]{iberdrošības aktualitātes & kiberhigiēnas pamati

Dana Ludviga

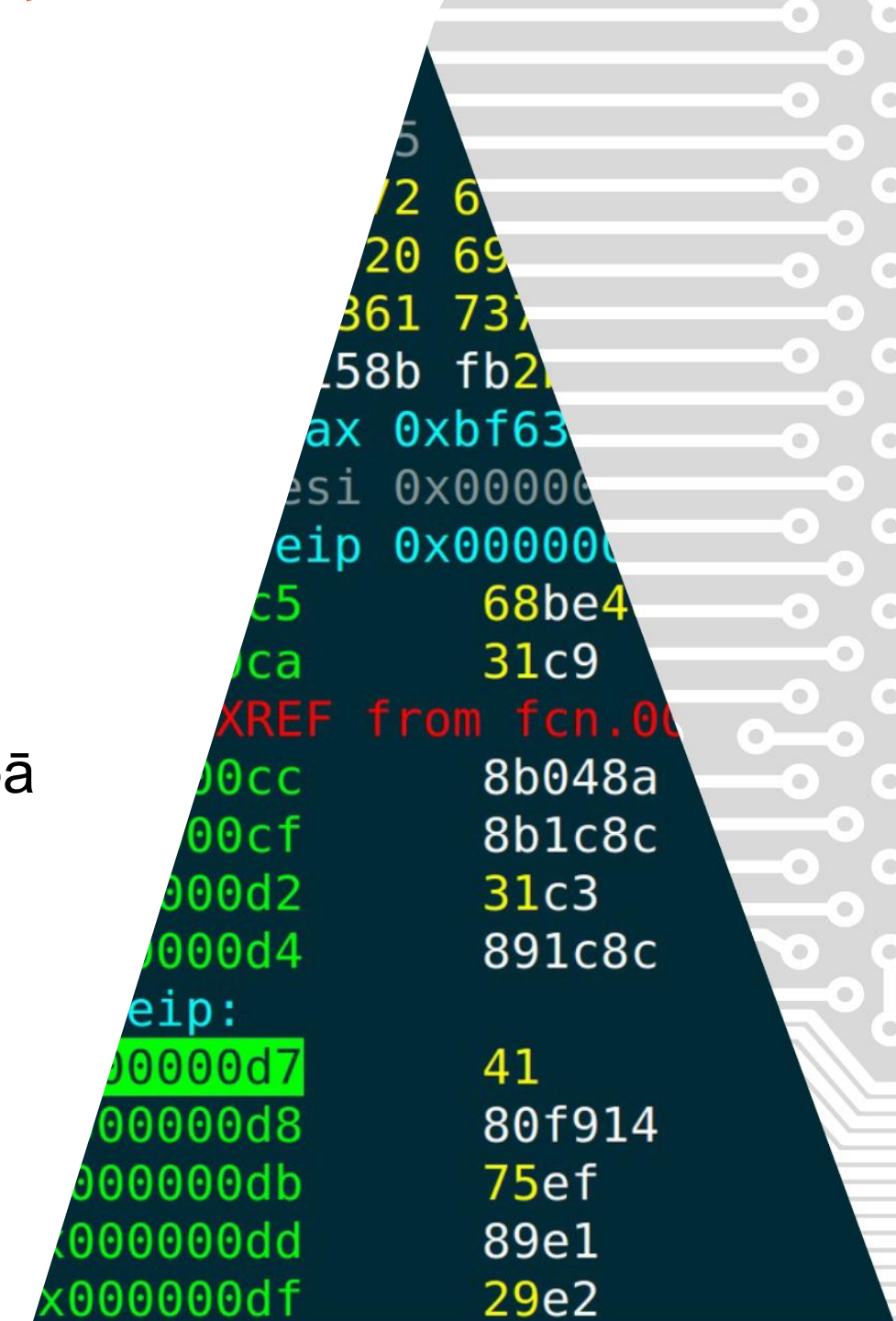
20.11.2025

CERT.LV
Kiberincidentu novēršanas institūcija

CERT.LV

CERT.LV

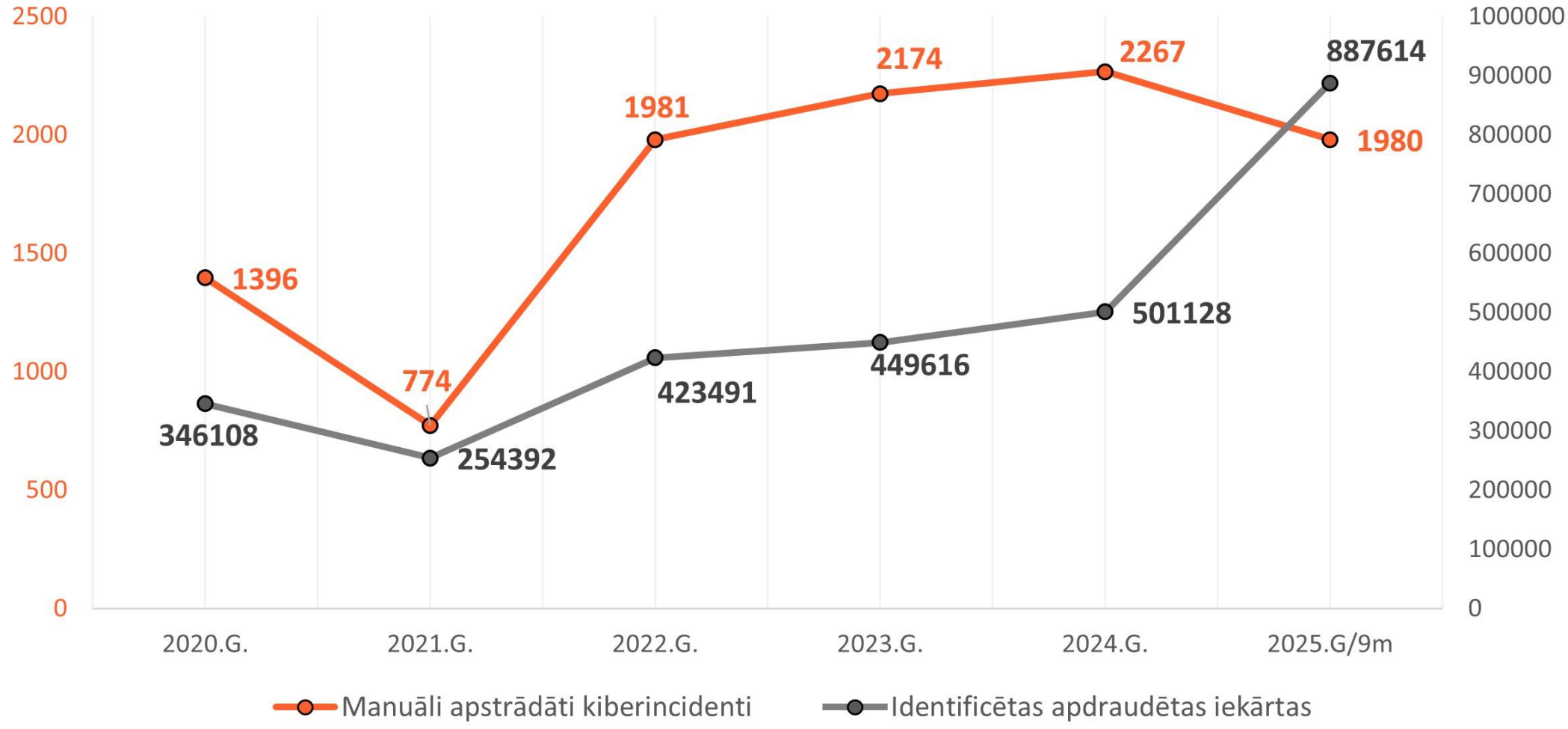
- **Kiberincidentu novēršanas institūcija**
- Atrodamies Latvijas Universitātes Matemātikas un informātikas institūtā (LUMII)
- Darbojamies LR Aizsardzības ministrijas pakļautībā Nacionālā kiberdrošības likuma (NKDL) ietvaros
- Visi pakalpojumi ir **bez maksas**
- Komanda darbojas kopš 2006.gada



CERT.LV

Latvijas kiberapdraudējuma līmenis noteikts kā augsts kopš 2022.gada janvāra

Kiberapdraudējumu dinamika 5 gadu griezumā



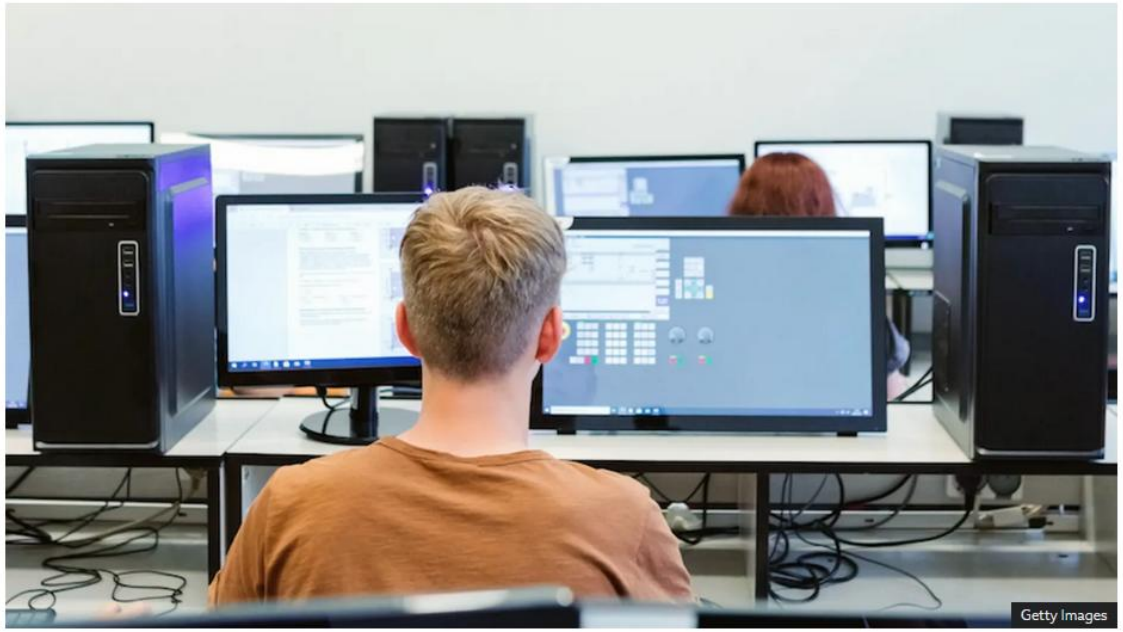
BBC

Children hacking their own schools for 'fun', watchdog warns

11 September 2025

Share Save

Joe Tidy
Cyber correspondent, BBC World Service


Getty Images

The Information Commissioner's Office (ICO) has issued a warning about what it calls the "worrying trend" of students hacking their own school and college IT systems for fun or as part of dares.

It has told teachers that they are failing to understand and recognise what it calls the "insider threat" pupils pose.

It says more the majority of so-called "insider" cyber attacks and data breaches in education settings - meaning they have been carried out by someone with access to internal systems - originate with students.

"What starts out as a dare, a challenge, a bit of fun in a school setting can ultimately lead to children taking part in damaging attacks on organisations or critical infrastructure," said Heather Toomey, Principal Cyber Specialist at the ICO.

The Guardian

This article is more than **1 month old**

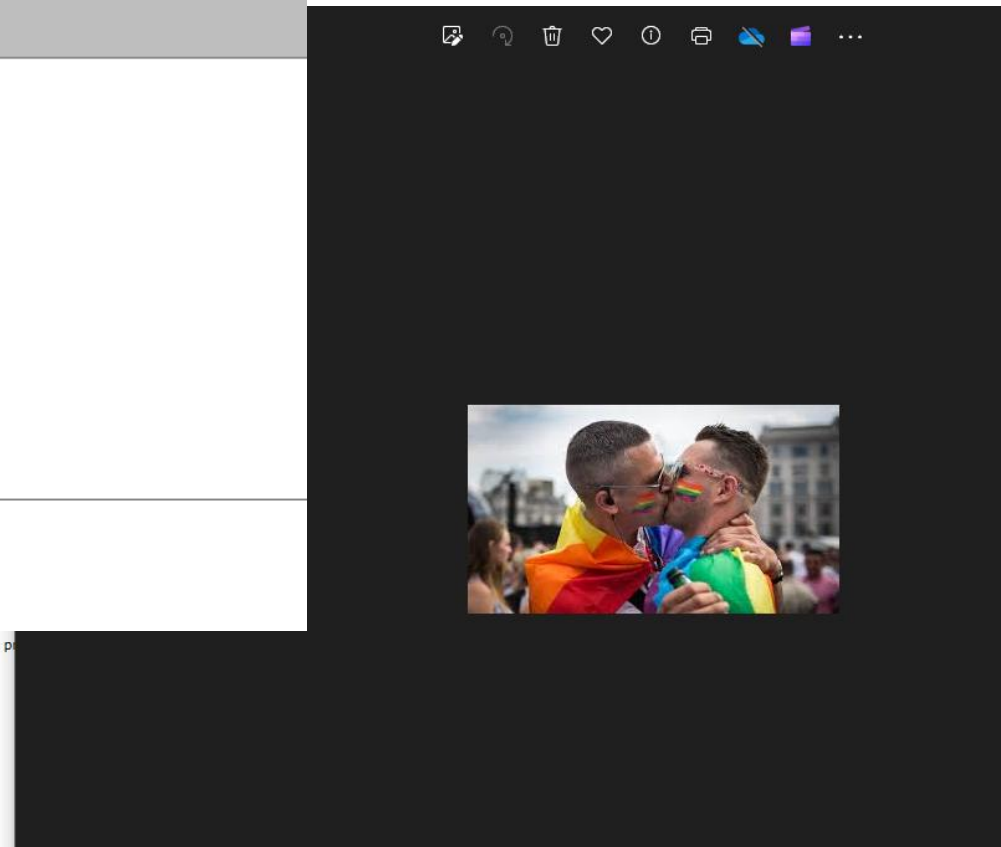
Six out of 10 UK secondary schools hit by cyber-attack or breach in past year

Hackers are more likely to target educational institutions than private businesses, government survey shows

State schools might be more vulnerable to attacks because of pressure on funding and a lack of

NEESI VĀJĀKAIS ĶĒDES POSMS

Skolēni atrod skolotājas e-klases piekļuves datus un samaina atzīmes, intereses pēc izsūta nevēlamu/smieklīgu saturu



GOZI vīruss

Adresāti: Adresātu saraksts
Autors: [redacted](skolēns), 7.a
Datums: 17.06.2022 09:14
Temats: Svarīgs paziņojums

Labdien, vēlējos arī Jums paziņot kādas nejēdzības notiek izglītības iestādē, kur mācās mūsu bērni!

