**
Pranešė apie incidentą	10	**1**	205	**13**	72	**4**	28	**8**	**10**	**1**

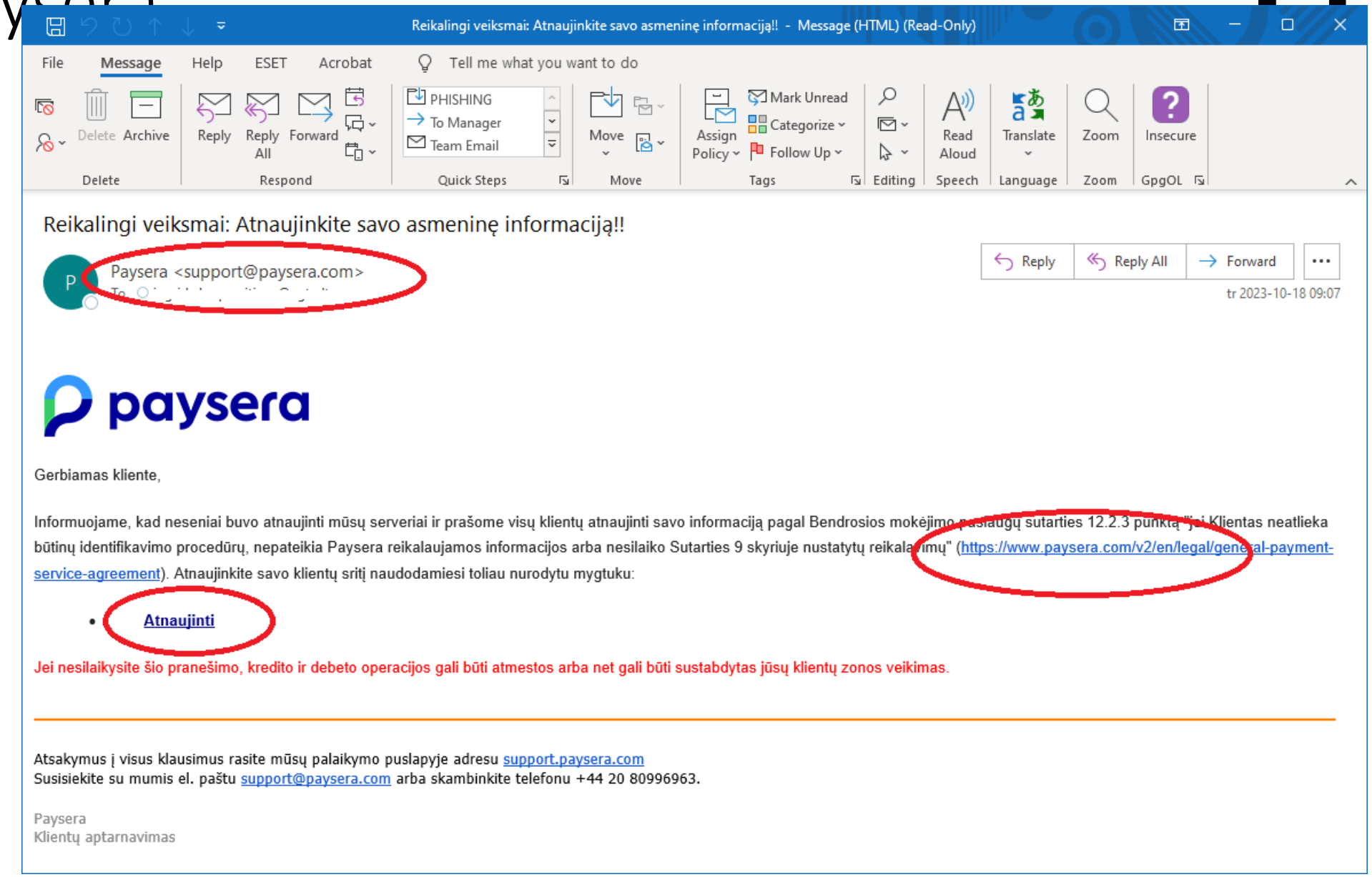
Išsiųstas laiškas



Kaip reikėjo atpažinti?

- Tikrinti siuntėjo adresą
  - Tikri adresai skelbiame svetainėje
- Identifikuoti ar yra tokia svetainė
- Susisiekti su ta įstaiga **viešais kontaktais iš patikimų šaltinių (Rekvizitai ir kitų)** ir paklausti ar tokį laišką siuntė.

