Finansē Eiropas Savienība

2027 Nacionālais attīstības plāns

Vides aizsardzības un reģionālās attīstības ministrija

CERT.LV

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

Aktivitāte tiek īstenota projekta "Pašvaldības kapacitātes stiprināšana to darbības efektivitātes un kvalitātes uzlabošanai, projekta Nr. 1.1.2.i.0/1/22/I/VARAM/001 ietvaros

saturs

Ievads

- 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

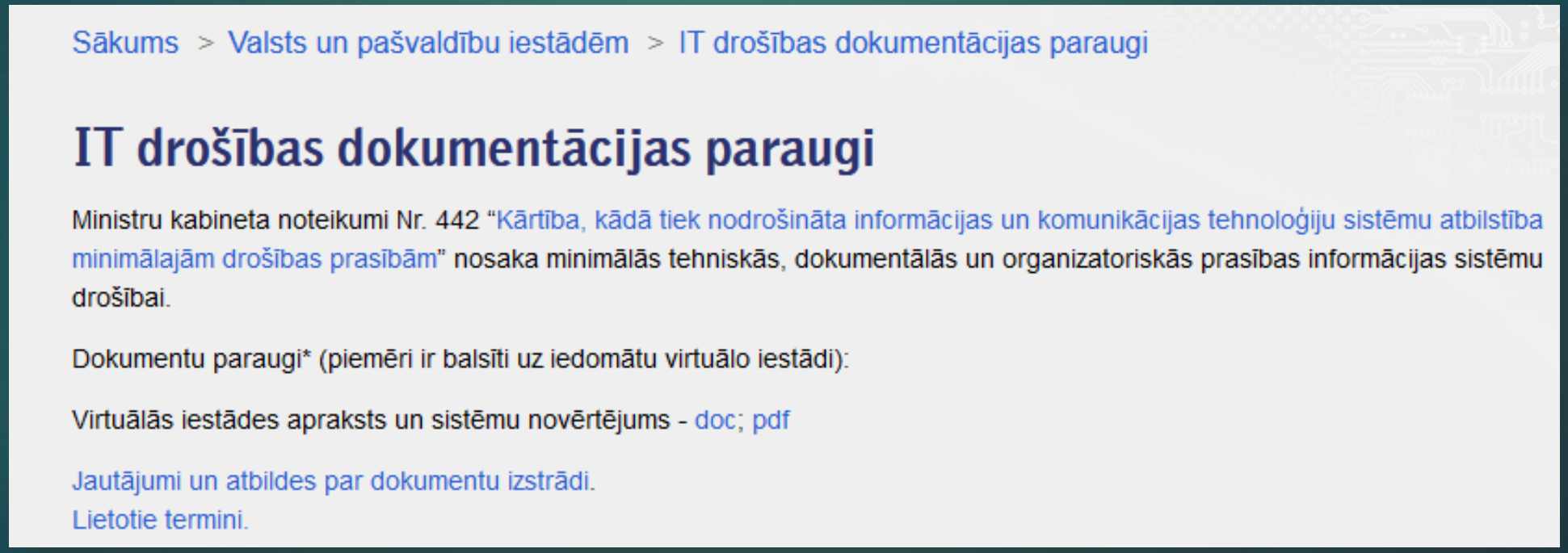
Ievads par IT datu drošību

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

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

- 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

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

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

Jautājumi?

