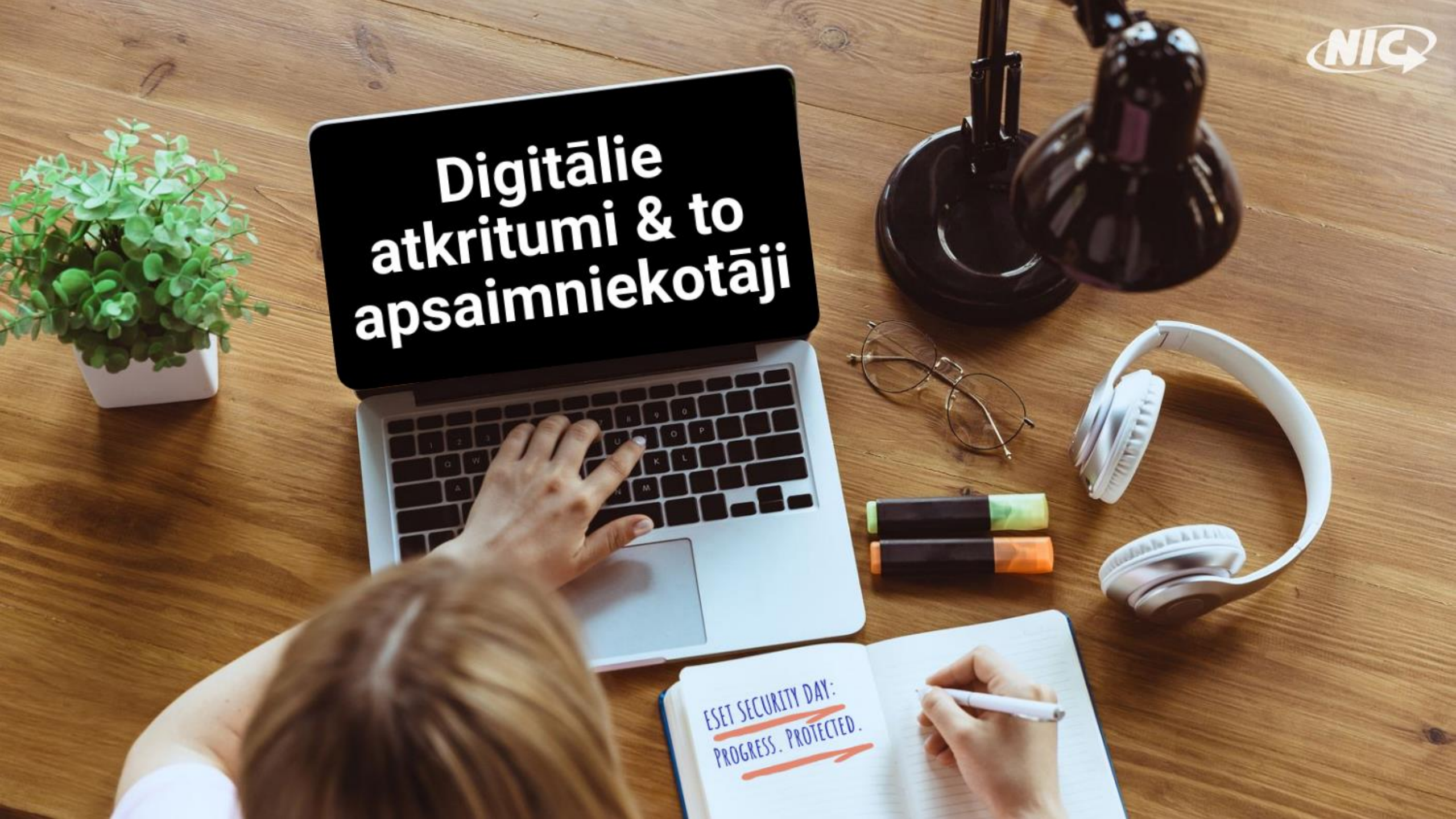
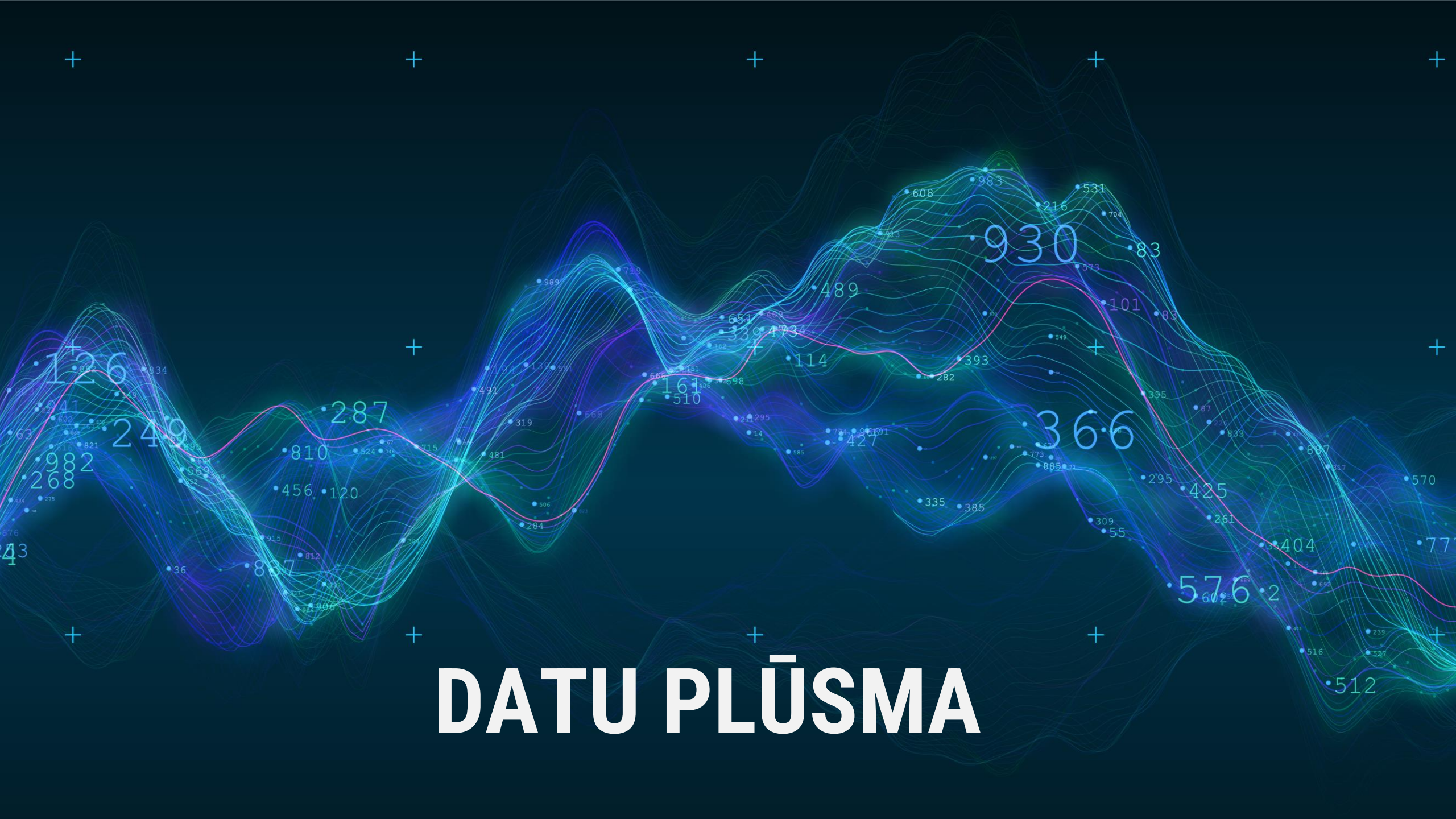