Paysera



Reikalingi veiksmai: Atnaujinkite savo asmeninę informaciją!! - Message (HTML) (Read-Only)

File Message Help ESET Acrobat Tell me what you want to do

Delete Archive Reply Reply All Forward PHISHING To Manager Team Email Move Assign Policy Mark Unread Categorize Follow Up Read Aloud Translate Zoom Insecure

Delete Respond Quick Steps Move Tags Editing Speech Language Zoom GpgOL

Reikalingi veiksmai: Atnaujinkite savo asmeninę informaciją!!

P Paysera <support@paysera.com>

Reply Reply All Forward

tr 2023-10-18 09:07

paysera

Gerbiamas kliente,

Informuojame, kad neseniai buvo atnaujinti mūsų serveriai ir prašome visų klientų atnaujinti savo informaciją pagal Bendrosios mokėjimo paslaugų sutarties 12.2.3 punktą "jei Klientas neatlieka būtinų identifikavimo procedūrų, nepateikia Paysera reikalaujamos informacijos arba nesilaiko Sutarties 9 skyriuje nustatytų reikalavimų" (https://www.paysera.com/v2/en/legal/general-payment-service-agreement). Atnaujinkite savo klientų sritį naudodamiesi toliau nurodytu mygtuku:

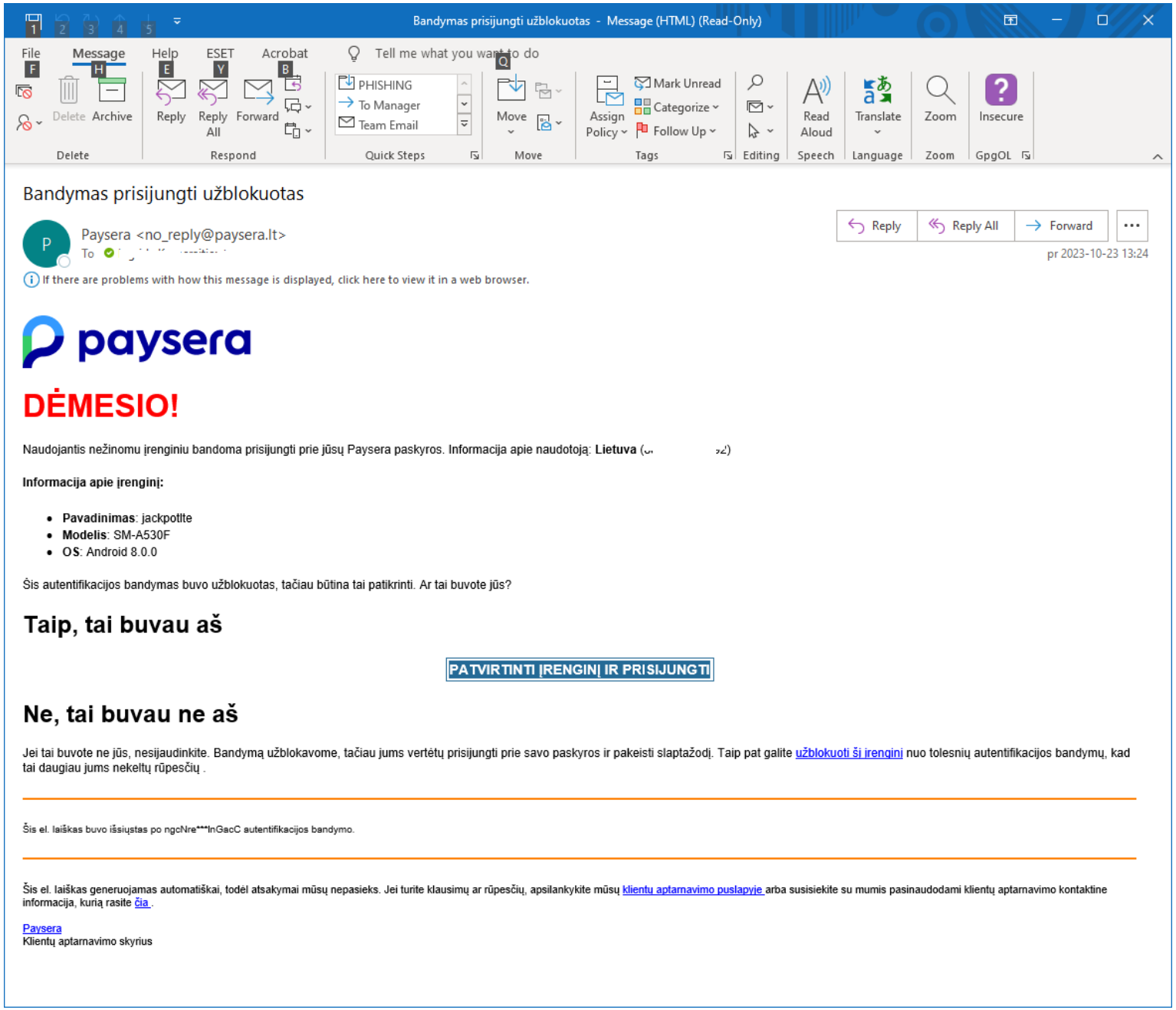
- Atnaujinti

Jei nesilaikysite šio pranešimo, kredito ir debeto operacijos gali būti atmestos arba net gali būti sustabdytas jūsų klientų zonos veikimas.

