



Finansē  
Eiropas Savienība  
NextGenerationEU

2027  
Nacionālais  
attīstības plāns



ĀRŠĀRĀDZĪBAS  
MINISTRIJA



Vides aizsardzības un  
reģionālās attīstības  
ministrija



CERT.LV  
Informācijas tehnoloģiju  
drošības centrs  
nodrošinot drošību



ZEMGALES  
PLĀNOŠANAS  
REĢIONS



trainify

CIVILMILITĀRĀS SADARBĪBAS VEICINĀŠANA REĢIONOS

## IT datu drošības pamati - praktiskas iemaņas ikdienas darbā

5.martā 13:00 - 16:30

6.martā 9:00 - 12:00

Tiešsaistē



- ▶ Ievads
- ▶ Ievads par IT datu drošību
- ▶ Datu drošība
- ▶ Pašvaldības Informācijas sistēmas drošības politika un pārvaldība
- ▶ Paroļu politika
- ▶ 2. diena
  - ▶ Darbs attālināti
  - ▶ E-pasta drošība
  - ▶ Jautājumi un atbildes

- ▶ Darba gaita
- ▶ Par mani
  - ▶ Vitālijs Grīnbergs
  - ▶ 17 gadu pieredze IT drošībā
  - ▶ Valsts informācijas sistēmas drošības pārvaldnieks (BURVIS, URIS), 2007-2020 gads
  - ▶ NBS IT speciālists, 1999-2019 gads
  - ▶ Vadošais programmatūras piegādes un drošības speciālists – DevSecOps (Tietoevry Banking Latvia), 2020 - ...

# Ievads par IT datu drošību

Noteiktās likumi, kārtības, standarti, vadlīnijas u.c.

- ▶ **ISO 27001** – IT pārvaldības standarts
- ▶ **PCI saime, SSF, DSS, 3DS** – maksājumu karšu drošības standarts
- ▶ **GDPR** – Vispārīgais personu datu aizsardzības regulējums
- ▶ **NIST** – drošības kontroles un labākās prakses, ASV standartu un tehnoloģiju institūts
- ▶ **CSA** – mākoņdatošanas drošības prakses un vadlīnijas
- ▶ **COBIT** – pārvaldības, apmācības, integrācijas un kontroļu kopums

# Ievads par IT datu drošību

Noteiktās likumi, kārtības, standarti, vadlīnijas u.c.

- ▶ **NIS2** – obligātās drošības un incidentu paziņošanas prasības attiecībā uz digitālajiem pakalpojumiem kritiskiem pakalpojumiem
- ▶ **DORA** - digitālās darbības noturības akts, Eiropas finanšu sektors
- ▶ **CER** - pasākumus kritiskajām iestādēm un infrastruktūras objektiem, piemēram, enerģētikas, transporta, telekomunikāciju, finanšu vai veselības aprūpes nozarei
- ▶ **CRA** – attiecas uz Eiropas Savienības digitālo infrastruktūru un uzņēmumiem, kuriem ir svarīga loma digitālajā vidē

# Ievads par IT datu drošību

Noteiktās kārtības, standarti, vadlīnijas u.c.

- ▶ Informācijas tehnoloģiju drošības likums
- ▶ Valsts informācijas sistēmu likums
- ▶ Fizisko personu datu apstrādes likums
- ▶ MK noteikumi Nr. 442
  - ▶ Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām

# Ievads par IT datu drošību

7

Noteiktās kārtības, standarti, vadlīnijas u.c., [cert.lv dokumentācijas paraugi](#)

[Sākums](#) > [Valsts un pašvaldību iestādēm](#) > [IT drošības dokumentācijas paraugi](#)

## IT drošības dokumentācijas paraugi

Ministru kabineta noteikumi Nr. 442 "[Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām](#)" nosaka minimālās tehniskās, dokumentālās un organizatoriskās prasības informācijas sistēmu drošībai.

Dokumentu paraugi\* (piemēri ir balsīti uz iedomātu virtuālo iestādi):

Virtuālās iestādes apraksts un sistēmu novērtējums - [doc](#); [pdf](#)

[Jautājumi un atbildes par dokumentu izstrādi.](#)

[Lietotie termini.](#)

# Ievads par IT datu drošību

- ▶ Sertifikācijas piemēri iestādēm





# Ievads par IT datu drošību

- ▶ Kvalifikācijas un sertifikācijas profesionāļiem



# Ievads par IT datu drošību

10

- ▶ Sertifikācijas auditi, ārējie
  - ▶ PWC
  - ▶ Deloitte
  - ▶ KPMG
  - ▶ Ernst & Young
  - ▶ U.c.

# Ievads par IT datu drošību

## Apmācības

- ▶ LIKTA – Latvijas Informācijas un Komunikācijas Tehnoloģijas (IKT) Asociācija
- ▶ BDA – Baltijas Datoru Akadēmija
- ▶ RTK – Rīgas Tehniskā Koledža
- ▶ DVI – Datu Valsts Inspekcija

## Seminari

- ▶ Cert.lv
- ▶ citi

# Ievads par IT datu drošību

12

Vai sertifikāciju esamība garantē drošību?

- ▶ IT drošības pārvaldības procesi aprakstīti, bet netiek ievēroti
- ▶ Sertifikācija ir tikai formalitāte
- ▶ Kontroles nav piemērotas atbilstoši reālajai situācijai
- ▶ Darbiniekiem trūkst zināšanas par pastāvošo kārtību

# Ievads par IT datu drošību

13

Vai drošības pasākumu ieviešana garantē sertifikāciju?

- ▶ Ieviestās prakses atbilst labai pieredzei, bet ne standartiem
- ▶ Raksturīgi maziem uzņēmumiem, resursu trūkumu dēļ
- ▶ Sertifikācija nav nepieciešama

# Ievads par IT datu drošību

14

Jautājumi?

# Datu drošība

# Datu drošība

16

Kas tad ir datu drošība?

- ▶ Balanss starp vajadzībām, prasībām un iespējām
- ▶ Sajūta ka dati kalpos tiem paredzētiem mērķiem

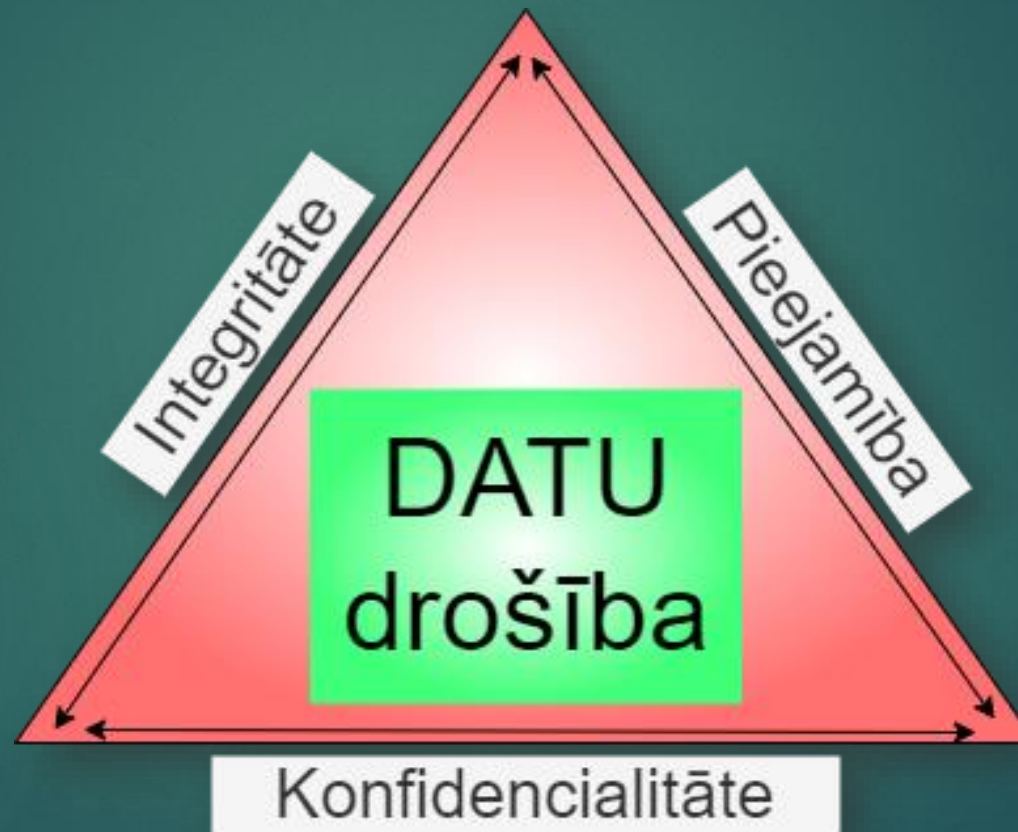
Raksturīpašības:

- ▶ **Konfidencialitāte**
- ▶ **Pieejamība**
- ▶ **Integritāte**



# Datu drošība

17



# Datu drošība

Konfidencialitātes raksturīpašības:

- ▶ Noteiktā informācija pieejama tikai noteiktam personu lokam
- ▶ Nepieciešamība zināt vai need-to-know princips
- ▶ Informācijas aizsardzība pret neautorizētu piekļuvi

Konfidenciālo datu piemēri:

- ▶ Personu dati
- ▶ Maksājumu karšu dati
- ▶ Līgumi, vienošanās
- ▶ Iepirkumu dati, pretendentu vai dalībnieku saraksti
- ▶ Sistēmu piekļuves rekvizīti
- ▶ Šifrēšanas atslēgas, paroles
- ▶ U.c.

# Datu drošība

20

Konfidencialitāte, datu klasifikācija:

- ▶ **vispārpieejamā informācija**
- ▶ **Ierobežotas pieejamības**
- ▶ **Informācija dienesta vajadzībām**
- ▶ **Konfidenciāla**
- ▶ **Slepena**
- ▶ **Sevišķi slepena**

Informācijas atklātības likums

Likusms Par Valsts noslēpumu

# Datu drošība

21

Konfidencialitāte, aizsardzība:

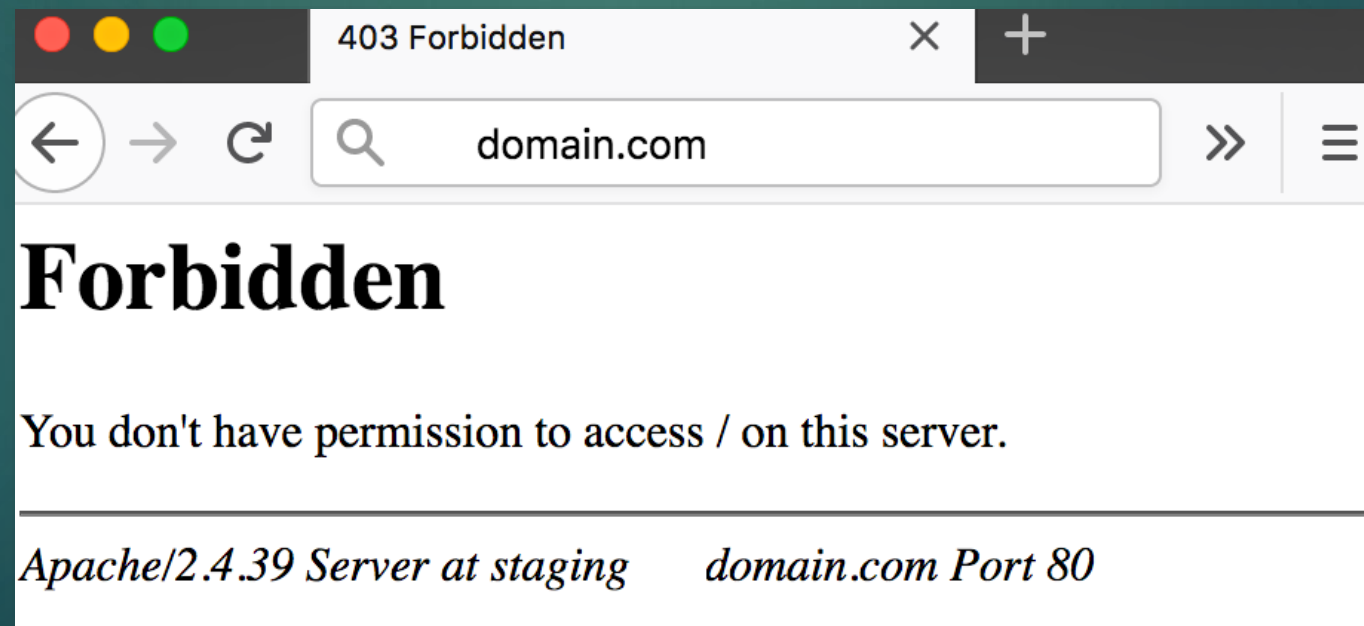
- ▶ Datu anonimizēšana
- ▶ Vienošanās par datu neizpaušanu (NDA - non-disclosure agreement)

# Datu drošība

22

Pieejamības raksturīpašības:

- ▶ Autorizēta piekļuve informācijai laikā un vietā



Pieejamības raksturīpašības, aizsardzība:

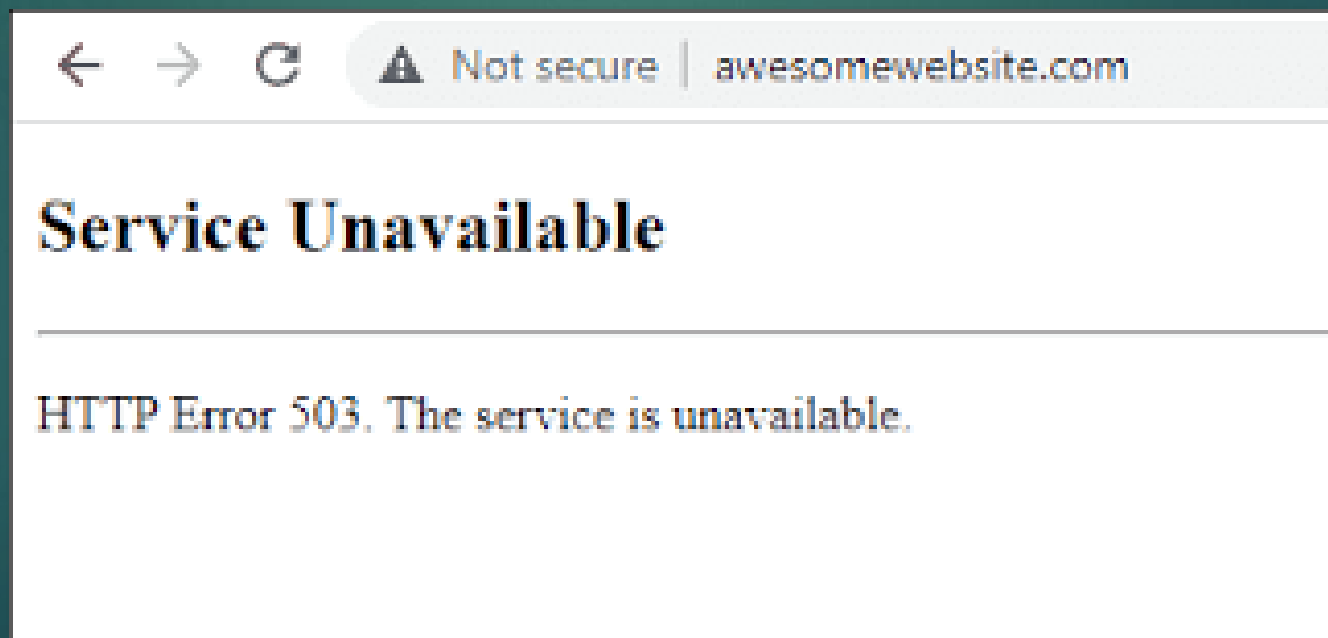
- ▶ Sistēma ir pieejama tikai darba laikā, darba dienās, utt.
- ▶ Sistēma ir pieejama tikai notiktām valstīm
- ▶ Sistēma ir pieejama tikai no saderīgas ierīces
- ▶ Dinamiskā pieejamība:
  - ▶ Atrašanās vieta, IP adrese, MFA

# Datu drošība

24

Pieejamības raksturīpašības, kļūmes:

- ▶ Kļūmes dēļ, sistēmā nav pieejama





Pieejamības raksturīpašības, uzturēšana:

- ▶ Plānoto uzturēšanas darbu dēļ, sistēmā nav pieejama



## Website under maintenance

This website is currently undergoing scheduled maintenance. We should be back shortly.

Pieejamības raksturīpašības, SLA:

- ▶ Latvija.lv lapa pieejama 99,99% gada laikā:
  - ▶ Gada laikā sistēma nebūs pieejama 52 minūtes
- ▶ SLA neiekļauj plānotos uzturēšanas darbus

<https://uptime.is/>

## Uptime and downtime with 99.99 % SLA

[ [simple](#) / [flexible](#) / [compare](#) / [reverse](#) / [about](#) / [API](#) ]

Agreed SLA level:  % (enter SLA level and hit the <enter> key)

SLA level of 99.99 % uptime/availability results in the following periods of allowed downtime/unavailability:

- **Daily:** 8.6s
- **Weekly:** 1m 0.48s
- **Monthly:** 4m 21s
- **Quarterly:** 13m 2.4s
- **Yearly:** 52m 9.8s

Direct link to the page with these results: [uptime.is/99.99](https://uptime.is/99.99) (or [uptime.is/four-nines](https://uptime.is/four-nines))

The SLA calculations assume a requirement of continuous uptime (i.e. 24/7 all year long) with additional approximations as described in the [source](#). *uptime.is* was originally implemented in [newLISP](#), which had powered uptime and downtime calculations for more than a decade.

For convenience, there are special CEO and SEO friendly links for *N nines*: [three nines](#), [four nines](#), [five nines](#), [six nines etc.](#)

Integritātes raksturīpašības:

- ▶ Sistēmu, programmu un datu aizsardzība pret nefīšu vai ļaunprātīgu bojāšanu vai pārveidošanu

Integritātes nodrošināšana

- ▶ Atbilstoša datu šifrēšana to pārraides laikā
- ▶ Datu veseluma nodrošināšana to glabāšanas laikā

# Datu drošība

28

Integritāte nodrošināšana

- ▶ Datu validācija to ievades laikā

The screenshot shows an 'Order Form' with several input fields. The 'First Name' field contains 'Linda' and the 'Last Name' field contains 'Johnson'. The 'Email Address' field contains 'linda.johnson2gmail.co,' and is highlighted with a red border and a red error message below it: 'Please enter a valid email address.' The 'Credit Card Number' field contains '1234 5678 9999 1111'. The 'Expiration Date (MM/DD/YYYY)' field contains '01-20-34' and is also highlighted with a red border and a red error message below it: 'Please use the MM/DD/YYYY format.'

**Order Form**

First Name: Linda

Last Name: Johnson

Email Address: linda.johnson2gmail.co,  
Please enter a valid email address.

Credit Card Number: 1234 5678 9999 1111

Expiration Date (MM/DD/YYYY): 01-20-34  
Please use the MM/DD/YYYY format.

# Datu drošība

29

▶ Jautājumi

# Pašvaldības Informācijas drošības politika un pārvaldība

# Pašvaldības Informācijas drošības politika un pārvaldība

31

- ▶ Informācijas tehnoloģiju drošības likums
- ▶ Valsts informācijas sistēmu likums
- ▶ Fizisko personu datu apstrādes likums
- ▶ MK noteikumi Nr. 442

# Pašvaldības Informācijas drošības politika un pārvaldība

Nosaka informācijas sistēmu veidus to funkcijas, atbildības utt.

Nosaka to minimālās aizsardzības prasības:

- ▶ Kritiskās Eiropas un/vai valsts infrastruktūrai
- ▶ VIS Savietotajās un tā noteikumi, piemēram **latvija.lv**
- ▶ VIS noteikumi



# Pašvaldības Informācijas drošības politika un pārvaldība

MK noteikumi Nr. 442

Sistēmu klasifikācija pēc drošības klasēm, pieejamība:

- ▶ A – sistēmas darbības pārtraukums < 4st mēnesī
- ▶ B – sistēmas darbības pārtraukums < 24st mēnesī
- ▶ C – sistēmas darbības pārtraukums > 24st mēnesī



# Pašvaldības Informācijas drošības politika un pārvaldība

34



Kā jūs raksturotu datu pieejamību?

Ierakstiet lūdzu čatā savu variantu

# Pašvaldības Informācijas drošības politika un pārvaldība

Datu pieejamības piemēri:

- ▶ Interneta pieejamība
- ▶ Sistēmas pieejamība
- ▶ Maksājumu pieejamība
- ▶ Pakalpojuma pieejamība



# Pašvaldības Informācijas drošības politika un pārvaldība

36

MK noteikumi Nr. 442

Sistēmu klasifikācija pēc drošības klasēm, integritāte:

- ▶ A, B, C līmeņi



# Pašvaldības Informācijas drošības politika un pārvaldība

37



Kā jūs raksturotu datu integritāti?

Ierakstiet lūdzu čatā savu variantu

# Pašvaldības Informācijas drošības politika un pārvaldība

38

## Datu integritāte

- ▶ Algu saraksti
- ▶ Personu dati
- ▶ Lietvedības datu bāze
- ▶ Uzticamas datu rezerves kopijas
- ▶ U.c.



# Pašvaldības Informācijas drošības politika un pārvaldība

39

MK noteikumi Nr. 442

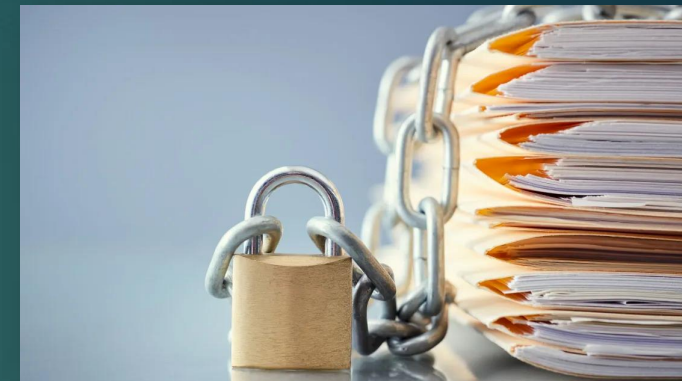
Sistēmu klasifikācija pēc drošības klasēm, konfidencialitāte:

- ▶ A, B, C līmeņi



# Pašvaldības Informācijas drošības politika un pārvaldība

40



Kā jūs raksturotu datu konfidencialitāti?

Ierakstiet lūdzu čatā savu variantu



# Pašvaldības Informācijas drošības politika un pārvaldība

41

Datu konfidencialitāte

- ▶ Slepena
- ▶ Sensitīvi personu dati
- ▶ Paredzēta tikai noteiktam personu lokam



# Pašvaldības Informācijas drošības politika un pārvaldība

MK noteikumi Nr. 442

Sistēmu klasifikācija pēc drošības klasēm:

- ▶ ja sistēmai piešķirtas **trīs B drošības klases vai vismaz viena A drošības klase**, sistēma ir uzskatāma par **paaugstinātas drošības sistēmu**
- ▶ Ierakstiet lūdzu čatā ar kuru sistēmas klasi, pēc jūsu domām, jūs strādājat ikdienā

# Pašvaldības Informācijas drošības politika un pārvaldība

43

NVA - BURVIS

UR - URIS

# Pašvaldības Informācijas drošības politika un pārvaldība

VIS normatīvo dokumentu bāze

- ▶ **Sistēmas drošības politika**
- ▶ Sistēmas drošības iekšējie noteikumi, (tikai paaugstinātas drošības sistēmām)
- ▶ Sistēmas lietošanas noteikumi, (tikai paaugstinātas drošības sistēmām)
- ▶ Sistēmas drošības riska pārvaldības plāns, (tikai paaugstinātas drošības sistēmām)
- ▶ Sistēmas darbības atjaunošanas plāns, (tikai paaugstinātas drošības sistēmām)

# Paroles

# Paroļu politika

46

Kā ieviest drošu un vienkārši pārvaldāmu paroļu sistēmu?