Datu drošība

Datu drošība

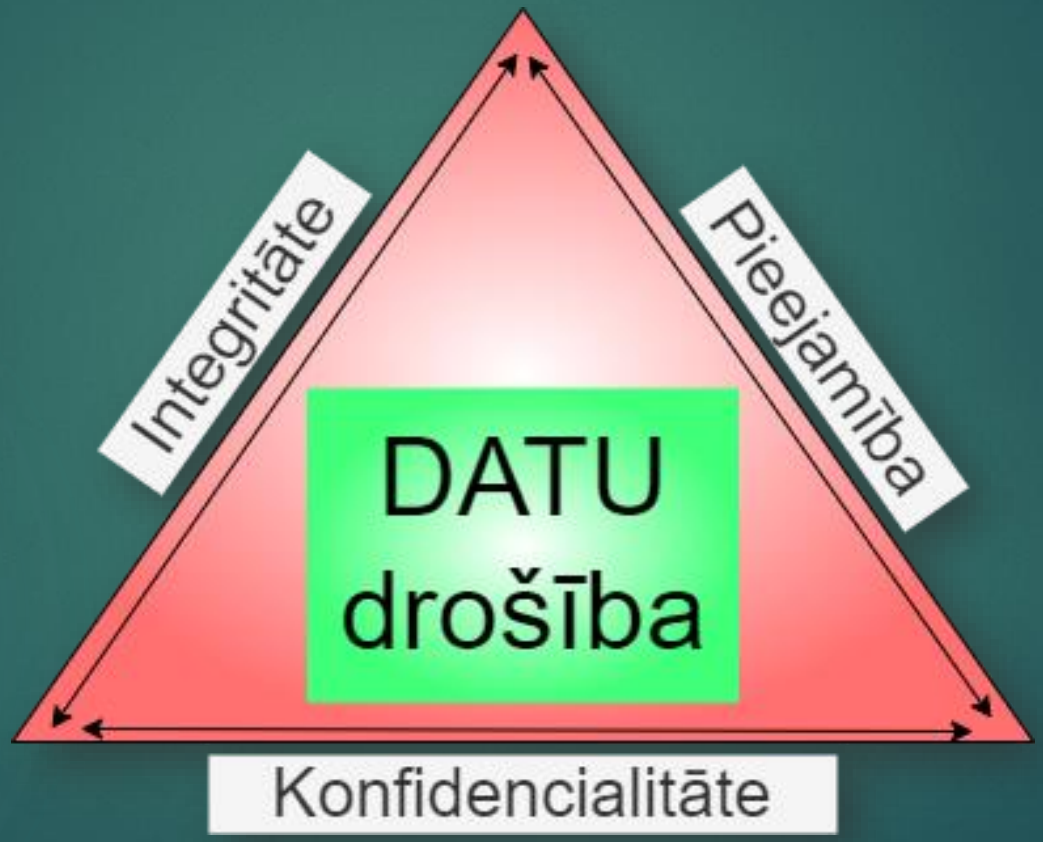
Kas tad ir datu drošība?

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

Raksturīpašības:

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

Datu drošība



Datu drošība

Konfidencialitātes raksturīpašības:

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

Datu drošība

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

Konfidencialitāte, datu klasifikācija:

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

Informācijas atklātības likums

Likusms Par Valsts noslēpumu

Datu drošība

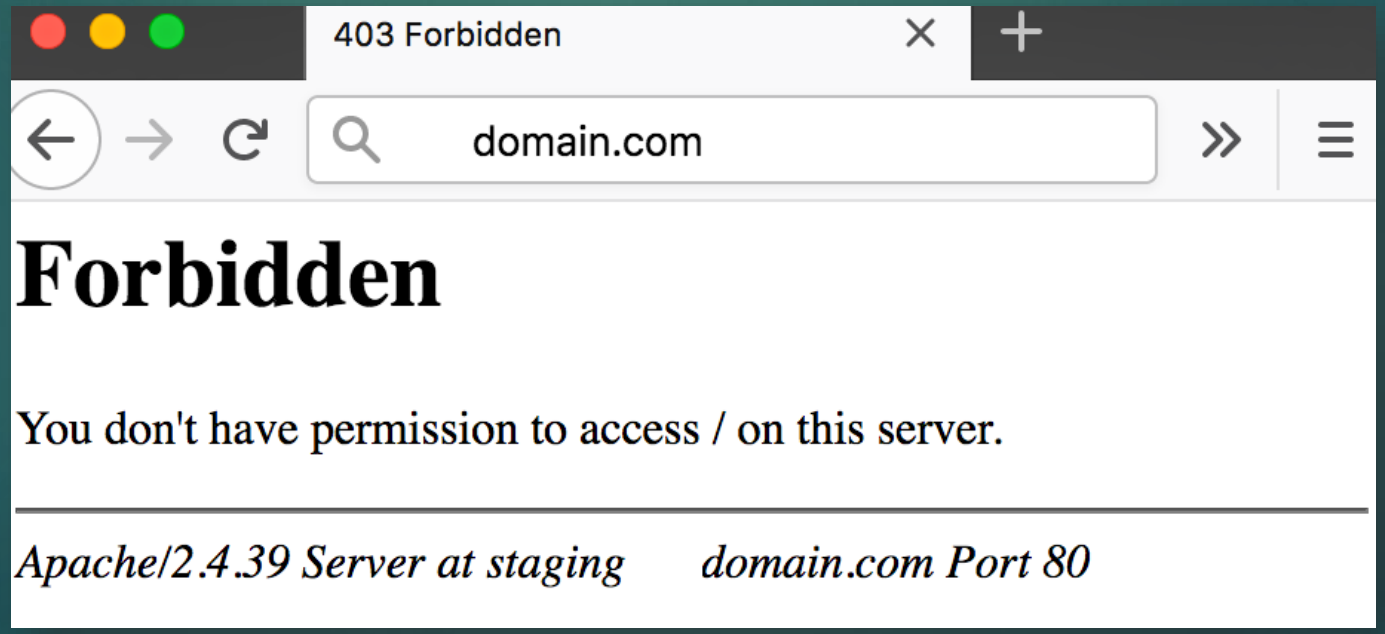
Konfidencialitāte, aizsardzība:

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

Datu drošība

Pieejamības raksturīpašības:

- Autorizēta piekļuve informācijai laikā un vietā



Datu drošība

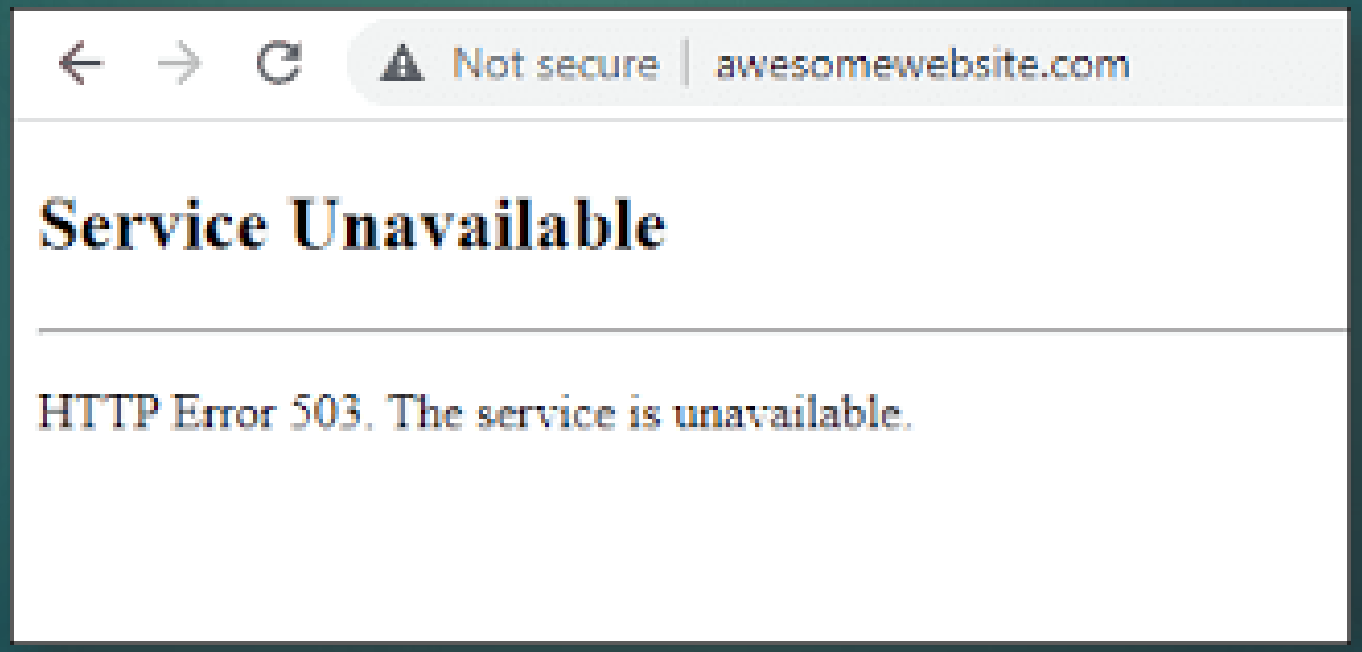
Pieejamības raksturīpašības, aizsardzība:

- 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

Pieejamības raksturīpašības, kļūmes:

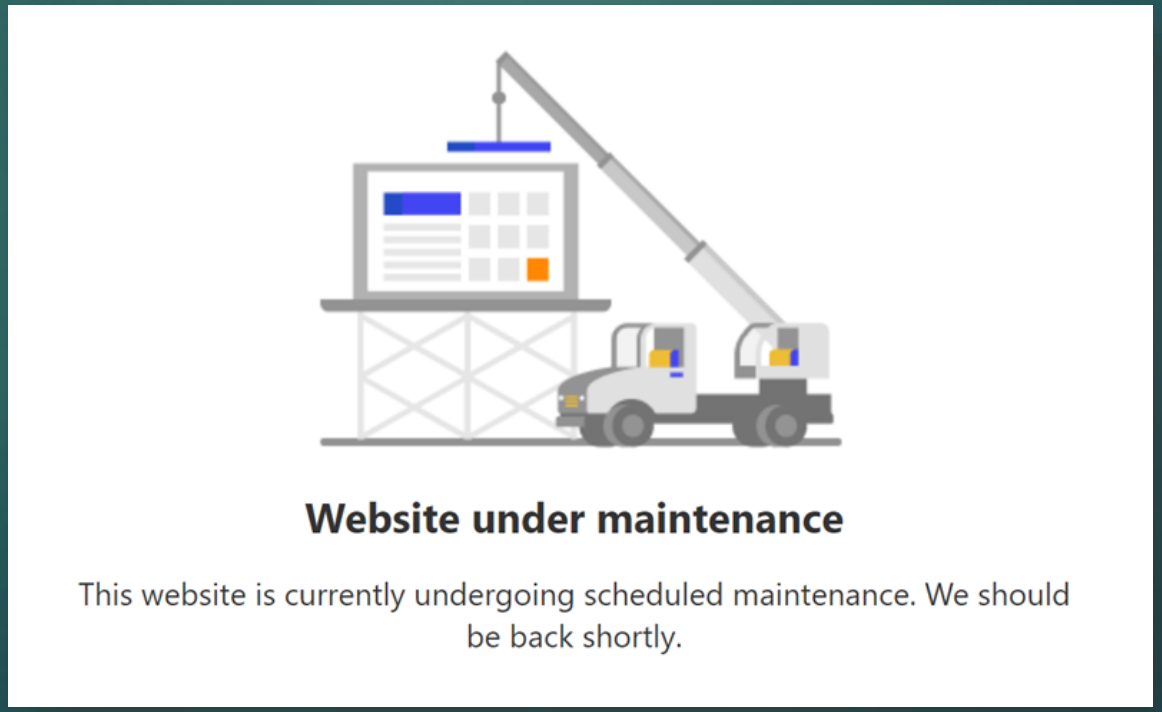
- Kļūmes dēļ, sistēmā nav pieejama



Datu drošība

Pieejamības raksturīpašības, uzturēšana:

- Plānoto uzturēšanas darbu dēļ, sistēmā nav pieejama

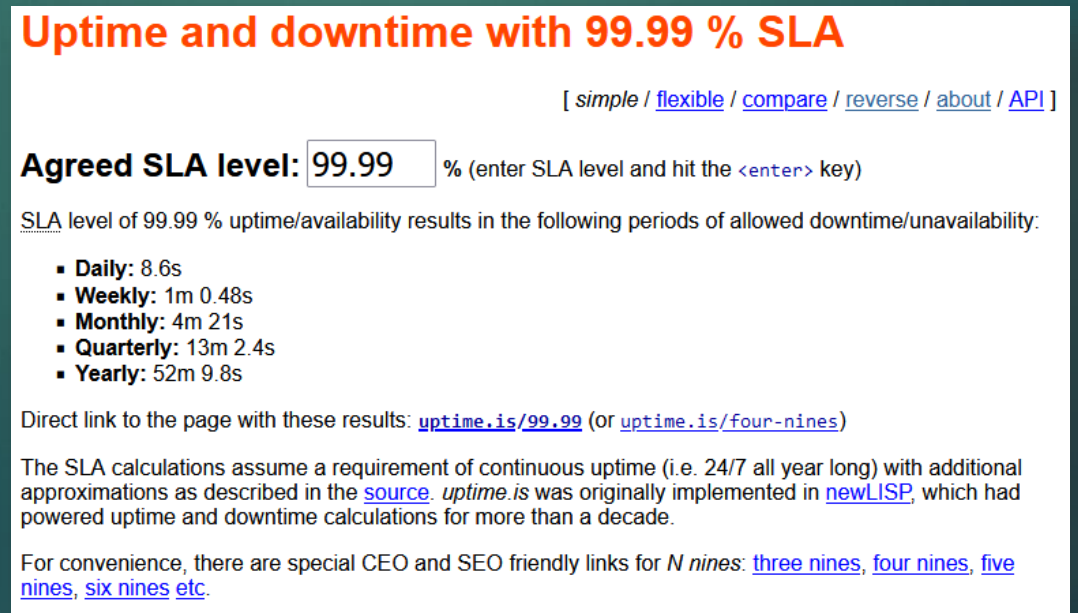


Datu drošība

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: 99.99 % (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 (or 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.