Atsakymus į visus klausimus rasite mūsų palaikymo puslapyje adresu support.paysera.com
Susisiekite su mumis el. paštu support@paysera.com arba skambinkite telefonu +44 20 80996963.

Paysera
Klientų aptarnavimas

Payse



VILNIUS TECH

Sąskaitos detalizacija

File | Message | ESET | Tell me what you want to do...

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | IM | More | PHISHING | Team Email | Reply & Delete | To Manager | Done | Create New | Move | Rules | OneNote | Actions | Assign Policy | Mark Unread | Categorize | Follow Up

Delete | Respond | Quick Steps | Move | Tags

detalizacija . <detalizacija@enefit-lt.com> [redacted]@enefit-lt.com; saskaitos@enefit-lt.com

Sąskaitos detalizacija

If there are problems with how this message is displayed, click here to view it in a web browser.

Enefit.pdf
44 KB

Laba diena,
Dėl atliekamo metinio banko sąskaitos "LT74 7044 0600 0745 0694" sutikrinimo audito keičiasi banko informacija.
Iš savo apskaitos skyriaus gavome informaciją, kad turėtume vadovautis pridedamos sąskaitos apmokėjimu.

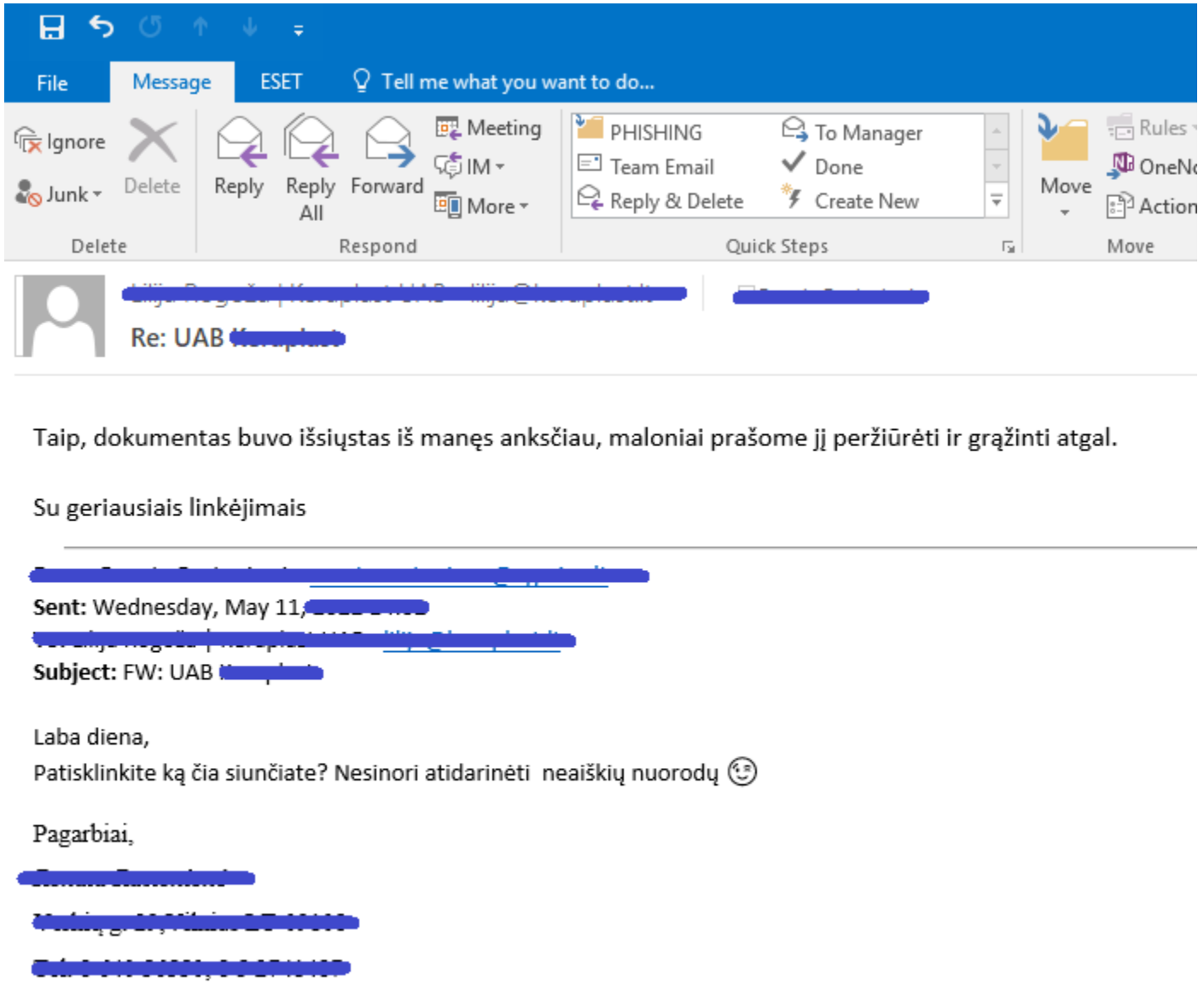
Kada yra pridedamos sąskaitos faktūros apmokėjimo data. kad galėtume perduoti jums mūsų dukterinio banko duomenis apmokėjimui.