Sīkāku informāciju lūdzu skatīt manā iesniegumā, zemāk pievienotajā saitē!

iesniegums

ar cieņu,

[redacted]mamma

Galvenās tendences & draudi:

1. **Krāpšana**
   - Pikšķerēšana, vikšķerēšana, smikšķerēšana, kvikšķerēšana
   - u.c.
2. **Ievainojamības** (CVE)
3. **Ļaunatūras & izspiedējvīrusi**
4. **Piegādes ķēdes uzbrukumi**
5. **Pakalpojumu pieejamība**
   - DDOS
   - GPS signālu bloķēšana

Galvenās tendences & draudi:

1. **Krāpšana**
   - Pikšķerēšana, vikšķerēšana, smikšķerēšana, kvikšķerēšana
   - u.c.
2. **Ievainojamības** (CVE)
3. **Ļaunatūras & izspiedējvīrusi**
4. **Piegādes ķēdes uzbrukumi**
5. **Pakalpojumu pieejamība**
   - DDOS
   - GPS signālu bloķēšana

FINANŠU NOZARES ASOCIĀCIJA

Ik mēnesi izdodas nosargāt miljonu eiro, vēl tik pat - izkrāpj

Novērstais krāpšanas apmērs 2024. gadā: **12 152 718 eiro**

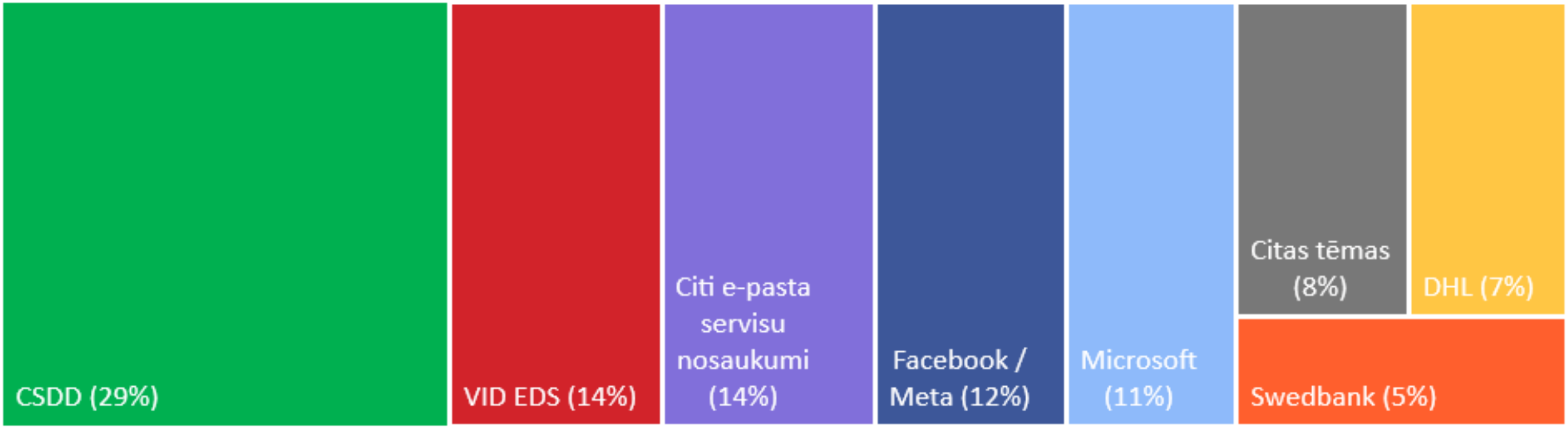
Izkrāptās naudas apmērs 2024. gadā: **15 529 599 eiro**

2025. GADA SĀKUMĀ LIELĀKĀS IZKRĀPTĀS SUMMAS

https://www.vp.gov.lv/lv/jaunums/iedzivotaji-turpina-krapniekiem-atdot-skaidru-naudu-kreditkartes-un-atklat-bankas-kontu-datus

Izplatītākās pikšķerēšanas kampaņas, izmantojot zināmu organizāciju nosaukumus

(procentuālā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gada 3. cet.)



Krāpniecība CSDD vārdā

- Hide quoted text -

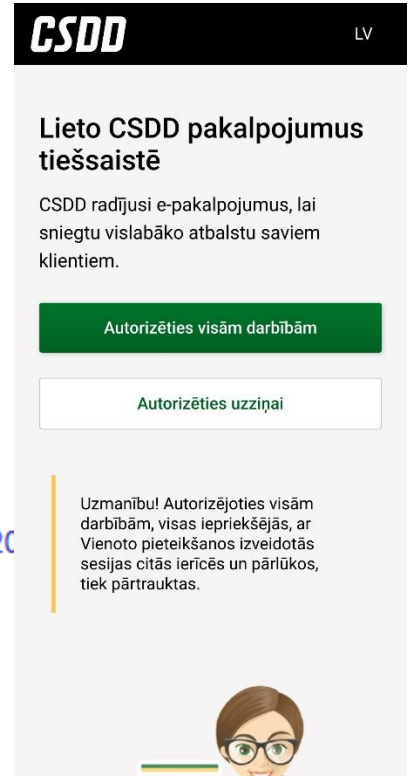
------ Forwarded message --------
Subject: FWD: CSDD info
Date: Fri, 28 Feb 2025 09:15:50 +0200
From: noreply@csdd.gov.lv <55177@199.lv>
To: [redacted]

Sakarā ar CSN pārkāpumu (datums 23.01.2025, lēmuma numurs 23764267274769, pārkāpuma pants 55.12, lēmuma spēkā stāšanās datums 28.02.2025), Jums ir piemērots naudas sods 160.00 EUR. Iepazīties ar lēmumu var e-CSDD. Ceļu satiksmes likuma 43.pants nosaka pakalpojumu saņemšanas ierobežojumus, ja sods nav samaksāts likumā noteiktā termiņā - 30 dienu laikā.

Maksājuma rekvizīti:

Saņēmējs: **VALSTS KASE**
Reģistrācijas Nr.: **90000050138**
Konta Nr.: **LV31TREL1060141015220**
Saņēmēja banka: **VALSTS KASE**
Bankas kods: **TRELLV22**
Maksājuma summa: **160.00 EUR**
Maksājuma mērķis: **23764267274769**
Maksājumu var veikt **e-CSDD**

* Informācija no Transportlīdzekļu un to vadītāju valsts reģistra sagatavota 28.02.2025
Šis e-pasts ir izveidots automātiski, lūdzam uz to neatbildēt.



Krāpniecība CSDD vārdā

- Hide quote

------ Forw

Subject: FV

Date: Fri, 2

From: nore

To: [redacted]

Sakarā a

Jums ir p

ierobežo

Maksāju

Saņēm

Reģistr

Konta N

Saņēm

Bankas

Maksāj

Maksāj

Maksāju

* Informā

Šis e-pas

Vienotās pieteikšanās modulis

https://csddkonts.lv-bridinajums.net/pages

Vienotās pieteikšanās modulis EN

Piekrītu identifikācijas veikšanas noteikumiem un manu datu (vārda, uzvārda un personas koda) nosūtīšanai e-pakalpojuma sniedzējam – Ceļu satiksmes drošības direkcija (S.Eizenšteina iela 6, Rīga, LV-1079).

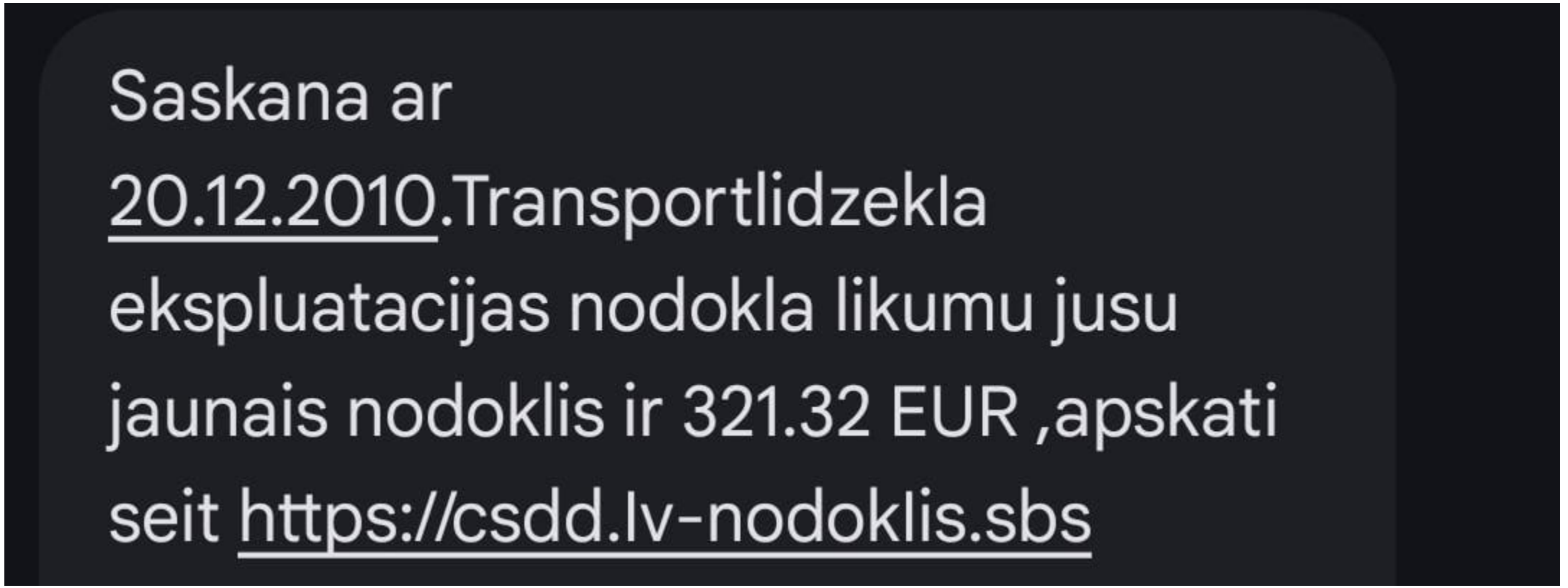
Identifikācija ar banku identifikācijas līdzekli

Citadele

SEB

INDUSTRA

Luminor


Saskana ar
20.12.2010.Transportlidzekla
ekspluatacijas nodokla likumu jusu
jaunais nodoklis ir 321.32 EUR ,apskati
seit https://csdd.lv-nodoklis.sbs

eds-vid.pages

Valsts ieņēmumu dienests

Ceram, ka Jums viss ir labi. Lai turpinātu nodokļu atmaksas procesu, lūdzu, izpildiet sekojošās instrukcijas. Izmantojiet savu viedtālruni, lai skenētu pievienoto QR kodu un ievadītu savu personīgo kodu, kā norādīts. Šī procedūra ir izstrādāta, lai aizsargātu Jūsu datus un nodrošinātu drošu darījumu veikšanu. Svarīgs paziņojums: Ja Jūs neveiksiet šo darbību laikus, Jūsu atmaksa var tikt aizkavēta vai pat atcelta. Tādēļ ir ļoti svarīgi, lai Jūs skenētu QR kodu un veiktu nepieciešamos soļus, lai saņemtu savu gada atmaksu.

Instrukcijas:
Ieslēdziet savu viedtālruņa kameru vai izmantojiet QR koda skenēšanas lietotni.
Nolasiet pievienoto QR kodu.
Izpildiet ekrānā redzamās instrukcijas, lai ievadītu savu personīgo kodu un pabeigtu nepieciešamos soļus.

Vai arī Jūs varat noklikšķināt uz zemāk esošās pogas, lai tiešsaistē piekļūtu nepieciešamajai lapai un veiktu nepieciešamās darbības.
Lūdzu, pārliecinieties par šī paziņojuma autentiskumu pirms turpināšanas, lai aizsargātu savu personīgo informāciju.
Paldies par Jūsu ātro uzmanību un sadarbību.
Ar cieņu,

NACIONĀLAIS ATTĪSTĪBAS PLĀNS 2020 | EIROPAS SAVIENĪBA Eiropas Reģionālās attīstības fonds
IEGULDĪJUMS TAVĀ NĀKOTNĒ

Valsts ieņēmumu dienests
Elektroniskās deklarēšanas sistēma

LV EN

Nodokļu atmaksas kopsavilkums

Tālāk ir sniegts kopsavilkums par jūsu automātisko nodokļu atmaksu elektroniski, izmantojot EDS tiešsaistes portālu. Atgādinām, ka par automātisku veidlapas iesniegšanu mēs maksājam 10 €.

PVN aprēķina bāze uz rēķina	08/01/2025
Taksācijas periods	08/01/2025-08/01/2025
Valūta	EURO
PVN atmaksa par pirkumu s[T1]	232.57
PVN atmaksa par citiem izdevumiem [T2]	74.24
Pilna nodokļu atmaksa (bez izmaiņām)	306.81
Automātiskās nodokļu atmaksas maksa	-10.00
Galīgā nodokļu atmaksas summa	296.81 €

Izvēlieties nodokļu atmaksas metodi

Saņem ar bankas pārskaitījumu
Izvēlieties savu banku

Swedbank | SEB | Citadele | RIETUMU | BluOr Bank

67120000
Terms of use
Processing personal data in the SRS
Cookie Use Policy
Become a user

Swedbank

Nosūtīts no
SRS Latvia

Date of transfer:
01/08/2025

Summa
296.81 €

Kartes numurs
**** **** ****

Izvēlieties autentifikācijas veidu

Smart-ID

Lietotāja kods

Personela kods

Turpināt

ESI UZMANĪGS!

Uz autostāvvietu apmaksas automātiem **izvietotas krāpnieciskas uzlīmes.**

IESAKĀM!

Nekādā gadījumā neskenē šādus vai līdzīgus kvadrātkodus - tie var novest uz krāpnieciskām vietnēm, kur tiek izkrāpta nauda vai personīgā informācija.

RĪGAS SATIKSME

Investīciju krāpniecība

Delfi

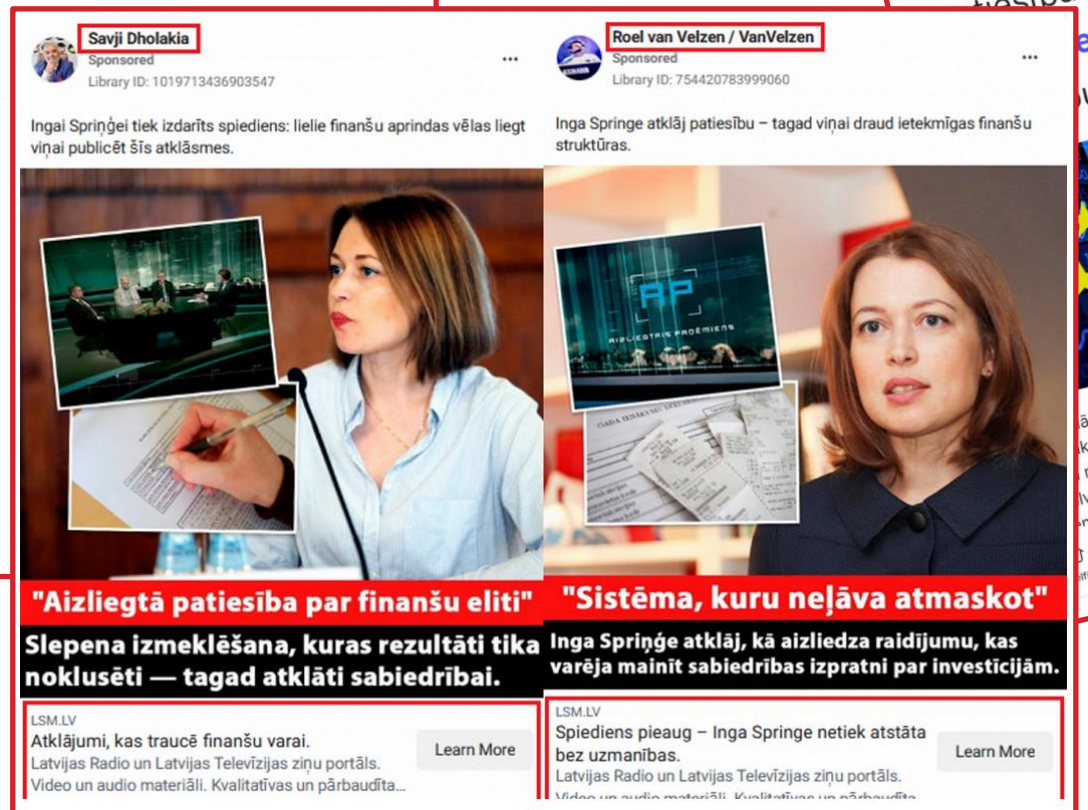
Ziņas Bizness Life Sports Kultūra Auto Cālis Tasty Abonē Pieslēdzies

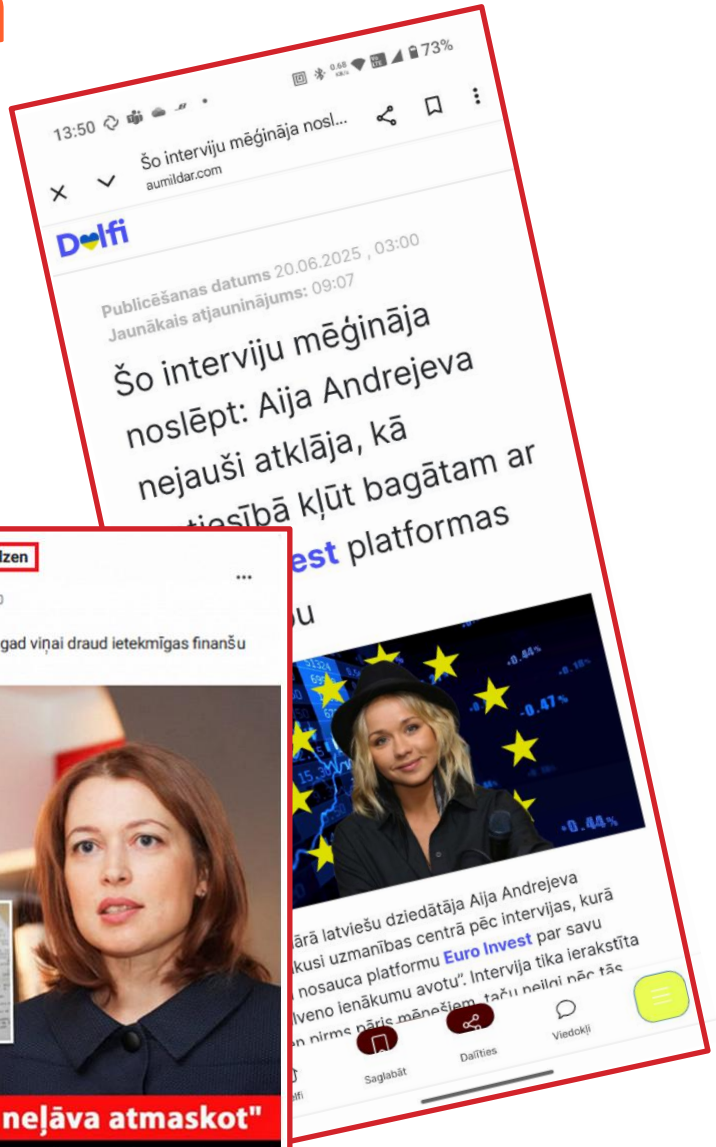
VERSIJAS 02.04.2025 11:01:51

Pēc Ventspilī atrastā mirušā 24 gadus vecā dēla – vēl viens trieciens: „Nespēju noticēt, ka tā ir patiesība." (8)

Kārlis Arājs, Nacionālo ziņu nodaļas redaktors

Foto: Privātais arhīvs





„Domāju, ka viņš tikai sēž pie pudeles un dzer, bet izrādās, ka viņš bija daudz apdāvinātāks un gudrāks, nekā mēs zinājām," – ar pārsteigumu un asarām acīs sacīja māte. Viņa atcerējās, ka dēls dažreiz pieminēja papildu nodarbošanos, taču ģimene tam nepievērsa lielu uzmanību.