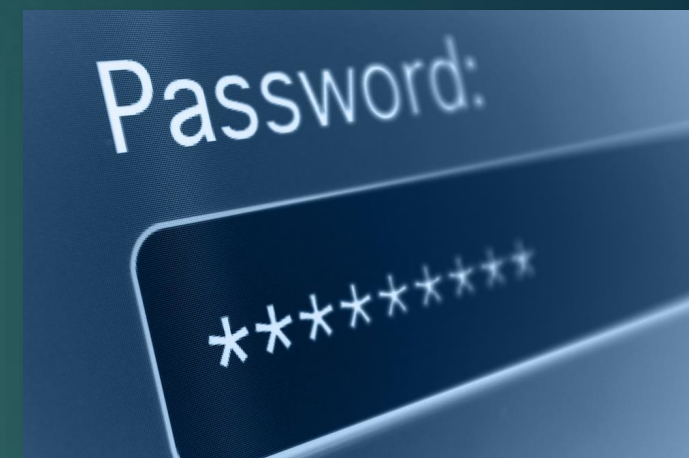


# Paroļu politika

47

Ieliekat + čatā ja lietojat kādu parolu pārvaldības programmu, pārlūku, citu aplikāciju

Ieliekat - čatā ja nelietojat parolu pārvaldības programmu



# Paroļu politika

48

Jāzina paroles prasības uzņēmumā.

To parasti nosaka Lietošanas noteikumi.

Parasti:

- ▶ 8-9 simbolus gara, satur 3 simbolu grupas, termiņš 90 dienas





# Paroļu politika

49

Vai lietot vienu **sarežģītu** paroli visur?

Sarežģīta parole:

**4 simbolu grupas:** cipari, mazie, LIELIE burti, sp@ciālie \$imboli

!QAZ@WSX3edc

Gara dažādu nesaistītu vārdu parole:

Zirgi sk@pis div1 viens

# Parolu politika

<https://www.security.org/how-secure-is-my-password/>

Zirgi sk@pis div1 kas

!QAZ@WSX3edc

## How Secure Is My Password?

✔ The #1 Password Strength Tool. Trusted and used by millions.

It would take a computer about

3 octillion years

to crack your password

## How Secure Is My Password?

✔ The #1 Password Strength Tool. Trusted and used by millions.

It would take a computer about

34 thousand years

to crack your password

# Parolu politika

51

<https://www.security.org/how-secure-is-my-password/>

Marts 15!%

## How Secure Is My Password?

✔ The #1 Password Strength Tool. Trusted and used by millions.



It would take a computer about

**3 weeks**

to crack your password

# Paroļu politika

52

Ko darīt?

Izmantot paroļu glabāšanas programmas, aplikācijas

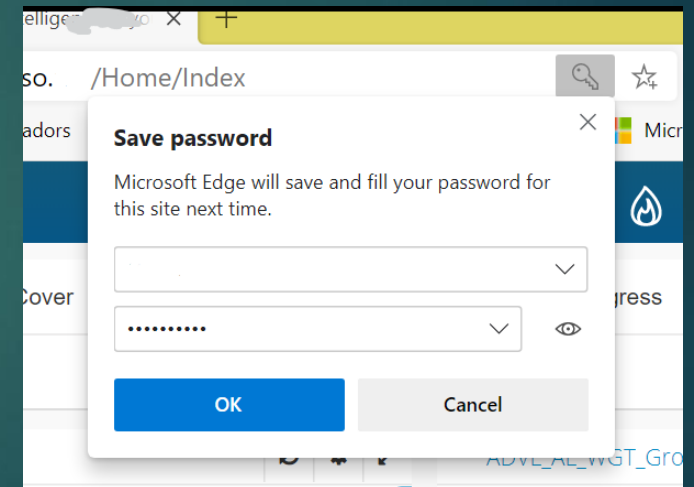
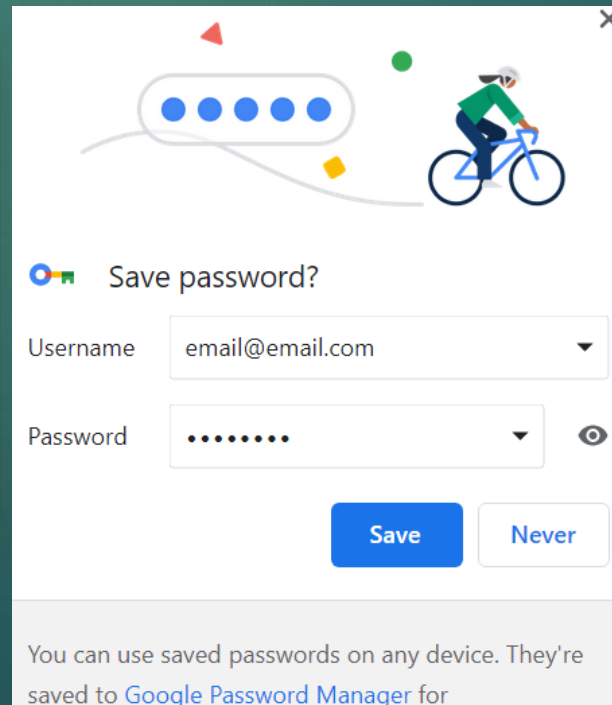
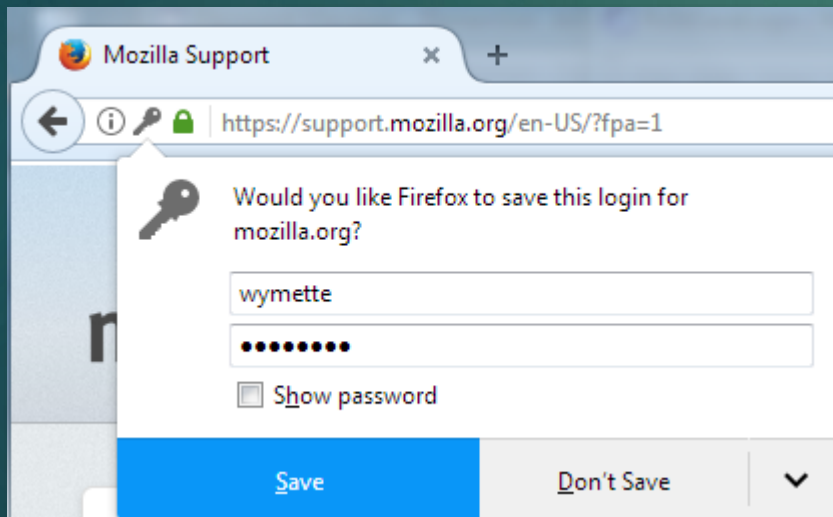
Programmatūras instalāciju jāsaskaņo ar drošības specialistu.



# Paroļu politika

53

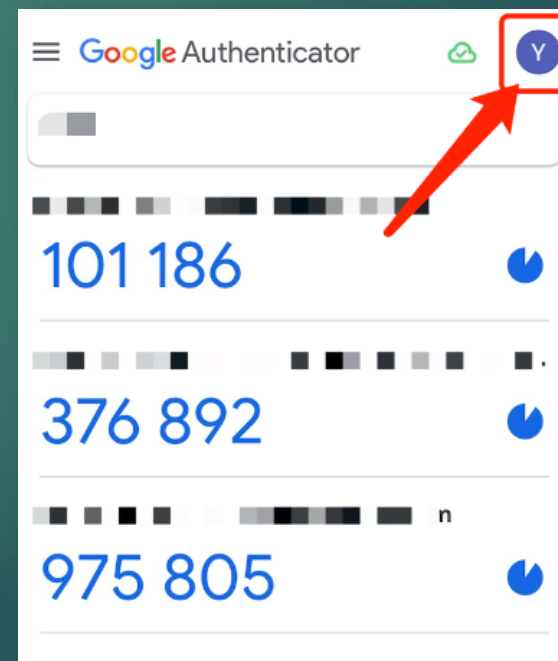
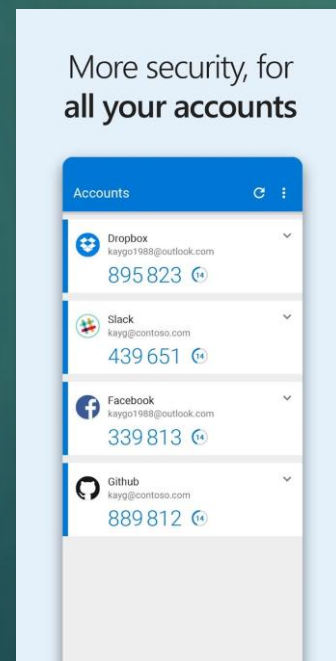
Izmantot paroļu ģenerēšanas un glabāšanas iespējas pārlūkā vai mobilajā ierīcē



# Paroļu politika

54

Izmantot paroļu ģenerēšanas un glabāšanas iespējas pārlūkā vai mobilajā ierīcē



# Paroļu politika

55

## Izmantot savu paroļu sistēmu

- ▶ Sadalīt paroli daļās: statiskā daļa, piederība, mainīgā daļa

m@n@BANKA02@\$

m@n@BANKA02)@

# Paroļu politika

56

Izmantot savu paroļu sistēmu un kombinēt tās

- ▶ Sadalīt paroli daļās: statiskā daļa, piederība, mainīgā daļa  
m@n@BANKA02)@



**How Secure Is My Password?**

✔ The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about  
**2 million years**  
to crack your password

The image shows a blue interface for a password strength tool. At the top, it asks 'How Secure Is My Password?'. Below that, it states 'The #1 Password Strength Tool. Trusted and used by millions.' with a green checkmark icon. There is a white input field containing a password represented by dots. Below the input field, it says 'It would take a computer about 2 million years to crack your password'.



# Paroļu politika

57

Kur vien iespējams izmantot daudzfaktorū autentifikāciju, MFA



# Paroļu politika

58

Kas ir MFA?

- ▶ ko es zinu – PAROLE
- ▶ kas man ir – aplikācija, eID, e-paraksts mobile, SmartID, u.c.
- ▶ kas esmu – biometrijas dati
- ▶ kur es atrodos – lokācijas dati

# Paroļu politika

59

Izmantot savu paroļu sistēmu un kombinēt tās:

- ▶ Saglabāt paroles pārlūkā un izmantot daudzfaktoru autentifikāciju
- ▶ Kur iespējams izmantot oficiāli atzītus autentifikācijas pakalpojumu sniedzējus:
  - ▶ E-paraksts mobile
  - ▶ Smart-ID
  - ▶ MS vai Google authenticator

# Paroļu politika

60

Nosacījumu piekļuve, Conditional access



# Darbs attālināti

# Darbs attālināti

62

Šie ieteikumi palīdzēs nodrošināt, ka jūsu darbs no mājām būs drošs un sasniegs informācijas drošības prasības



# Darbs attālināti

63

Vai ir iespējams veikt darbu attālināti?

Jāzina vai Informācijas sistēma pieejama:

- ▶ tiki darba vietā
- ▶ no speciāli tam darbam sagatavota datora

Sevišķā lietvedība, klasificēta informācija u.c. ierobežojošie faktori

# Darbs attālināti

- ▶ Izveidojiet drošu un atjauninātu tīkla savienojumu
- ▶ Aizsargājiet savu datoru
- ▶ Izmantojiet drošu pieslēgšanos
- ▶ Aizsargājiet savu darba informāciju
- ▶ Uzmanieties no phishing uzbrukumiem
- ▶ Nodrošiniet savu darba vietu
- ▶ Regulāri veiciet datu dublēšanu



# Darbs attālināti

65

Izveidojiet drošu un atjauninātu tīkla savienojumu

- ▶ Izvēlaties uzticamu WiFi tīklu, mājās, darbā, hotspot (mobilais tīklājs)
- ▶ Nomainiet mājas rūtera noklusējuma paroli
- ▶ Atjauniniet rūtera programmatūru

# Darbs attālināti

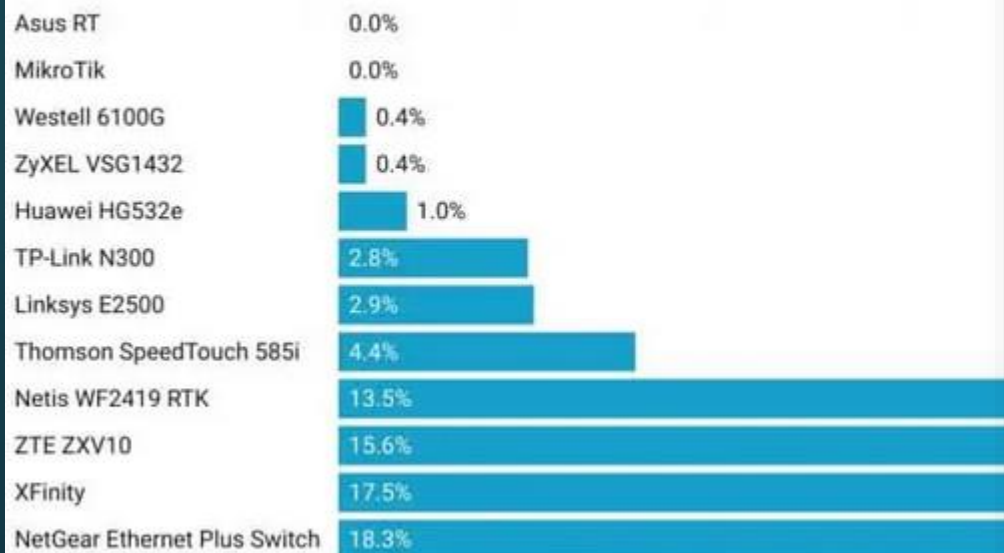
66

Izveidojiet drošu un atjauninātu tīkla savienojumu

► Nomainiet mājas rūtera noklusētos uzdevus

## Wi-fi routers vulnerable to default logins attack

The percentages of internet-connected wi-fi routers that could be accessed using the default login credentials. These are the best-selling wi-fi routers on Amazon.com as of June 2021.



Source: Comparitech.com • Created with Datawrapper

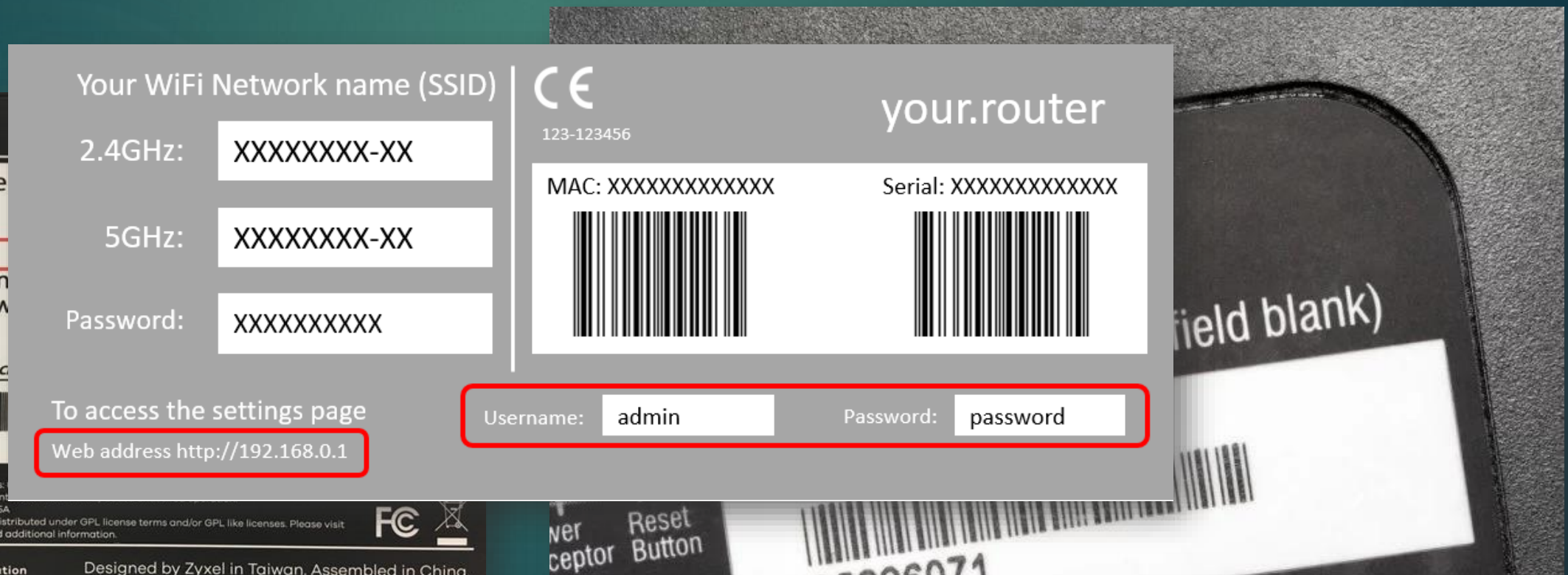
Router model	Successful logins	# Tested
Asus RT	0.00%	307
MikroTik	0.00%	463
Westell 6100G	0.40%	753
ZyXEL VSG1432	0.40%	1001
Huawei HG532e	1.00%	546
TP-Link N300	2.80%	1000
Linksys E2500	2.90%	1000
Thomson SpeedTouch 585i	4.40%	998
Netis WF2419 RTK	13.50%	1000
ZTE ZXV10	15.60%	859
XFINITY	17.50%	1000
NetGear Ethernet Plus Switch	18.30%	1000

# Darbs attālināti

67

Izveidojiet drošu un atjauninātu tīkla savienojumu

- ▶ Kā atjaunināt mājas rūtera programmatūru un nomainīt paroles



# Darbs attālināti

68

Izveidojiet drošu un atjauninātu tīkla savienojumu

- ▶ Nomainiet noklusējumu

The screenshot displays the NETGEAR genie web interface. At the top, there is a navigation bar with 'BASIC' and 'ADVANCED' tabs. A notification banner states 'A router firmware upgrade is available.' The top right corner includes a 'Logout' button, 'Firmware Version V1.0.2.54\_1.0.56', and a language dropdown set to 'English'. The main content area shows a '2.4GHz Basic Settings' dialog box with the following fields:

- Network Name(SSID) \* : My ZTE Wi-Fi
- Broadcast SSID
- All the wireless client device is completely isolated
- Security Mode : WPA2(AES)-PSK
- Password \* : .....
- Display Password
- Max Station Number : 32

An 'Apply' button is located at the bottom right of the dialog box. In the background, another 'Apply' and 'Cancel' button pair is visible on the main page.

# Darbs attālināti

69

Izveidojiet drošu un atjauninātu tīkla savienojumu

► Pārbaudiet vai ir pieejami rūtera atjauninājumi

The image shows two overlapping screenshots of router firmware update interfaces. The top screenshot is for a Netgear R6080 router, displaying the 'Check For Updates' window with 'Channel: stable', 'Installed Version: 7.13.3', and 'Latest Version: 7.13.3'. The 'ADVANCED' tab is highlighted in red. The bottom screenshot is for a D-Link router, showing the 'Firmware Update' page with 'Local Update' and 'Remote Update' sections. The 'CHECK FOR UPDATES' button is highlighted in green. A yellow box at the bottom left of the D-Link interface states 'System is already up to date'.

**NETGEAR**  
R6080  
BASIC **ADVANCED**

Channel: stable  
Installed Version: 7.13.3  
Latest Version: 7.13.3

Router Firmware Version V1.0.0.42  
Logout  
English

**D-Link**  
Building Networks for People

Home **Firmware Update**

Advanced  
Firewall  
System  
Configuration  
Firmware Update  
Log  
Ping

Local Update  
Current firmware version: 1.0.1  
CHOOSE FILE... File is not selected  
UPDATE FIRMWARE

Remote Update  
Remote server URL  
fwupdate.dlink.ru  
Check for updates automatically  
CHECK FOR UPDATES APPLY SETTINGS

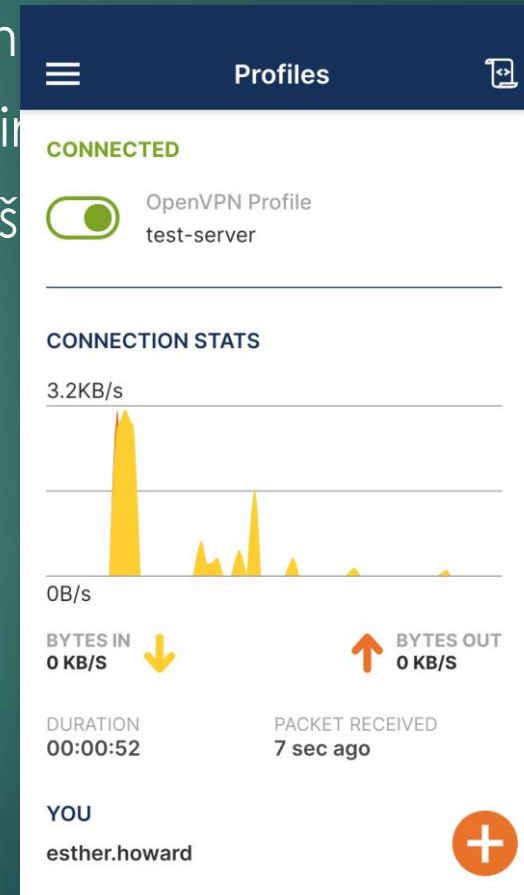
System is already up to date

# Darbs attālināti

- Izveidojiet
- ▶ Pieslēgš
- ▶ Lietojiet



- vienojum
- a paplašin
- nepiecieš

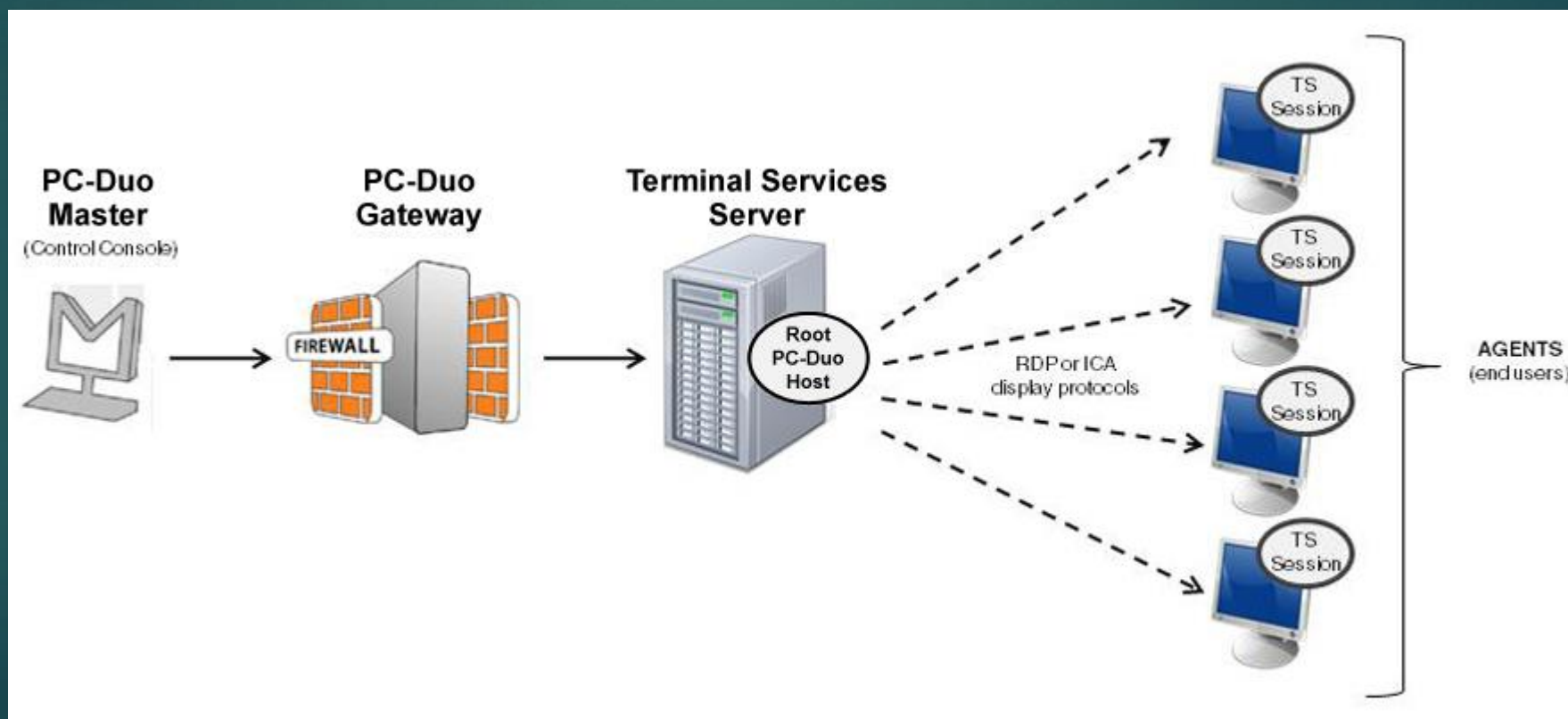


# Darbs attālināti

71

Izveidojiet drošu un atjauninātu tīkla savienojumu

- ▶ Starpniekservera izmantošana



Aizsargājie

- ▶ datora  
piedāv



## Use Windows Hello with your account

Your organization requires you to set up your work or school account with Windows Hello Face, Fingerprint, or PIN.