Iš anksto dėkojame.

Enefit UAB
+370 5 201 9141 | detalizacija@enefit.lt
V. Gerulaičio g. 10, LT-08200 Vilnius | www.enefit.lt

VILNIUS TECH

Naujausi


File
Message
ESET
Tell me what you want to do...
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
Delete
Respond
PHISHING
Team Email
Reply & Delete
To Manager
Done
Create New
Quick Steps
Move
Rules
Action
Move
Re: UAB
Taip, dokumentas buvo išsiųstas iš manęs anksčiau, maloniai prašome jį peržiūrėti ir grąžinti atgal.
Su geriausiais linkėjimais
Sent: Wednesday, May 11,
Subject: FW: UAB
Laba diena,
Patisklinkite ką čia siunčiate? Nesinori atidarinėti neaiškių nuorodų
Pagarbiai,

Prisiminimui

R: Banko pavedimas - 2021 03 25_Swift kopija

From: **Swedbank lizingas, UAB**
To: **info@juverta.lt**
Date: **Today 12:07**

Labas rytas,

Mūsų klientas paprašė mūsų atsiųsti pridėto pervedimo mokėjimo kopiją jūsų el.

Pašto adresu:info@juverta.lt.

Patvirtinkite gavimą ir atitinkamai patarkite.

Pagarbiai.

Jūratė Gumuliauskienė.
(Customer Service Division)

Swedbank

Swedbank lizingas, UAB
Registered office address: Konstitucijos pr.20A, 09321 Vilnius, Lithuania
Phone: 1884, fax: (8 5) 2782 401
E-mail: J.Gumuliauskienė@swedbank.lt
Corporate code: 111568069
VAT ID code: LT115680610
Bank account No LT16 7300 0100 0000 0447
Bank code 73000
www.swedbank.lt

Norėdami peržiūrėti įmonės duomenis Swedbank lizingas, UAB. https://www.swedbank.lt/

Šiame el. Laiške esanti informacija yra konfidenciali ir konfidenciali, todėl ją platinti bet kokiu būdu draudžiama. Jei nesate asmuo, kuriam skirtas šis pranešimas, kviečiame jo neskleisti ir ištrinti, maloniai informuodami siuntėją.

Rekomendacijos

- Vartotojų švietimas;
- [PRATYBOS PRATYBOS PRATYBOS];
- Tikrinti laiško antraštes;
- Tvarkyti el. pašto apsaugos priemones;
- Naudoti ir nuolat atnaujinti galinių įrenginių (kompiuterių) antivirusinę programinę įrangą;
- Naudoti stiprius slaptažodžius; 2FA;
- Įvykus incidentui – pasikeisti slaptažodžius;
- Kibernetinio saugumo informacinis tinklas – siūlo grėsmių indikatorių platformą (MISP)

*2021 01 26 organizuoto Kibernetinio saugumo subjektų ir NKSC susitikimo demonstruotų skaidrių informacija

Ko nedaryti

1. Nedaryti veiksmų kurių prašoma
2. Nepildyti formų
3. Nerašyti jiems laiškų su klausimais
4. Neatsisiųsti paveikslėlių laiške
5. Nesilankyti nuorodose, kurias prašomą paspausti

Kaip apsisaugoti?

- Nemokėti išpirkos!
- Turėti kompiuterio, failų kopijas.
- Reguliariai daryti atsargines kopijas.
- Reguliariai atnaujinti antivirusinę programinę įrangą ir kompiuterio operacinę sistemą.

ITSC Saugumo rekomendacijos

Ačiū kad klausėtės.

Klausimai?