Pēc šīs sarunas bankas darbiniece sagatavoja nepieciešamos dokumentus un apliecināja, ka konts tiks slēgts, bet nauda tiks pārskaitīta mātei 14 darba dienu laikā. „Tagad, kad viss kļūst skaidrs, jūtu gan skumjas, gan dīvainu mierinājumu – vismaz zinu, ka viņš centās," – noslēdzot sarunu, sacīja sieviete. Tikmēr izmeklēšana par jaunieša nāves cēloni joprojām turpinās.

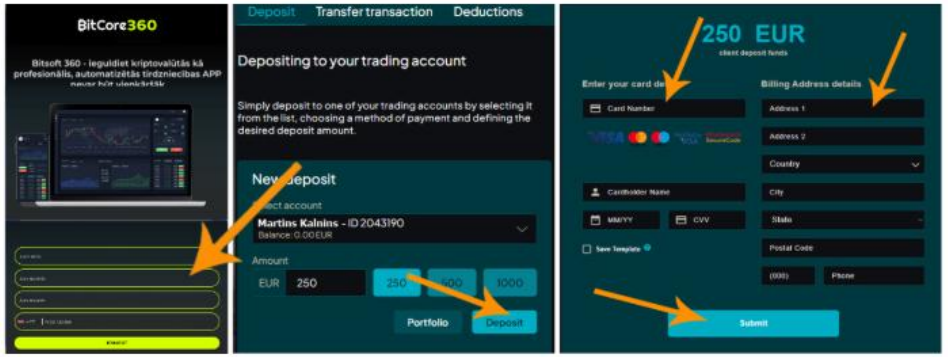
„BitCore360" platformas pētījums: vai ir vērts ieguldīt?

DELFI.lv izpētes komanda veica detalizētu analīzi par ieguldījumu platformu „„BitCore360"", lai novērtētu tās likumību un ienesīgumu. Praktiskā analīze sniedza interesantus rezultātus, kurus piedāvājam visiem mūsu lasītājiem.

DELFI redakcija sāka patstāvīgi interesēties, kas ir „BitCore360".

Kā izrādījās,tā ir jaunizveidota elektroniskā platforma, kurā tiek izmantotas tādas mākslīgā intelekta tehnoloģijas kā **"ChatGPT"** un **"Midjourney"**. Šo divu tehnoloģiju apvienošanas rezultātā patērētājiem tiek garantēta minimāla peļņa no ieguldījumiem. DELFI testēšanas laikā, iemaksājot sākotnējo 200 eiro iemaksu, programmas rezultāti bija šokējoši:

ĪSA INSTRUKCIJA, KĀ REĢISTRĒTIES:



Nākamajā dienā mēs pieslēdzāmies „BitCore360" un redzējām, ka kontā jau ir uzkrāti **7180,25 eiro**, kurus mēs uzreiz mēģinājām pārskaitīt uz savu bankas kontu, lai pārbaudītu, vai bankas pārskaitījumi tiešām tiek veikti, vai arī tie nav tikai cipari telefona vai datora ekrānā.

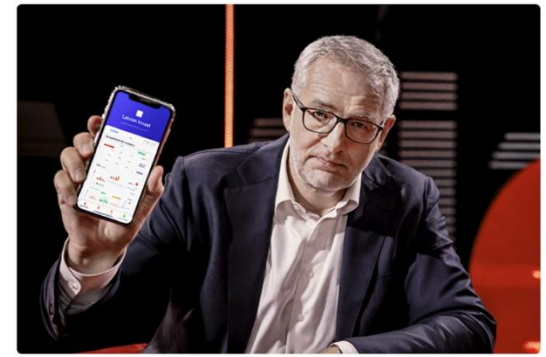
Un patiešām – naudu uz bankas kontu veiksmīgi saņēmām pēc dažām stundām. DELFI komanda šos līdzekļus ziedoja karojošajai Ukrainai, kas šobrīd cīnās par visu pasauli un kurai ir ļoti svarīga jebkāda palīdzība.

POLITIKA 27.10.2025, 14:13

Sensacionālas ziņas:10 000 eiro tautai jeb kāpēc varas pārstāvji noraida iespēju iegūt pasīvos ienākumus

Ziņu nodaļa
Jauns.lv/LETA

Evika Silina: Es saprotu sociālo problēmu asumu...

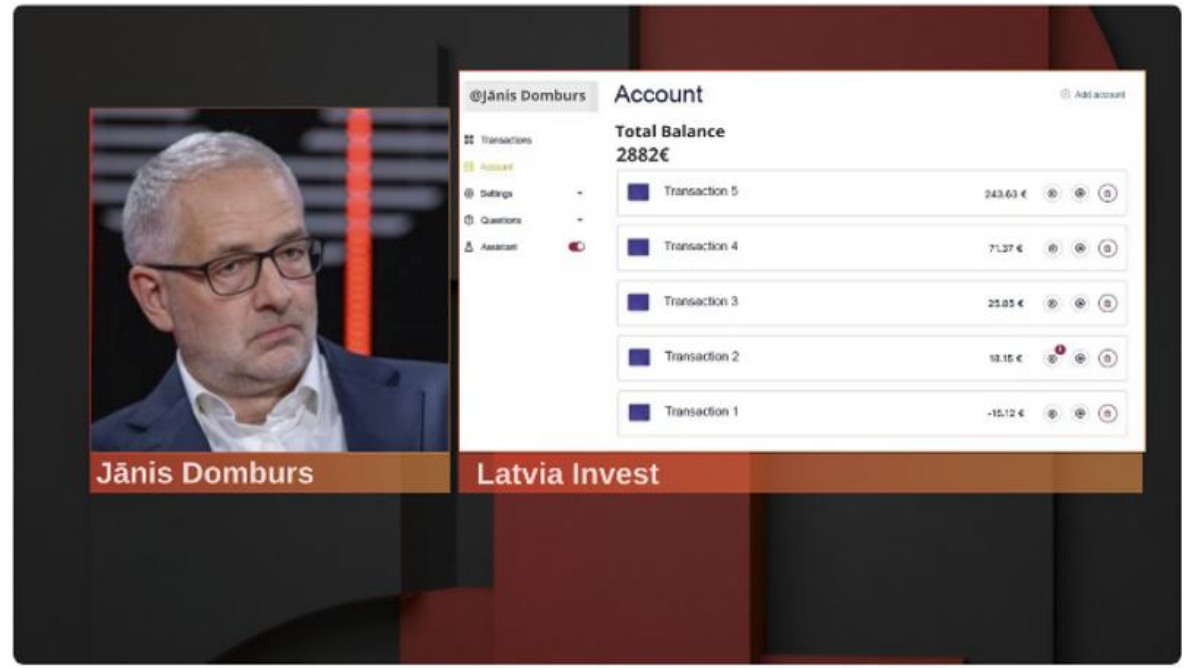


Jānis Domburs: Pāriesim no vārdiem pie darbiem. Tieši pirms nedēļas es reģistrējos "Latvian Invest" un iemaksāju 250 eiro. Es vēl neesmu pārbaudījis bilanci — izdarīšu to tagad, jūsu klātbūtnē. Vai drīkstu?

Evika Silina: Es nedomāju, ka tā ir laba doma...

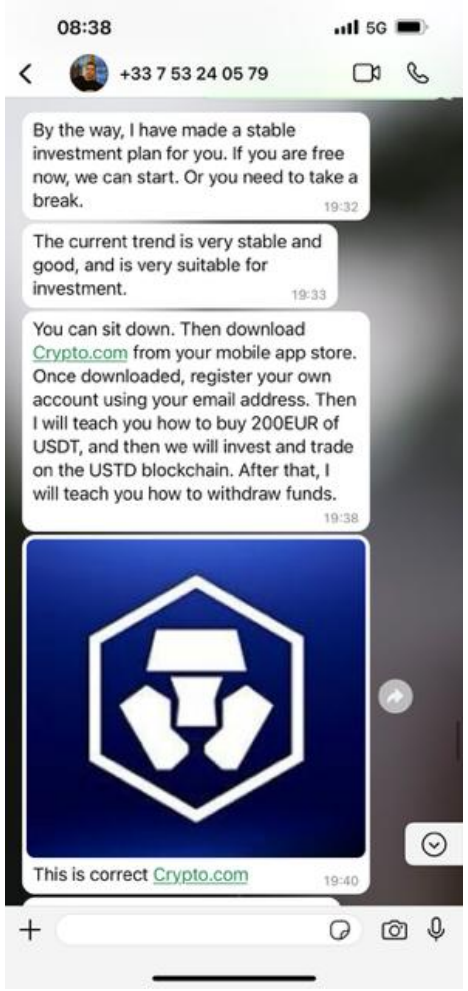
Jānis Domburs: Tas ir neticami... Mana bilance — 2882 eiro. Tikai nedēļas laikā

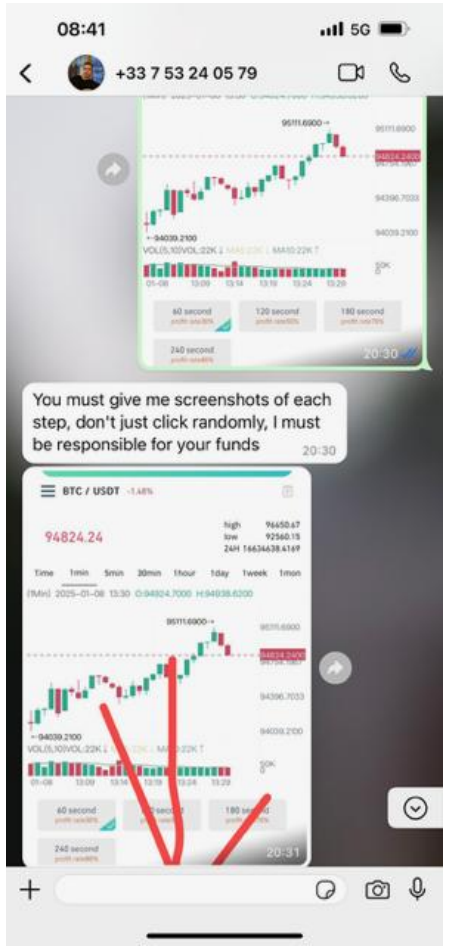
Jānis Domburs: Jūs redzat šos ciparus, Evika. Tā nav maģija. Tā ir tehnoloģija. Un pats ironiskākais — šo platformu izveidojis nevis starptautisks konglomerāts, bet parasts puisis no Valmieras. Mūsējais, latvietis.

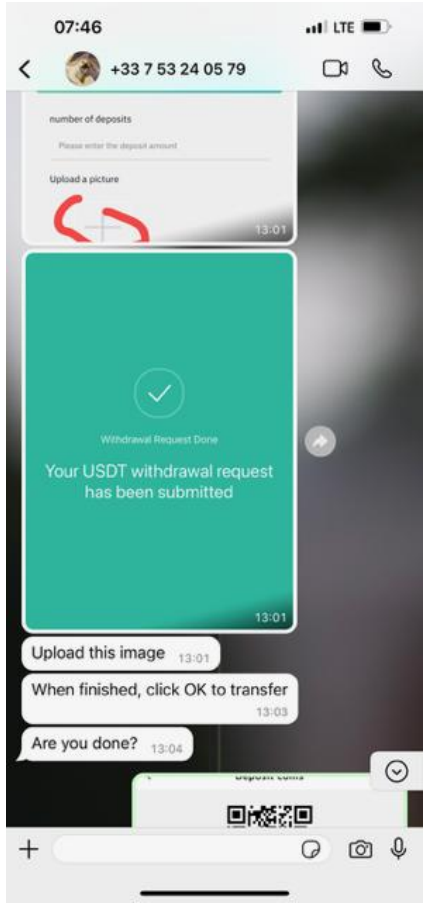


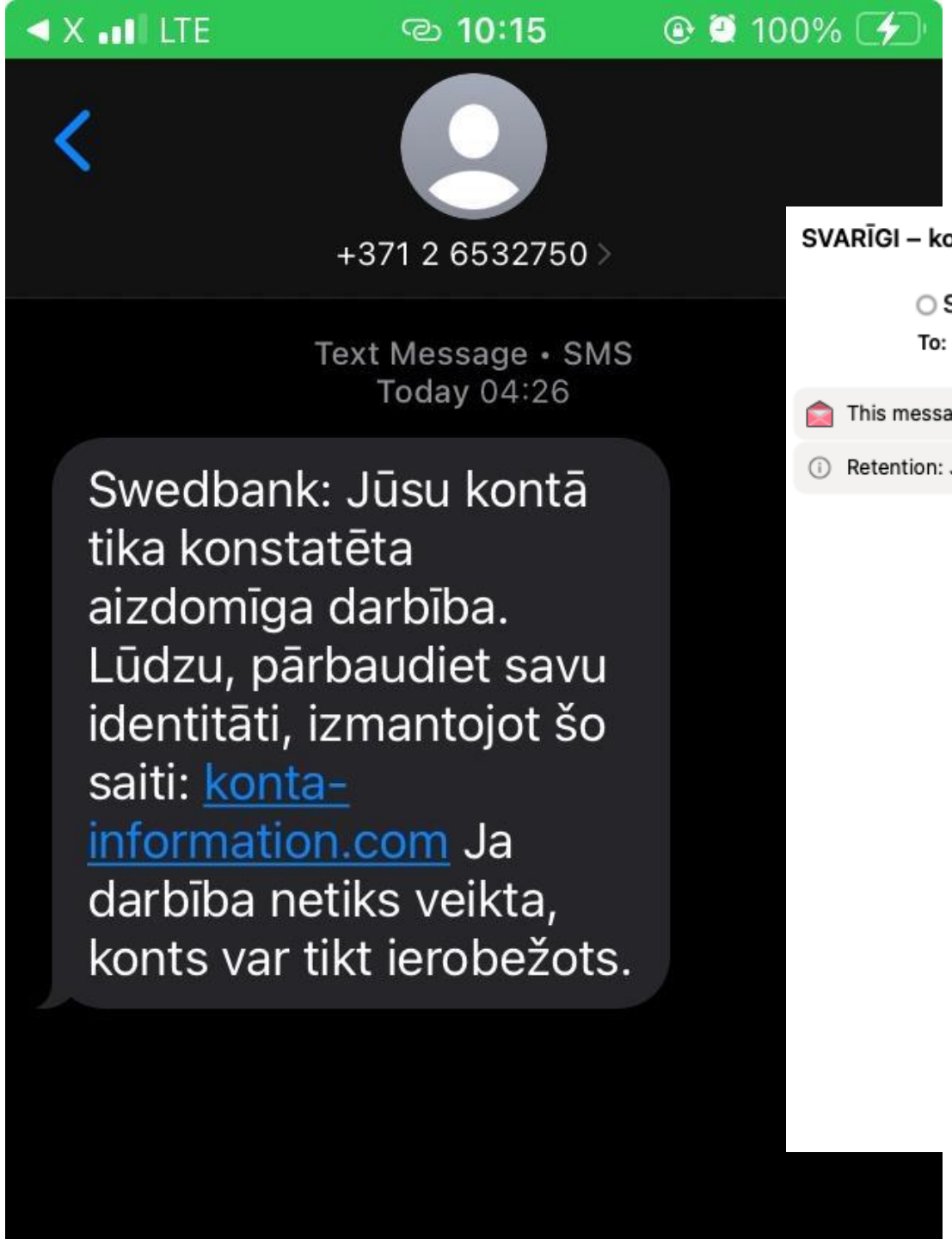
CERT.LV

Krāpniecības Tinder









SVARĪGI – konta atjaunināšana

SEB <contact@tatematsuchuzo.co.jp>

To: Andris Gabrānovs

This message appears to be Junk. Links and other functionality will not work.

