



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.

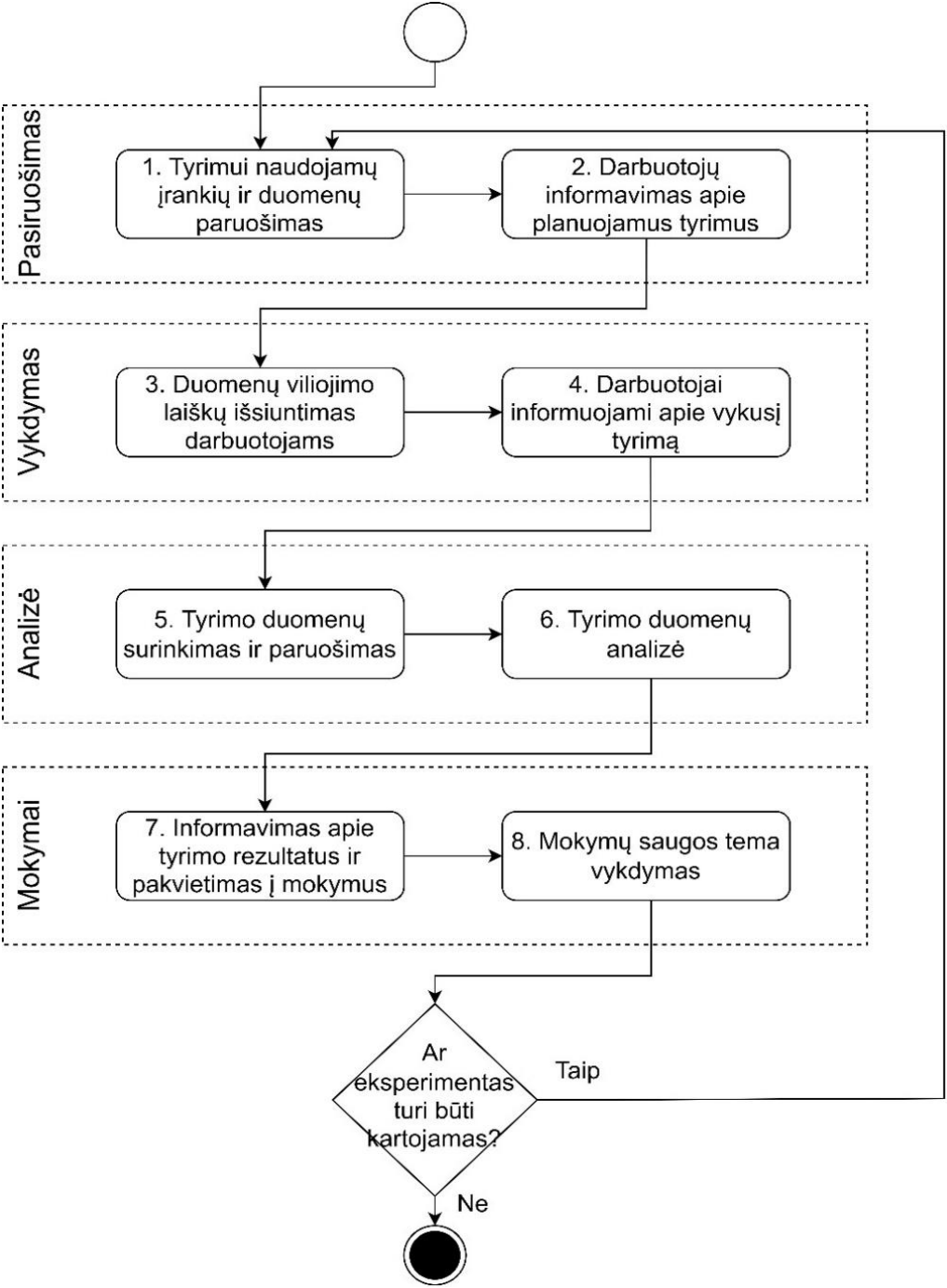
Problematika

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