If you've already set up Windows Hello on this device, we'll automatically add it for this account. You may be asked to re-verify with Windows Hello.

If your organization requires a more complex PIN, Windows will prompt you to change it.

OK











# Darbs attālināti

73

Windows drošība

Īsumā par drošību

Noskaidrojiet, kāda ir jūsu ierīces drošība un darbspēja, un veiciet nepieciešamās darbības.

 <p><b>Pretvīrusu un pretdraudu aizsardzība</b> Nav jāveic neviena darbība.</p>	 <p><b>Konta aizsardzība</b> Nav jāveic neviena darbība.</p>
 <p><b>Programmu un pārlūku vadība</b> Nav jāveic neviena darbība.</p>	 <p><b>Ierīces drošība</b> Skatīt statusu un pārvaldīt aparātūras drošības līdzekļus.</p>
 <p><b>Ģimenes opcijas</b> Pārvaldiet to, kā jūsu ģimene izmanto savas ierīces.</p>	 <p><b>Aizsardzības vēsture</b> Skatiet jaunākās aizsardzības darbības un ieteikumus.</p>

## Pašreizējie apdraudējumi

Pašreizējo apdraudējumu nav.  
Pēdējā skenēšana: 07.02.2024 04:44 (ātrā skenēšana)  
Atrasts(i) 0 apdraudējums(i).  
Skenēšanas ilgums: 16 minūtes 17 sekundes  
20637 skenētie faili.

Ātrā skenēšana

Skenēšanas opcijas

Atļautie apdraudējumi

Aizsardzības vēsture

## Pretvīrusu un pretdraudu aizsardzības iestatījumi

Nav jāveic neviena darbība.

Pārvaldīt iestatījumus

## Pretvīrusu un pretdraudu aizsardzības atjauninājumi

Drošības informācija ir atjaunināta.  
Pēdējā atjaunināšana: 07.02.2024 04:44

Aizsardzības atjauninājumi

## Uguns mūra un tīkla aizsardzība

Lietotāji un programmas, kas var piekļūt jūsu tīkliem.

### Domēna tīkls

Uguns mūris ir ieslēgts.

### Privātais tīkls

Uguns mūris ir ieslēgts.

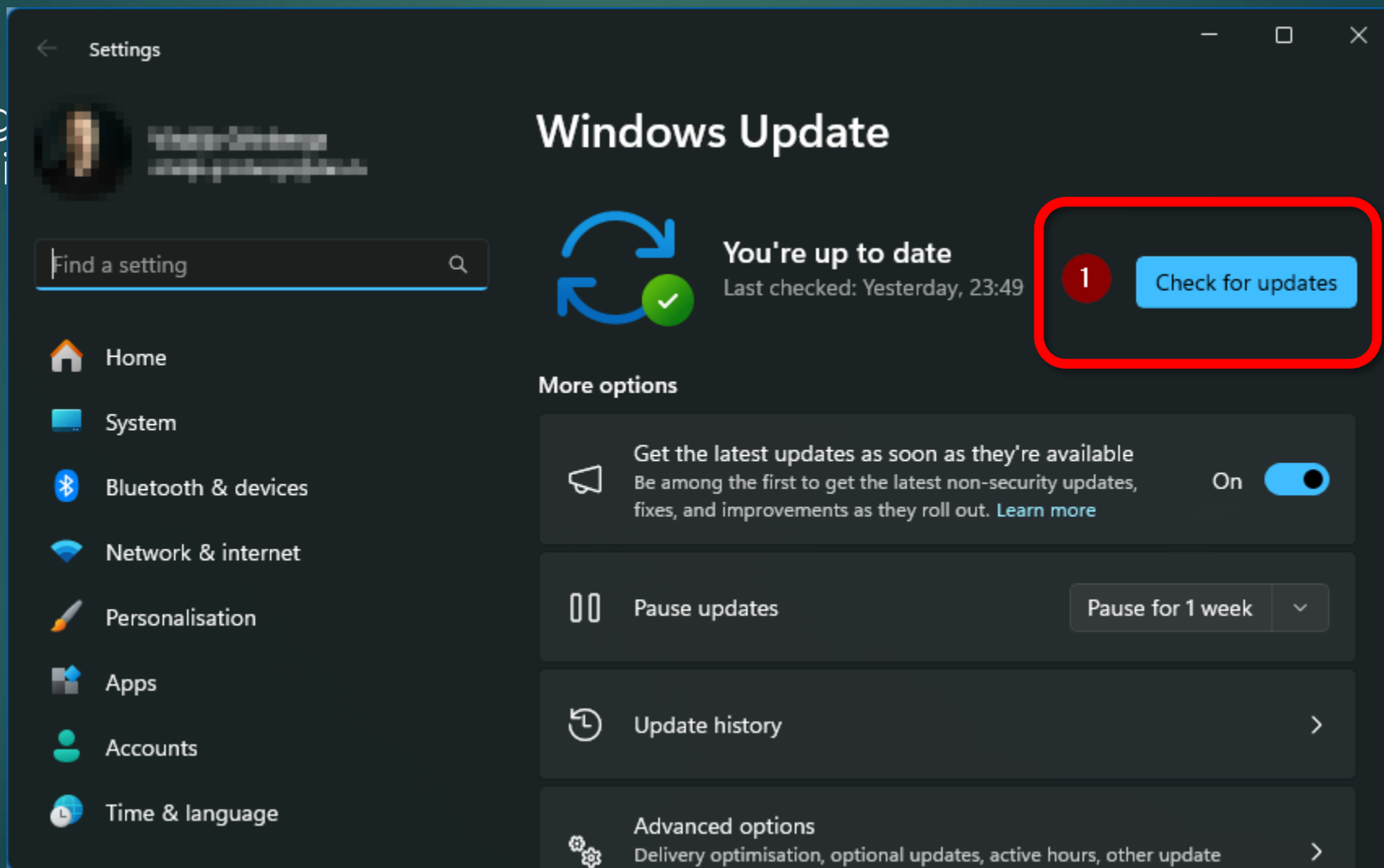
### Publiskais tīkls (aktīvs)

Uguns mūris ir ieslēgts.

# Darbs attālināti

74

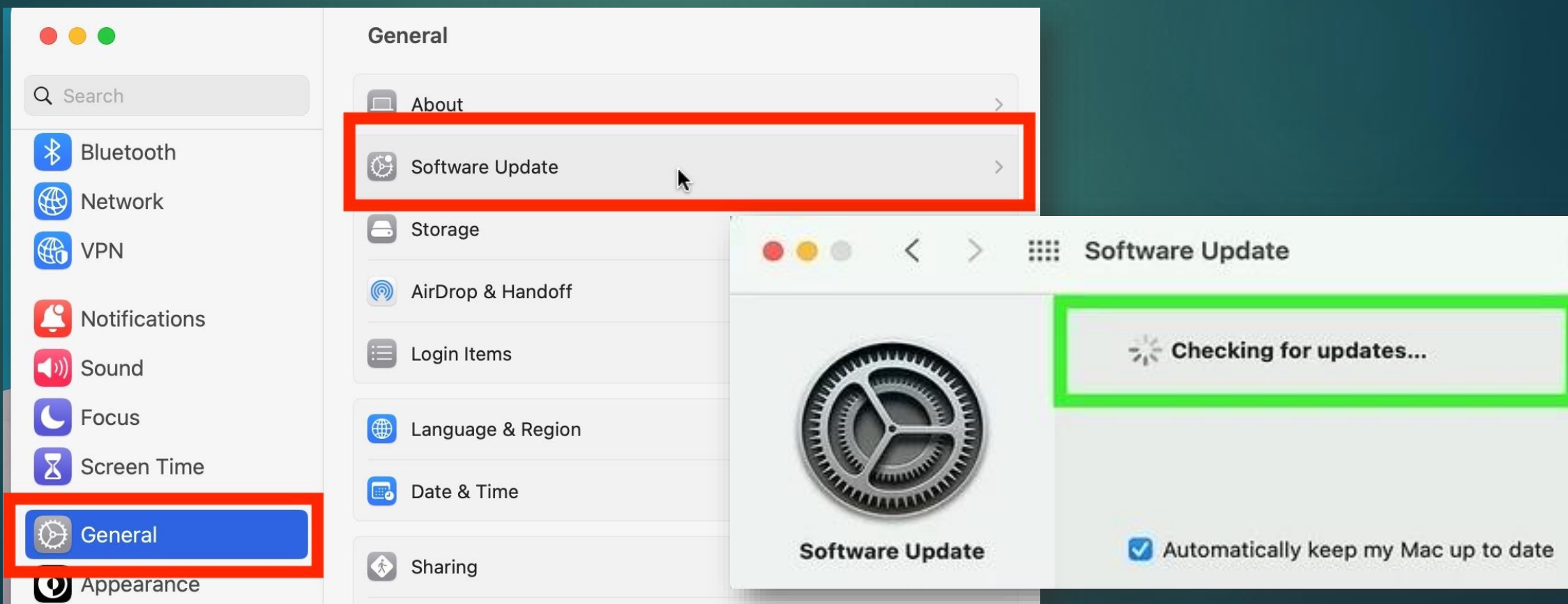
Aizsarg  
atjauni



# Darbs attālināti

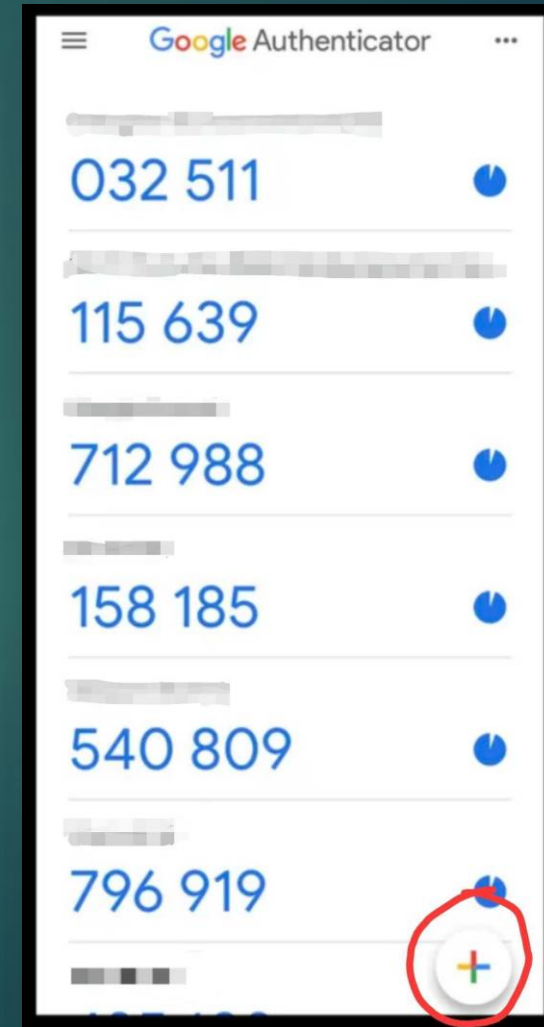
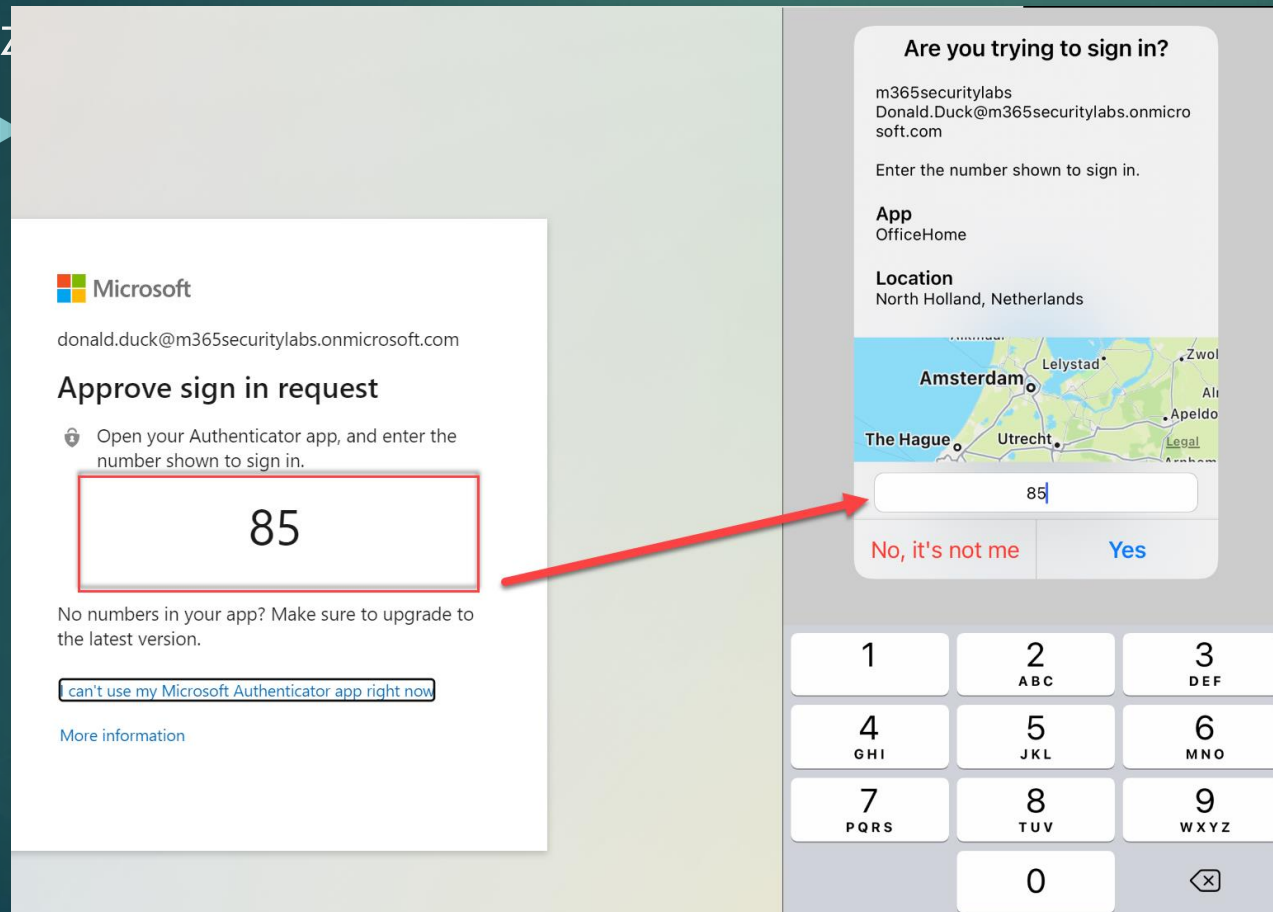
75

Aizsargājiet sava datora operētājsistēmu veicot tās pieejamo atjauninājumu pārbaudi MAC OS



# Darbs attālināti

76

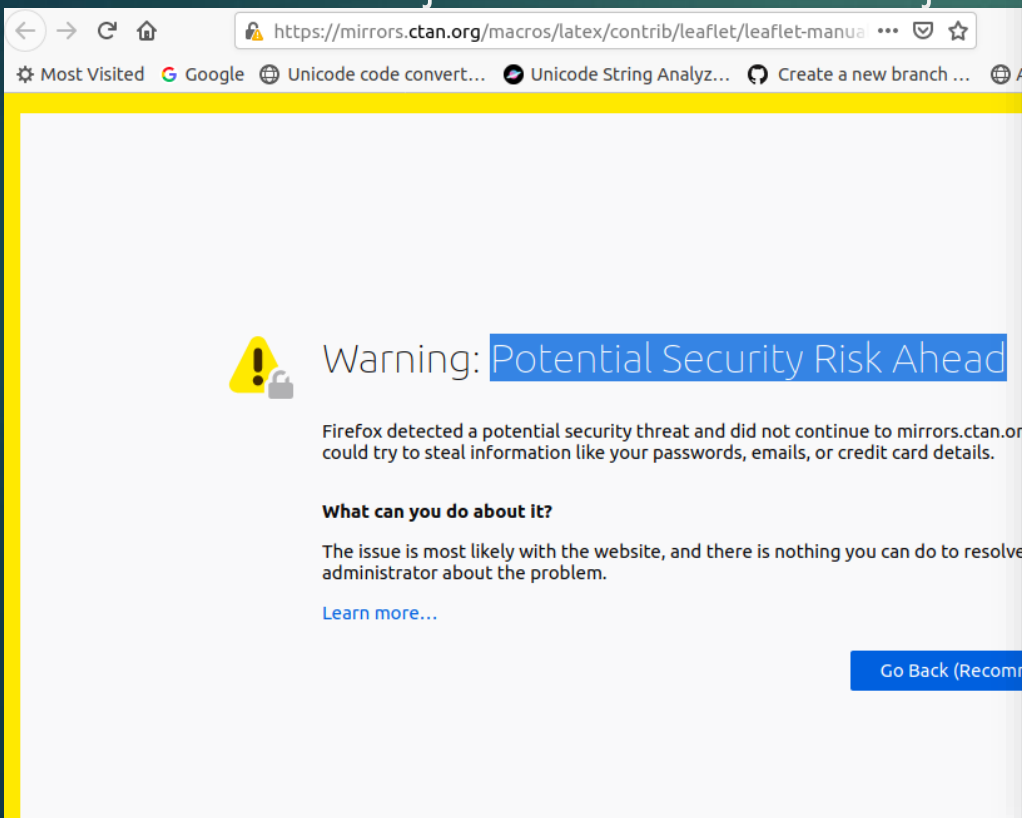


# Darbs attālināti

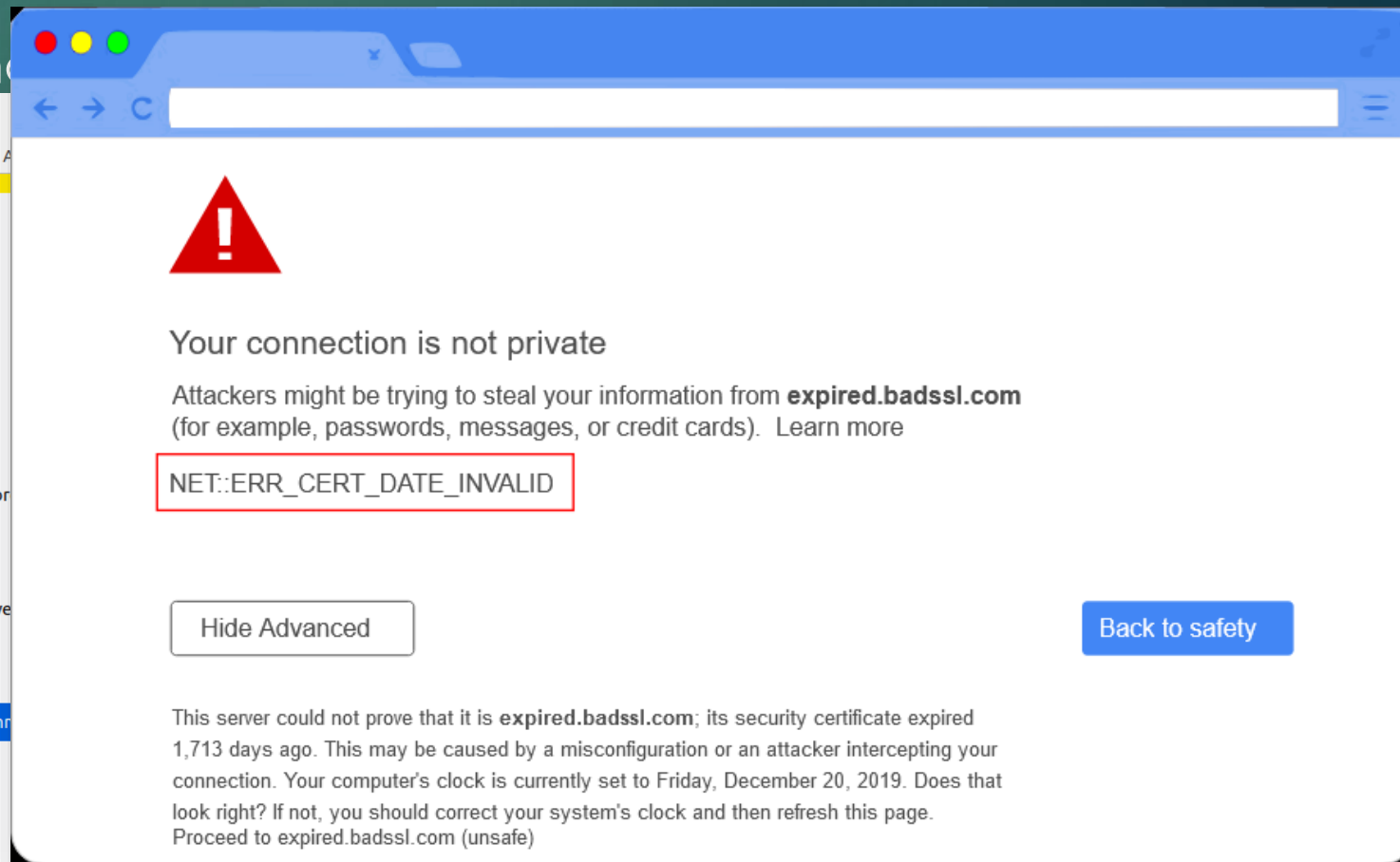
77

Izmantojiet drošu pieslēgšanos

► Sekojiet drošam savienojumam



A screenshot of a Firefox browser warning page. The address bar shows the URL `https://mirrors.ctan.org/macros/latex/contrib/leaflet/leaflet-manua`. The main content area features a yellow warning icon and the text: "Warning: Potential Security Risk Ahead". Below this, it states: "Firefox detected a potential security threat and did not continue to mirrors.ctan.org because it could try to steal information like your passwords, emails, or credit card details." There are sections for "What can you do about it?" and a "Go Back (Recommended)" button.