Datu drošība

Integritātes raksturīpašības:

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

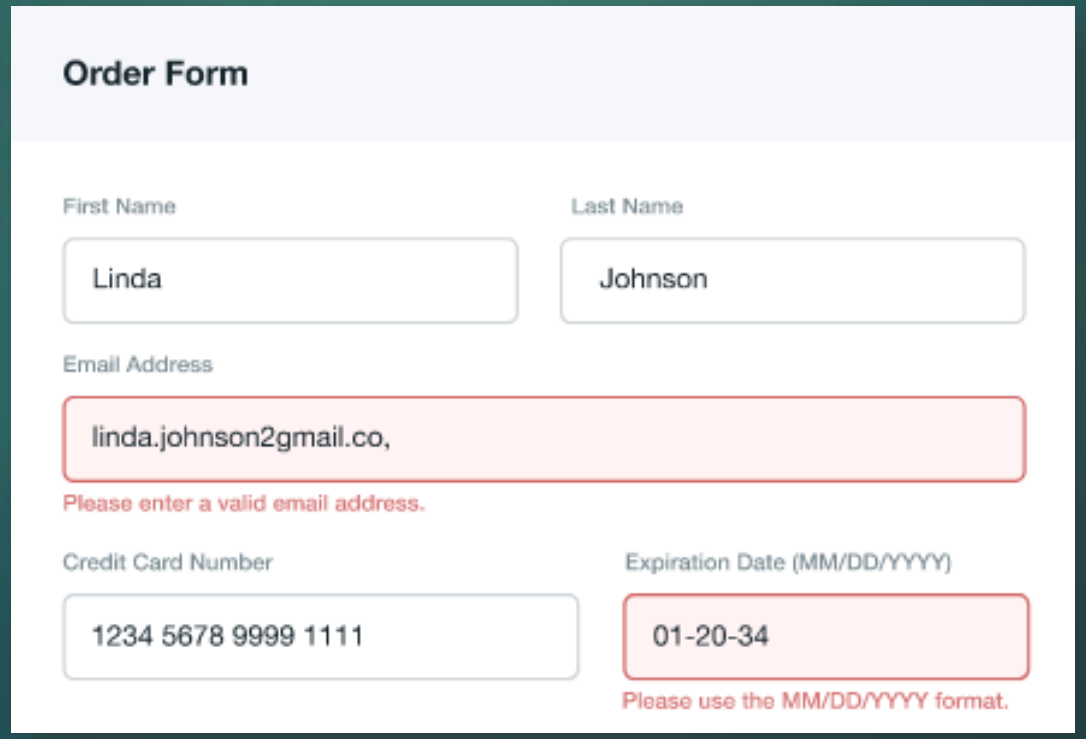
Integritātes nodrošināšana

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

Datu drošība

Integritāte nodrošināšana

- Datu validācija to ievades laikā



Datu drošība

- Jautājumi

Pašvaldības Informācijas drošības politika un pārvaldība

Pašvaldības Informācijas drošības politika un pārvaldība

- 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

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

MK noteikumi Nr. 442

Sistēmu klasifikācija pēc drošības klasēm, integritāte:

- A, B, C līmeņi

Pašvaldības Informācijas drošības politika un pārvaldība

Kā jūs raksturotu datu integritāti?

Ierakstiet lūdzu čatā savu variantu

Pašvaldības Informācijas drošības politika un pārvaldība

Datu integritāte

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

Pašvaldības Informācijas drošības politika un pārvaldība

MK noteikumi Nr. 442

Sistēmu klasifikācija pēc drošības klasēm, konfidencialitāte:

- A, B, C līmeņi

Pašvaldības Informācijas drošības politika un pārvaldība

Kā jūs raksturotu datu konfidencionalitāti?

Ierakstiet lūdzu čatā savu variantu

Pašvaldības Informācijas drošības politika un pārvaldība

Datu konfidencionalitāte

- 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

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

Kā ieviest drošu un vienkārši pārvaldāmu paroļu sistēmu?