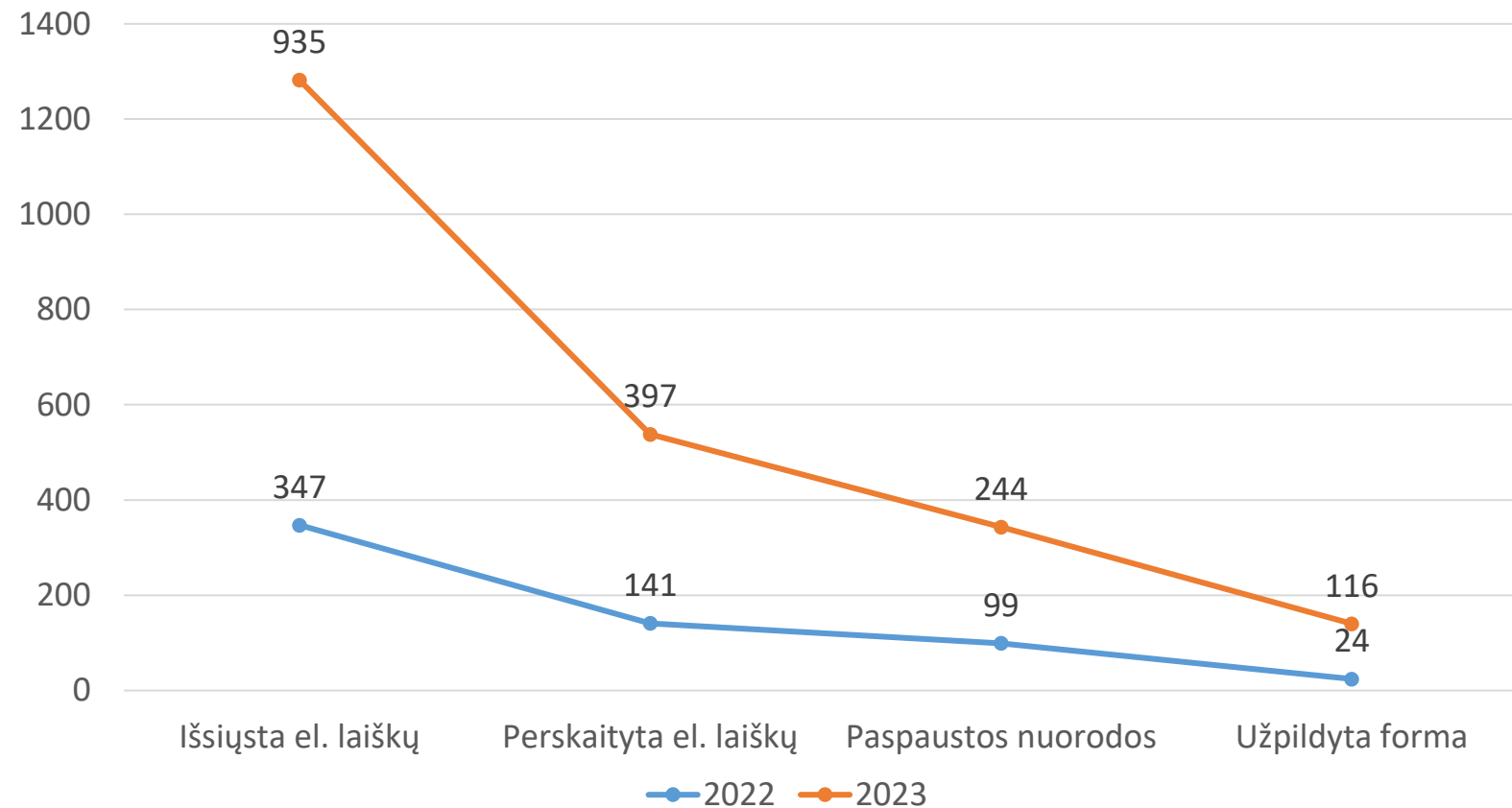
Užsikrėtus virusu pavagiama arba po “phishing” atakos (priklauso dar ir nuo versijos)*:

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

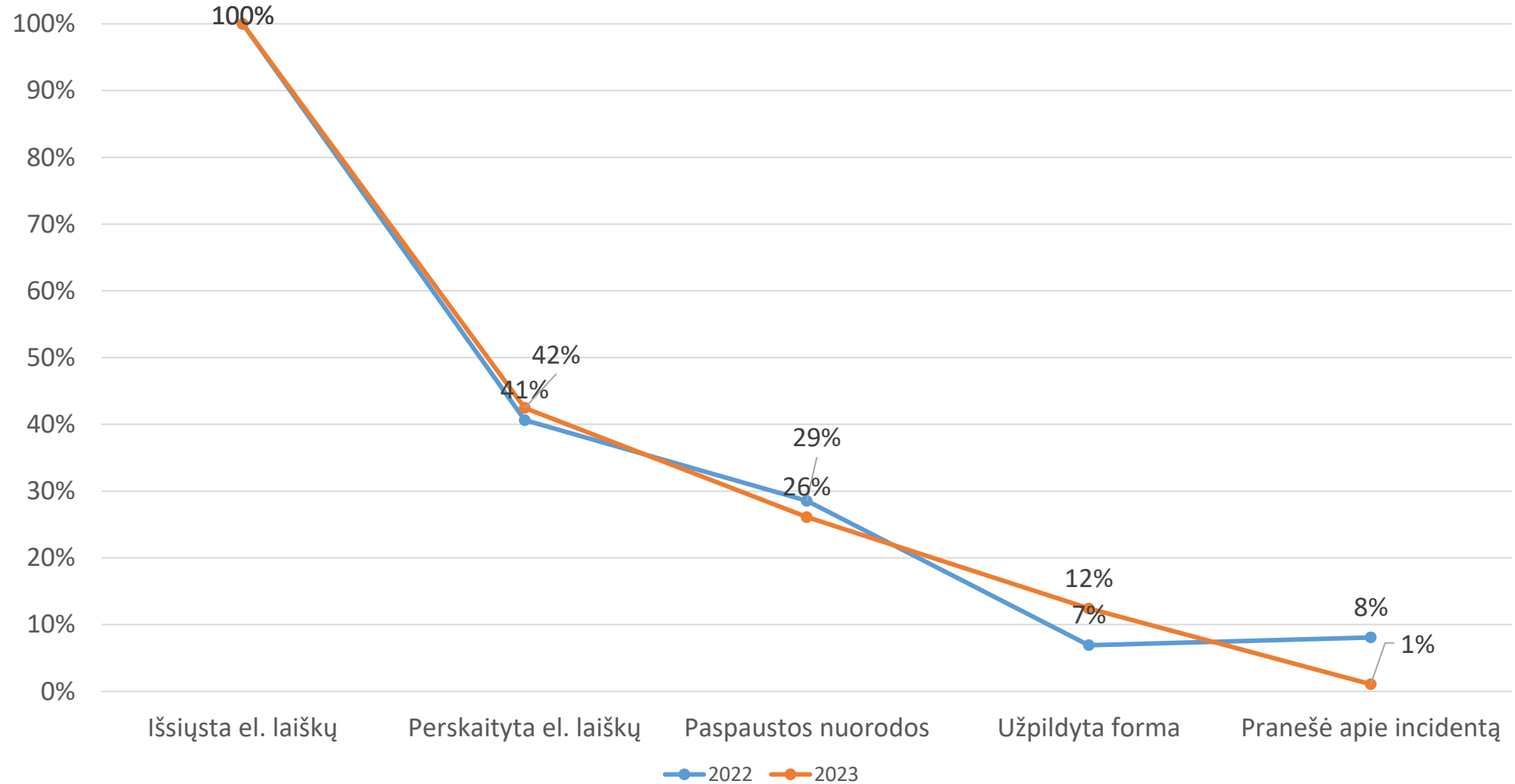
Eksperimentas



Rezultatai



Rezultatai

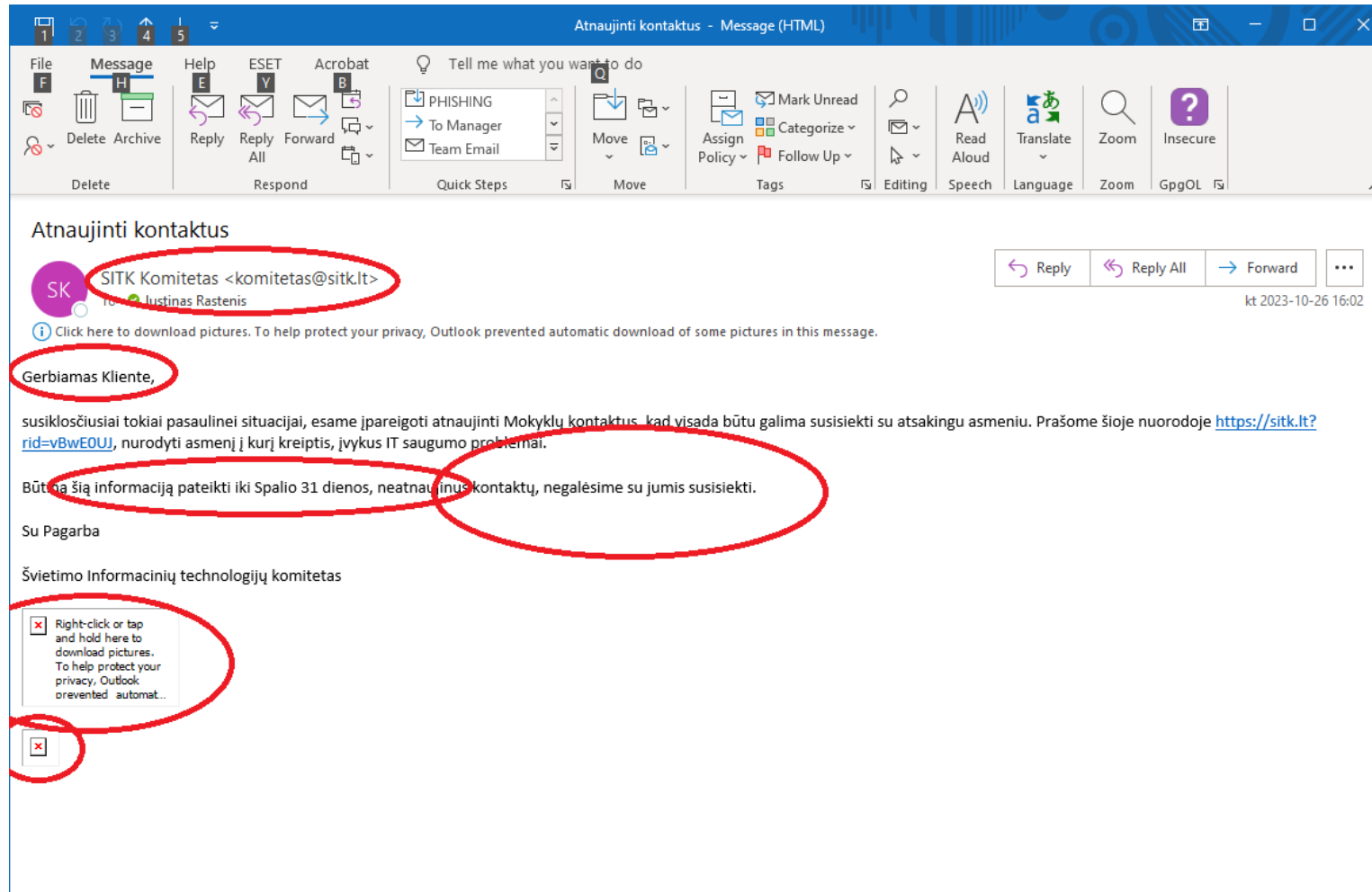


Atsparumo duomenų viliojimo atakos rezultatai



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 kiti)** ir paklausti ar tokį laišką siuntė.


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 Delete Respond Quick Steps Move Assign Policy Tags Mark Unread Categorize Follow Up Editing Speech Language Zoom Insecure GpgOL

Reikalingi veiksmai: Atnaujinkite savo asmeninę informaciją!!

 Paysera <support@paysera.com> tr 2023-10-18 09:07



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](#)

Jeį nesilaikysite šio pranešimo, kredito ir debeto operacijos gali būti atštos 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



Bandymas prisijungti užblokuotas - Message (HTML) (Read-Only)

File Message Help ESET Acrobat
Delete Archive Reply Reply Forward
Delete Respond Quick Steps Move Tags Editing Speech Language Zoom GpgOL

Bandymas prisijungti užblokuotas

Paysera <no_reply@paysera.lt>
To: [redacted]
pr 2023-10-23 13:24

Reply Reply All Forward

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

DĖMESIO!