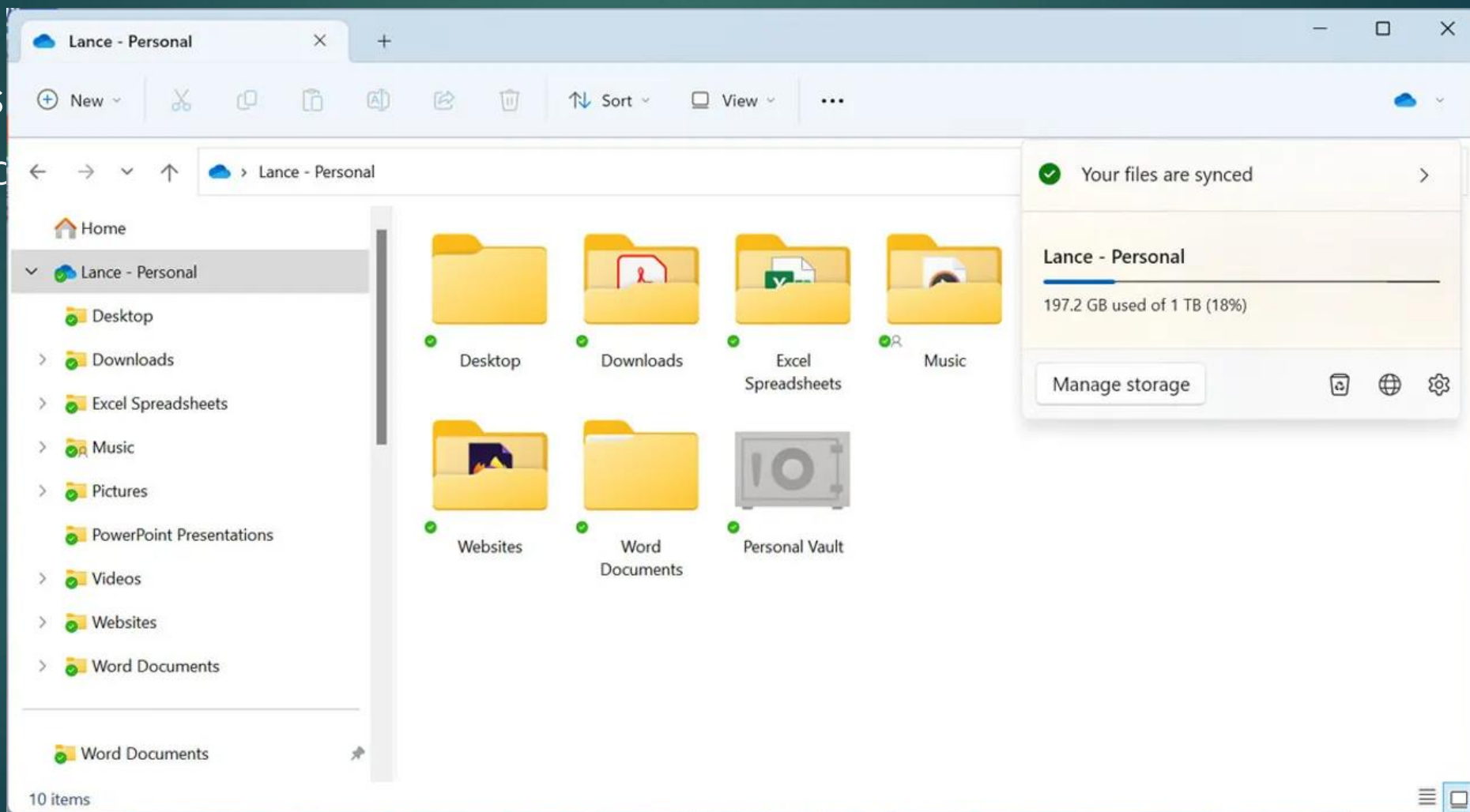


A screenshot of a Chrome browser error page. At the top is a red warning triangle with an exclamation mark. The main heading is "Your connection is not private". Below it, the text reads: "Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more". A red box highlights the error code: `NET::ERR_CERT_DATE_INVALID`. At the bottom, there is a "Hide Advanced" button and a "Back to safety" button. The footer text explains: "This server could not prove that it is **expired.badssl.com**; its security certificate expired 1,713 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Friday, December 20, 2019. Does that look right? If not, you should correct your system's clock and then refresh this page. Proceed to expired.badssl.com (unsafe)".

# Darbs attālināti

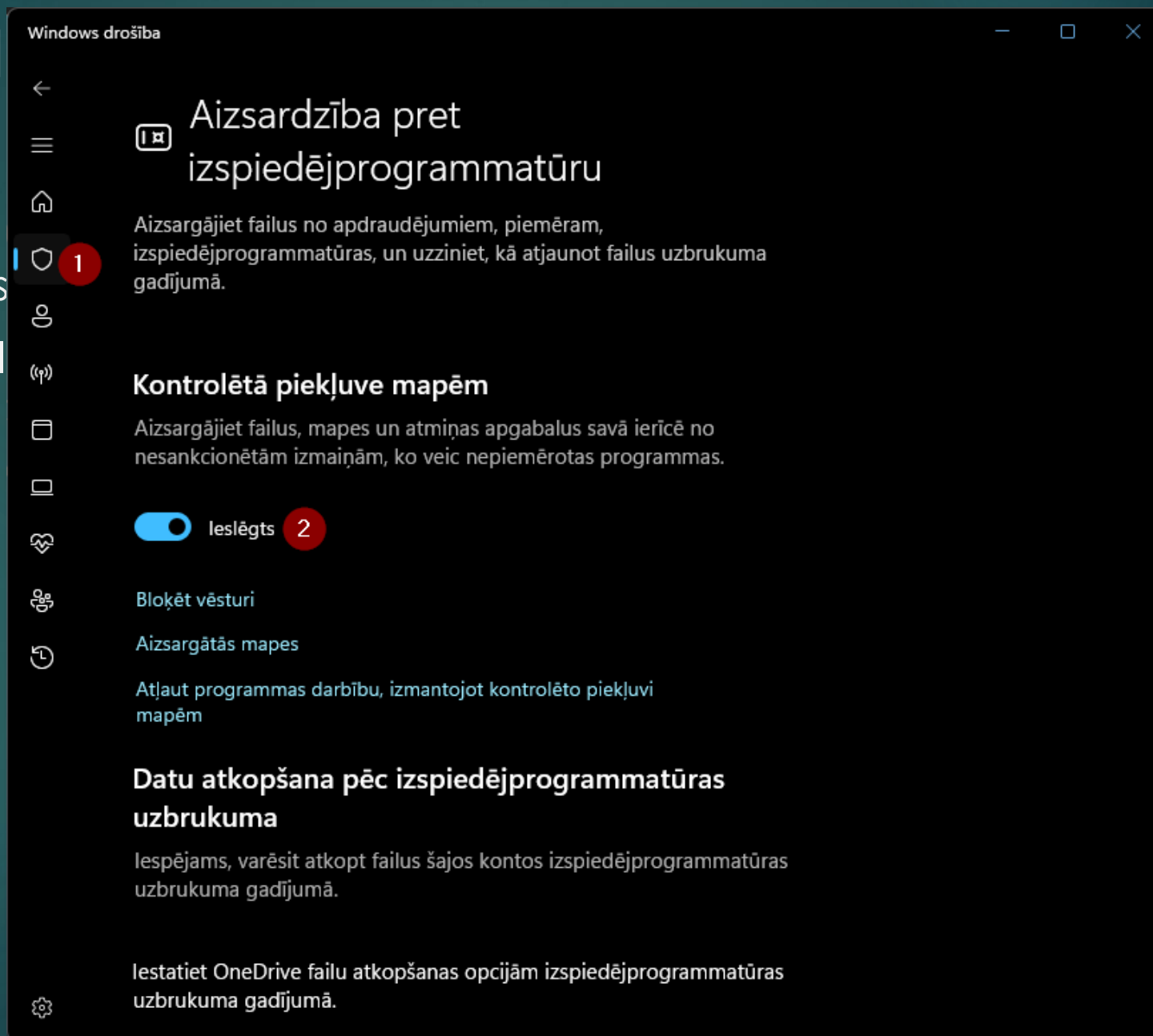
78

Aizs



# Darbs ar

Aizsargājiet s  
▶ darba fail



The screenshot shows the Windows Security application window titled "Windows drošība". The main heading is "Aizsardzība pret izspiedējprogrammatūru". Below the heading, there is a descriptive paragraph: "Aizsargājiet failus no apdraudējumiem, piemēram, izspiedējprogrammatūras, un uzziniet, kā atjaunot failus uzbrukuma gadījumā." A red circle with the number "1" highlights the shield icon in the left-hand navigation pane. The next section is "Kontrolētā piekļuve mapēm", which includes a sub-heading "Aizsargājiet failus, mapes un atmiņas apgabalus savā ierīcē no nesankcionētām izmaiņām, ko veic nepiemērotas programmas." Below this, a toggle switch is shown in the "Ieslēgts" (On) position, with a red circle and the number "2" next to it. Further down, there are sections for "Bloķēt vēsturi" and "Aizsargātās mapes", with a sub-heading "Atļaut programmas darbību, izmantojot kontrolēto piekļuvi mapēm". The final section is "Datu atkopšana pēc izspiedējprogrammatūras uzbrukuma", with a sub-heading "Iespējams, varēsīt atkopt failus šajos kontos izspiedējprogrammatūras uzbrukuma gadījumā." and a final paragraph: "Iestatiet OneDrive failu atkopšanas opcijām izspiedējprogrammatūras uzbrukuma gadījumā." A gear icon is visible at the bottom left of the window.

# Darbs attālināti

80

Uzmanieties no pikšķērēšanas uzbrukumiem

- ▶ Pārliedzinieties, ka e-pasts ir no uzticama avota, pirms atveriet pielikumus vai sekojiet pievienotām saitēm

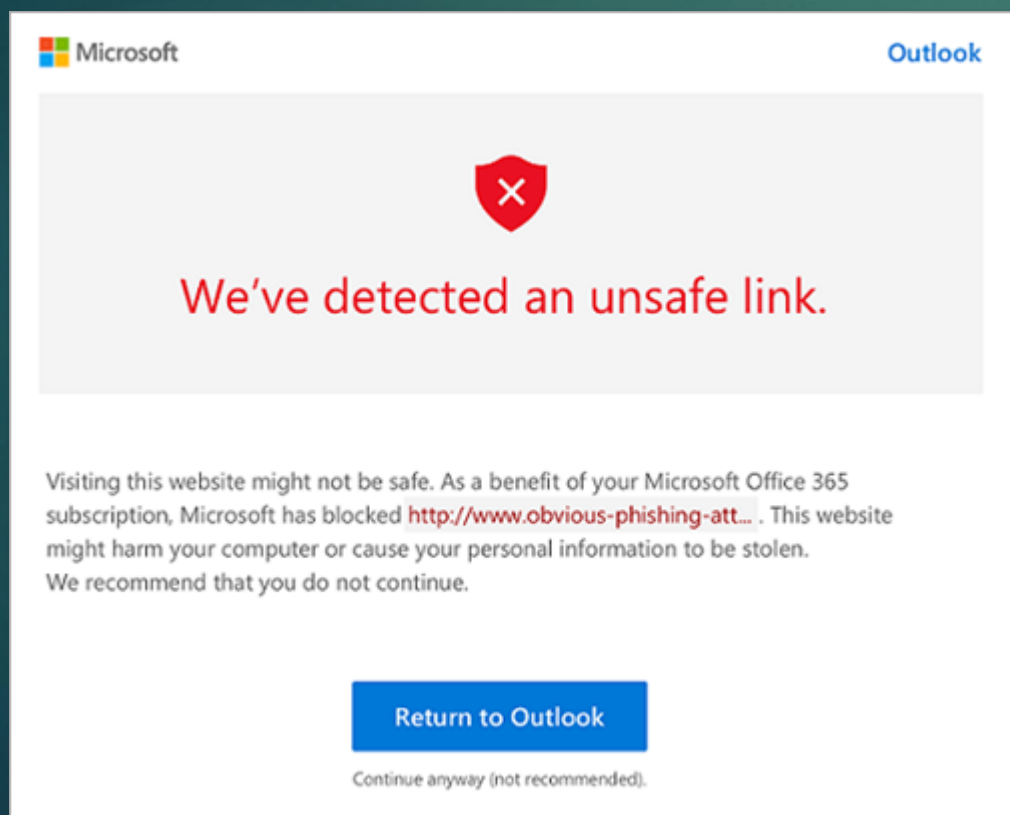


# Darbs attālināti


81

Uzmanieties no pikšķērēšanas uzbrukumiem

- ▶ Saites no nezināmiem avotiem



Microsoft Outlook

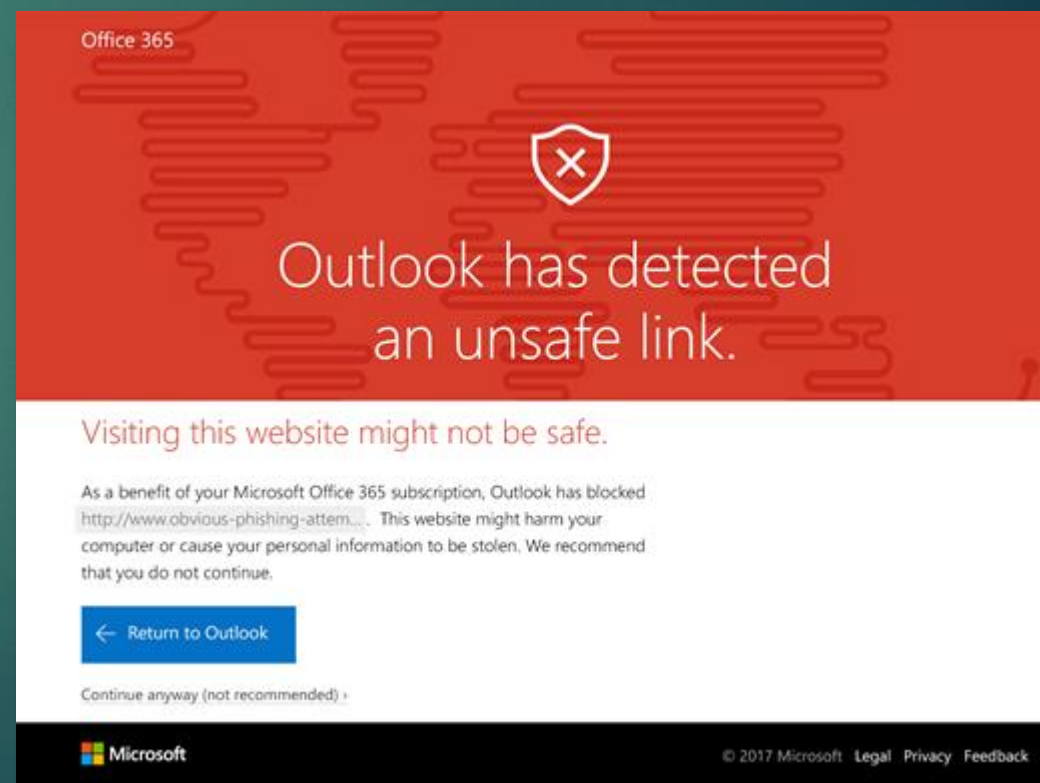


**We've detected an unsafe link.**


Visiting this website might not be safe. As a benefit of your Microsoft Office 365 subscription, Microsoft has blocked <http://www.obvious-phishing-att...>. This website might harm your computer or cause your personal information to be stolen. We recommend that you do not continue.

[Return to Outlook](#)

Continue anyway (not recommended).



Office 365



**Outlook has detected an unsafe link.**

Visiting this website might not be safe.

As a benefit of your Microsoft Office 365 subscription, Outlook has blocked <http://www.obvious-phishing-attem...>. This website might harm your computer or cause your personal information to be stolen. We recommend that you do not continue.

[Return to Outlook](#)

Continue anyway (not recommended) >

Microsoft © 2017 Microsoft Legal Privacy Feedback

# Darbs attālināti

Nodrošiniet savu darba vietu

- ▶ Iepazīties ar noteikumiem par darbu no mājām
  - ▶ Kādas ierīces atļauts izmantot, tikai darba dators, mājas dators, jebkāds dators
  - ▶ Datora atbilstība minimālajām drošības prasībām
  - ▶ Virtuālo sapulču noteikumi, fons, logo utt.

# Darbs attālināti

Nodrošiniet savu darba vietu

- ▶ Pārlicinieties, ka jūsu darba vide ir privāta
- ▶ Apmeklētāji nevar piekļūt jūsu darba datoram vai dokumentiem

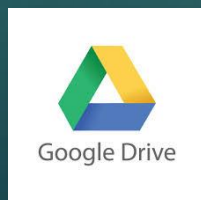
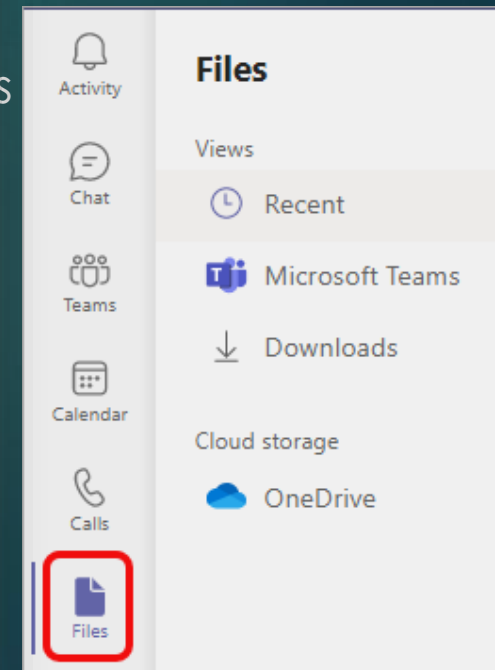
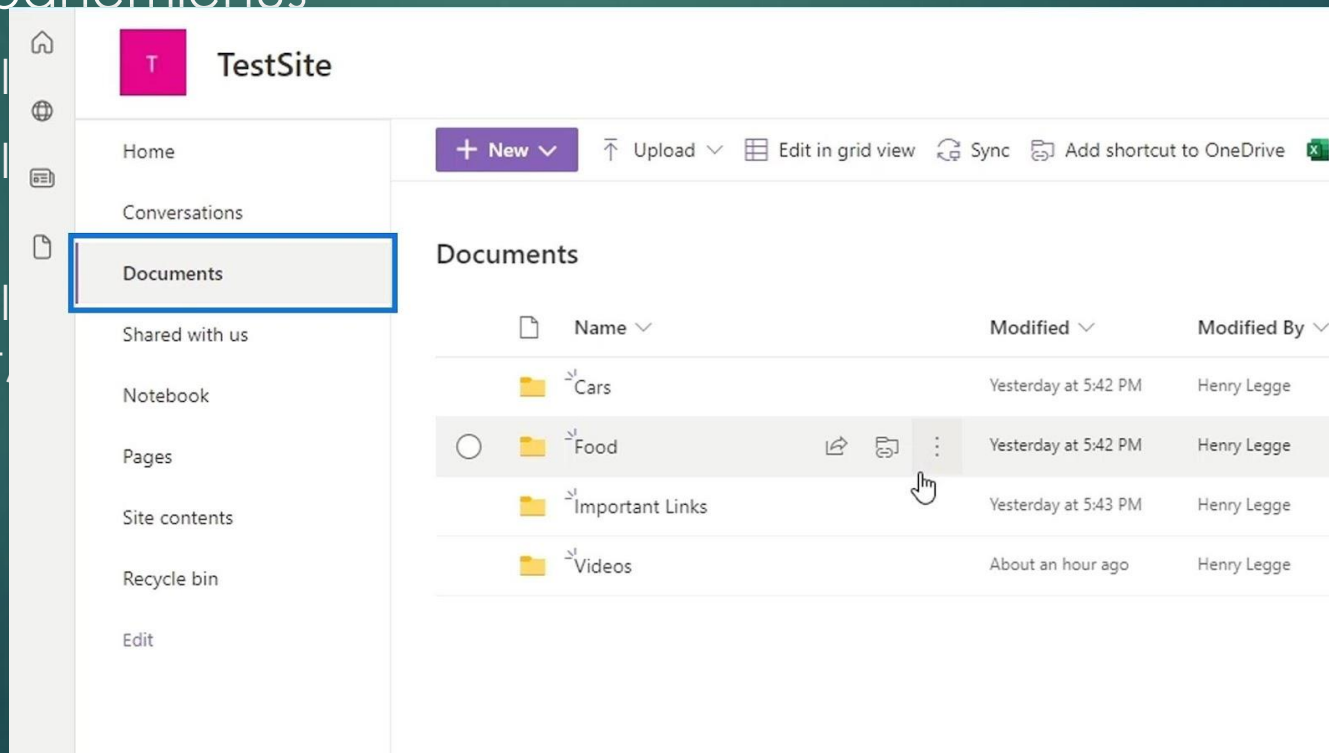
# Darbs attālināti

84

Regulāri veiciet datu dublēšanu

- ▶ Atkarībā no datu klasifikācijas tiem piemēro atbilstošos datu dublēšanas panēmienu

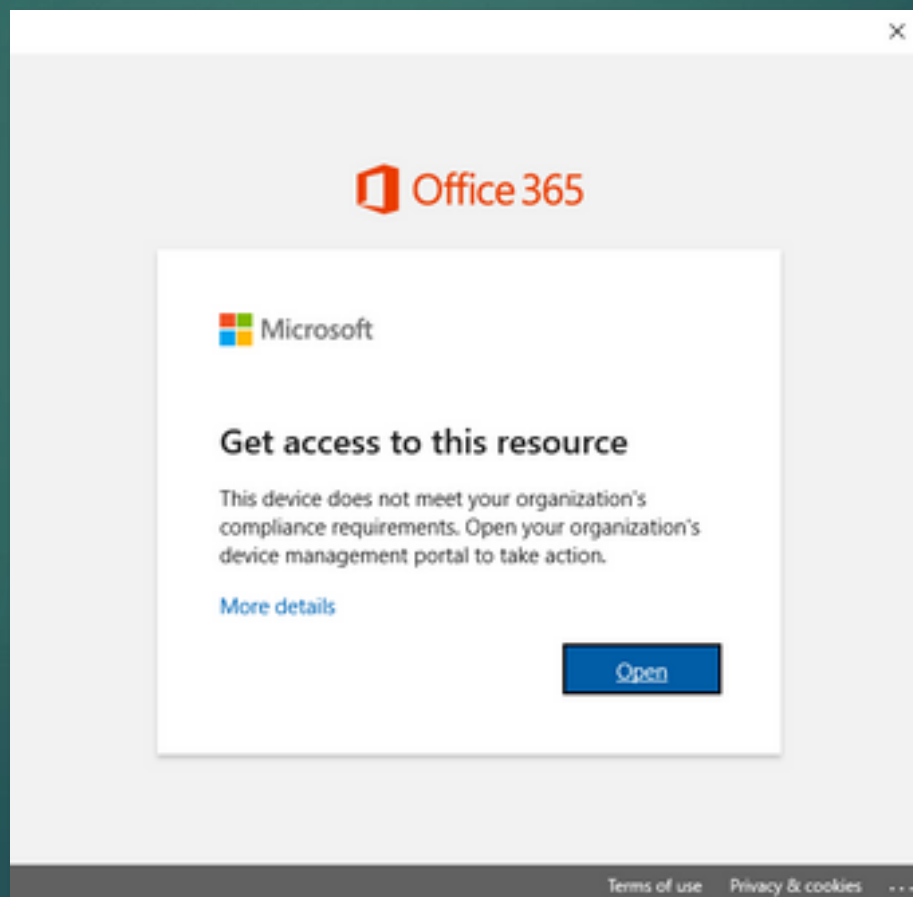
- ▶ Dati, kuri glabājas SharePoint
- ▶ Dati, kuri glabājas OneDrive kopijām
- ▶ Dati, kuri glabājas Google Drive



# Darbs attālināti

85

Nesaderīgas ierīces



# E-pasta drošība

# E-pasta drošība

Mēstuļu o

Avots: [sta](#)

Kā jums š



# E-pasta drošība

88

Samazinājums dēļ e-pasta drošības protokolu ieviešanas:

▶ DMARC

CERT.lv rekomendē ieviest šo drošo praksi, [avots](#)

Valsts iestādēm **DMARC** obligāts, MK Noteikumi 442. 15.15.p.