Digitālie atkritumi & to apsaimniekotāji
ESET SECURITY DAY:
PROGRESS. PROTECTED.

DIGITĀLIE ATKRITUMI

DOMĒNA VĀRDS IR NEVIS TĒRIŅŠ, BET AKTĪVS


DATU PLŪSMA


930
366


20
EURO
BCE ECB EZB EKP EKT EKB BCE EBC 2015

DOMĒNA VĀRDU OTRREIZĒJAIS TIRGUS

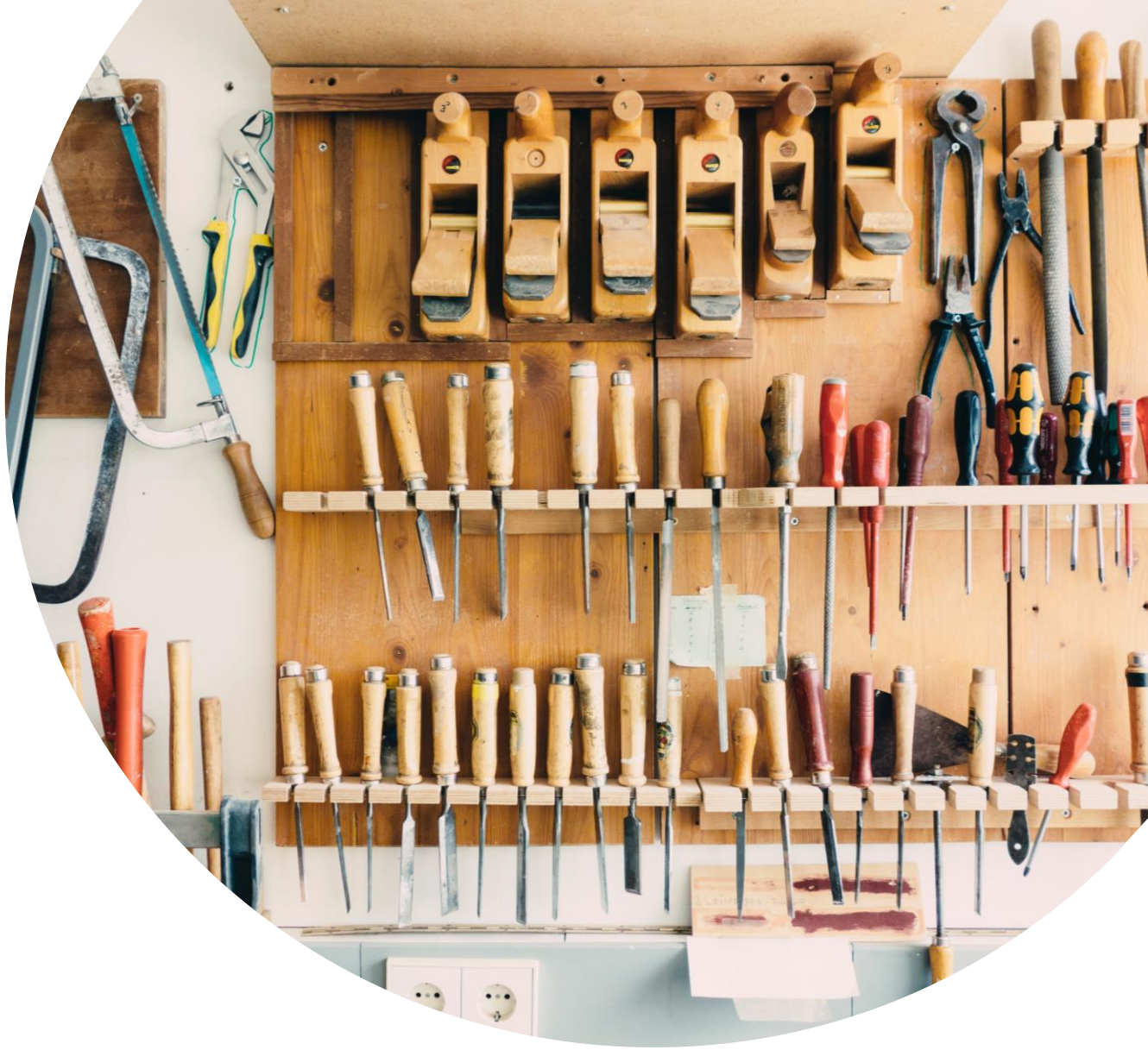
TIRGUS SPĒLĒTĀJI

- Domeineri
- Lietotāji
- Vidutāji
- Domēna vārdu parkošanās platformas
- Reklāmdevēji


KURŠ ATBILDĪGS?