Naudojantis nežinomu įrenginiu bandoma prisijungti prie jūsų Paysera paskyros. Informacija apie naudotoją: Lietuva (u, z)

Informacija apie įrenginį:

- Pavadinimas: jackpottle
- Modelis: SM-A530F
- OS: Android 8.0.0

Šis autentifikacijos bandymas buvo užblokuotas, tačiau būtina tai patikrinti. Ar tai buvote jūs?

Taip, tai buvau aš

PATVIRTINTI ĮRENGINĮ IR PRISIJUNGTI

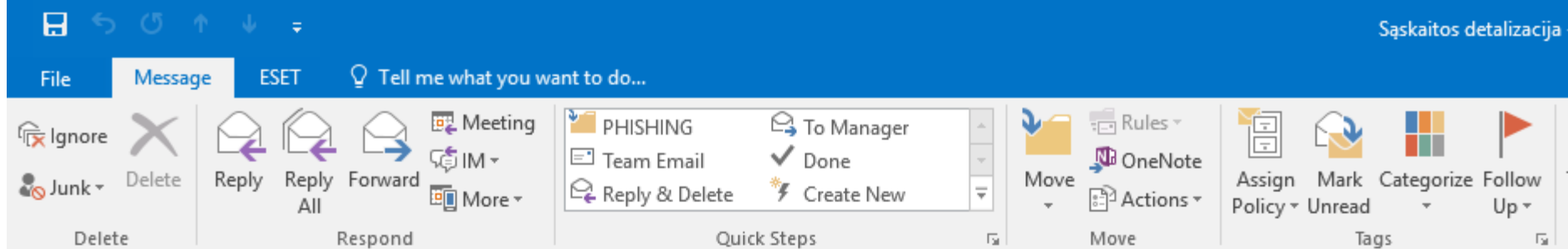
Ne, tai buvau ne aš

Jei tai buvote ne jūs, nesijaudinkite. Bandymą užblokavome, tačiau jums vertėtų prisijungti prie savo paskyros ir pakeisti slaptažodį. Taip pat galite [užblokuoti šį įrenginį](#) nuo tolesnių autentifikacijos bandymų, kad tai daugiau jums nekeltų rūpesčių.


Šis el. laiškas buvo išsiųstas po ngcNre***InGacC autentifikacijos bandymo.

Šis el. laiškas generuojamas automatiškai, todėl atsakymai mūsų nepasieks. Jei turite klausimų ar rūpesčių, apsilankykite mūsų [klientų aptarnavimo puslapyje](#) arba susisiekite su mumis pasinaudodami klientų aptarnavimo kontaktine informacija, kurią rasite [čia](#).

[Paysera](#)
Klientų aptarnavimo skyrius



 detalizacija . <detalizacija@enefit-lt.com> | [@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.



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.