Retention: Junk Email Expires: 23/05/2025.

Cienījamais klients,

Sakarā ar jaunajām drošības prasībām ir steidzami nepieciešams atjaunināt Jūsu SEB kontu. Atjaunināšana tiek veikta droši, un mūsu komanda Jūs vadīs visā procesa gaitā.

ATJAUNINĀT TAGAD

Savlaicīgas darbības ir būtiskas, lai nodrošinātu drošu un nepārtrauktu pakalpojumu izmantošanu.

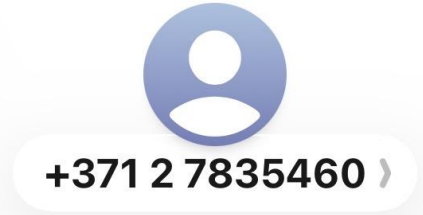
Piezīme: Lūdzu, neatveriet citus logus un neatstājiet šo lapu, līdz atjaunināšana nav pilnībā pabeigta.

Paldies, ka uzticaties SEB.

SEB banka

Smart-ID

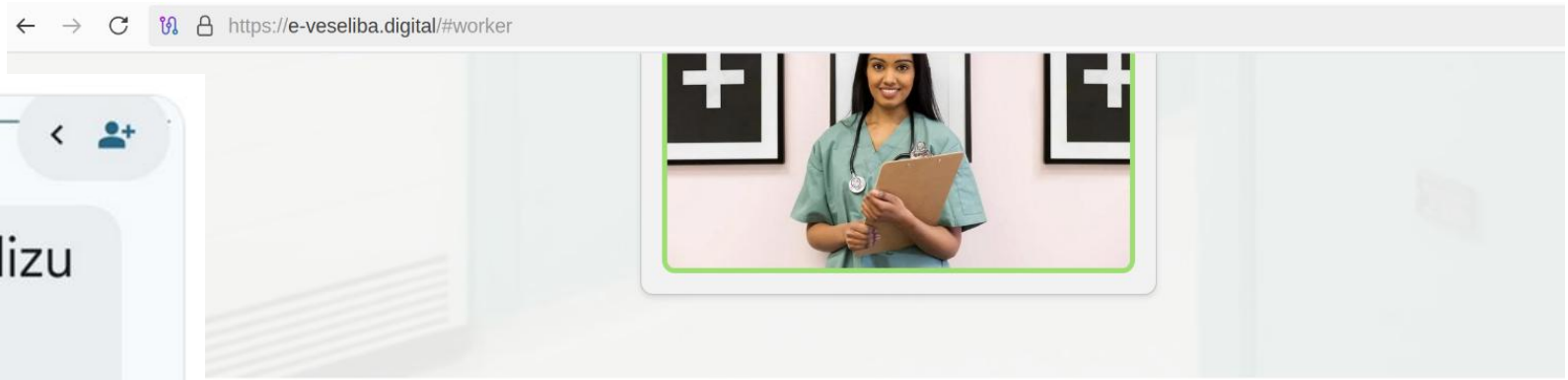

17:09
+371 2 3280137
Text Message • SMS
Today 17:04
[Smart-ID]
Jūsu Smart-ID derīguma termiņš beidzas 31.10.2025.
Lūdzu, atjaunojiet savu reģistrāciju, izmantojot šo saiti:
https://20250103.com


+371 2 7835460
Text Message • SMS
Today 20:12
[SWEDBANK]
Jūsu Smart-ID reģistrācija beigsies 25.10.2025.
Atjaunojiet savus datus, izmantojot šo saiti: https://reaktivejiet-swed.com/1

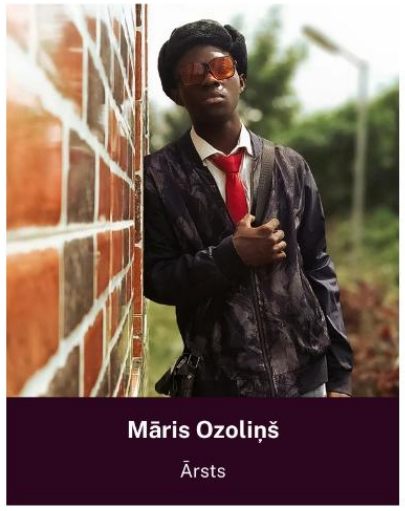

+371 28 770 868
Today, October 26
[SWEDBANK]
Jūsu Smart-ID reģistrācija beigsies 26.10.2025.
Atjaunojiet savus datus, izmantojot šo saiti:
https://atjaunot.com
20:51

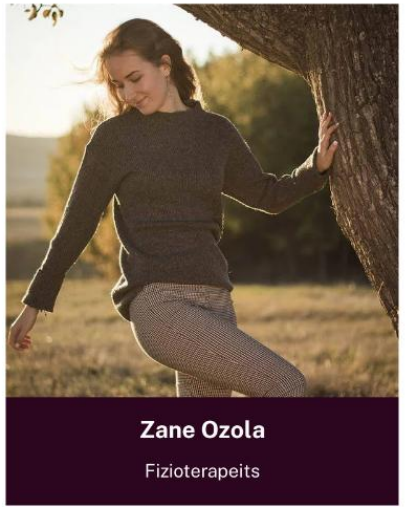

[SWEDBANK]
Jūsu Smart-ID reģistrācija beigsies 27.10.2025.
Atjaunojiet savus datus, izmantojot šo saiti:
https://atjauninat-smart.com

e-veseliba.digital



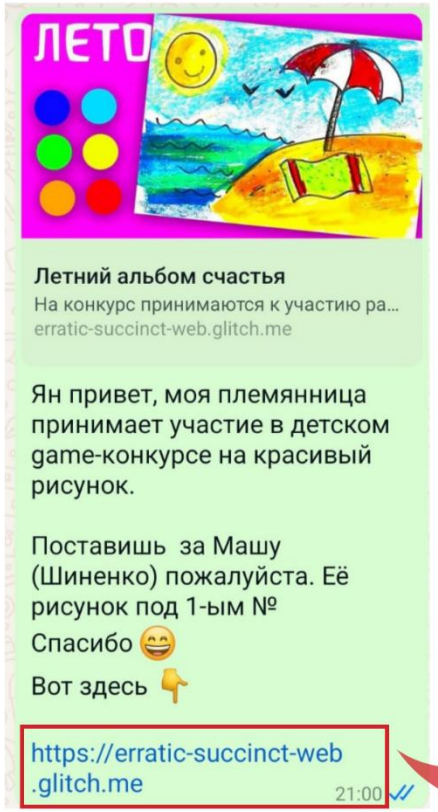
Mūsu darbinieki

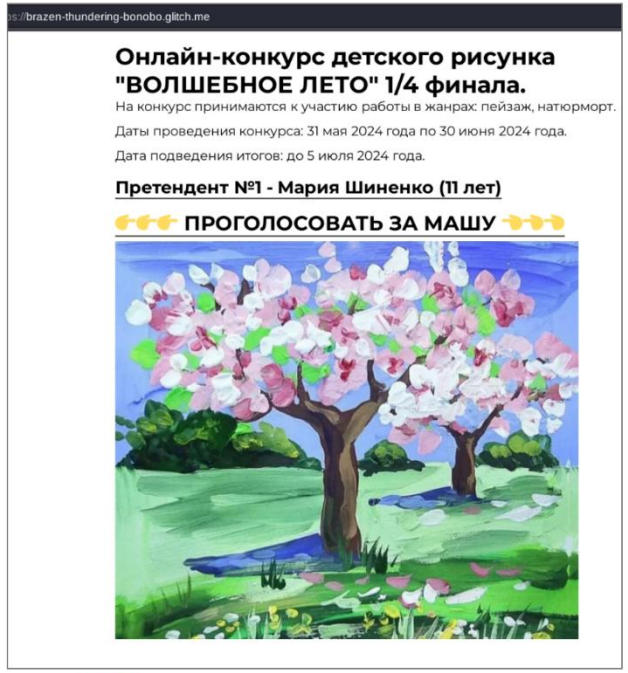




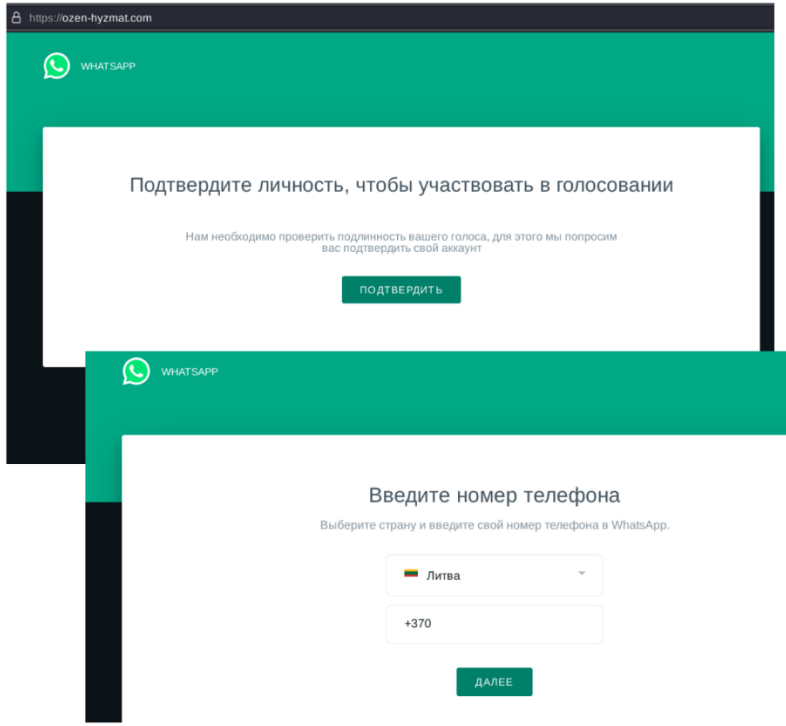
Whatsapp/Telegram/Signal krāpniecība

- Pievieno Jūsu Whatsapp/Telegram kontu citai iekārtai/nr ar mērķi izspiegot vai izplatīt krāpnieciskas ziņas jūsu vārdā
- Pievieno Jūs jaunai sarakstes grupai, kurā tiek izsūtīta ļaunatūra, izplatīta dezinformācija, utt.
- Izsūta ļaunprātīgas ziņas ar mērķi izkrāpt finanses





WhatsApp norādīta saite, kas it kā aizved uz konkursa mājaslapu.



Tālāk lietotāju aicina autentificēties ar savu WhatsApp kontu.

Drošības iestatījumi Whatsapp lietotnē:

1. Pārbaudiet sasaistītās ierīces

Iestatījumi → Sasaistītās ierīces

2. Atspējojiet automātisko failu ielādi

Iestatījumi → Krātuve un dati

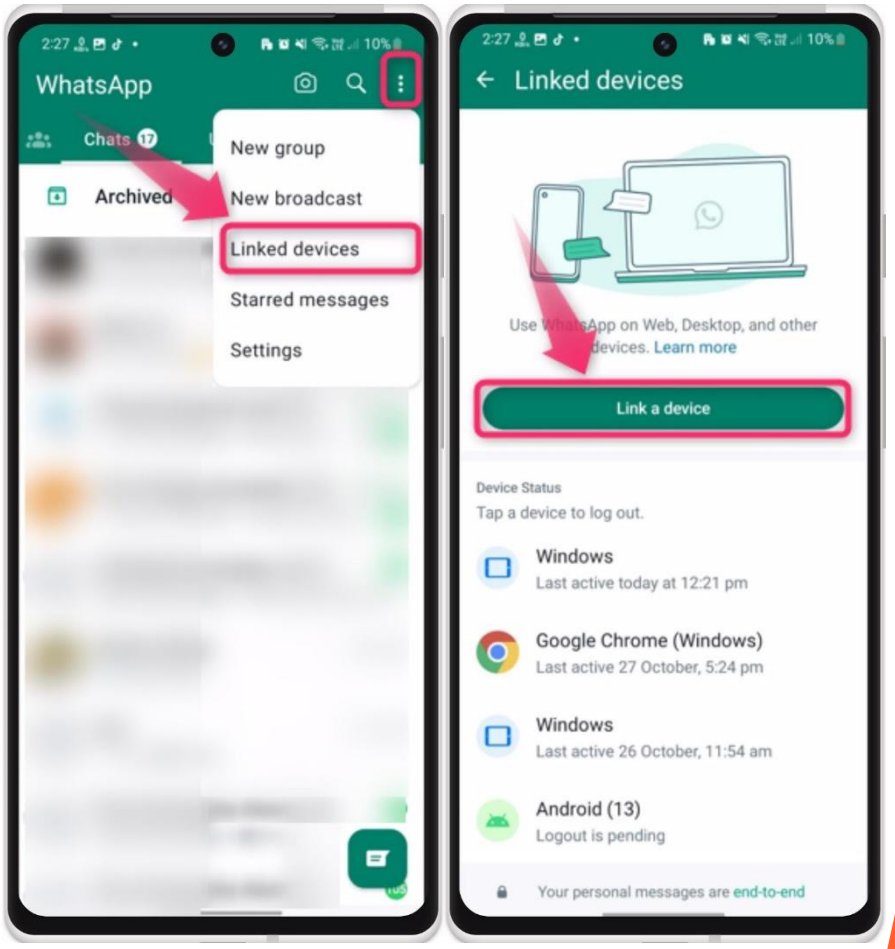
– Mobilie dati
– Wi-Fi
– Viesabonēšana

3. Ierobežojiet iespēju pievienot Jūs grupām

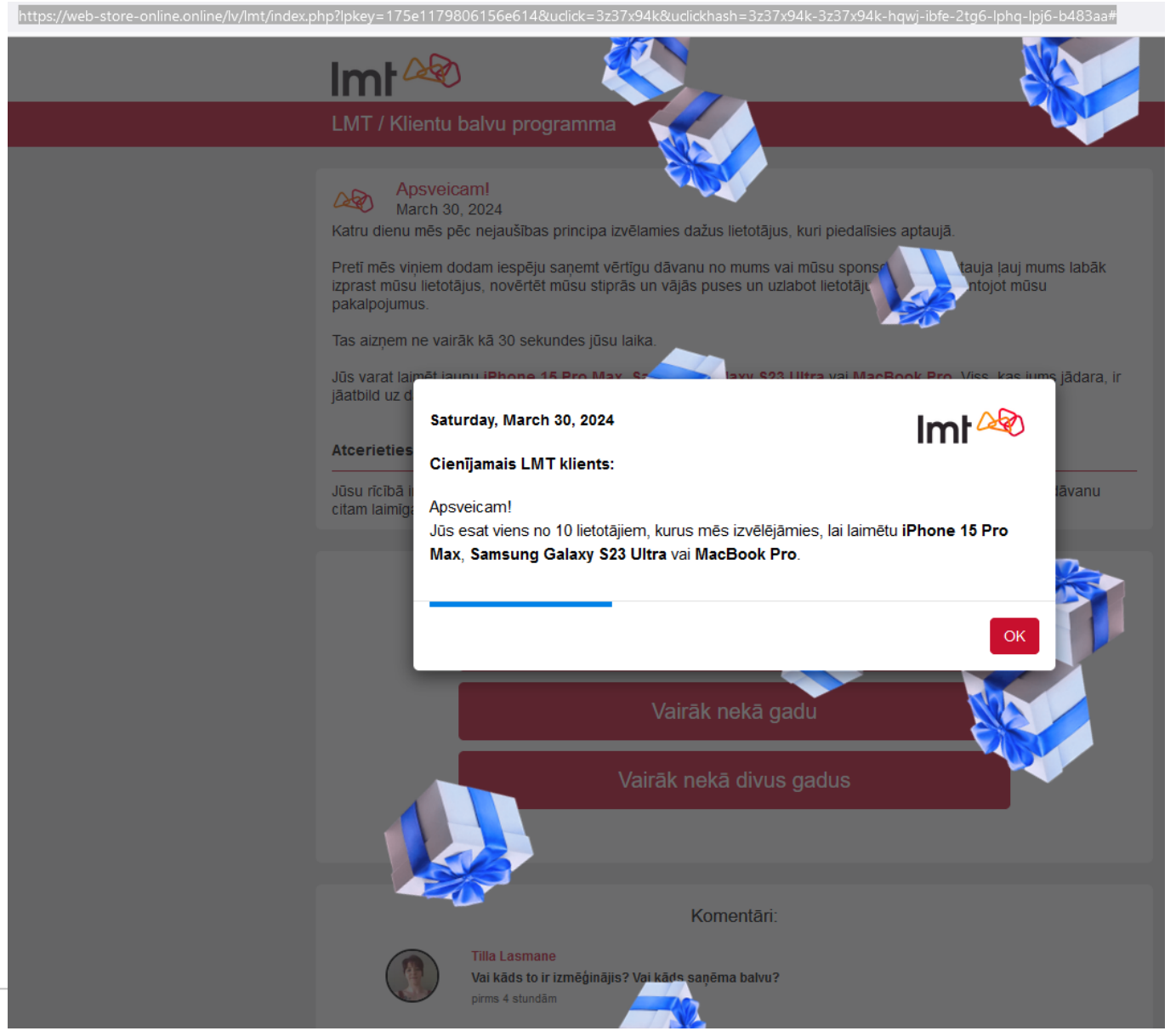
Iestatījumi → Privātums → Grupas

4. Aktivizējiet divpakāpju verifikāciju (2FA)

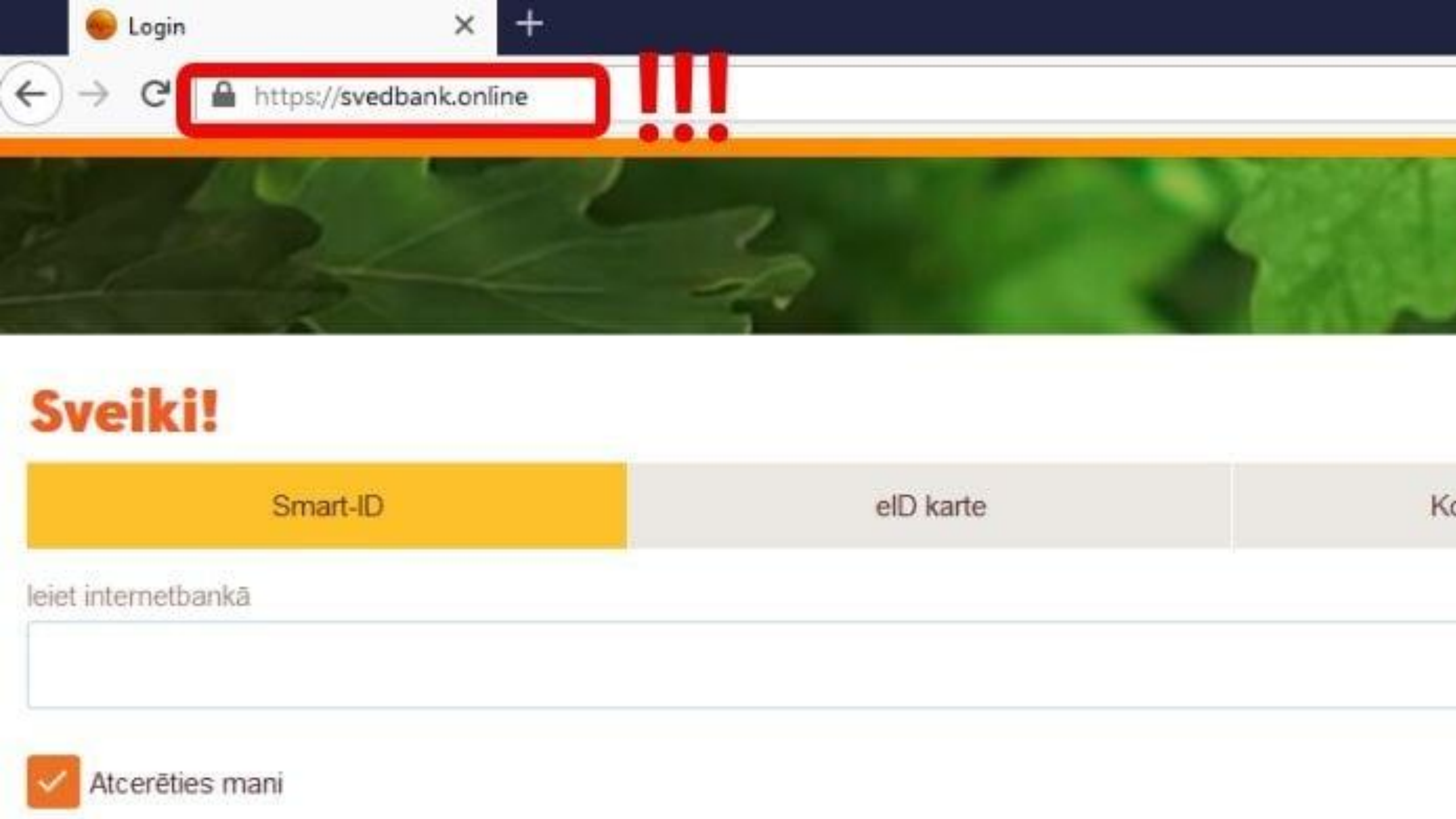
Iestatījumi → Konts → Divpakāpju verifikācija



Loterijas


https://web-store-online.online/lv/lmt/index.php?lpkey=175e1179806156e614&uclick=3z37x94k&uclickhash=3z37x94k-3z37x94k-hqwj-ibfe-2tg6-lphq-lpj6-b483aa#
LMT / Klientu balvu programma
Apsveicam!
March 30, 2024
Katru dienu mēs pēc nejaušības principa izvēlamies dažus lietotājus, kuri piedalīsies aptaujā.
Saturday, March 30, 2024
Cienījamais LMT klients:
Apsveicam!
Jūs esat viens no 10 lietotājiem, kurus mēs izvēlējāmies, lai laimētu iPhone 15 Pro Max, Samsung Galaxy S23 Ultra vai MacBook Pro.
OK
Vairāk nekā gadu
Vairāk nekā divus gadus
Komentāri:
Tilla Lasmane
Vai kāds to ir izmēģinājis? Vai kāds saņēma balvu?
pirms 4 stundām


Irregular Verbs
go – went – gone
begin – began – begun
did – done
produced


Login
https://svedbank.online
!!!
Sveiki!
Smart-ID
eID karte
Ko
Ieiet internetbankā
Atcerēties mani

Kādus trikus izmanto ļaundari?

5H11 Z1NJ4
1R d0M44A, L4I P13R44D11TU, K4
MU5U PR44T5 V4R P4V31KT BR11NUM L13T45!
135P41D11G45 L13T45! SA44KUM44 T45 B1J4
GRUT1, B3T T4G4D T4V5 PR44T5 ŠO L454 J4U
4UTOM44T15K1, P4T N3PIEDOM44J0T.
V4R1 BUUT L3PN5! T1K41 D4ZH1 PR44TI
SP33J PH0 54L4511T!

info@intemet.lv

www.drauqiem.lv

www.faceboook.com

itunes.cm

defi.lv

info@intemet.lv

www.drauqiem.lv

www.faceboook.com

itunes.cm

defi.lv (kur palika «l» ?)

Kādus trikus izmanto ļaundari?

i vietā izmanto l

g vietā izmanto q

o vietā izmanto 0

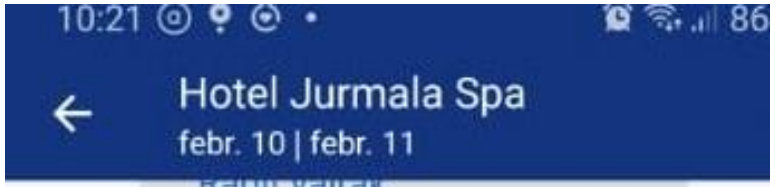
m vietā izmanto r+n

m vietā izmanto n

Domuzīmes (-) domēnos

Kādus trikus izmanto ļaundari?

- rakstzīmju atkārtojumu (www.faceboook.com);
- burtu maiņu vietām (www.faecbook.com)
- daudzskaitļa identifikatora pievienošanu vai noņemšanu (www.facebooks.com);
- izliekas par www (wwwfacebook.com);
- domēna vārda papildināšana: (www.appleshop.com, www.gucci-bags.com).



25. nov., 16:34

Dear [redacted]

Thank you for choosing Hotel Jurmala Spa for your stay.

Unfortunately your booking might be cancelled due to an error during verification of your reservation.

This is a mandatory process to prevent credit card fraud. This must be done within 12 hours or YOUR RESERVATION WILL BE CANCELLED and we will not be able to accept you as a guest!

- You must be verified even if you have paid for your reservation
- Please enter your payment details and wait for verification
- Booking will charge your payment method with your reservation amount, and in a minute will credit it back - this is your payment method verification

You can verify your payment method through a personal link:

https://booking.com-req-prog.com/p/6259385756

The best banking apps to use are: Revolut, Monzo, Starling, N26, C24. Make sure you have enough money on your bank card and your online transaction limits are raised.

THIS MESSAGE WAS SENT AUTOMATICALLY, PLEASE DO NOT REPLY TO IT.