RĪKI

- Domēna vārda autoritāte:
  - AHREFS (https://ahrefs.com)
  - Majestic SEO (https://majestic.com)
  - Moz Tools (https://moz.com)
  - AdSense Sandbox
- Domēna vārda novērtēšana:
  - GoDaddy Domain Appraisal
  - SEDO (Sedo.com)
  - ESTIBOT (Estibot.com)
  - Empire Flippers (https://empireflippers.com)
  - Domain price checker (https://pc.domains)
  - Website Outlook (https://www.websiteoutlook.com)
  - NameBio



KĀ AR KIBERDROŠĪBU?

ATSAKIES NO DOMĒNA VĀRDA ATBILDĪGI

Balstīts uz 2018. gada pētījumu ("Possible Security")

Analizēja 180 tikko atbrīvojušos .LV domēna vārdus un veica kvantitatīvu un kvalitatīvu saņemto datu analīzi, t.sk. saglabājot FTP, SSH, TELNET, SMTP, DNS, HTTP, POP3, IMAP, HTTPS, RDP, VNC protokolos saņemtos pieprasījumus.

https://www.nic.lv/lv/atsakies-no-domena-varda-atbildigi

Ar ko uzņēmums riskē?

Domēna vārds ir kā vārti uz citiem tiešsaistes pakalpojumiem, kas padara to par lielisku mērķi kiberuzbrukumiem!

Piereģistrējot Jūsu veco domēna vārdu, jaunais lietotājs var iegūt kontroli pār tā saturu, vecajām e-pasta adresēm un web pieprasījumiem, līdz ar to rodas iespēja:

- Saņemt konfidenciālu informāciju
- Veikt saraksti Jūsu vārdā
- Kontrolēt Jūsu sociālo tīklu kontus
- Izmantot vai bojāt zīmola reputāciju
- Pārvaldīt vai dezinformēt Jūsu tīmekļa vietnei piesaistītās sistēmas/vietnes

1. SAŅEMT KONFIDENCIĀLU VAI PRIVĀTU INFORMĀCIJU.

Lai cik publiski aktīvi uzņēmums sludinātu par sava jaunā zīmola un domēna vārda maiņu, klienti, ieraduma vai vienkārši e-pasta programmas iestatījumu dēļ, sazināsies ar Jums izmantojot sev ierasto (Jūsu acīs veco) domēna vārdam piesaistīto e-pasta adresi. Tādēļ liela daļa klientu var turpināt pēc domēna vārda dzēšana pārsūtīt savu konfidenciālo informāciju jaunajam domēna vārda lietotājam. Bieži tiek piemirsti arī sadarbības partneri (tādi kā bankas un ar Jūsu darbību saistītās valsts vai pašvaldību iestādes), kuras savukārt būtu atsevišķi jāinformē par sava kontakta e-pasta adreses maiņu.

SAŅEMT KONFIDENCIĀLU INFORMĀCIJU

- Pieeja konfidenciālai e-pasta sarakstei (CC:)
- Pieeja konfidenciāliem dokumentiem un uzņēmējdarbības noslēpumiem

30% saņemto e-pastu saturēja pielikumu, no kuriem 22% bija .pdf vai .doc

Informācija no Valsts ieņēmumu dienesta

Dokuments pieņemts

Nodokļu maksātāja Nr. [redacted] iesniegtais dokuments "**Darba devēja ziņojums (VSAOI un IIN)**" Nr. [redacted] par taksācijas periodu no [redacted] **2018** līdz [redacted] **2018** pieņemts un iekļauts VID datubāzē.
Dokumentā ir 1 obligāti sociāli apdrošināmi darba ņēmēji, kam uzrādīta riska nodeva, bet nostrādāto stundu skaits ir 0.

Šis e-pasts ir izveidots automātiski, lūdzam uz to neatbildēt.
Pieslēgties VID Elektroniskās deklarēšanas sistēmai: eds.vid.gov.lv.

Document - European

File: [redacted]

Size: [redacted]

Attachments

lemums.rtf

Signatures

DINA [redacted]

Signature properties

Signer: DINA [redacted]

Time stamp: 2018 [redacted]

LATVIJAS REPUBLIKAS UZŅĒMUMU REĢISTRS

FUNKCIJU IZPILDES DEPARTAMENTS

Rīgas reģiona komercķīlu un laulāto mantisko attiecību reģistrācijas nodaļa

Reģ. Nr. 90000270634, Pērses iela 2, Rīga, LV-1011, tālrunis 67031703, fakss 67031793
e-pasts: info@ur.gov.lv, www.ur.gov.lv

LĒMUMS

Rīga

[redacted]

[redacted]

Ķīlas ņēmējs

BlueOrange

Kontu pārskats

[redacted]

Reģ. Nr.: [redacted]

Konta Nr.:
Konta Nr. (LV[redacted])

Periods:
01.01.2018 - [redacted]

Sagatavots: [redacted]