<https://en.wikipedia.org/wiki/DMARC>



# E-pasta drošība

Kāpēc tas ir svarīgi?

- ▶ Lietotājs ir pieslēgts iekšējam tīklam
- ▶ Lietotājs ir cilvēks kuram ir emocijas
- ▶ Lietotājam ir kaut kādas tiesības sistēmā
- ▶ Lietotājs ir saistīts ar citiem iekšējiem lietotājiem

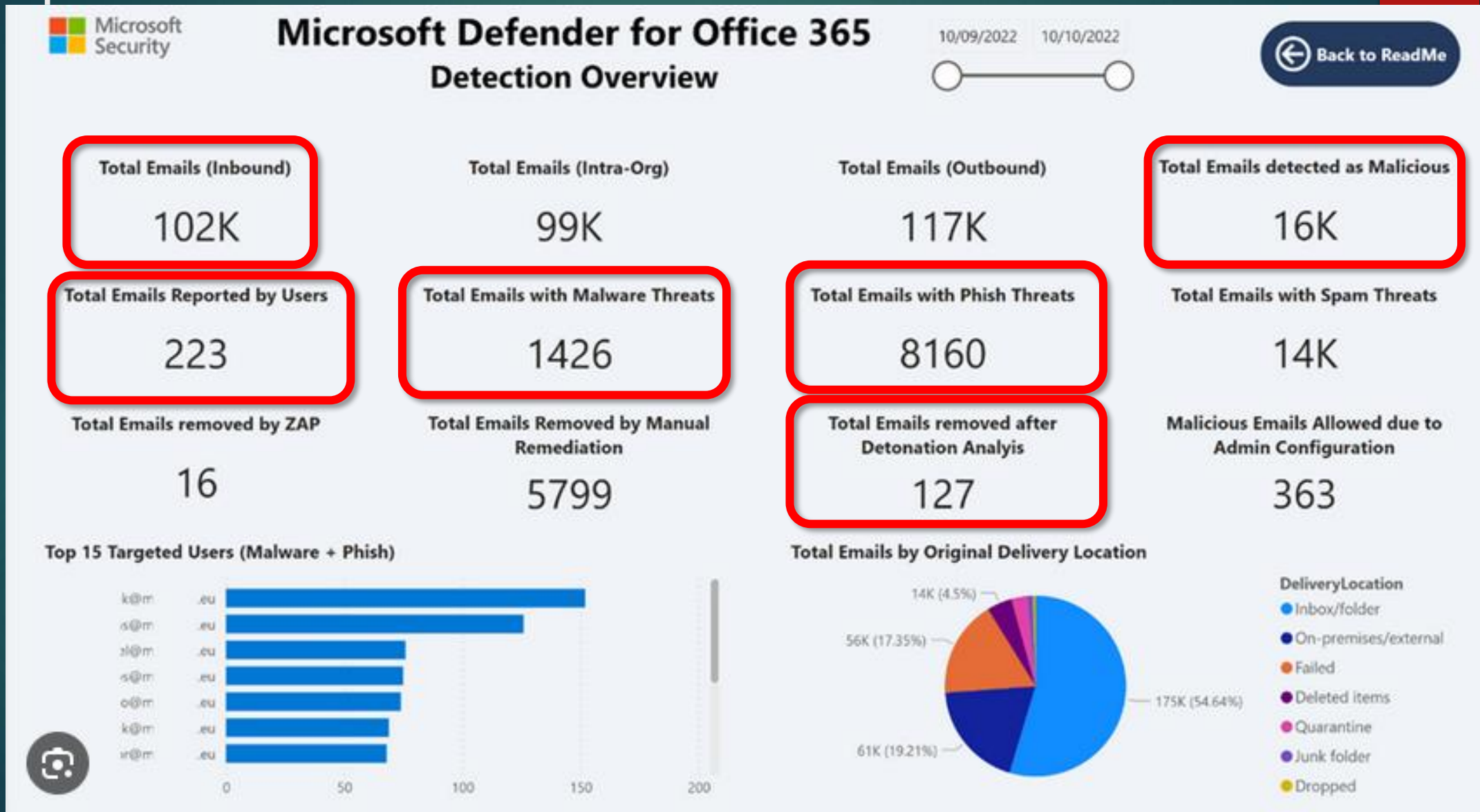
# E-pasta drošība

90

Draudu mērķi:

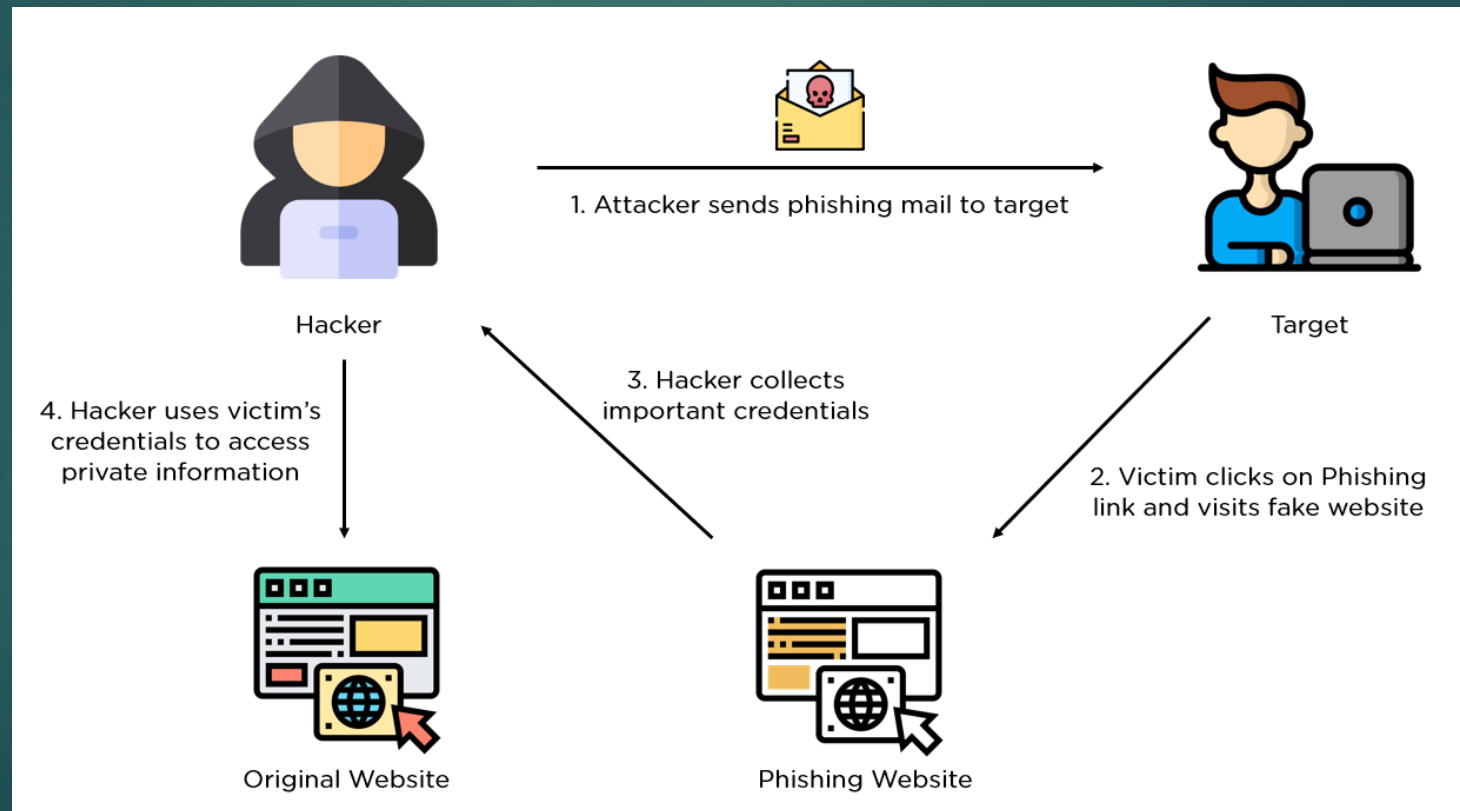
- ▶ Naudas izspiešana
- ▶ Ļaunatūras piegāde
- ▶ Datu izpaušana
- ▶ U.c.

# E-pasta drošība



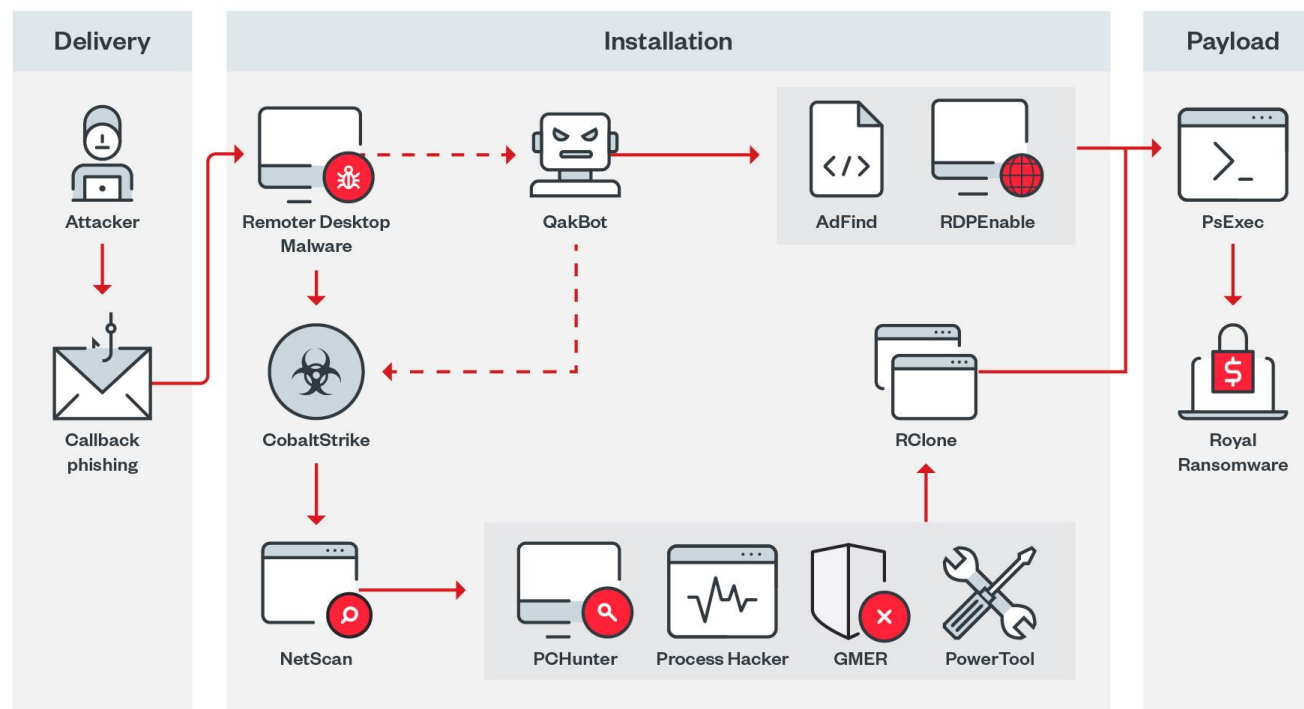
# E-pasta drošība

## Pikšķerēšanas piemērs



# E-pasta drošība

## Launatūras piegādes piemērs



# E-pasta drošība

Kā atšķirt sliktu e-pastu:


- ▶ Vai šis e-pasts ir gaidīts, vai negaidīts?
- ▶ Vai e-pasta valoda ir korekta, vai tomēr manāmas dīvainības?
- ▶ Vai e-pasta sūtīšanas laiks ir ierasts, vai aizdomīgs?
- ▶ Vai e-pasta vēstījums satur steigas vai potenciālu draudu norādi?


# E-pasta drošība

95

pikšķe

High-severity alert: Phish delivered due to tenant or user override Σ Inbox x 🖨 🔗

 **Microsoft** <microsoft@email-records.com> 4:22 PM (14 minutes ago) ☆ ↶ ⋮  
to me ▾

 Office 365

**A high-severity alert has been triggered**


Phish delivered due to tenant or user override

Severity: — High  
Time: 01/22/2021  
Activity: Protection  
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

[View alert details](#)

Thank you,  
The Office 365 Team

---

 Microsoft  
One Microsoft Way  
Redmond, WA  
98052-6399 USA

# E-pasta drošība

96

pikšķerēšana



## Refund Notification

Due to a system error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID:



# E-pasta drošība

97

pikšķerēšana

Email De-Activation Request < Warning >

Zimbra Portal ! <arida.marsa@ogresnovads.lv>

Trešd. 2023. gada .20.12 00:59

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

Hi [redacted],

We have received your Email account deactivation request and this request was made accidentally or by mistake or you have no knowledge now. However, if you do not cancel this request, your account will be shut down permanently. If this request is not cancelled within 24 hours, your account data will be lost permanently.

<https://firebasestorage.googleapis.com/v0/b/zimbra-e4109.appspot.com/o/index.html?alt=media&token=82649150-32e4-4926-b715-5c594db085ea>  
Click or tap to follow link.

[CANCEL DE-ACTIVATION HERE](#)

Thanks  
Zimbra Portal !

Internet headers

```
C_BODY_TEXT_LINE,  
URIBL_BLOCKED autolearn=no autolearn_force=no version=3.4.6  
Received: from unknown (HELO mail.ogresnovads.lv) (94.100.9.4)  
by srv-mail-gw with SMTP; 20 Dec 2023 02:43:58 -0000
```

# E-pasta drošība

98



LMT / Klientu balvu programma



Apsveicam!

17 декабря 2023 г.

Katru dienu mēs pēc nejaušības principa izvēlamies dažus lietotājus, kuri piedalīsies aptaujā.

Pretī mēs viņiem dodam iespēju saņemt vērtīgu dāvanu no mums vai mūsu sponsoriem. Šī aptauja ļauj mums labāk izprast mūsu lietotājus, novērtēt mūsu stiprās un vājās puses un uzlabot lietotāju pieredzi, izmantojot mūsu pakalpojumus.

Tas aizņem ne vairāk kā 30 sekundes jūsu laika.

Jūs varat laimēt jaunu iPhone 15 Pro Max, Samsung Galaxy S23 Ultra vai MacBook Pro. Viss, kas jums jādara, ir jāatbild uz dažiem jautājumiem.

**Atcerieties:** šo ielūgumu saņēma 10 nejauši izvēlēti lietotāji, dāvinājumu skaits ir ierobežots.

Jūsu rīcībā ir 3 minūtes un 28 sekundes lai atbildētu uz tālāk minētajiem jautājumiem, pirms mēs nodosim dāvanu citam laimīgajam uzvarētājam! Veiksmi!

Cik ilgi esat LMT lietotājs?

Mazāk nekā gadu

Vairāk nekā gadu

Vairāk nekā divus gadus



Bite / Klientu balvu programma



Apsveicam!

December 15, 2023

Katru dienu mēs pēc nejaušības principa izvēlamies dažus lietotājus, kuri piedalīsies aptaujā.

Pretī mēs viņiem dodam iespēju saņemt vērtīgu dāvanu no mums vai mūsu sponsoriem. Šī aptauja ļauj mums labāk izprast mūsu lietotājus, novērtēt mūsu stiprās un vājās puses un uzlabot lietotāju pieredzi, izmantojot mūsu pakalpojumus.

Tas aizņem ne vairāk kā 30 sekundes jūsu laika.

Jūs varat laimēt jaunu iPhone 15 Pro Max, Samsung Galaxy S23 Ultra vai MacBook Pro. Viss, kas jums jādara, ir jāatbild uz dažiem jautājumiem.

**Atcerieties:** šo ielūgumu saņēma 10 nejauši izvēlēti lietotāji, dāvinājumu skaits ir ierobežots.

Jūsu rīcībā ir 2 minūtes un 27 sekundes lai atbildētu uz tālāk minētajiem jautājumiem, pirms mēs nodosim dāvanu citam laimīgajam uzvarētājam! Veiksmi!

Cik ilgi esat Bite lietotājs?

Mazāk nekā gadu

Vairāk nekā gadu

Vairāk nekā divus gadus

# Darbs attālināti

99

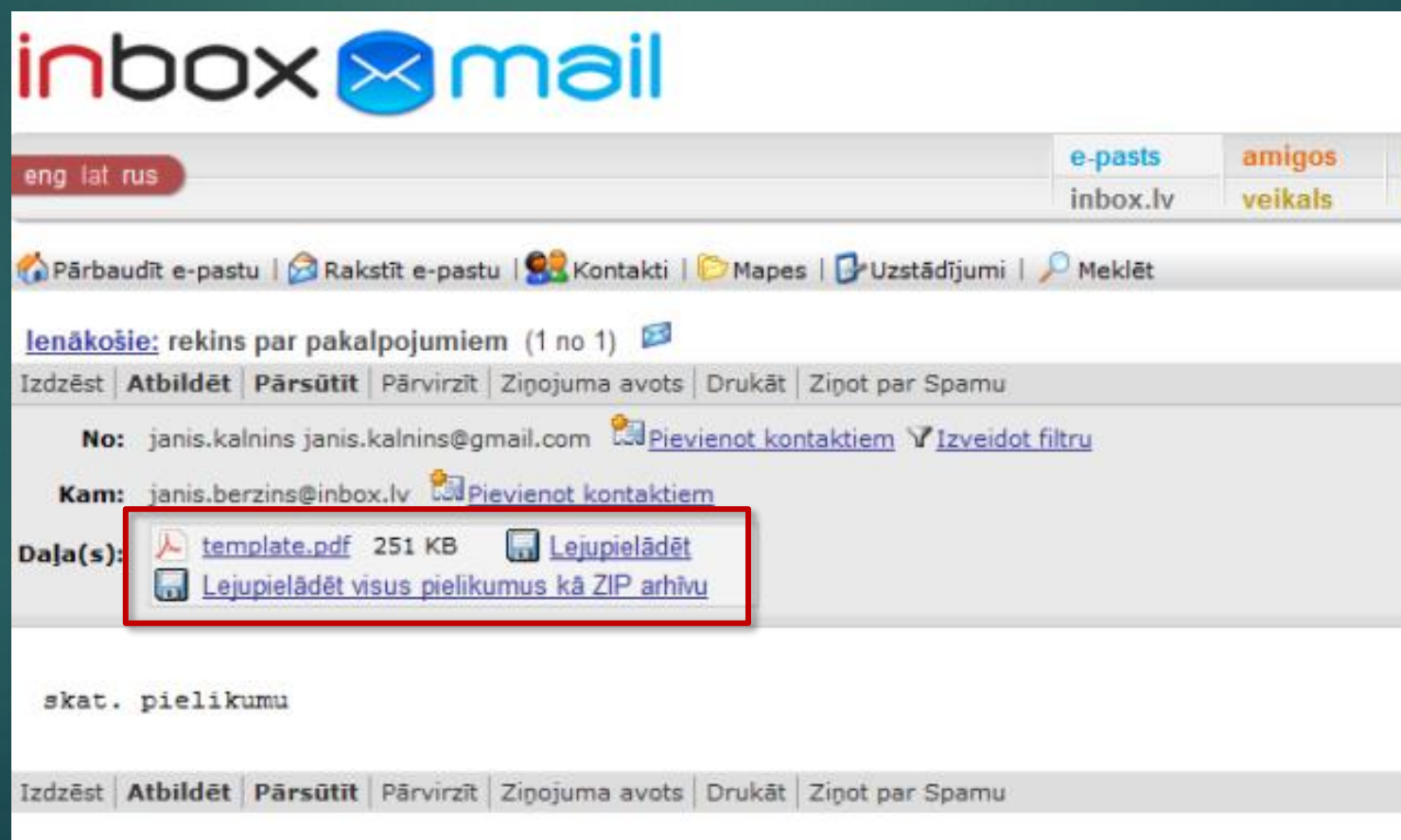
Uzmanieties no pikšķērēšanas uzbrukumiem

- ▶ e-pasta pielikumi kuros:
  - ▶ Steidzami kaut kas jāizdara
    - ▶ konts tiks bloķēts
    - ▶ Aizdomīgas darbības ar jūsu kontu
  - ▶ Apvaino, draud
  - ▶ Vieglas naudas iegūšanas piedāvājums

# E-pasta drošība

100

Launatūras piemēri



The screenshot displays the inbox interface of 'inbox mail'. At the top, there are language options ('eng', 'lat', 'rus') and account information ('e-pasts: inbox.lv', 'amigos: veikals'). A navigation bar includes links for 'Pārbaudīt e-pastu', 'Rakstīt e-pastu', 'Kontakti', 'Mapes', 'Uzstādījumi', and 'Meklēt'. The main content area shows an email from 'janis.kalnins@inbox.lv' with the subject 'lenākošie: rekins par pakalpojumiem (1 no 1)'. The email header includes 'No: janis.kalnins@inbox.lv' and 'Kam: janis.berzins@inbox.lv'. The attachment list under 'Daļa(s):' contains 'template.pdf' (251 KB) and a link to download all attachments as a ZIP archive. A red box highlights the attachment information. The email body contains the text 'skat. pielikumu'.