Best Regards, Hotel Jurmala Spa

Rādīt mazāk

Domēna vārda līmeņi

https://booking.com-req-prog.com/p/6259385756

Domēna vārda līmeņi

https://booking.com-req-prog.com/p/6259385756

Domēna vārda līmeņi

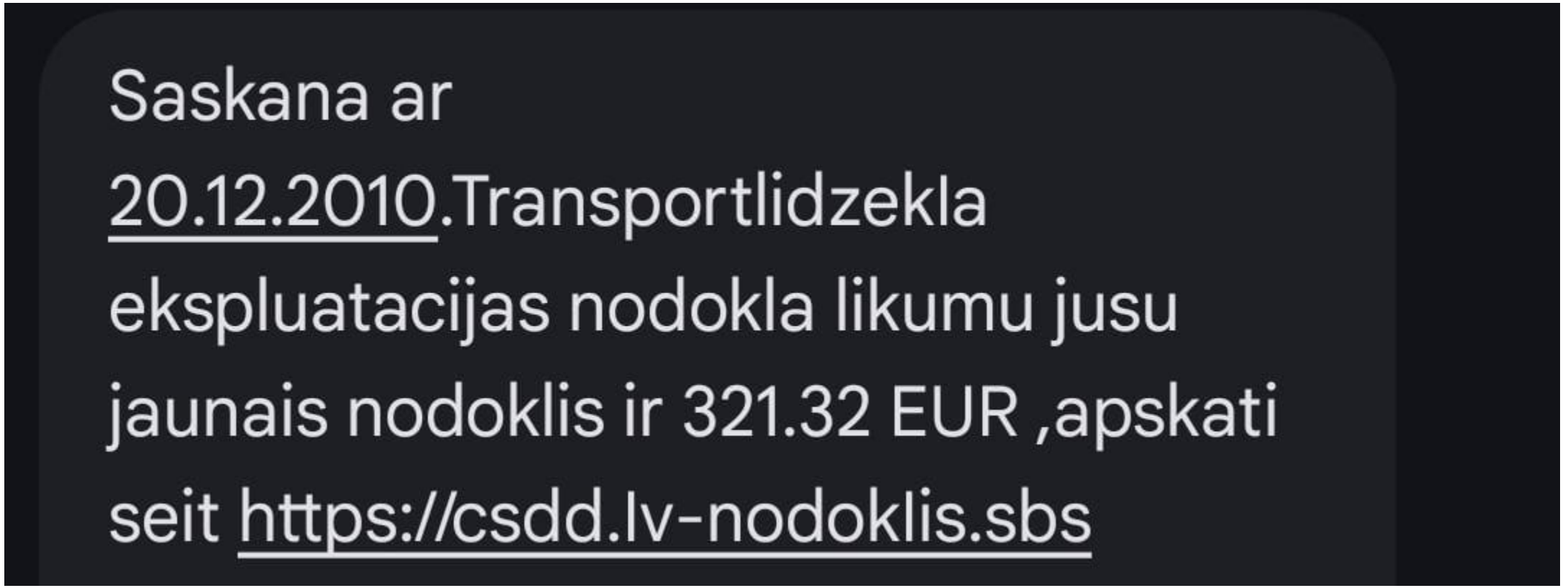
https://booking.com-req-prog.com

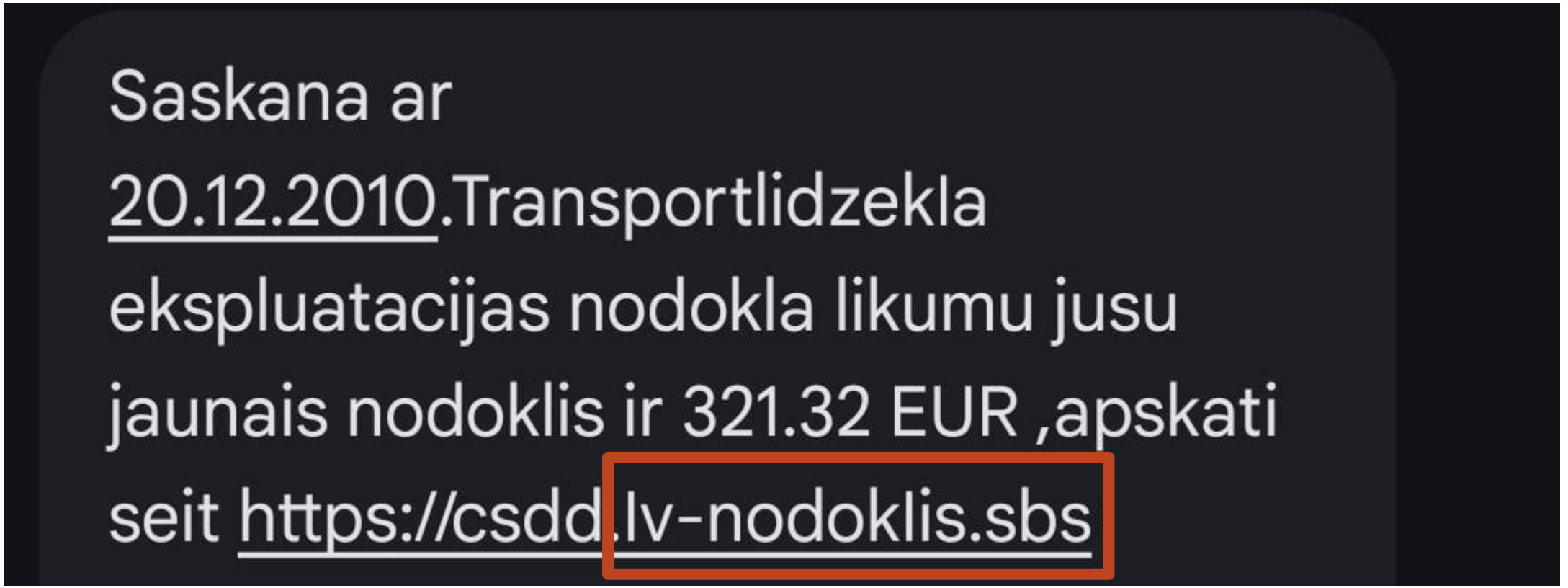
Domēna vārda līmeņi

https://booking.com-req-prog.com

Domēna vārda līmeņi

ib.swedbank.lv
www.swedbank.lv

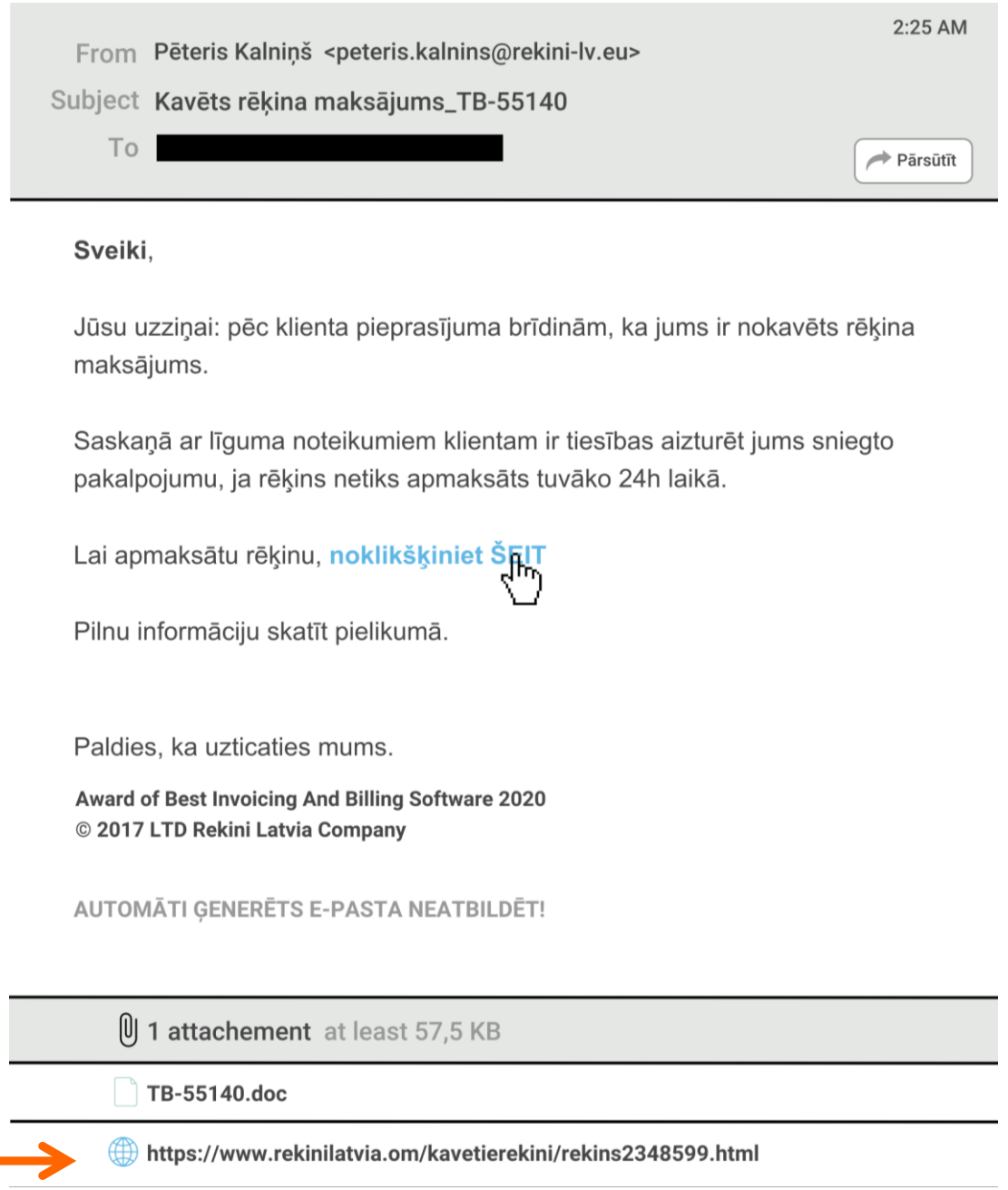

Saskana ar
20.12.2010.Transportlidzekla
ekspluatacijas nodokla likumu jusu
jaunais nodoklis ir 321.32 EUR ,apskati
seit https://csdd.lv-nodoklis.sbs

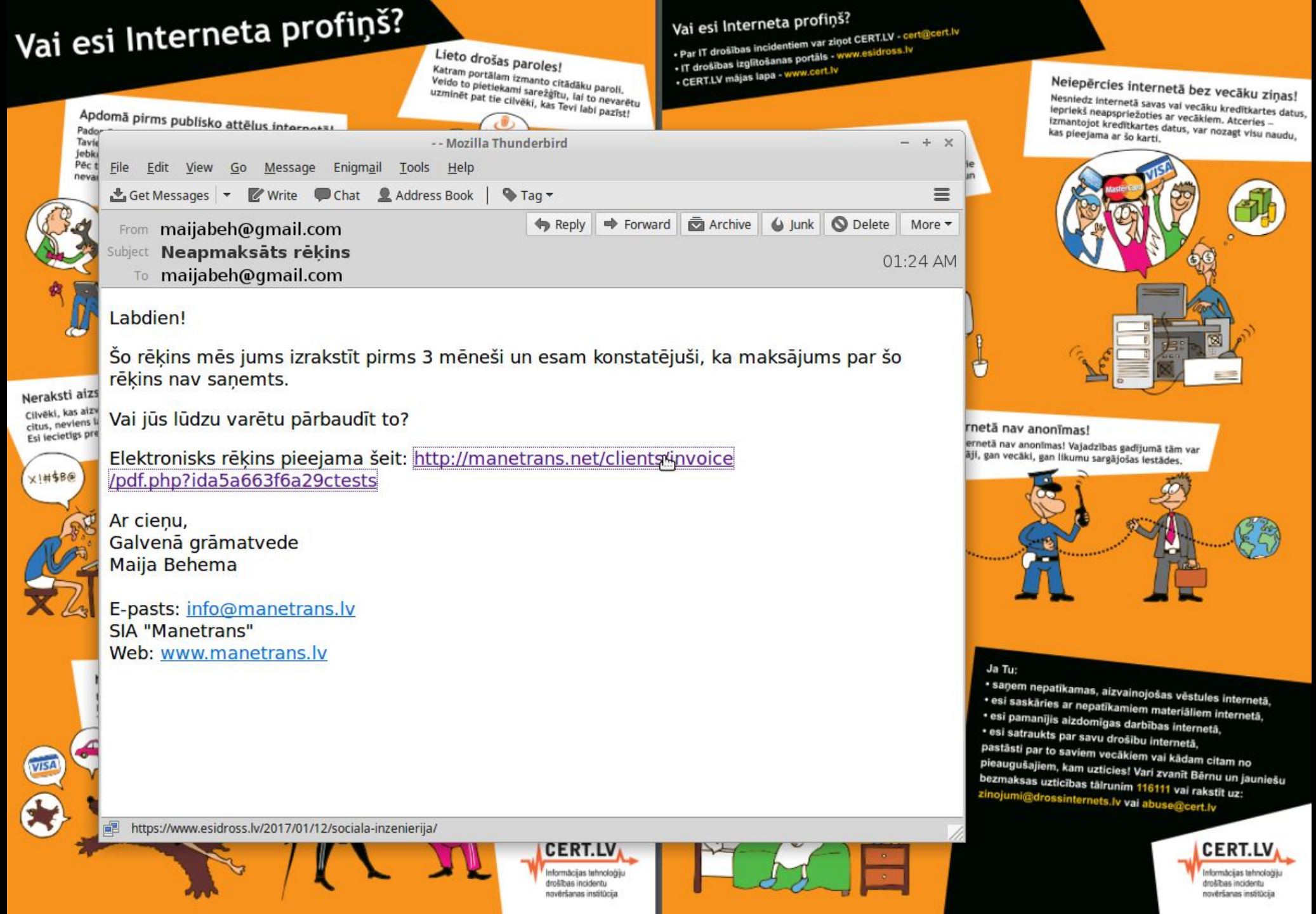

Saskana ar
20.12.2010.Transportlidzekla
ekspluatacijas nodokla likumu jusu
jaunais nodoklis ir 321.32 EUR ,apskati
seit https://csdd.lv-nodoklis.sbs

CERT.LV

Kam pievērst uzmanību?

- Sūtītāja e-pasta adresei
- Saņemšanas plkst. laikam
- Uzrunai
- Gramatikas kļūdām
- Valodas stilam
- Saitēm e-pastā
- Sociālās inženierijas pazīmēm
- Vai ir tekstā minēts pielikums
- Failu paplašinājumiem - .zip, .exe, .scr, etc., .iso, .doc, .xls, .ppt., u.c.





-- Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages | Write | Chat | Address Book | Tag

Reply | Forward | Archive | Junk | Delete | More

From maijabeh@gmail.com
Subject **Neapmaksāts rēķins**
To maijabeh@gmail.com
01:24 AM

Labdien!

Šo rēķins mēs jums izrakstīt pirms 3 mēneši un esam konstatējuši, ka maksājums par šo rēķins nav saņemts.

Vai jūs lūdzu varētu pārbaudīt to?

Elektronisks rēķins pieejama šeit: http://manetrans.net/clients/invoice/pdf.php?ida5a663f6a29ctests

Ar cieņu,
Galvenā grāmatvede
Maija Behema

E-pasts: info@manetrans.lv
SIA "Manetrans"
Web: www.manetrans.lv

https://www.esidross.lv/2017/01/12/sociala-inzenierija/

DNS ugunsmūris Instrukcijas **https://www.dnsmuris.lv**

CERT.LV Kiberincidentu novēršanas institūcija NIC

Liec mūri pret krāpnieka dūri!

Atvairi kiberuzbrukumus, uzstādot DNS ugunsmūri

Lejupielādē Google Play

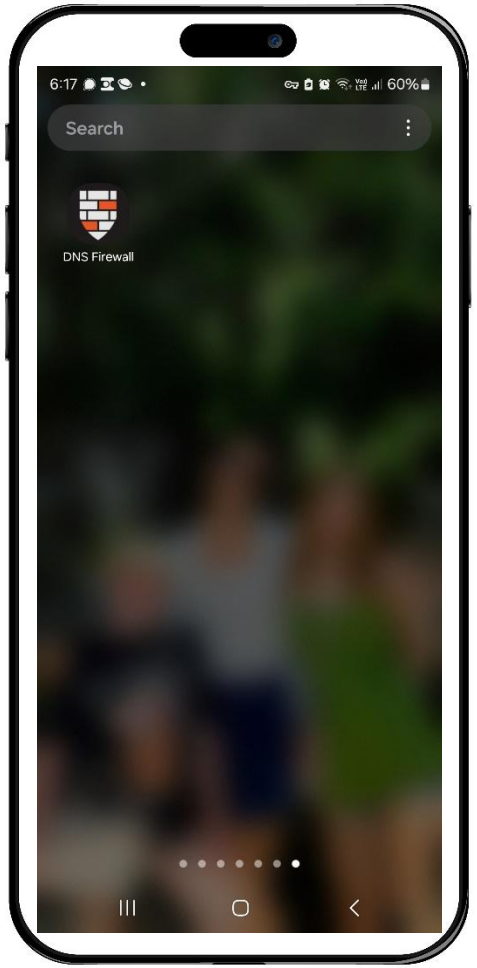
Lejupielādē App Store

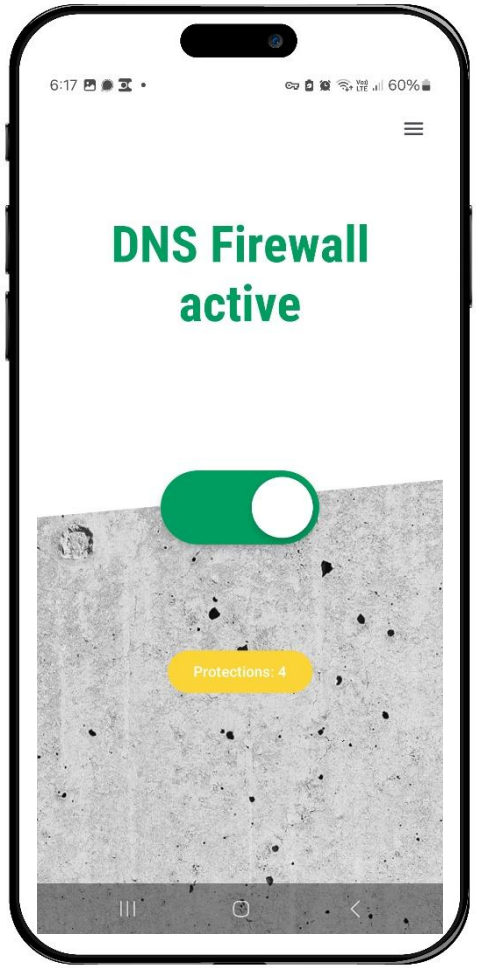
JUMS IR AKTĪVS

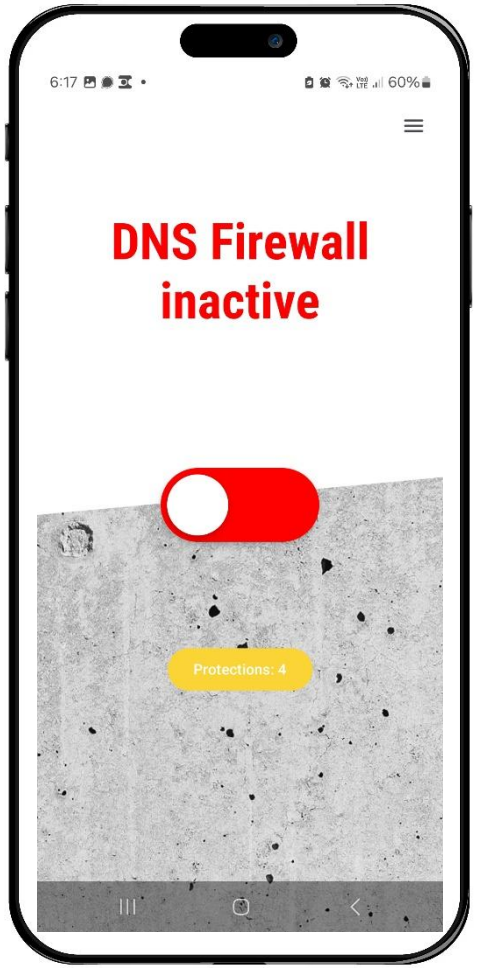
Kas ir DNS ugunsmūris?

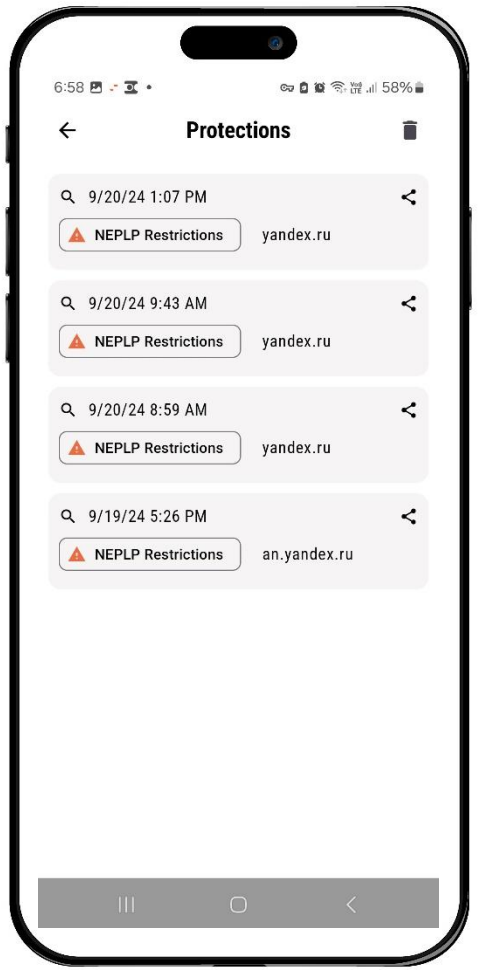
CERT.LV sadarbībā ar NIC (.LV domēna vārdu reģistra uzturētāju) ir izveidojuši DNS ugunsmūri - bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no kiberapdraudējumiem, tādiem kā viltus banku lapas, krāpnieciskas tirdzniecības platformas, vīrusus izplatošas vietnes u.c.

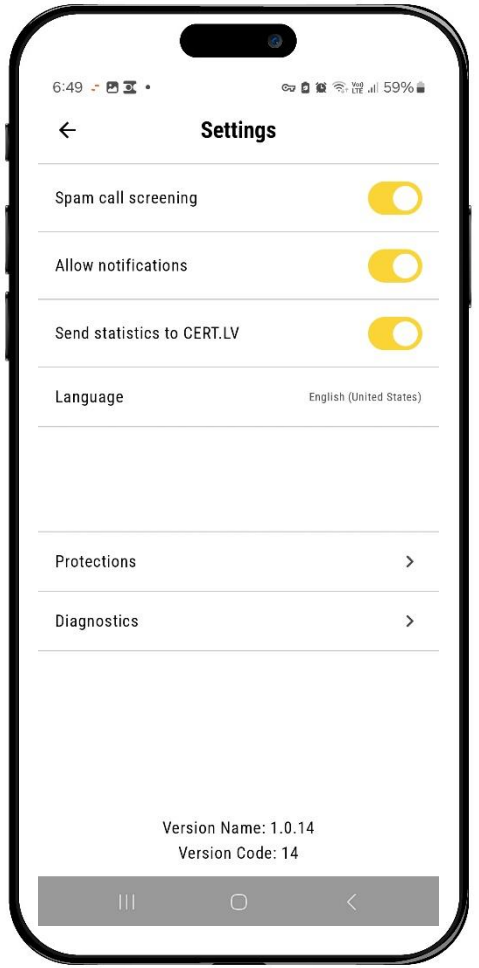
DNS ugunsmūra lietotne











https://checkshorturl.com

CheckShortURL

Expand and verify all your shortened links

CheckShortURL supports **a wide range of URL shortening services**, including t.co, goo.gl, bit.ly, amzn.to, tinyurl.com, ow.ly, youtu.be, and many others.