Pārskaitījumu virzieni:
Visi

Summa:
Visi

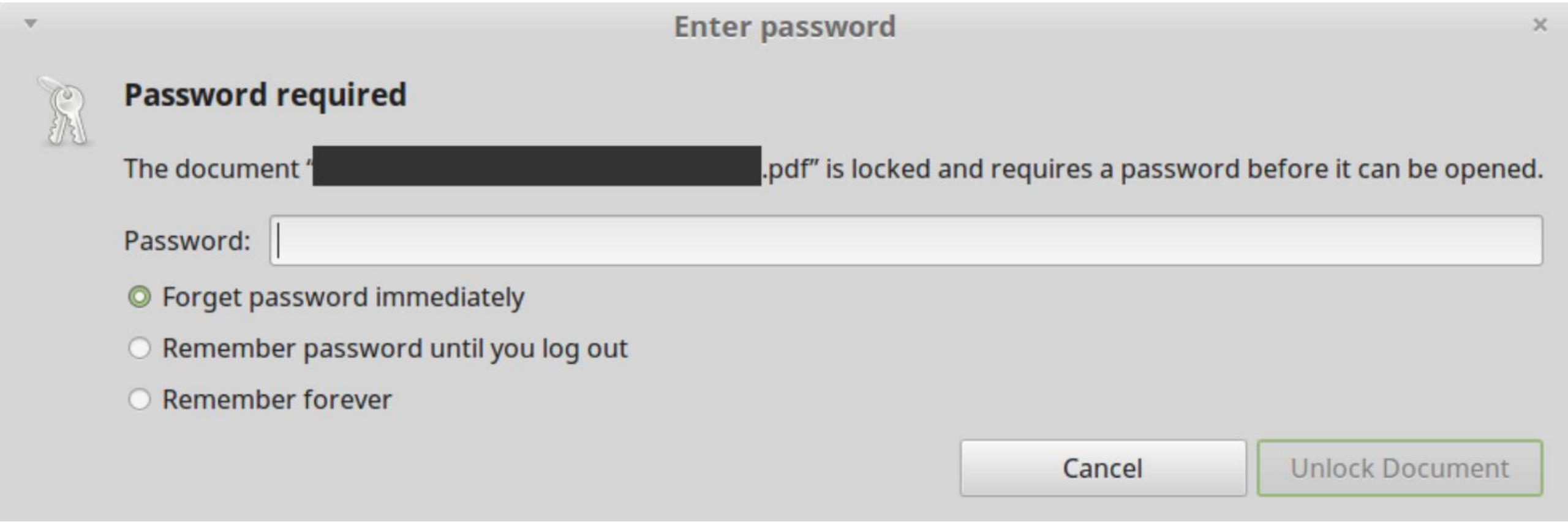
Sākuma atlikums **EUR:** [redacted]

Datums	Da[redacted]na veids	Debets	Kredīts
[redacted]2018	[redacted]		[redacted]
[redacted]2018	[redacted]		[redacted]
[redacted]2018	[redacted]		[redacted]

PIEEJA DARBINIEKU PERSONĪGAI INFORMĀCIJAI

Nereti darbinieki darba e-pasta adreses izmanto privātām vajadzībām, tādēļ uzbrucējs var:

- Pārņemt kontroli par tiešsaistes kontiem
- Saņemt sensitīvu informāciju (veselības dati)
- Saņemt vecajam lietotājam adresētus pasūtījumus


Enter password
Password required
The document “[redacted].pdf” is locked and requires a password before it can be opened.
Password:
Forget password immediately
Remember password until you log out
Remember forever
Cancel
Unlock Document

OBLIGĀTĀS VESELĪBAS PĀRBAUDES KARTE

I. Norīkojums uz obligāto veselības pārbaudi

(ārstniecības iestādes nosaukums) (norāda, ja nepieciešams)

1. Darba devējs (nosaukums, adrese, tālrunis) SIA [redacted]

2. Personas vārds, uzvārds

3. Personas kods

4. Dzīvesvieta

5. Profesija

6. Veselībai kaitīgie darba vides apstākļi

Your trip

Booking ref: [redacted]
Issued date: [redacted] 2018

Check My Trip
Baggage Info

Traveler Mr [redacted]

Agency [redacted]

Telephone
Fax
Email

[redacted]

Wednesday 26 September 2018

Air Baltic BT 641

airBaltic

Check-in

Departure	**26 September 07:50**	**Riga, (Riga Intl)** (+)
Arrival	**26 September 09:20**	**Zurich, (Zurich Airport)** (+)
Duration		02:30 (Non stop)
Distance		1481 Kms
Booking status		Confirmed
Class		Economy (U)
Baggage allowance		[redacted]
Equipment		BOEING 737-300
Flight meal		Food and beverages for purchase

CITY WEST
HOTEL RESTAURANT EVENTS

[redacted]

E-Mail: [redacted]

[redacted]

Confirmation

Dear Mrs. [redacted]

Thank you for your interest in the **CITY** WEST **HOTEL RESTAURANT EVENTS**. For the stay in our hotel we confirm the following:

Arrival	Departure	Quant.	Category		Price in CHF
		[redacted]	Comfort Single rooms	room with breakfast This rate is per room/night and includes breakfast, tourist tax, service and taxes.	128.00

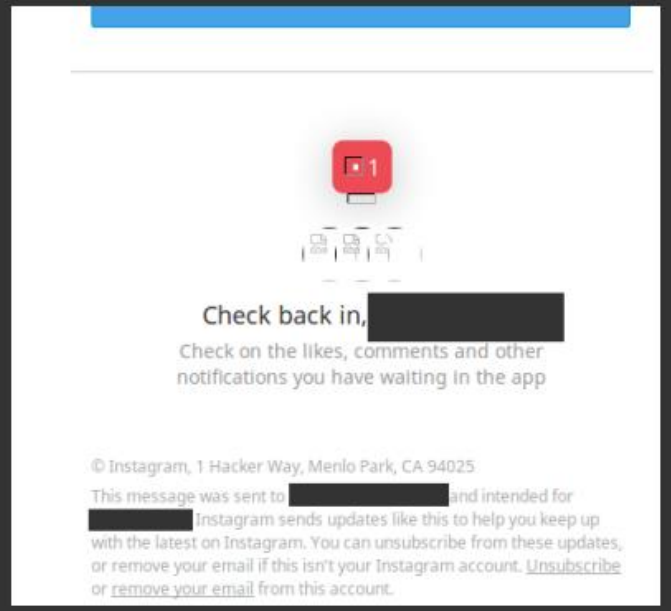
The reservation is for the following clients:

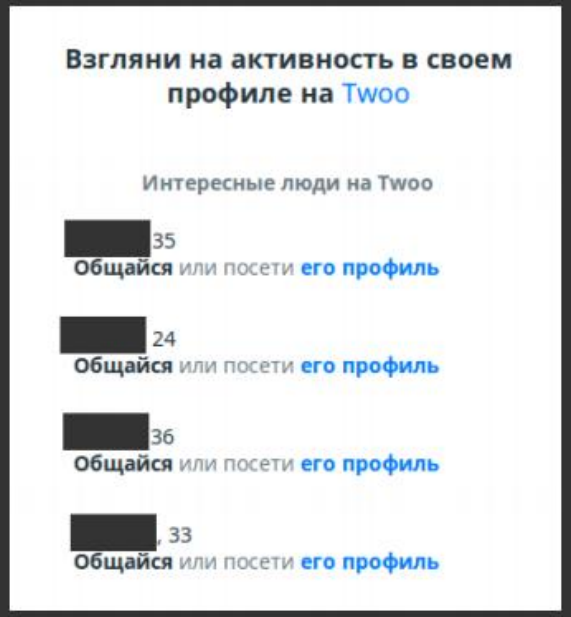
26.09.2018	[redacted] 2018	Mr.	[redacted]
26.09.2018	2018	Mr.	
26.09.2018	2018	Mr.	
26.09.2018	2018	Mrs.	
26.09.2018	2018	Mrs.	
26.09.2018	2018	Mrs.	