**inbox mail**

eng lat rus e-pasts amigos s  
inbox.lv veikals c

Pārbaudīt e-pastu | Rakstīt e-pastu | Kontakti | Mapes | Uzstādījumi | Meklēt

**lenākošie:** rekins par pakalpojumiem (1 no 1)

Izdzēst | **Atbildēt** | **Pārsūtīt** | Pārvirzīt | Ziņojuma avots | Drukāt | Ziņot par Spamu

**No:** janis.kalnins@inbox.lv [Pievienot kontaktiem](#) [Izveidot filtru](#)

**Kam:** janis.berzins@inbox.lv [Pievienot kontaktiem](#)

**Daļa(s):** [template.pdf](#) 251 KB [Lejupielādēt](#)  
[Lejupielādēt visus pielikumus kā ZIP arhīvu](#)

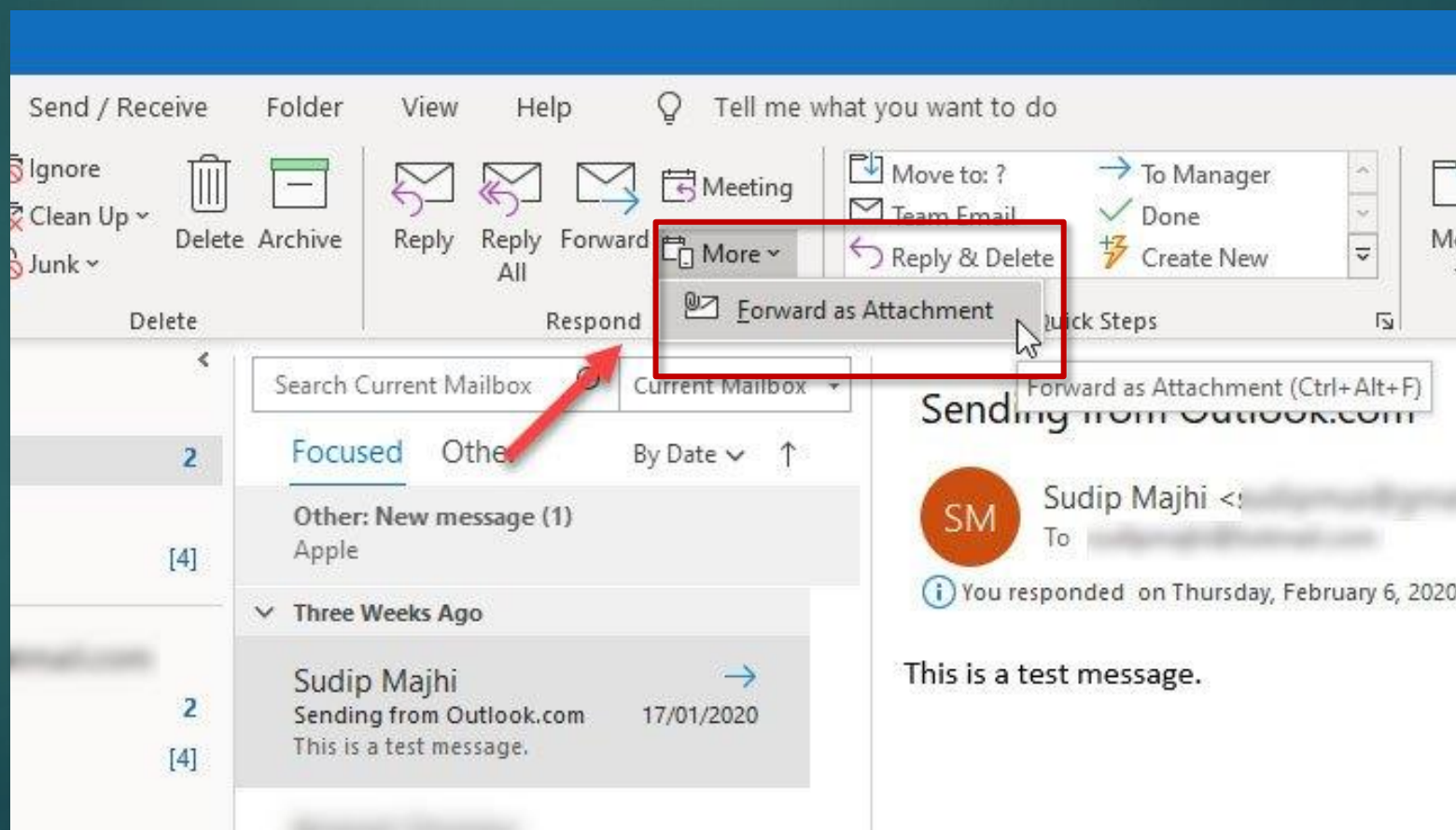
skat. pielikumu

Izdzēst | **Atbildēt** | **Pārsūtīt** | Pārvirzīt | Ziņojuma avots | Drukāt | Ziņot par Spamu

# E-pasta drošība

101

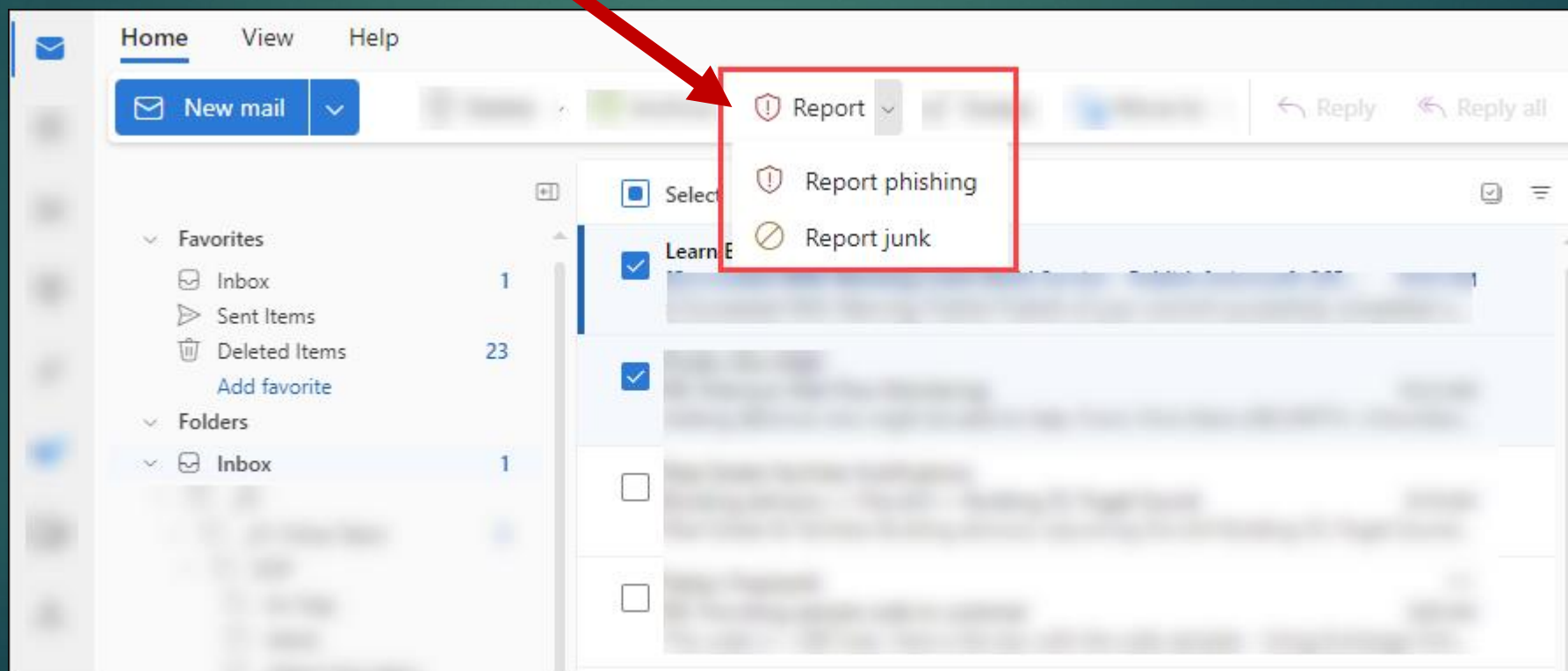
Ko darīt ja saņemts «slikts» e-pasts:



# E-pasta drošība

102

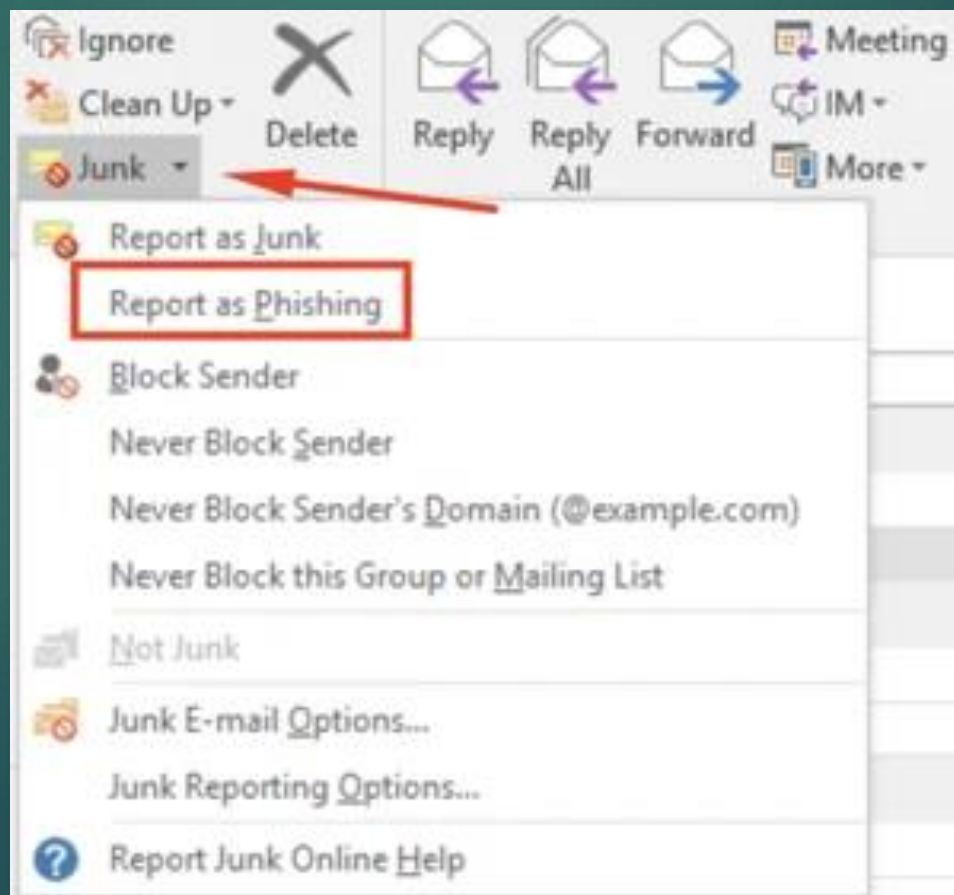
Ko darīt ja saņemts «slikts» e-pasts:



# E-pasta drošība

103

Ko darīt ja saņemts «slikts» e-pasts:



# E-pasta drošība

104

Apmācību platformas

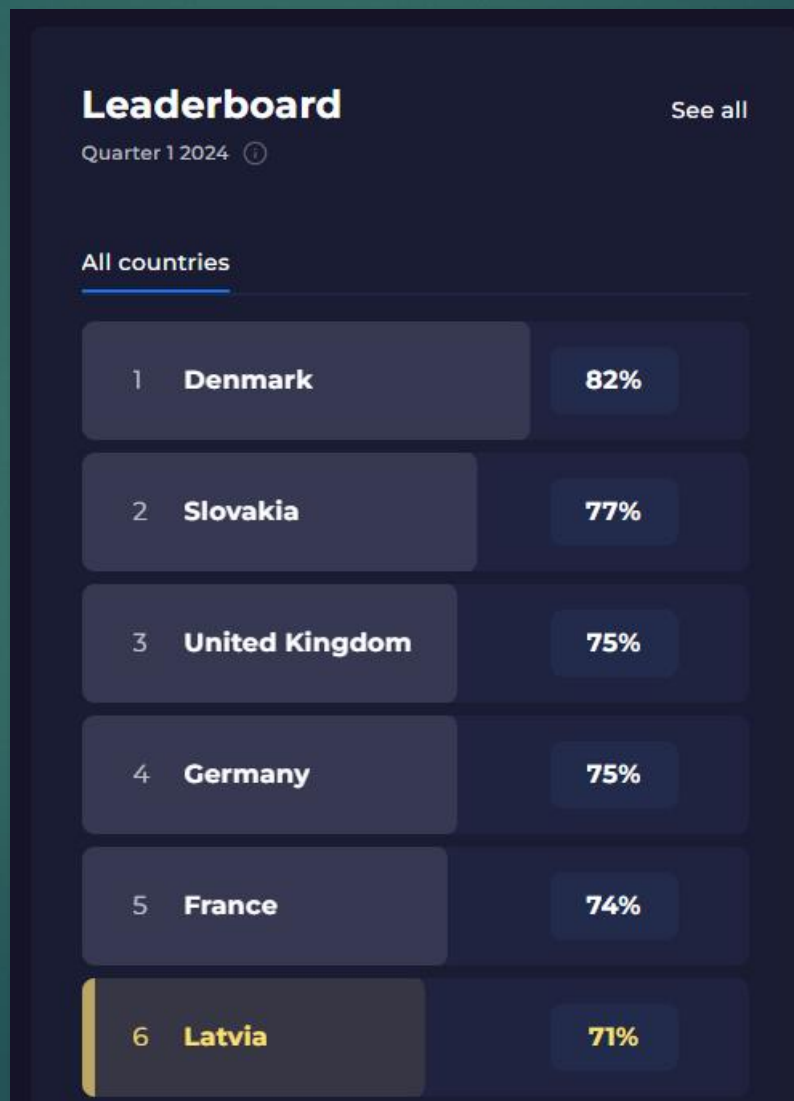




# E-pasta drošība

105

Apmācību platformas



# E-pasta drošība

Apmācību platformas

The screenshot displays a list of email notifications on a dark background. Each notification includes a date, a subject line, a status (all are 'Reported'), and a rating (three stars). The notifications are as follows:

Date	Subject	Status	Rating
Feb 15, 2024	Brenden Dach has shared report_internal_security_2024.pdf with you	Reported	3 stars
Feb 5, 2024	Parking violation 02/02/2024	Reported	3 stars
Jan 22, 2024	Attack Alerts Deactivated	Reported	3 stars
Jan 15, 2024	Issues with multiple accounts	Reported	3 stars
Jan 8, 2024	Meeting invite: Strategic Security meeting	Reported	3 stars
Jan 2, 2024	Novareresults (documents@novareresults.com) has sent you a protected message	Reported	3 stars
Dec 27, 2023	Vitālijs, people are looking at your profile	Reported	3 stars

# Draudu pārskats

107

Draudu veidi

- ▶ Iekšējie
- ▶ Ārējie

# Draudu pārskats

108

Draudu veidi. Iekšējie

Darbinieks apzināti veic destruktīvas vai neatļautās darbības

- ▶ Iekšējā spiegošana
- ▶ Datu nopludināšana
- ▶ Datu izpaušana
- ▶ Ļaunprātīga dienesta stāvokļa izmantošana



# Draudu pārskats

109

Draudu veidi. Iekšējie

Darbinieks neapzināti veic destruktīvas vai neatļautās darbības

- ▶ Zināšanu trūkums
- ▶ Neuzmanība



# Draudu pārskats

110

Draudu veidi. Iekšējie. Kā pasargāties

- ▶ Regulāra lomu, risku, ievainojamību caurskatīšana
- ▶ Lietotāju aktivitāšu uzraudzība, netipiskās aktivitātes
- ▶ Papildus kontroļu ieviešana, 4 acu princips
- ▶ Darbinieku rotācija
- ▶ Apmācības, instruktažas



# Draudu pārskats

111

Draudu veidi. Ārējie.

- ▶ Sistēmu ievainojamības
- ▶ Konfigurāciju pārvaldība
- ▶ Destruktīvās darbības



# Draudu pārskats

112

Sistēmu ievainojamības. Nepietiekama ievainojamību pārvaldība

- ▶ Laicīga noteikšana
- ▶ Klasifikācija
- ▶ Ielāpu uzstādīšana
- ▶ Pārbaude, atkārtotā testēšana



# Draudu pārskats

113

Sistēmu ievainojamības. Konfigurāciju pārvaldība

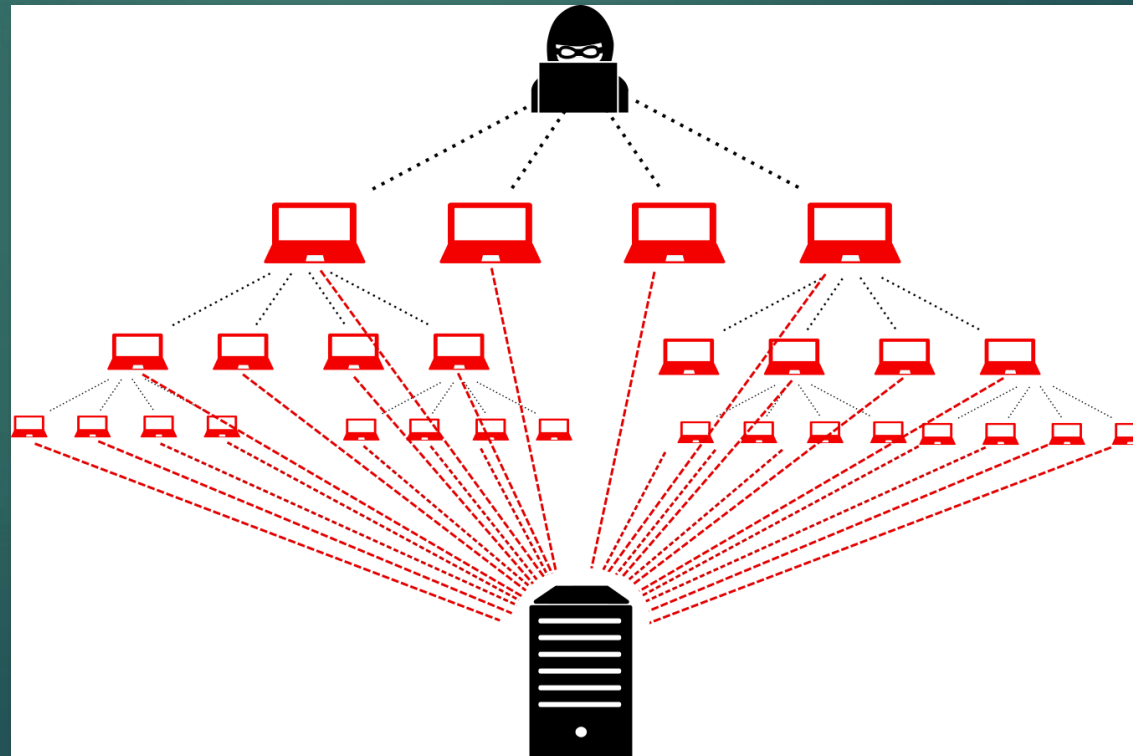
- ▶ Sistēmu konfigurāciju pārbaude, automatizācija
- ▶ Konfigurācijas validācija, 4 acu princips
- ▶ Integrāciju testi, savietojamība

# Draudu pārskats

114

Sistēmu ievainojamības. Destruktīvās darbības

- ▶ DDoS uzbrukumi



# Draudu pārskats

115



SHODAN

Explore

Downloads

Pricing [↗](#)

product:PostgreSQL country:"LV" **1**



Account

TOTAL RESULTS

214 **2**

TOP CITIES

Rīga	190
Piņķi	15
Salaspils	4
Daugavpils	1
Jelgava	1

[More...](#)

TOP ORGANIZATIONS

SIA Tet	30
SIA VEESP	30
RETN Baltic, SIA	6
CloudHosting Data Center	5
GARMTECH LP	5

[More...](#)

[View Report](#) [View on Map](#)

**Access Granted:** Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

**136.169.46.164**

Baltcom SIA

Latvia, Riga

database

PostgreSQL

FATAL: no pg\_hba.conf entry for host "224.123.157.23", user "postgres", database "template0", SSL off

2024-02-17T03:59:21.223285

**195.13.203.120**

VSM, SIA

Latvia, Riga

database

PostgreSQL

FATAL: no pg\_hba.conf entry for host "224.136.243.158", user "postgres", database "template0", SSL off

2024-02-17T02:53:55.650748

**80.233.166.68**

Stream Net Ltd.

Latvia, Riga

database self-signed

**SSL Certificate**

PostgreSQL

fe\_sendauth: no password supplied

Issued By:

|- Common Name:  
localhost

Issued To:

|- Common Name:  
localhost

2024-02-17T02:39:56.498412

# Draudu pārskats

116



SHODAN

Explore

Downloads

Pricing [↗](#)

mikrotik port:80 country:"LV" 1



Account

TOTAL RESULTS

640 2

TOP CITIES

Rīga	521
Piņķi	74
Mārupe	24
Liepāja	10
Tukums	2

[More...](#)

TOP ORGANIZATIONS

SIA Tet	147
Latvijas Mobilais Telefons SIA	56
Baltcom SIA	53
Telenet SIA	40
Tele2 Latvia	34

[More...](#)

[View Report](#) [View on Map](#)

**Access Granted:** Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

## RouterOS router configuration page [↗](#)

2024-02-17T04:10:19.680381

86.63.188.138  
[My CRM](#)  
 Latvia, Riga  
HTTP/1.1 200 OK  
Connection: Keep-Alive  
Content-Length: 7064  
Content-Type: text/html  
Date: Sat, 17 Feb 2024 04:10:19 GMT  
Expires: 0

**MikroTik** RouterOS:  
Version: 6.44.6 3

## RouterOS router configuration page [↗](#)

2024-02-17T03:53:35.015298

213.21.221.135  
[Skygroup Tech](#)  
 Latvia, Riga  
HTTP/1.1 200 OK  
Connection: Keep-Alive  
Content-Length: 7065  
Content-Type: text/html  
Date: Sat, 17 Feb 2024 03:53:33 GMT  
Expires: 0

**MikroTik** RouterOS:  
Version: 6.49.8

# Draudu pārskats

117

Ļaunprātīgās programmatūras piemēri

- ▶ Vīrusi
- ▶ Spiegu programmas
- ▶ Datu šifrētāji
- ▶ Identitātes zagļi
- ▶ U.c.