Enter Short URL

Expand

*This service is free and limited to **120 requests** per day*

What is CheckShortURL made fo

CheckShortURL is an **expand link facility**: our website is designe
information online by allowing you to **check the safety** of short
internet becoming increasingly crowded and complex, it's impor
click on to avoid falling victim to phishing scams or other malici

https://who.is

Premium Domains Transfer Features Login Sign Up

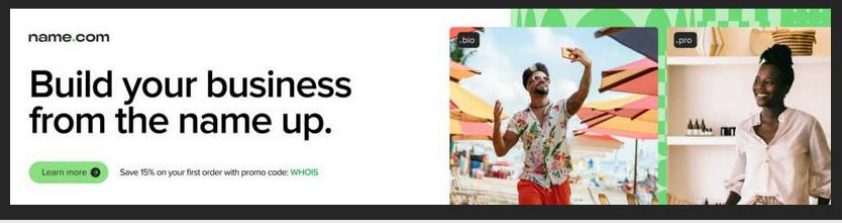
who.is

WHOIS Search, Domain Name, Website, and IP Tools

Domain names or IP addresses...

Your IP address is 91.240.246.246

Looking to get a website? Web Hosting Website Builder SSL Certificates

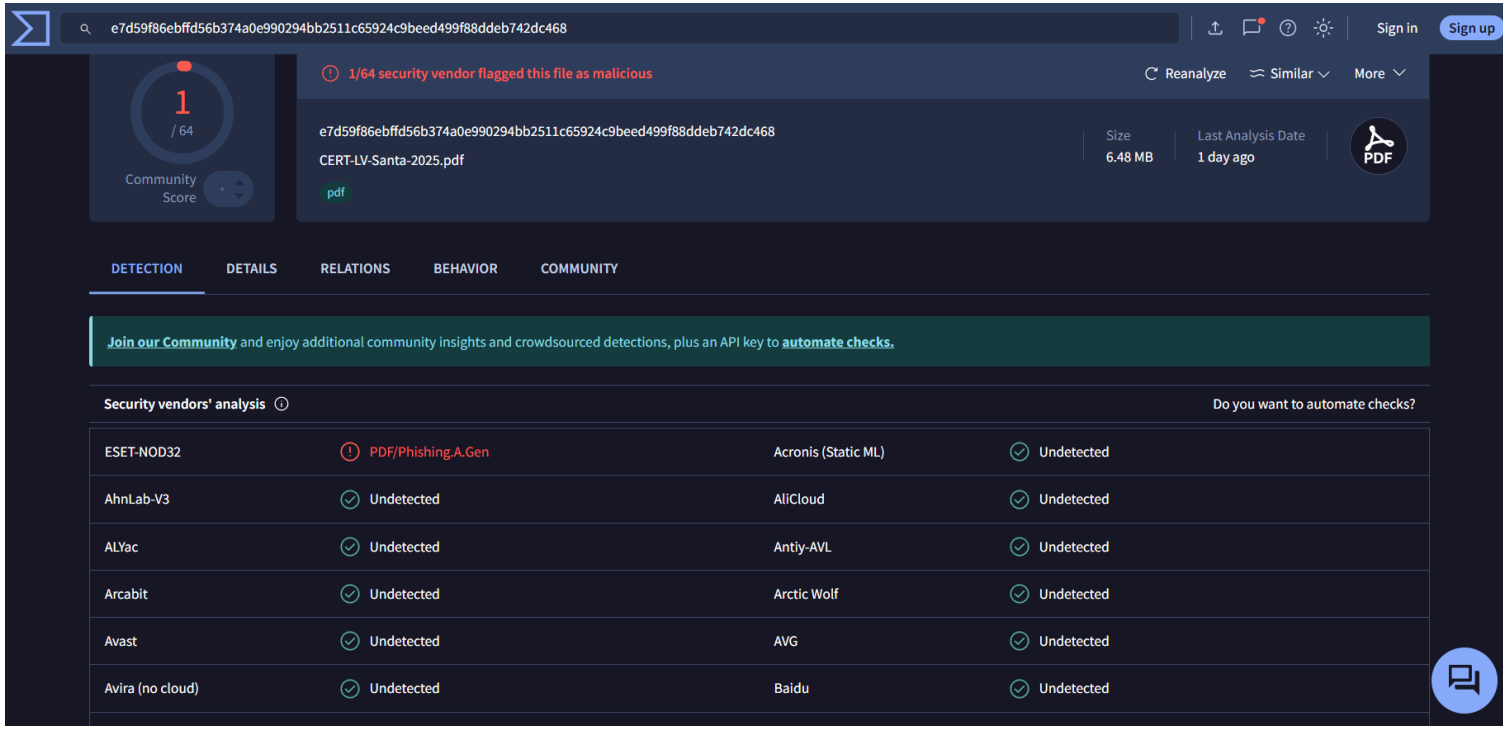


See Website Information

On Demand Domain Data

Register Domain Names

https://www.virustotal.com



CERT.LV

Vai Jūsu e-pasta adrese vai lietotājvārds ir uzlauzts?

https://haveibeenpwned.com

Ja esat kļuvis par krāpnieku upuri?

DARBĀ:

- Rīkojieties atbilstoši **iestādes incidentu reaģēšanas plānam;**

MĀJĀS:

- Mainiet visas savas paroles, izmantojot citu datoru;
- Skenējiet datoru ar antivīrusa programmu;
- Ziņojiet **policijai** par datu zādzību un SAGLABĀJIET iesnieguma kopiju;
- Ziņojiet savai **bankai** un **CERT.LV**;
- Aktivizējiet DNS ugunsmūri (**www.dnsmuris.lv**).

Ziņo CERT.LV:

- Pārsūtot* krāpniecisko e-pastu uz **cert@cert.lv**
- Zvanot 24x7 **+371 67085888**
- Pārsūtot saņemto ziņu uz tālruņa numuru **+371 23230444****

Svarīgi! Šis tālruņa numurs nav pieejams sarunām

* https://cert.lv/lv/kontakti/ka-parsutit-kaitigus-e-pastus
** Lūdzu, ņemiet vērā, ka īsziņu pārsūtīšanas izmaksas tiek piemērotas saskaņā ar jūsu izmantotā tele operatora tarifiem

Starptautiskā operācijā Valsts policija likvidē IT infrastruktūru, kas izmantota tiešsaistes krāpšanā

Valsts policija

17. oktobrī, 2025
Lasīšanai: 7 minūtes

RUBRIKA: Relīze
TĒMA: Noziedzība

4

NILLTPF novērošana

Noziedzīgi iegūtu līdzekļu legalizācijas, terorisma un proliferācijas finansēšanas novēršanas (NILLTPFN) sistēma

Nacionālais NILLTPF risku novērtēšanas ziņojums par 2020.–2022. gadu (NRA 2023)

Nacionālā finanšu noziegumu novēršanas un apkarošanas stratēģija

(apstiprināta 10.01.2024.)

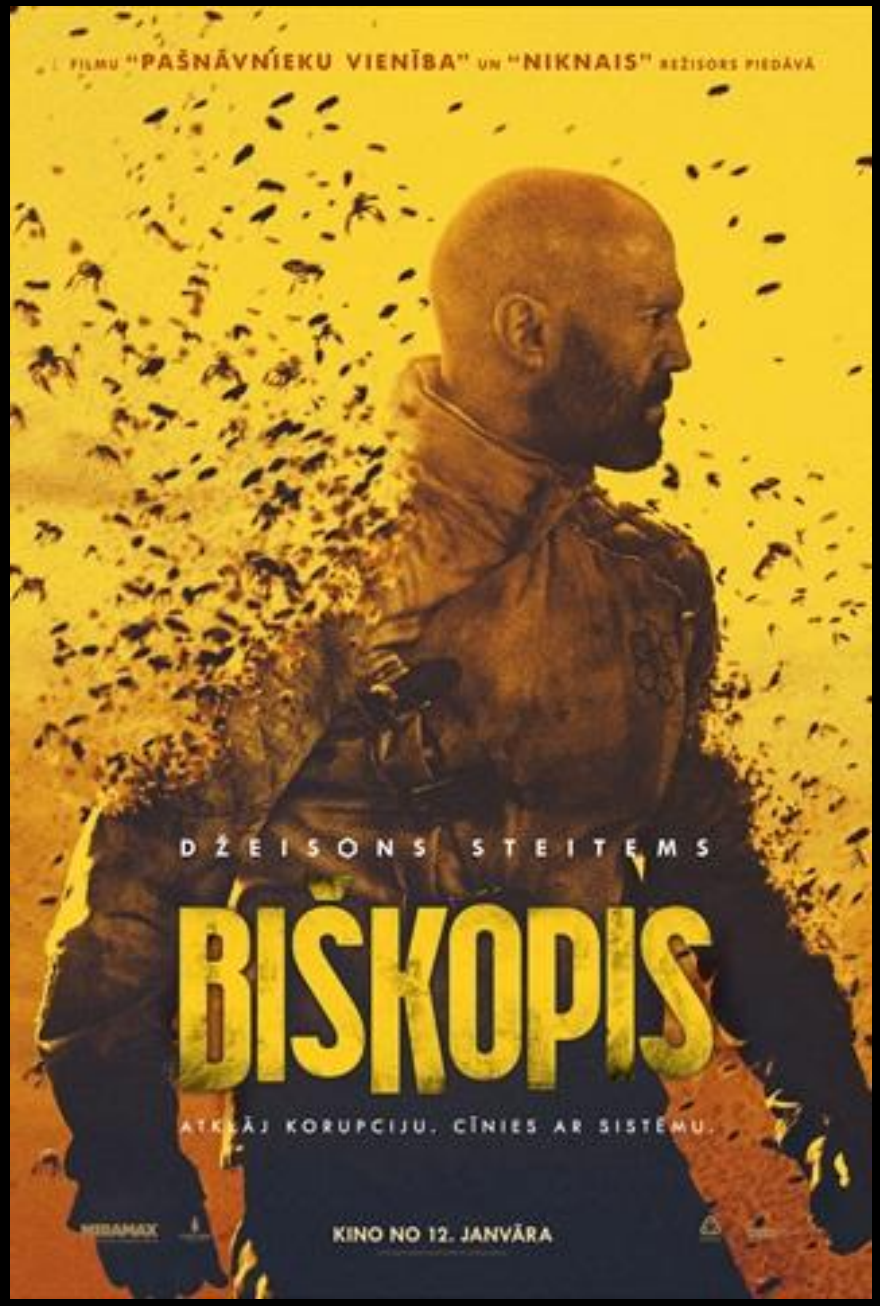
NILLTPFN pasākumu plāns 2024.–2026. gadam

(spēkā no 02.05.2024)

12 rīcības virzieni:

1. Riski, politika un koordinācija

CERT.LV


FILMU "PAŠNĀVNIEKU VIENĪBA" UN "NIKNAIS" REŽISORS PIEDĀVĀ
DŽEISONS STEITEMS
BIŠKOPIS
ATKLĀJ KORUPCIJU. CĪNIES AR SISTĒMU.
KINO NO 12. JANVĀRA

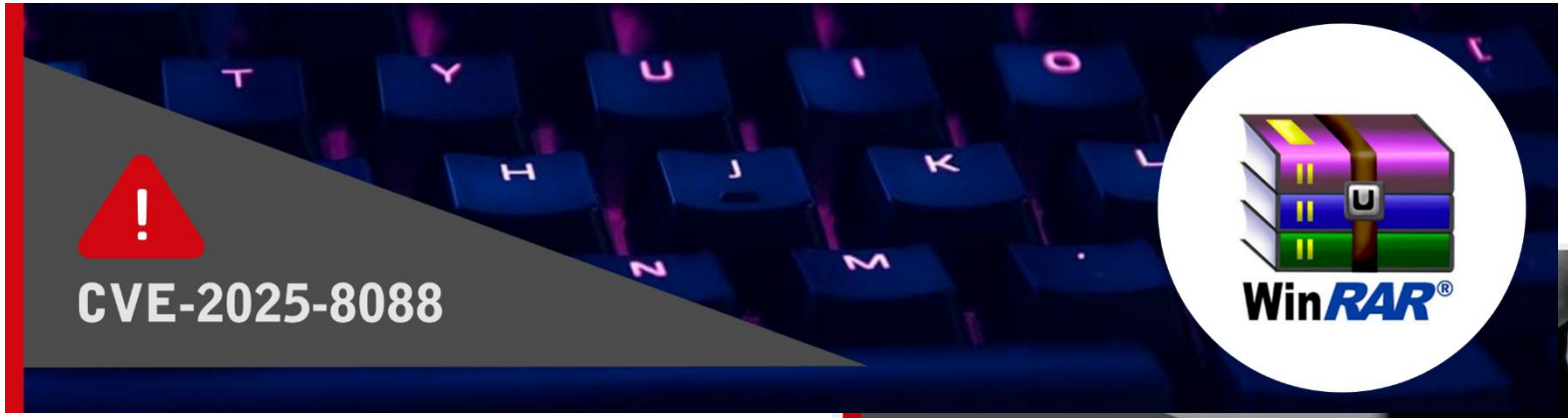

$0.00

Galvenās tendences & draudi:

1. Krāpšana
   - Pikšķerēšana, bikšķerēšana, smikšķerēšana, kvikšķerēšana
   - u.c.
2. Ievainojamības (CVE)
3. Ļaunatūras & izspiedējvīrusi
4. Piegādes ķēdes uzbrukumi
5. Pakalpojumu pieejamība
   - DDOS
   - GPS signālu bloķēšana

Ievainojamības

- Nulles dienas ievainojamības
- Zināmās ievainojamības



CVE (*Common Vulnerabilities and Exposures*) - standartizēta sistēma, kas paredzēta dažādu programmatūras un aparatūras produktu drošības ievainojamību identificēšanai un nosaukšanai.


BLESSING
CONTROL
TEMPERATURE SENSOR
CLEANING
TIMER
ENTERTAINMENT
SECURITY

TOP5 ieteikumi viedierīču lietošanā:

1. Pārskatiet, kādas ierīces pievienotas Jūsu tīklam
2. Mainiet noklusējuma paroles
3. Regulāri atjauniniet programmatūru
4. Atspējojiet nevajadzīgās/neizmantotās funkcijas
5. Aizsargājiet WiFi tīklu & izveidojiet viesu tīklu viedierīcēm

Galvenās tendences & draudi:

1. Krāpšana
   - Pikšķerēšana, bikšķerēšana, smikšķerēšana, kvikšķerēšana
   - u.c.
2. Ievainojamības (CVE)
3. Ļaunatūras & izspiedējvīrusi
4. Piegādes ķēdes uzbrukumi
5. Pakalpojumu pieejamība
   - DDOS
   - GPS signālu bloķēšana

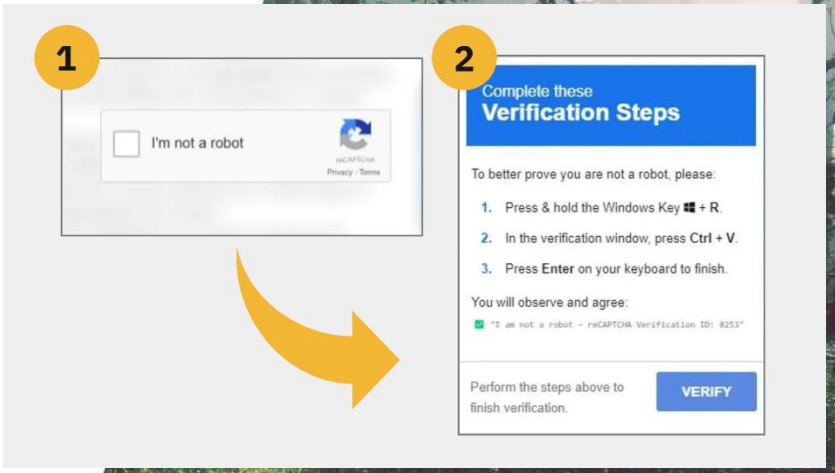
3. Ļaunatūras:

TOP inficēšanas metodes:

- Pikšķerēšanas e-pasti;
- Nezināmi USB
- Publiski zināmu ievainojamību ļaunprātīga izmantošana;
- Noklusējuma autentifikācijas piekļuves dati, paroles uzlauzšana (brute force),
- Noplūduši lietotāja piekļuves dati;
- Automatizēti uzbrukumi.
- u.c.