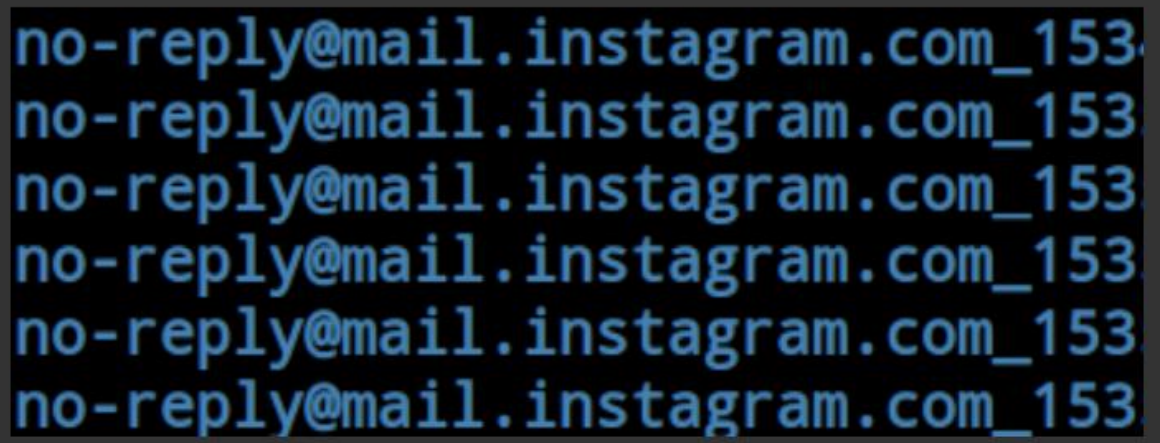

Sveiki, [redacted]
Šis ir automātisks atgādinājuma e-pasts no Mapon.com sistēmas.

Automašīna neatrodas objektā "[redacted]" laikā posmā
- [redacted]