# Draudu pārskats

118

Launprātīgā programmatūra

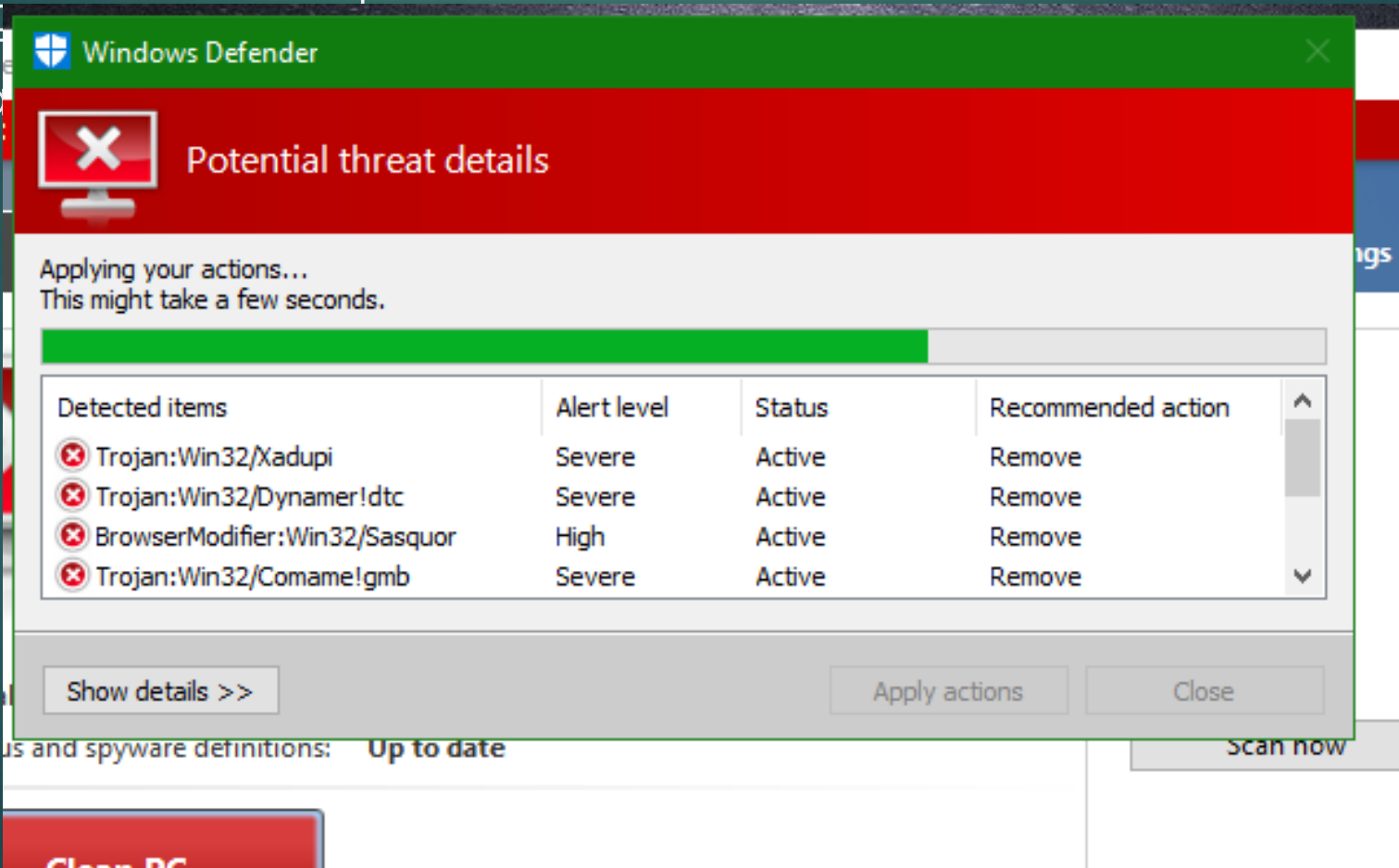
- ▶ Nodarīt kaitējumu
- ▶ Pārņemt kontroli tālākai izmantošanai
- ▶ Šifrēt datus lai izspiestu naudu
- ▶ Nozagt datus, intelektuālais īpašums

# Draudu pārskats

119

Launprātīgi

Nodarīt ko



Windows Defender

**Potential threat details**

Applying your actions...  
This might take a few seconds.

Progress bar: [Green bar indicating progress]

Detected items	Alert level	Status	Recommended action
Trojan:Win32/Xadupi	Severe	Active	Remove
Trojan:Win32/Dynamer!dte	Severe	Active	Remove
BrowserModifier:Win32/Sasquor	High	Active	Remove
Trojan:Win32/Comame!gmb	Severe	Active	Remove

Buttons: Show details >> Apply actions Close

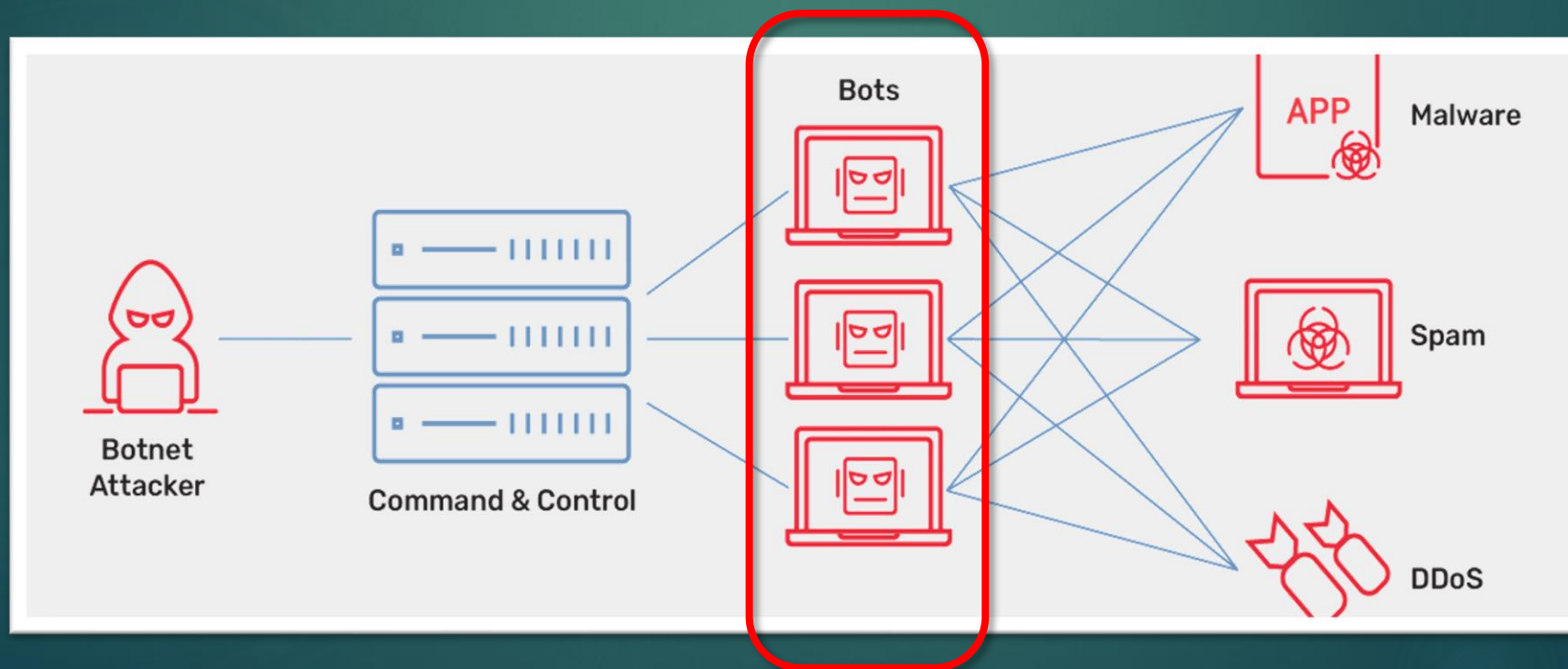
Background text: us and spyware definitions: **Up to date** Scan now

Bottom button: **Clean PC**

# Draudu pārskats

120

Ļaunprātīgā programmatūra.  
Pārņemt kontroli tālākai izmantošanai





# Draudu pārskats

121

Launprātīgā programmatūra.

Pārņemt kontroli tālākai izmantošanai

TECH / GOOGLE

## Google removes 300 Android apps that secretly hijacked phones for DDoS attacks



/ The Google Play apps offered services including storage managers, ringtones

# Draudu pārskats

122

Launprātīgā programmatūra.

Pārņemt kontroli tālākai izmantošanai



The screenshot shows the top portion of a BleepingComputer website article. The header features the site's name 'BLEEPINGCOMPUTER' in white on a dark blue background, with social media icons for Facebook, Twitter, and YouTube. A search bar is located on the right. Below the header is a navigation menu with categories: NEWS, TUTORIALS, VIRUS REMOVAL GUIDES, DOWNLOADS, DEALS, and VPN. The breadcrumb trail reads: Home > News > Security > Russian hackers use fake DDoS app to infect pro-Ukrainian activists. The main title of the article is 'Russian hackers use fake DDoS app to infect pro-Ukrainian activists'. The author is identified as 'By Sergiu Gatlan'. At the bottom right, the publication date is 'July 19, 2022', the time is '01:06 PM', and there are '0' comments.

**BLEEPINGCOMPUTER**

NEWS ▾ TUTORIALS ▾ VIRUS REMOVAL GUIDES ▾ DOWNLOADS ▾ DEALS ▾ VPN

Home > News > Security > Russian hackers use fake DDoS app to infect pro-Ukrainian activists

## Russian hackers use fake DDoS app to infect pro-Ukrainian activists

By [Sergiu Gatlan](#)

July 19, 2022 01:06 PM 0

# Draudu pārskats

123

Launprātīgā programmatūra.

Šifrēt datus



The screenshot shows the Wana Decrypt0r 2.0 ransomware interface. The window title is "Wana Decrypt0r 2.0". The main heading is "Ooops, your files have been encrypted!". On the left, there is a large padlock icon. Below it, two countdown timers are displayed: "Payment will be raised on 5/16/2017 00:47:55" with a time left of "02:23:57:37", and "Your files will be lost on 5/20/2017 00:47:55" with a time left of "06:23:57:37". The main text area contains sections: "What Happened to My Computer?", "Can I Recover My Files?", and "How Do I Pay?". At the bottom, there is a Bitcoin logo with the text "Send \$300 worth of bitcoin to this address:" and a Bitcoin address "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw" with a "Copy" button. Two buttons, "Check Payment" and "Decrypt", are at the bottom.

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

**What Happened to My Computer?**  
Your important files are encrypted.  
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>.  
But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled.  
Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.  
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.  
And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

Your files will be lost on  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

# Draudu pārskats

124

Launprātīgā programmatūra. Šifrēt datus  
Uzņēmuma politika nepieļauj maksāt jo:

- ▶ Nav nekādas garantijas ka atgūs datus
- ▶ Nav garantijas ka summa nepalielināsies
- ▶ Reputācijas zaudēšana



# Draudu pārskats

125

Launprātīgās programmatūra

- ▶ Nozagt datus
- ▶ Iegūt kontroli par ierīci

Screenshot of the Google Play Store page for Signal Private Messenger. The page shows the app icon, a rating of 4.5 stars, and over 100 million downloads. It features a large "Install on more devices" button. A red circle with the number "1" is over the rating and a red circle with the number "2" is over the download count.

Screenshot of the Google Play Store page for WhatsApp Messenger. The page shows the app icon, a rating of 4.2 stars, and over 5 billion downloads. It features a large "Install on more devices" button. A red circle with the number "1" is over the rating and a red circle with the number "2" is over the download count.

Screenshot of the Google Play Store page for Onchain Custodian. The page shows the app icon, a rating, and download information. A large red watermark reading "FAKE APP" is overlaid across the entire screenshot. A sidebar menu is visible on the left.

# Rīcība drošības incidenta un pārkāpumu gadījumos

126

- ▶ Kā pamanīt?
- ▶ Ko darīt ja gadījās?
- ▶ Publiskie kontakti

# Rīcība drošības incidenta un pārkāpumu gadījumos

Viedierīces ir tik gudras cik gudrs ir to lietotājs

Apzināties savu vidi

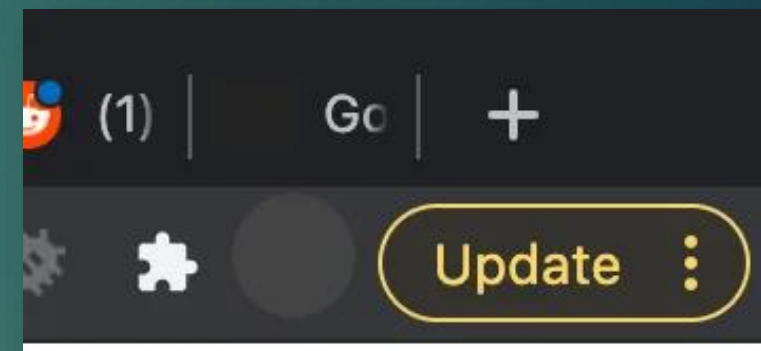
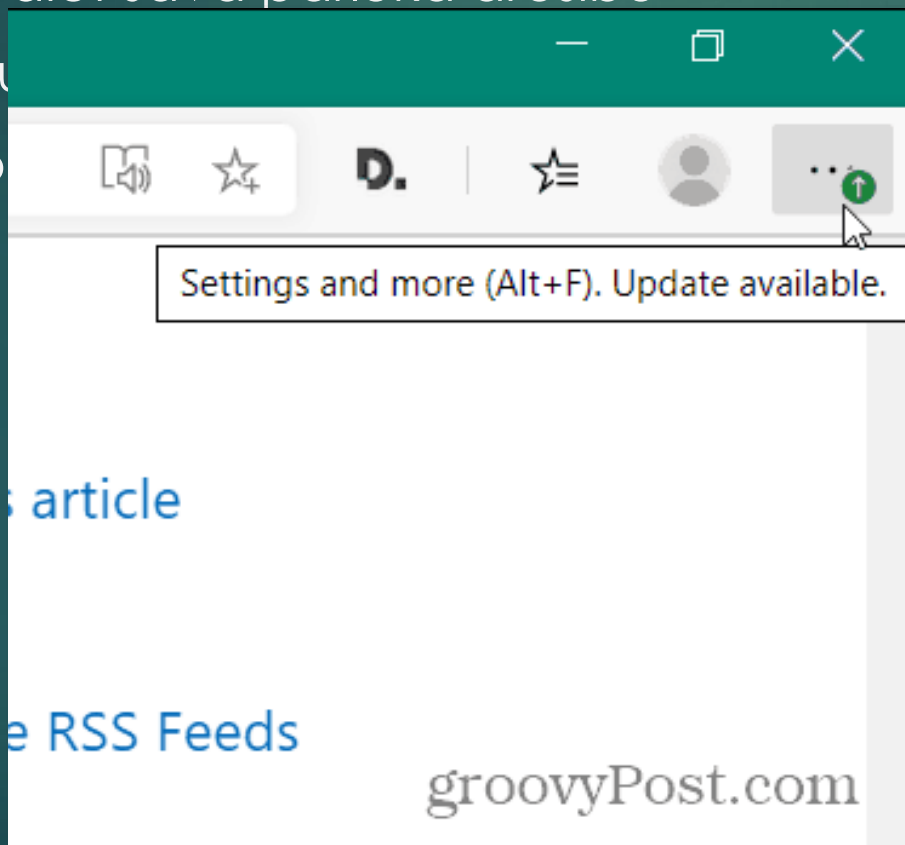
- ▶ Pamata darba komunikācijas vide: e-pasts, tālrunis, internets, Informācijas sistēmas
- ▶ Izmantot darbam IT ieteicamo pārlūku, pārējām lietām citu pārlūku
  - ▶ Darbam – MS Edge
  - ▶ Pārējām – Chrome, Firefox, Opera, u.c.

# Rīcība drošības incidenta un pārkāpumu gadījumos

128

Pārbaudiet sava pārlūka drošību

- ▶ Atjauno
- ▶ Atsp...





# Rīcība drošības incidenta un pārkāpumu gadījumos

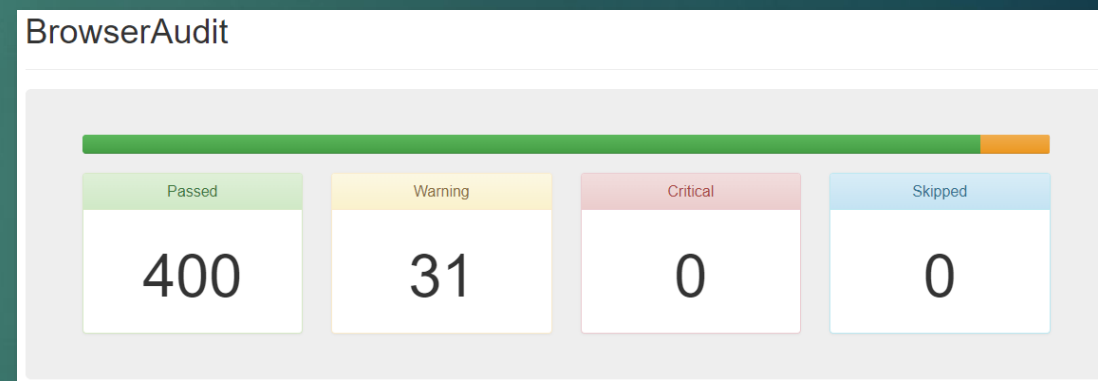
Pārbaudiet sava pārlūka drošību

▶ Pārbaudiet cik drošs ir pārlūks:

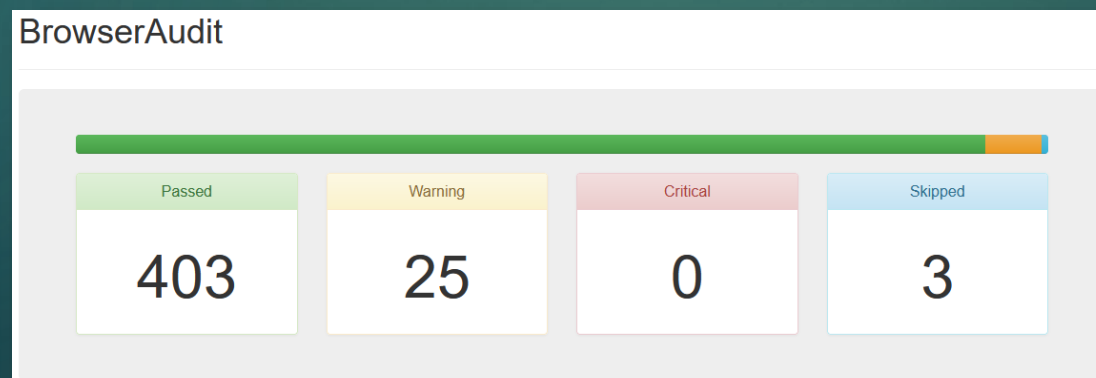
▶ <https://browseraudit.com/>, [apraksts](#)

▶ <https://browserleaks.com/>

MS Edge:



Firefox:



# Rīcība drošības incidenta un pārkāpumu gadījumos

130

Pārbaudiet sava pārlūka drošību

[Test Malware! - WICAR.org - Test Your Anti-Malware Solution!](http://www.wicar.org)

## Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org/>. You may wish to try each test systematically. Ideally, all tests should be blocked by your anti-malware defences. If a blank window loads, then it likely was not detected/prevented.

EICAR TEST-VIRUS

[SSL] The official EICAR.COM anti-virus test file. This is a 16bit DOS COM file and cannot run on recent OSes, but should be detected.

MS14-064 XP and below

[SSL] All Windows NT/95/98/2000/XP IE3+ Internet Explorer Windows OLE Automation Array (pre XP) CVE-2014-6332

MS14-064 2003 to Windows 10

[SSL] All Windows 2003/Vista/2008/7/8/10 IE6+ Internet Explorer Windows OLE Automation Array (post XP) CVE-2014-6332

Java JRE 1.7 Applet

[SSL] win32 (Java 7 JRE/JDK) Chrome Firefox IE Java 7 Applet Remote Code Execution (Browser Independent) CVE-2012-4681

MS03-020

[SSL] win32 NT/XP/2003 IE6 MS03-020 Internet Explorer's handling of the OBJECT type attribute CVE-2003-0344

MS05-054

[SSL] win32 XP IE6 MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler CVE-2005-1790

MS09-002

[SSL] win32 XP/Vista IE7 Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption CVE-2009-0075

MS09-072

[SSL] win32 IE6 Internet Explorer Style getElementsByTagName Memory Corruption CVE-2009-3672

MS10-090

[SSL] win32 IE6 Internet Explorer CSS SetUserClip Memory Corruption CVE-2010-3962

Firefox 5.0 - 15.0.1 exposedProps

[SSL] Windows Firefox 5.0 to 15.0.1 exposedProps CVE-2012-3993

Embedded VLC AMV

[SSL] Windows VLC v1.1.4 to 1.1.8 Browser Independent AMV invalid pointer CVE-2010-3275

Adobe Flash Hacking Team leak

[SSL] Hacking Team July 2015 data leak Adobe Flash 18.0.0.194 Use After Free CVE-2015-5119

# Rīcība drošības incidenta un pārkāpumu gadījumos

131


Pārbaudiet sava pārlūka drošību

Malwarebytes | Browser Guard

## Website blocked due to trojan

Website Blocked: [malware.wicar.org](https://malware.wicar.org)  
v2.6.22 | Trojan: 2.0.202402221618

Malwarebytes Browser Guard blocked this page because it may contain malicious activity.

 We strongly recommend you do not continue. You may be putting your safety at risk by visiting this site. For more information, visit [Malwarebytes Support](#).

← Go back

Continue to this website


Do not block this site again.



This site has been reported as unsafe  
Hosted by [malware.wicar.org](https://malware.wicar.org)

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing harmful programs that may try to steal personal or financial information.

Go back

More information 

Microsoft Defender SmartScreen

# Rīcība drošības incidenta un pārkāpumu gadījumos

132

Kā pamanīt. Acīmredzami

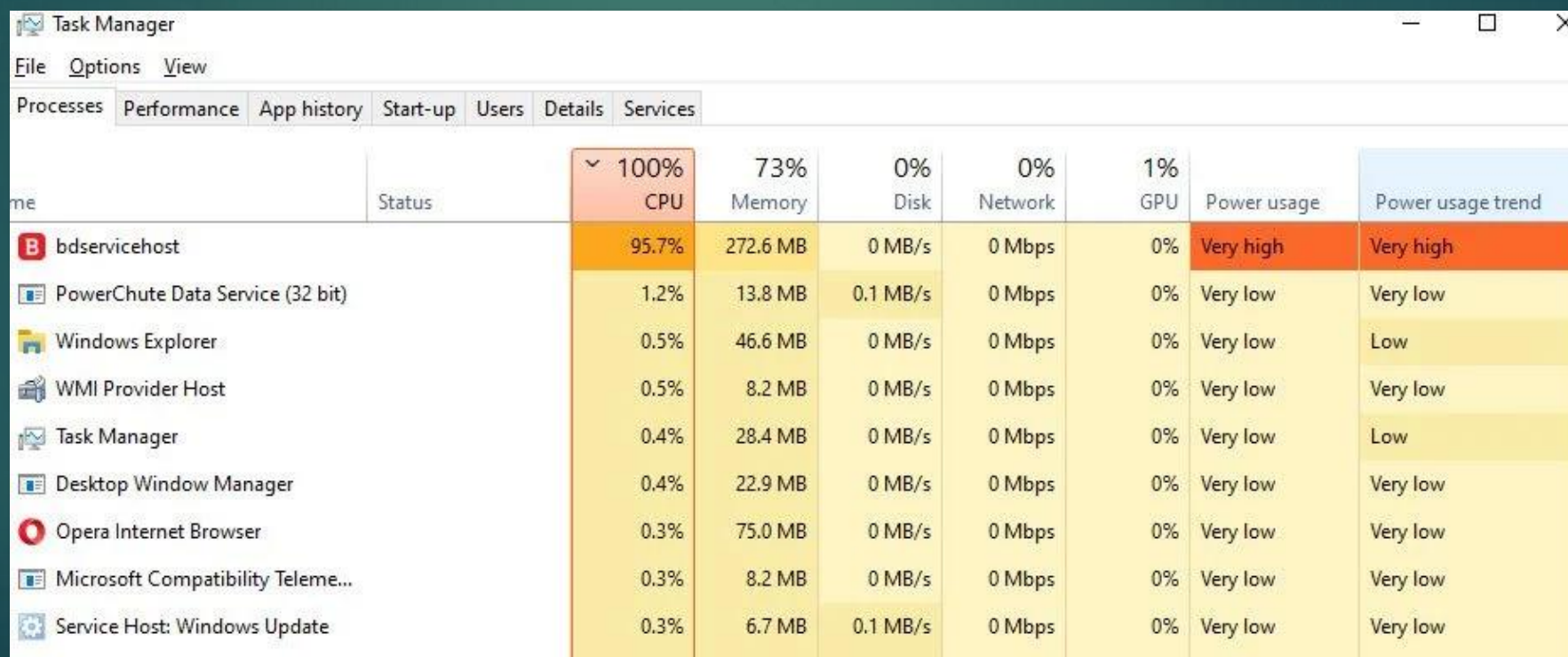


# Rīcība drošības incidenta un pārkāpumu gadījumos

133

Kā pamanīt. Slēptie procesi.