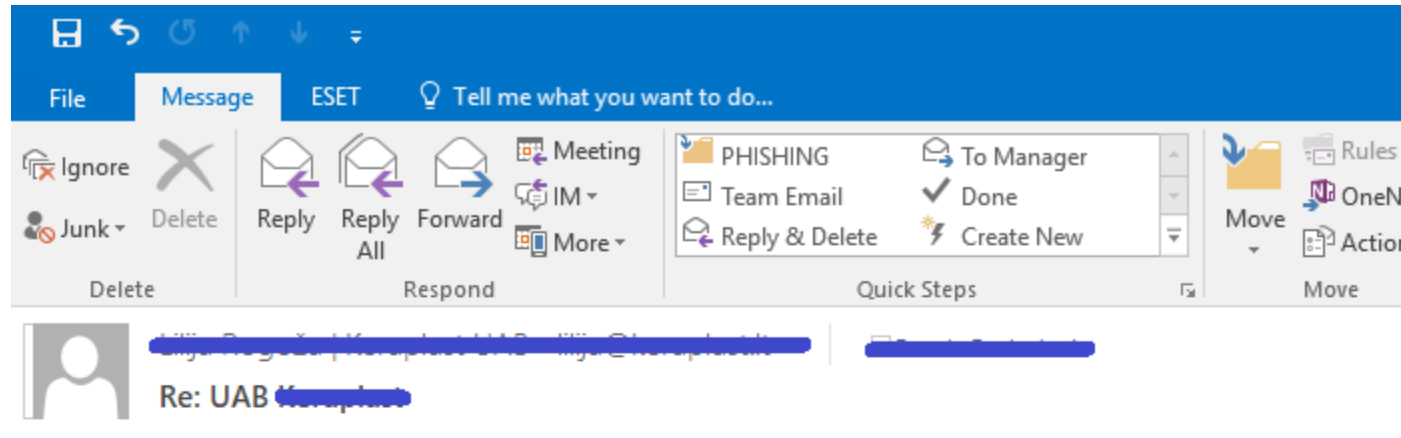
Enefit UAB  

+370 5 201 9141 | detalizacija@enefit.lt

V. Gerulaičio g. 10, LT-08200 Vilnius | www.enefit.lt



Naujausi



Taip, dokumentas buvo išsiųstas iš manęs anksčiau, maloniai prašome jį peržiūrėti ir grąžinti atgal.

Su geriausiais linkėjimais

[redacted]

Sent: Wednesday, May 11, [redacted]

[redacted]

Subject: FW: UAB [redacted]

Laba diena,

Patisklinkite ką čia siunčiate? Nesinori atidarinėti neaiškių nuorodų 😊

Pagarbiai,

[redacted]

[redacted]

[redacted]

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 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 koku 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)

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



← → ↻ vilniustech.lt/informaciniu-technologiju-ir-sistemu-centras/it-paslaugos-vilnius-tech-bendruomenei/saugumo-rekomendacijos/313357?lang=1



🔍 | 📍 | 👤 | [Mano VILNIUSTECH](#) | [EN](#)

[Apie mus](#) | [IT paslaugos VILNIUS TECH bendruomenei](#) | [IT paslaugos verslui](#) | [ES finansuojami projektai](#) | [IT pagalba](#) | [Kontaktai](#)

[Kompiuterių priežiūra](#)

[Elektroninis paštas](#)

[Belaidis ryšys](#)

[Virtualus privatus tinklas \(VPN\)](#)

[Nuotolinis prisijungimas \(be VPN\)](#)

[Dviejų faktorių autentifikacija](#)

[Spausdinimo paslauga](#)

[IS vystymas](#)

[IS priežiūra](#)



[Informacinių technologijų ir sistemų centras](#) > [IT paslaugos VILNIUS TECH bendruomenei](#) > [Saugumo rekomendacijos](#)

KIBERNETINĖ SAUGA

Informacinių technologijų ir sistemų centras, prižiūrėdamas universiteto informacines sistemas ir kompiuterines darbo vietas, diegia įvairias jų saugumą didinančias priemones, vykdo nuolatinius jų saugumo patikrinimus. Tačiau užtikrinti informacinių sistemų, darbo vietų saugumo vien techninėmis bei progaminėmis priemonėmis neužtenka, čia labai svarbus ir žmogiškasis faktorius. Žmogus, sistemų naudotojas, dažnai ir yra silpniausia kibernetinės saugos grandis. Todėl labai svarbu, kad universiteto darbuotojai, studentai kibernetinėje erdvėje elgtųsi visada atsakingai, būtų pasiruošę tinkamai įvertinti ateinantį į jų kompiuterius interneto duomenų srautą - el. laiškus, kitas gaunamas užklausas, nes už jų gali slypėti ir kibernetinė ataka, naudojanti socialinės inžinerijos metodus.

ITSC parengė atmintinę-instrukciją "[Kaip atpažinti kenkėjiškus laiškus](#)", kuri turėtų palengvinti atpažinti gaunamus pavojingus el. laiškus. Kviečiame susipažinti su ja.

Be to, ITSC vykdo kibernetines pratybas, organizuoja seminarus ar kitaip informuoja darbuotojus apie grėšiančius pavojus. Informaciją apie tai talpiname Mano VILNIUSTECH portale.

Taip pat rekomenduojame apsilankyti [Nacionalinio kibernetinio saugumo centro interneto puslapyje](#). Jame skelbiamos saugumo naujienos, ten galite patikrinti savo namų kompiuterį, kitus išmaniuosius įrenginius ar jie nėra pažeidžiami.

Ačiū kad klausėtės.
Klausimai?