www.mapon.com



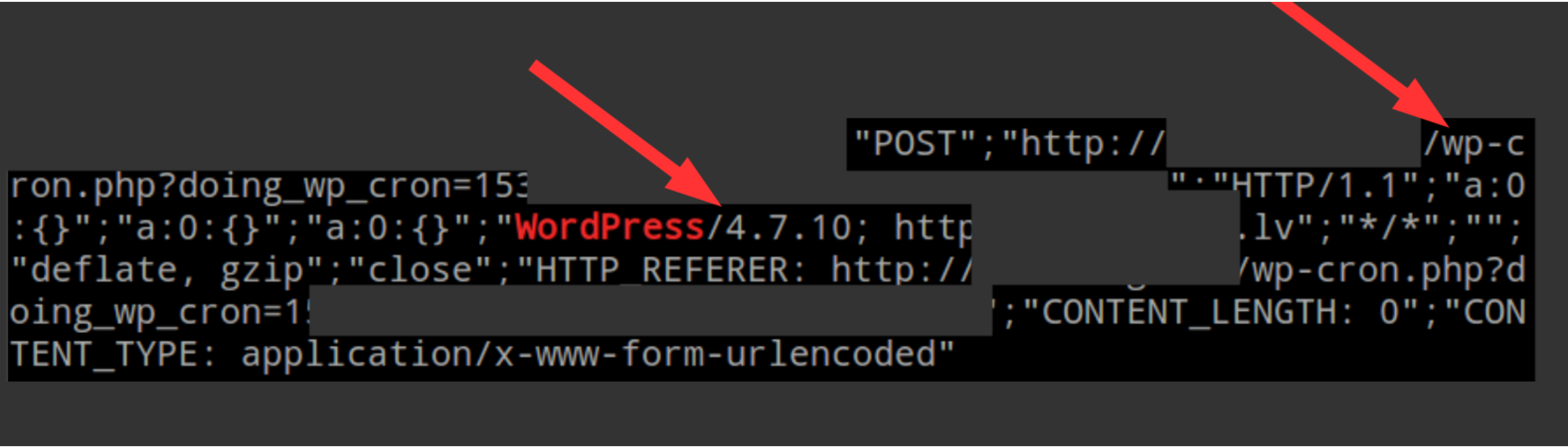


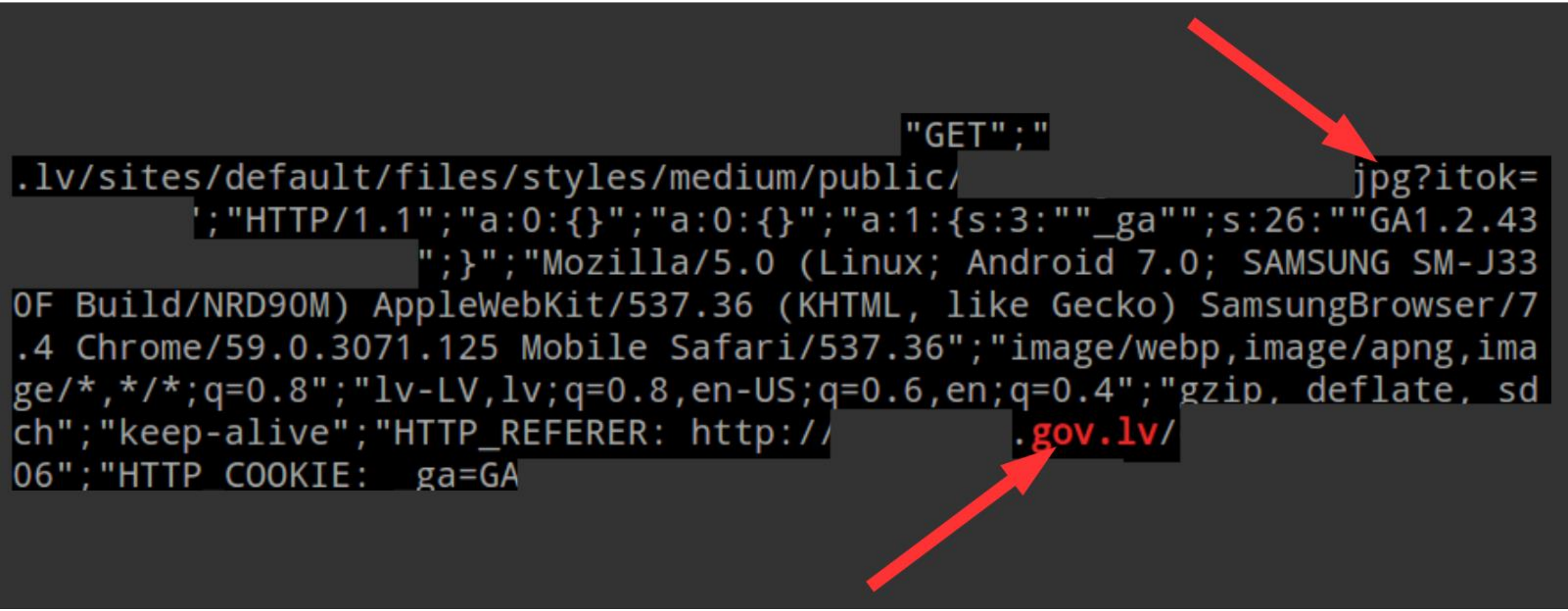


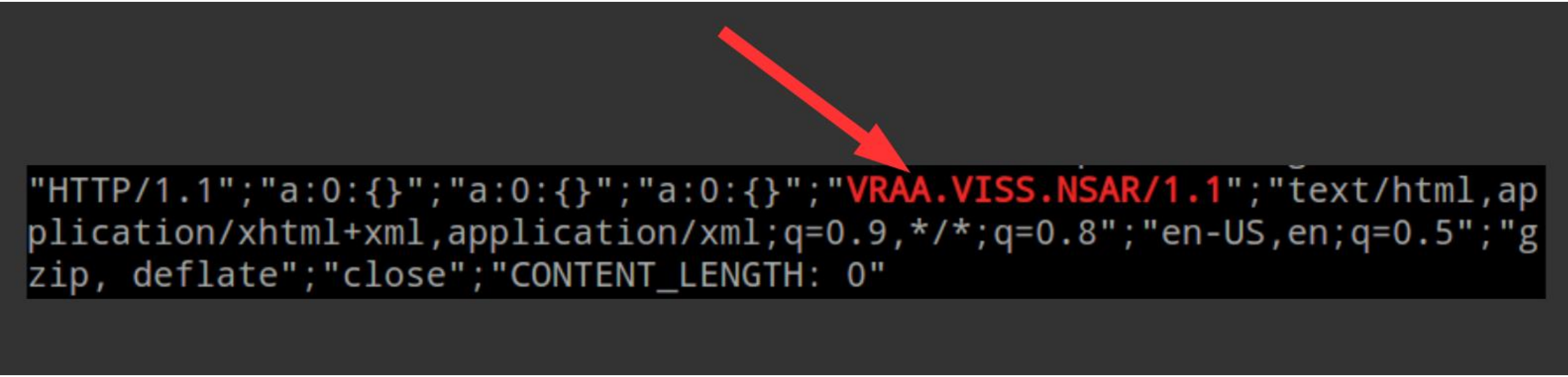
Tu saņēmi šo e-pastu, jo esi izveidojis draugiem.lv lapu. Ja turpmāk nevēlies saņemt šādus e-pasta sūtījumus, vari no tiem atteikties katras draugiem.lv lapas uzstādījumos. "Manas lapas rīki -> Profila informācija -> Paziņojumi uz e-pastu".
Ja vēlies uzreiz atteikties no šī e-pasta saņemšanas par visām lapām, kurām ir piesaistīts Tavs e-pasts, tad dodies uz šo saiti.

PĀRVALDĪT, DEZINFORMĒT DOMĒNA VĀRDAM PIESAISTĪTĀS SISTĒMAS

- Citu vietņu iegulti (embedded) html elementi ar kuru palīdzību var izveidot neautorizētu savienojumu, izplatīt vīrusu vai pārņemt kontroli pār šo vietni


"POST";"http://
/wp-c
ron.php?doing_wp_cron=153
":"HTTP/1.1";"a:0
:{}";"a:0:{}";"a:0:{}";"WordPress/4.7.10; http
.lv";"*/*";"";
"deflate, gzip";"close";"HTTP_REFERER: http://
/wp-cron.php?d
oing_wp_cron=1
;"CONTENT_LENGTH: 0";"CON
TENT_TYPE: application/x-www-form-urlencoded"


"GET";"
.lv/sites/default/files/styles/medium/public/
jpg?itok=
';"HTTP/1.1";"a:0:{}";"a:0:{}";"a:1:{s:3:""_ga"";s:26:""GA1.2.43
";}";"Mozilla/5.0 (Linux; Android 7.0; SAMSUNG SM-J33
0F Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/7
.4 Chrome/59.0.3071.125 Mobile Safari/537.36";"image/webp,image/apng,ima
ge/*,*/*;q=0.8";"lv-LV,lv;q=0.8,en-US;q=0.6,en;q=0.4";"gzip, deflate, sd
ch";"keep-alive";"HTTP_REFERER: http://
.gov.lv/
06";"HTTP_COOKIE: _ga=GA


"HTTP/1.1";"a:0:{}";"a:0:{}";"a:0:{}";"VRAA.VISS.NSAR/1.1";"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8";"en-US,en;q=0.5";"gzip, deflate";"close";"CONTENT_LENGTH: 0"

RISKI:

Reģistrējot Jūsu veco domēna vārdu tā jaunais lietotājs var iegūt kontroli pār tā saturu, vecajām e-pasta adresēm un web pieprasījumiem, līdz ar to rodas iespēja:

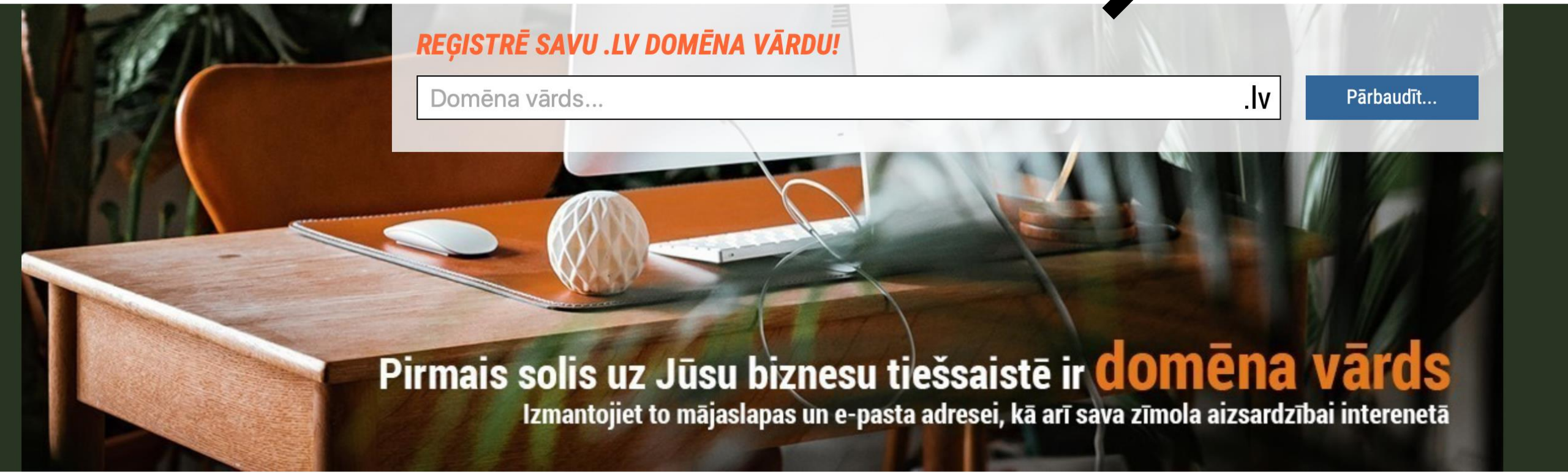
- Saņemt konfidenciālu informāciju
- Izsūtīt e-pastus Jūsu vārdā
- Pārņemt kontroli pār Jūsu sociālo tīklu kontiem
- Pārvaldīt Jūsu vietnei un domēna vārdam piesaistītās tiešsaistes sistēmas
- Bojāt reputāciju


THIS WAY
THAT WAY
ANOTHER WAY

AUDITS

- Kādus domēna vārdus mans uzņēmums izmanto un kādām vajadzībām?
- Uz kā vārda tie ir reģistrēti?
- Kurš ir/būs atbildīgs par domēna vārdiem, to reģistrāciju, administrēšanu?
- Izstrādājiet reģistrēšanas politiku: kurš uz kā vārda norādot kādu kontaktinformāciju turpmāk reģistrēs uzņēmumam nepieciešamos domēna vārdus.

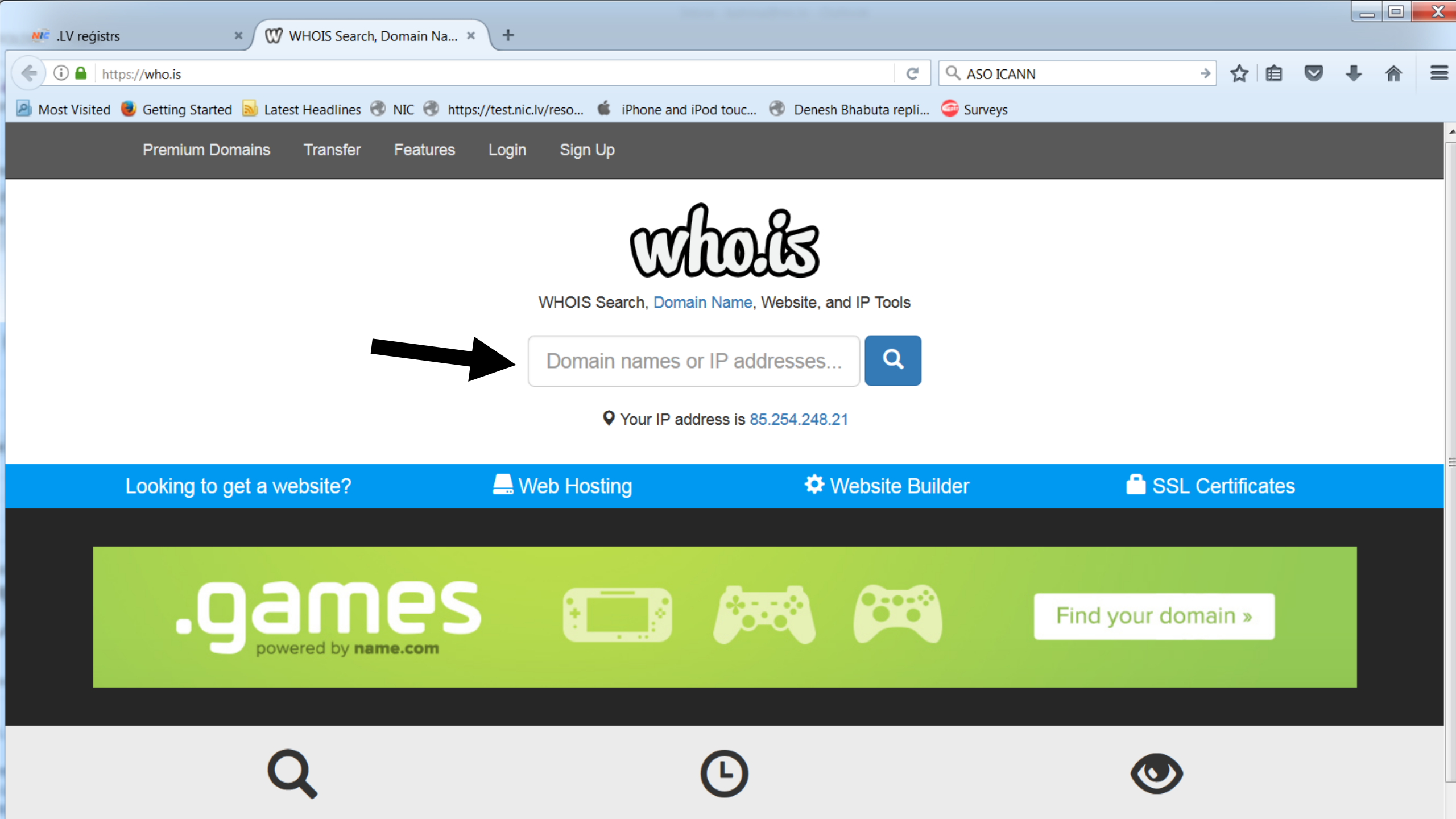
Raiņa bulv. 29,Rīga, LV-1459,Latvija •Tel. +371 67085858•E-pasts: dns@nic.lv