Ļaunatūru tipi:

- Lietotāju datu zadzēji (paroļu iegūšanu no tīmekļa pārlūka vai nešifrētiem failiem, kā interneta pārlūka spraudnis),
- Bot-net,
- Izpiedējvīrusi,
- Attālinātās kontroles trojāni (mērķēti uz datu izgūšanu vai tālāko infrastruktūras kompromitēšanu)
- ….



Kaitīgi paplašinājumi:

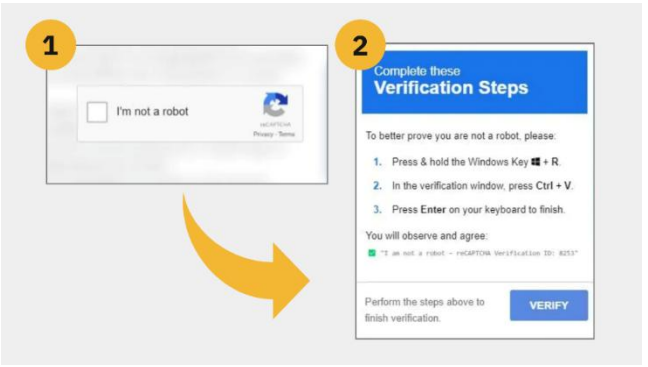
pārvirza lietotājus uz ļaundabīgām vietnēm & zog lietotāju datus

Google chrome

- Emoji keyboard online – copy&paste your emoji
- Free Weather Forecast
- Video Speed Controller – Video Manager
- Unlock Discord – VPN Proxy to Unblock Discord Anywhere
- Dark Theme – Dark Reader for Chrome
- Volume Max – Ultimate Sound Booster
- Unblock TikTok – Seamless Access with One-Click Proxy
- Unlock YouTube VPN
- Color Picker, Eyedropper – Geco colorpick
- Weather

Microsoft Edge

- Unlock TikTok
- Volume Booster – Increase your sound
- Web Sound Equalizer
- Header Value
- Flash Player – games emulator
- Youtube Unblocked
- SearchGPT – ChatGPT for Search Engine
- Unlock Discord



Pārējo paplašinājumu pārbaudei izmanto rīku: **www.extensiontotal.com**

CERT.LV

Izspiedējvīrusi

TVNET > Financenet > Nozares

Kiberuzbrukumā noplūduši alkohola ražotāja "Amber Beverage Group" dati

Foto: Schutterstock.com

Alkoholisko dzērienu ražotājs "Amber Be
piedzīvojis šifrējošā izspiedējvīrusa uzbr
rezultējies uzņēmuma datu noplūdē, ap
informācijas tehnoloģiju drošības incid
institūcijas "Cert.lv" pārstāvji.

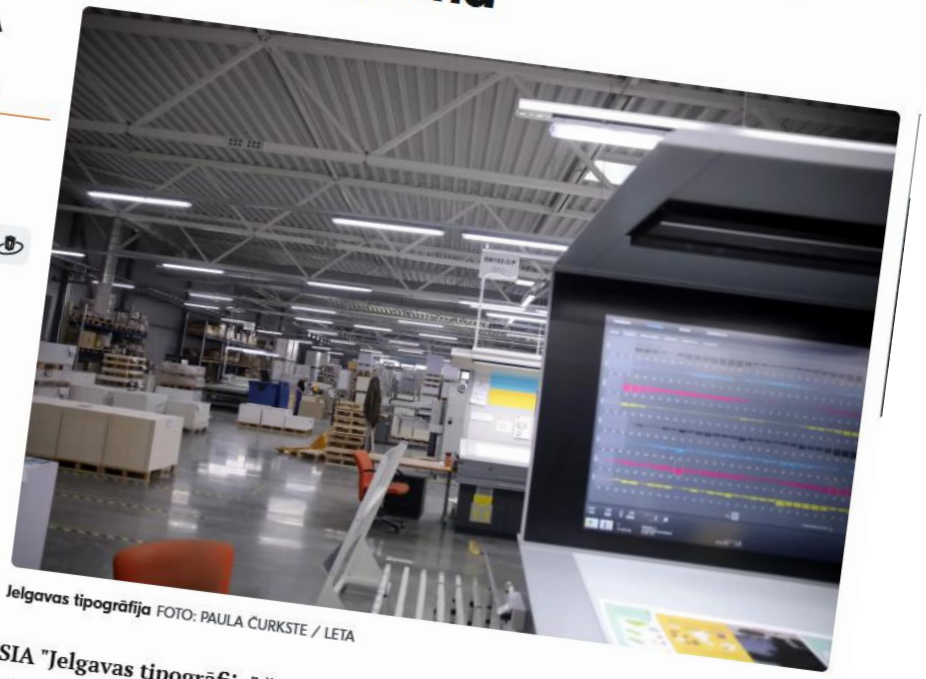
TVNET > Bizness > TechBiz > Internets

"Jelgavas tipogrāfija" cietusi kiberuzbrukumā

TVNET / LETA

2025. gada 4. jūnijs 14:14

Noklausies



Jelgavas tipogrāfija FOTO: PAULA ČURKSTE / LETA

SIA "Jelgavas tipogrāfija" šonedēļ ir cietusi no kiberuzbrukuma,
aģentūrai LETA pastāstīja uzņēmuma valdes priekšsēdētājs Māris
Matrevics.

Noticis kiberuzbrukums kultūras nozares informācijas sistēmām

Dalīties:

DIVE BRIEF

Ransomware attacks in education jump 23% year over year

Education was the fourth-most-targeted sector during the first half of 2025, according to a report from Comparitech.

Published July 21, 2025

By Briana Mendez-Padilla

Getty Images

Listen to the article 3 min

Dive Brief:

- Ransomware attacks against schools, colleges and universities rose 23% year over year in the first half of 2025, according to a report from Comparitech, a cybersecurity and online privacy product review website.
- The six months saw 130 confirmed and unconfirmed ransomware attacks against educational institutions, with an average ransom demand of $556,000.
- Education was the fourth-most-targeted sector during the first half of

MOST POPULAR


Education Department outsources program management to other agencies


Lessons learned from Arizona's universal school choice program


Access to 8th grade algebra divided along socioeconomic, racial lines


School bus driver shortage improves slightly with bump in hiring, pay

LIBRARY RESOURCES

PODCAST
Get Ready for BASC-4: What the Authors Want You To Know About the Latest Edition
Custom content for Pearson

CERT.LV

BBC

West Lothian schools hit by ransomware cyberattack

6 May 2025

Share Save

West Lothian Council confirmed a cyberattack on its education network

Schools in West Lothian have been the victim of a suspected criminal ransomware cyberattack.

A council spokesperson said the attack had affected its education network and contingency plans to keep schools open was under way.

Ransomware is a type of malware which prevents someone from accessing a device and the data stored on it, usually by encrypting files, according to **the National Cyber**

Izspiedējvīrusi

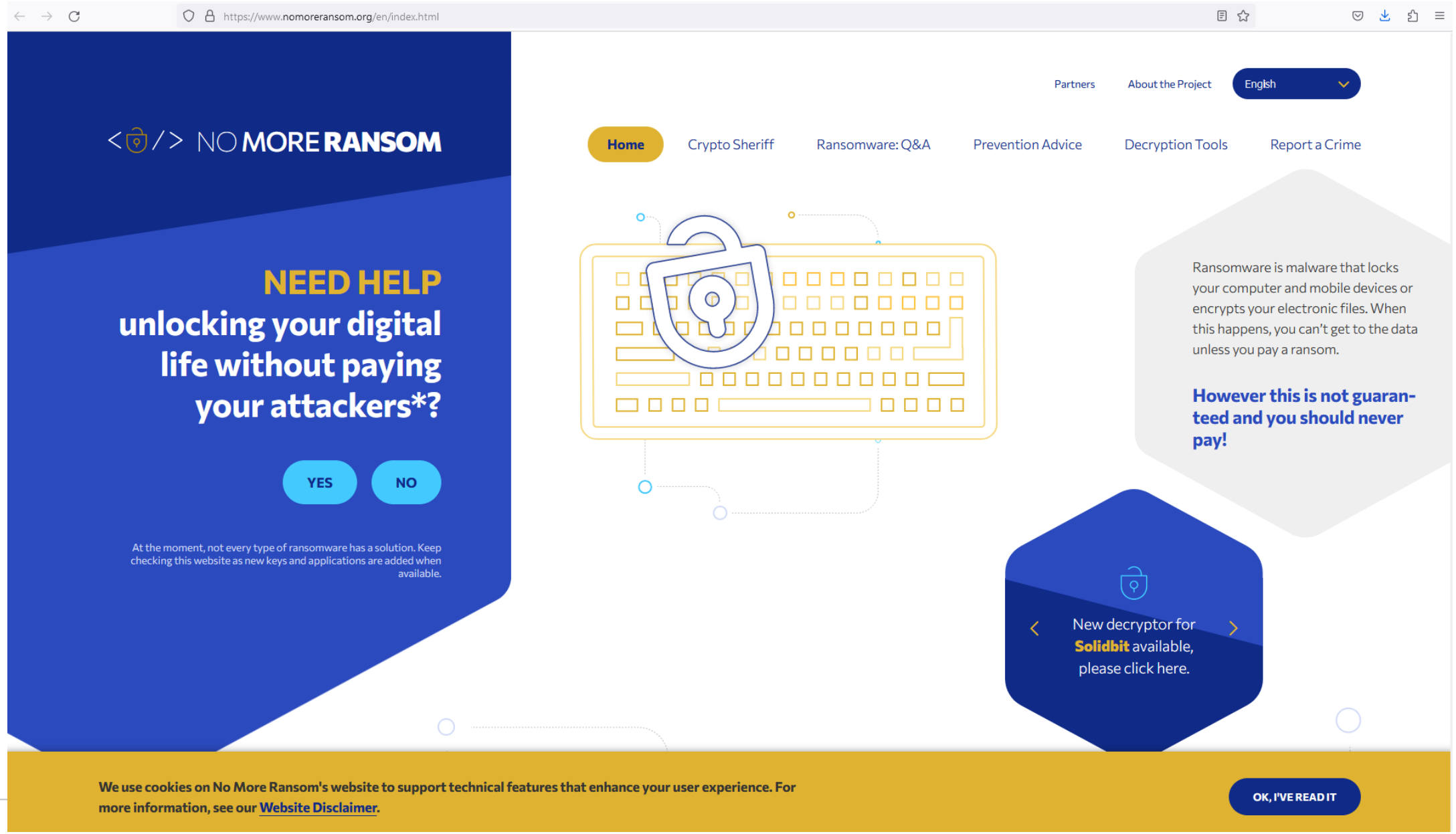
```
################################################################
################## YOUR FILES WERE ENCRYPTED ###################
############## AND MARKED BY EXTENSION .corona-lock ############
################################################################
--
DON'T WORRY! YOUR FILES ARE SAFE! ONLY MODIFIED :: ChaCha + AES
WE STRONGLY RECOMMEND you NOT to use any Decryption Tools.
These tools can damage your data, making recover IMPOSSIBLE.
Also we recommend you not to contact data recovery companies.
They will just contact us, buy the key and sell it to you at a higher price.
If you want to decrypt your files, you have to get RSA private key.
--
To get RSA private key you have to contact us via email to:
---------------------------->> support@covidworldcry.com <<
and send us your id: >> 1966883997 <<
--
HOW to understand that we are NOT scammers?
You can ask SUPPORT for the TEST-decryption for ONE file!
--
################################################################
################## LIST OF ENCRYPTED FILES #####################
----------------------------------------------------------------
            C:\autoexec.bat              24
            C:\install.log               45
C:\KAV\nkf1453-readme.txt                      6698
          C:\nkf1453-readme.txt      6698
C:\KAV\KES8Win\nkf1453-readme.txt  6698
```

Ransomware dzēstās kopijas:

```
Delete Shadows /all /quiet
 /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup*.*
c:\*.set c:\*.win c:\*.dsk
 /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.* d:\backup*.*
d:\*.set d:\*.win d:\*.dsk
 /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.* e:\backup*.*
e:\*.set e:\*.win e:\*.dsk
 /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.* f:\*.set
f:\*.win f:\*.dsk
 /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.* g:\backup*.*
g:\*.set g:\*.win g:\*.dsk
 /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.* h:\backup*.*
h:\*.set h:\*.win h:\*.dsk

 %0
```

https://www.nomoreransom.org



TOP 10 kiberdrošības draudi 2030. gadā

1. **Piegādes ķēžu drošība (programmatūru un piegādātāju atkarības)**
2. **Speciālistu trūkums**
3. **Cilvēciskās kļūdas un novecojušu sistēmu izmantošana kiber-fiziskajās ekosistēmās**
4. Neatjauninātu un novecojušu sistēmu izmantošana pārslodzes apstākļos starp sektoru tehnoloģiju ekosistēmā
5. Digitālās novērošanas autoritārisma pieaugums / Privātuma zudums
6. Pārrobežu IKT pakalpojumu sniedzēji kā vienots kļūmes punkts
7. Attīstītas dezinformācijas / ietekmes operāciju (IO) kampaņas
8. Attīstītu hibrīddraudu pieaugums
9. Mākslīgā intelekta ļaunprātīga izmantošana
10. Fiziska ietekme, ko rada dabas/vides traucējumi uz kritisko digitālo infrastruktūru

https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary

Kiberhigēnas ieteikumi

1. Izmanto drošas, garas, unikālas **paroles + 2FA** (Mar@2025_Skol!")
2. Izmanto **paroļu pārvaldnieku** (KeePass, Last pass, 1 pass)
3. **Kiberdrošības kultūra:**
   - **pārbaudi avotu un datu precizitāti**, kritiski izvērtējot saņemtās ziņas patiesumu un sūtītāja e-pasta adresi un saturu
   - **Nesūti** citām personām **attēlus vai video ar bankas kartēm, vai personu apliecinošiem dokumentiem**
   - **Nepakļaujies** krāpnieku **prasībām** viedierīcēs **instalēt attālinātas piekļuves programmatūru** (*AnyDesk, TeamViewer, HopToDesk, AeroAdmin* u.c.)
4. Neklikšķini uz steidzama vai emocionāla satura un aizdomīgām saitēm
5. Neizmantot personīgos e-pastus darba lietām
6. **Regulāri** un savlaicīgi **atjaunini** iekārtu OS un lietotnes

Kiberhigiēnas ieteikumi

7. **Nelejupielādē** materiālus **no aizdomīgām vietnēm**
8. **Neizmanto aizdomīgus/nezināmus USB**
9. **Nobloķē datoru** kad ej prom
10. **Neinstalēt programmas bez** IT personāla **atļaujas** (shadowIT)
11. **Izmanto** tikai skolas **oficiālo WiFi** tīklu/s
12. Veic svarīgo datu **rezerves kopijas**
13. Izmantot bezmaksas aktīvo aizsardzības pakalpojumu «**DNSMURIS.LV**»,
14. **Seko** līdzi **aktualitātēm** (@cert.lv)

Neklusē! Ziņo par krāpnieku aktivitātēm & ļaundabīgām vietnēm, pārsūtot informāciju uz cert@cert.lv

CERT.LV

cert@cert.lv

+371 23230444

Saglabā šo numuru savā telefona kontaktu sarakstā, lai nepieciešamības gadījumā nav tālu jāmeklē. Vari uz šo numuru pārsūtīt arī WatsApp ziņas.

Saņem krāpniecisku SMS, telefona zvanu vai pamani viltus saiti - ziņo CERT.LV!

CERT.LV
Kiberincidentu novēršanas institūcija

Kiberdrošība: mūsu kopīgā atbildība

Aizsardzības ministrija

Nacionālais kiberdrošības centrs

Latvijas Universitātes Matemātikas un informātikas institūts

@cert.lv

https://cert.lv

CERT.LV

Liec mūri pret krāpnieku dūri!

@cert.lv