- ▶ Pazeminājās datora veiktspēja, netipiskie procesi



The screenshot shows the Windows Task Manager Performance tab. The CPU usage is at 100%, and the bdservicehost process is highlighted in red, indicating it is the cause of the high CPU usage. Other processes like PowerChute Data Service, Windows Explorer, WMI Provider Host, Task Manager, Desktop Window Manager, Opera Internet Browser, Microsoft Compatibility Telemetry, and Service Host: Windows Update are also listed with their respective resource usage.

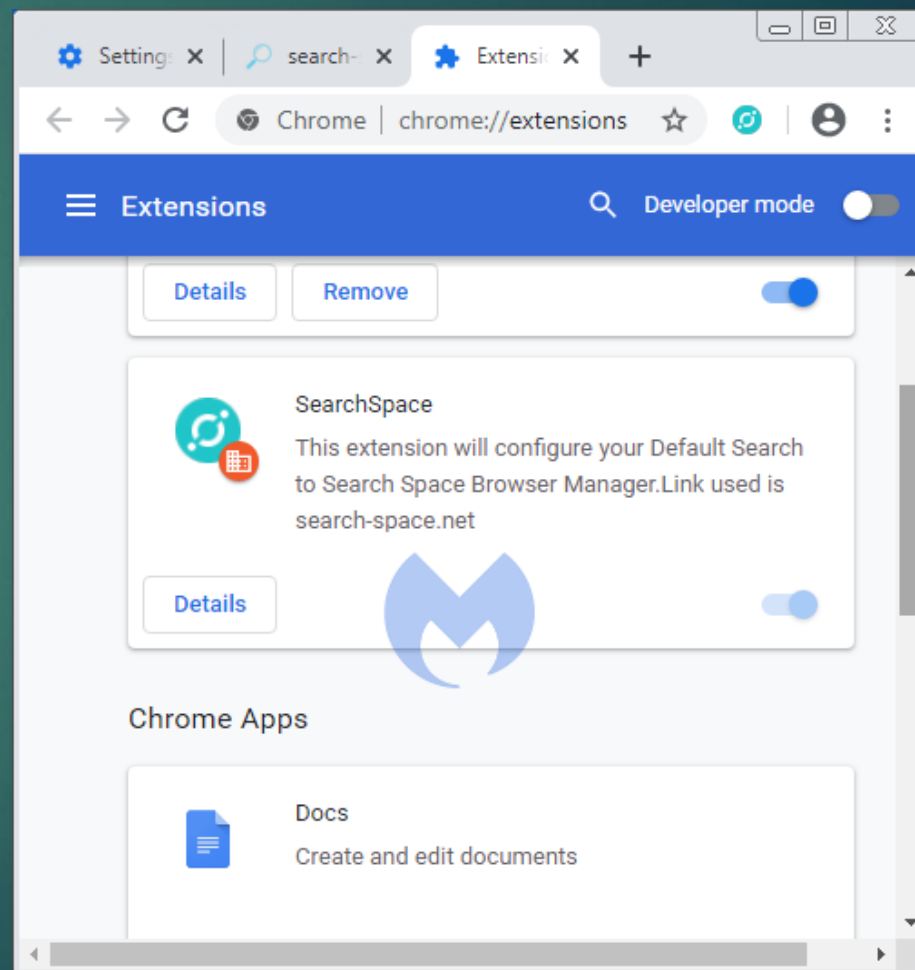
Process Name	Status	CPU	Memory	Disk	Network	GPU	Power usage	Power usage trend
bdservicehost		95.7%	272.6 MB	0 MB/s	0 Mbps	0%	Very high	Very high
PowerChute Data Service (32 bit)		1.2%	13.8 MB	0.1 MB/s	0 Mbps	0%	Very low	Very low
Windows Explorer		0.5%	46.6 MB	0 MB/s	0 Mbps	0%	Very low	Low
WMI Provider Host		0.5%	8.2 MB	0 MB/s	0 Mbps	0%	Very low	Very low
Task Manager		0.4%	28.4 MB	0 MB/s	0 Mbps	0%	Very low	Low
Desktop Window Manager		0.4%	22.9 MB	0 MB/s	0 Mbps	0%	Very low	Very low
Opera Internet Browser		0.3%	75.0 MB	0 MB/s	0 Mbps	0%	Very low	Very low
Microsoft Compatibility Telemetry		0.3%	8.2 MB	0 MB/s	0 Mbps	0%	Very low	Very low
Service Host: Windows Update		0.3%	6.7 MB	0.1 MB/s	0 Mbps	0%	Very low	Very low

# Rīcība drošības incidenta un pārkāpumu gadījumos

134

Kā pamanīt. Slēptie procesi.

- ▶ Parādījās neierasta datora uzvedība





# Rīcība drošības incidenta un pārkāpumu gadījumos

135


Ko darīt ja gadījās?

## Reset your browser settings

1. On your computer, open Chrome.
2. At the top right, select More  > **Settings**.
3. Select **Reset settings** > **Restore settings to their original defaults** > **Reset settings**.

If you reset your browser settings, you have to turn some extensions on. To turn extensions on, at the top right, select More  > **Extensions** > **Manage extensions**. Only turn on extensions you trust.

If the steps above don't work, go to the [Chrome Help Forum](#).

**Tip:** If you're a website owner, [learn how to resolve malware or unwanted software issues](#)  related to your downloads.

# Rīcība drošības incidenta un pārkāpumu gadījumos

136

Izmantot uzticamu pretvīrusu programmatūru

## Consumer antivirus software providers for Windows

**If you're running a supported version of Windows, you've already got Microsoft Defender Antivirus built in, helping to protect you against viruses, spyware, and other malware.**

Malware consists of viruses, spyware and other potentially unwanted software. Microsoft Defender Antivirus is free and is included in Windows, always on and always working to protect your PC against malware.

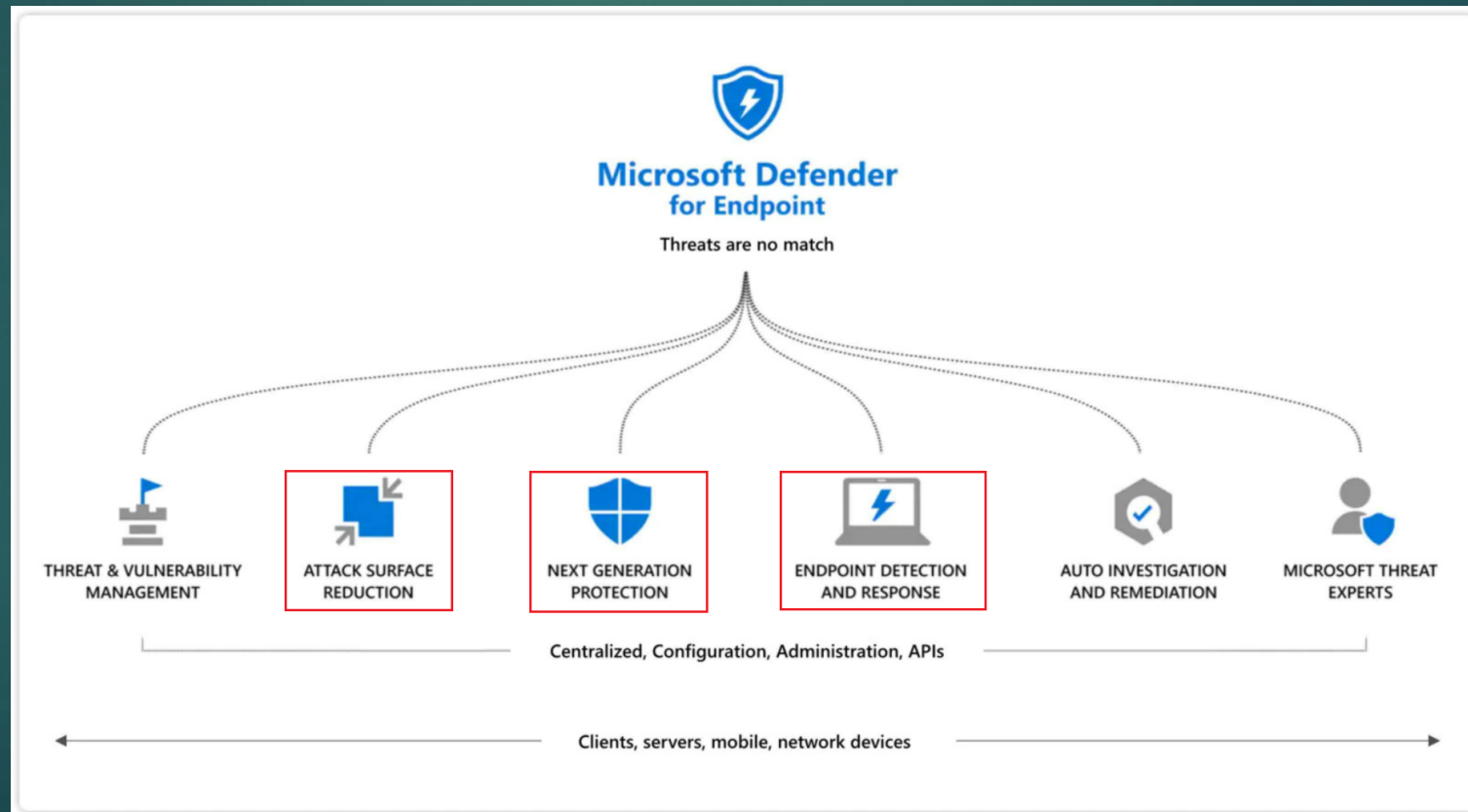
Hackers and scammers sometimes use fake antimalware software to trick you into installing viruses or malware on your computer. Should you wish to explore alternatives to the already installed or available Microsoft antimalware software on your Windows PC, the reputable security companies listed below provide consumer security software that is compatible with Windows. Just click the company name to see the Windows-compatible product they offer.



# Rīcība drošības incidenta un pārkāpumu gadījumos

137

Izmantot uzticamu pretvīrusu programmatūru



# Rīcība drošības incidenta un pārkāpumu gadījumos

138

Izmantot uzticamu pretvīrusu programmatūru



# Rīcība drošības incidenta un pārkāpumu gadījumos

139

Izmantot drošības spraudņus pārlūkos



**AdBlock — best ad blocker**

Size 12.7 MB Version 5.19.0



**Malwarebytes Browser Guard**

Size 45.7 MB Version 2.6.22

# Rīcība drošības incidenta un pārkāpumu gadījumos

140

Facebook reporti <https://www.facebook.com/hacked/>

## Report compromised account

If you believe your account has been compromised by another person or a virus, please click the "My account is compromised" button below. We'll help you log back into your account so that you can regain control.

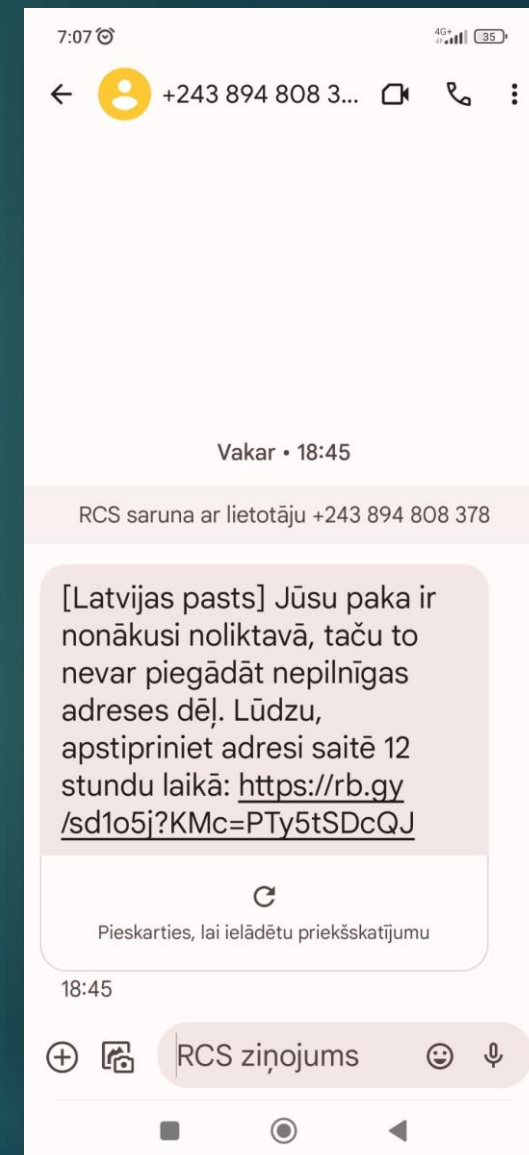
Cancel

My account is compromised

# Rīcība drošības incidenta un pārkāpumu gadījumos

141

## SMS krāpnieki



# Rīcība drošības incidenta un pārkāpumu gadījumos

142

## Kopējie kontakti

- ▶ Darba vietas kontakti, lokālais IT atbalsta dienests
- ▶ Kopējie kontakti: <https://cert.lv/lv/kontakti>

## Kontakti

**Adrese:** Raiņa bulvāris 29, Rīga, LV-1459, Latvija

**Telefons:** +371 67085888 (ziņojumu pieņemšana - 24x7, CERT.LV darba laiks - darba dienās no 9:00 līdz 18:00)

### E-pasts:

ziņot par incidentu: [cert@cert.lv](mailto:cert@cert.lv), [cert@cert.gov.lv](mailto:cert@cert.gov.lv)

par mēstuļu (SPAM) gadījumiem: [abuse@cert.lv](mailto:abuse@cert.lv), [abuse@cert.gov.lv](mailto:abuse@cert.gov.lv)

par atbildīgo personu: [kontakti@cert.lv](mailto:kontakti@cert.lv)

sabiedriskās attiecības: [prese@cert.lv](mailto:prese@cert.lv)

lai ziņotu par ievainojamību: [cvd@cert.lv](mailto:cvd@cert.lv)

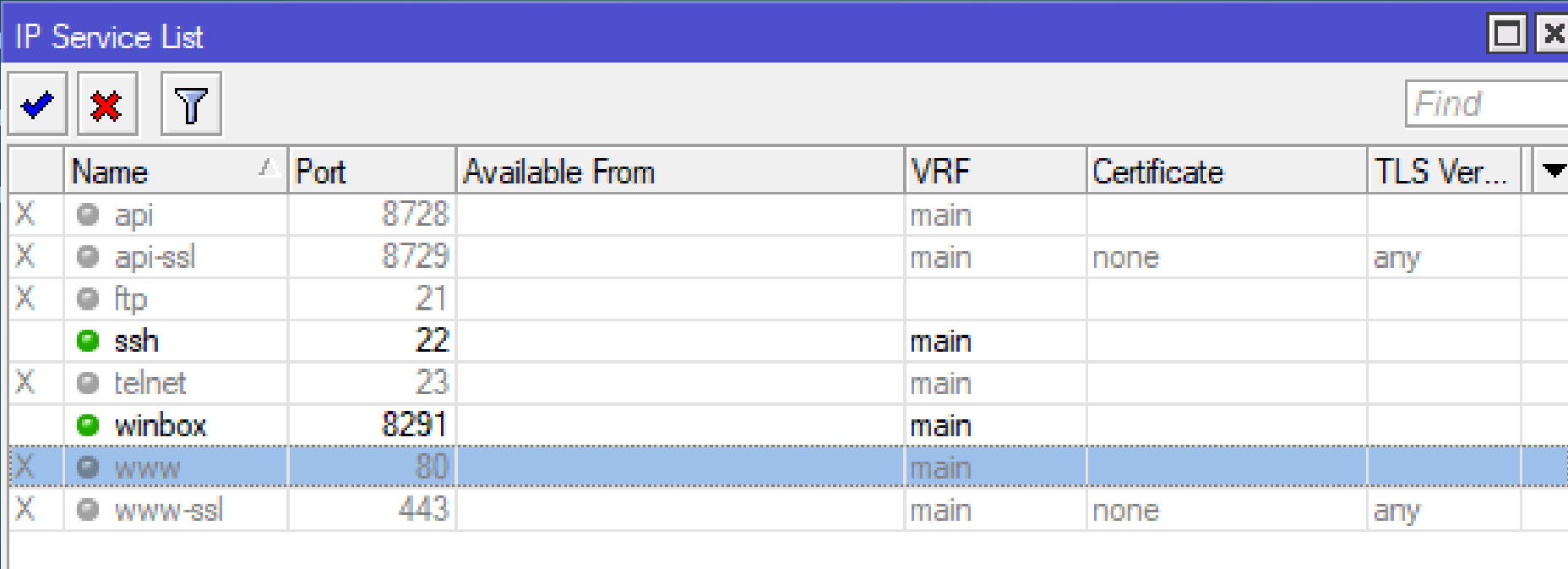
saziņai ar CERT.LV datu aizsardzības speciālistu: tel.nr. +371 67085888, e-pasts: [cert@cert.lv](mailto:cert@cert.lv)

# Audotorijas Jautājumi

143

Mikrotik ugunsmūra ieteicamā konfigurācija:

- ▶ Aizliegt noklusējuma Mikrotik servissus, SSH, HTTP, TELNET



The screenshot shows the 'IP Service List' window in Mikrotik WinBox. The window title is 'IP Service List'. Below the title bar, there are three icons: a blue checkmark, a red X, and a funnel. To the right of these icons is a search box labeled 'Find'. The main area contains a table with the following columns: Name, Port, Available From, VRF, Certificate, and TLS Ver... The table lists several services, with 'www' selected. The 'www' row is highlighted in blue. The 'ssh' and 'winbox' rows have green status indicators, while others have grey ones.

	Name	Port	Available From	VRF	Certificate	TLS Ver...
X	api	8728		main		
X	api-ssl	8729		main	none	any
X	ftp	21				
	ssh	22		main		
X	telnet	23		main		
	winbox	8291		main		
X	www	80		main		
X	www-ssl	443		main	none	any





# Audotorijas Jautājumi

145

Uzmācīgie zvanītāji, ko darīt:

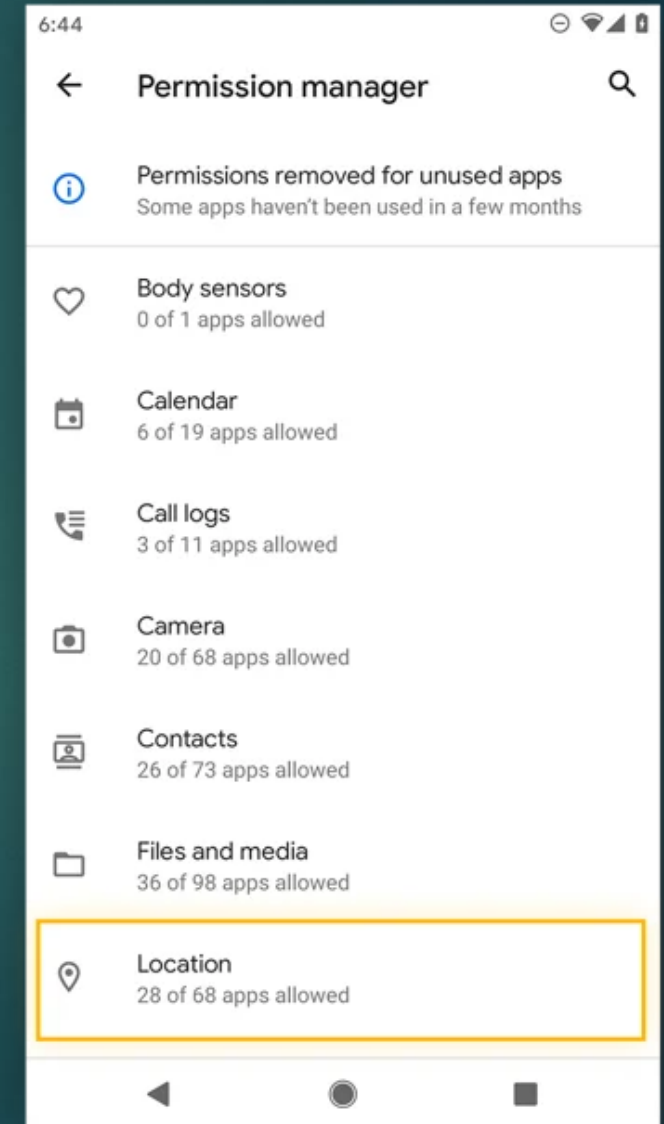
- ▶ Runājam latviski
- ▶ Bloķējam numuris
- ▶ Ja nav gaidāms zvans no ārzemēm neceļam
- ▶ Ziņojam CERT.lv par šo, CERT ir saziņas kanāli ar mobilo operatoru drošības pārstāvjiem.

# Audotorijas Jautājumi

146

Viedierīču aizsardzība:

- ▶ Izmantojam aplikācijas no drošiem avotiem
- ▶ Tiesību caurskatīšana aplikācijām
- ▶ Atpazīstamu pārlūku lietošana
- ▶ Drošības spraudņu lietošana pārlūkprogrammās





Finansē  
Eiropas Savienība  
NextGenerationEU

2027  
Nacionālais  
attīstības plāns



ĀRŠĀRĀDZĪBAS  
MINISTRIJA



Vides aizsardzības un  
reģionālās attīstības  
ministrija



CERT.LV  
Informācijas tehnoloģiju  
drošības centrs  
nodrošinot drošību



ZEMGALES  
PLĀNOŠANAS  
REĢIONS



trainify

CIVILMILITĀRĀS SADARBĪBAS VEICINĀŠANA REĢIONOS

## IT datu drošības pamati - praktiskas iemaņas ikdienas darbā

5.martā 13:00 - 16:30

6.martā 9:00 - 12:00

Tiešsaistē