IZVĒLIES SAVU REĢISTRATŪRU

Pilns saraksts

serveris.lv VOOG webwide internet communication deLink we build solutions. nano Ubilibet


.LV reģistrs
WHOIS Search, Domain Na...
https://who.is
ASO ICANN
Most Visited
Getting Started
Latest Headlines
NIC
https://test.nic.lv/reso...
iPhone and iPod touc...
Denesh Bhabuta repli...
Surveys
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 85.254.248.21
Looking to get a website?
Web Hosting
Website Builder
SSL Certificates
.games
powered by name.com
Find your domain »

KO DARĪT PIRMS ATSAKOS NO DOMĒNA VĀRDA?

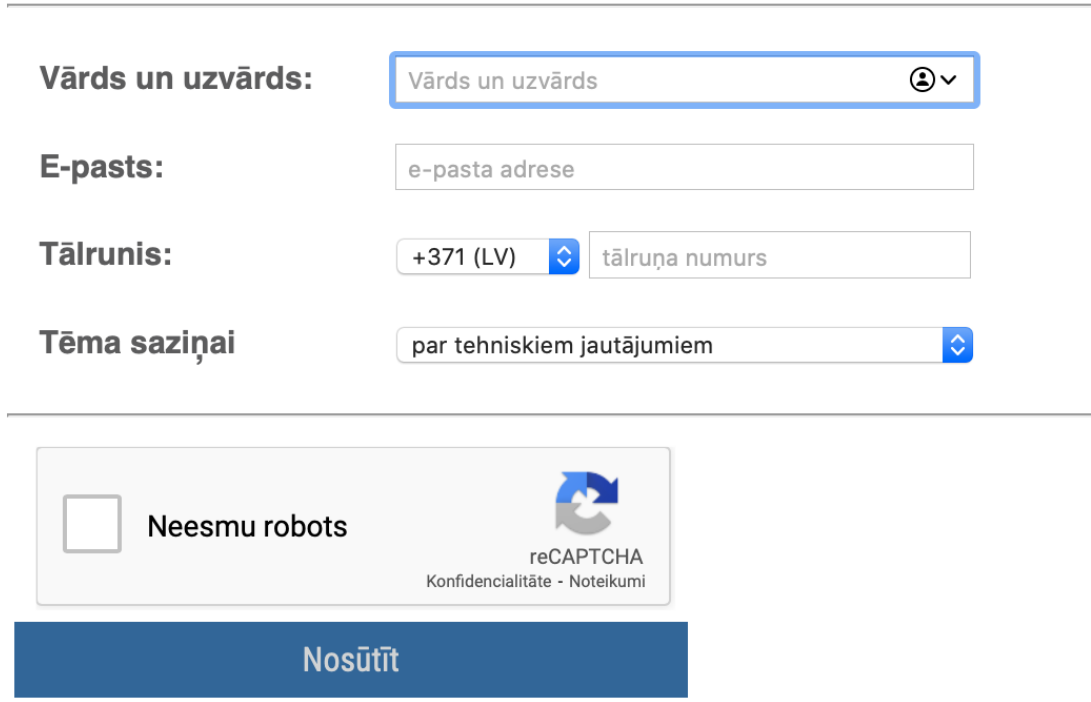
- Laicīgi un uzstājīgi informējiet savus klientus, sadarbības partnerus un trešās personas par domēna vārda maiņu;
- Atsaistiet vecās e-pasta adreses no visiem tiešsaistes kontiem un izglītojiet darbiniekus;
- Izmantojiet drošas paroles un divu faktoru autentifikāciju;
- Paturiet veco domēna vārdu 2 gadus un pārsūtiet datu plūsmu uz jauno domēna vārdu;
- Pārdodiet vai nododiet savu domēna vārdu citam interesentam.

KĀ MĒS VARAM PALĪDZĒT?

1. Sniegt konsultāciju
2. Sazināties ar domēna vārda lietotāju
3. Veikt domēna vārda lietotāja identitātes pārbaudi
4. Sniegt kompetentajām iestādēm .LV reģistrā pieejamo informāciju

.LV Whois saziņas forma

Lai sazinātos ar domēna vārda lauvasnams.lv kontaktpersonām, lūdzu



DOMĒNA VĀRDS IR NEVIS TĒRIŅŠ BET AKTĪVS

CyberChess 2023

Cybersecurity Conference
October 4 - 5
Riga, Latvia

CERT.LV
NIC
Ministry of Defence Republic of Latvia
NCC-LV Latvia Cybersecurity Coordination Centre
European Cyber Security Month
Co-funded by the European Union
ISACA Latvia Chapter
Eesti Interneti SA
Latvian Internet Association
DOM REG .lt
lmt
tet
CYBECIRCLE
Latvia State Radio and Television Center
Recorded Future
CSC
CLICO
SYNERGY CONSULTING
SANS
ICANN
CentralNic Registry

PALDIES JAUTĀJUMI?

DANA LUDVIGA,

TW, FB: @LVREGISTRS