Paroļu politika

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

Ieliekat – čatā ja nelietojat paroļu pārvaldības programmu

Paroļu politika

Jāzina paroles prasības uzņēmumā.

To parasti nosaka Lietošanas noteikumi.

Parasti:

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

Paroļu politika

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:

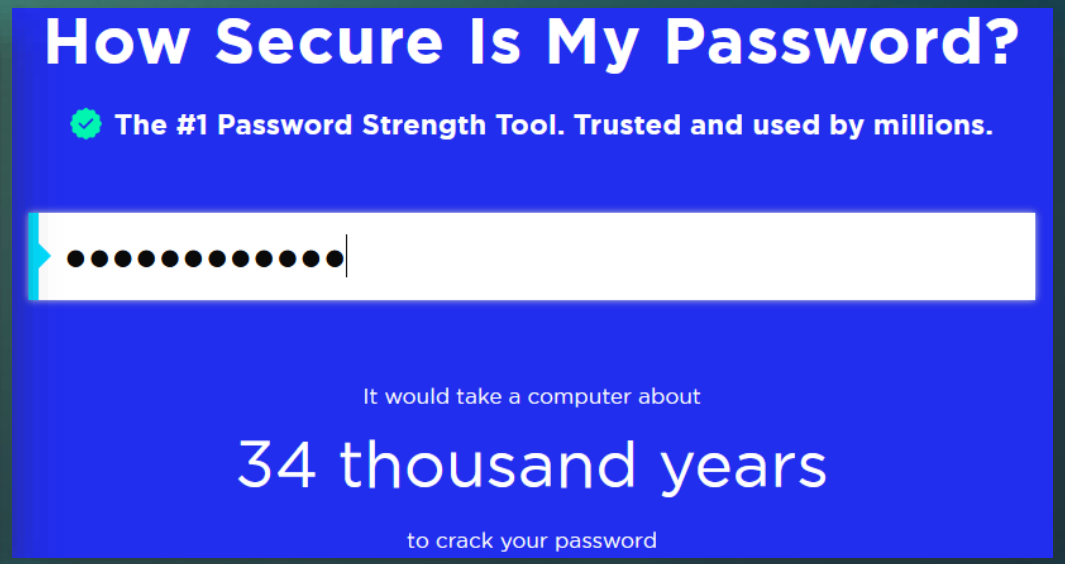
Zirgi sk@pis div1 viens

Paroļu politika

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

Zirgi sk@pis div1 kas

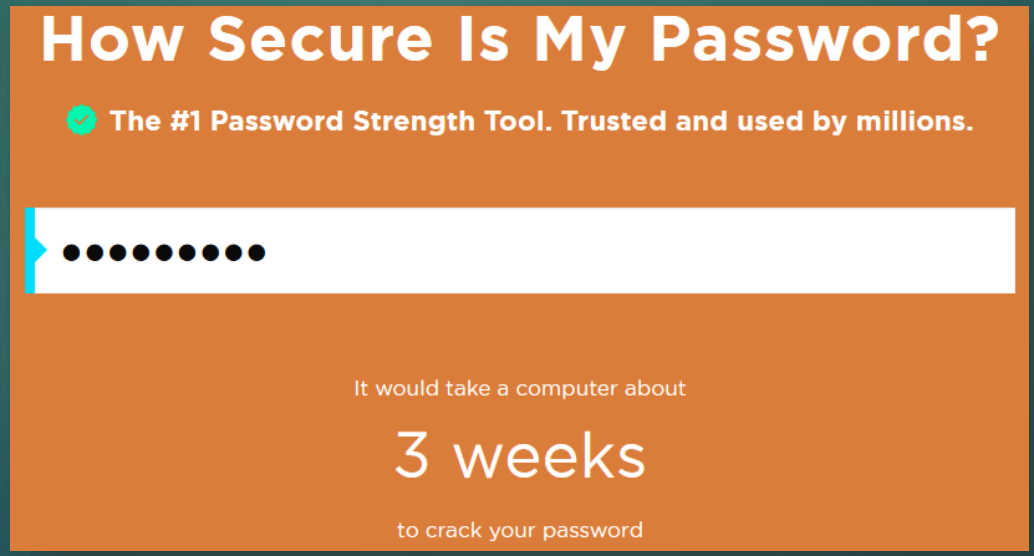
!QAZ@WSX3edc



Paroļu politika

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

Marts15!%



Paroļu politika

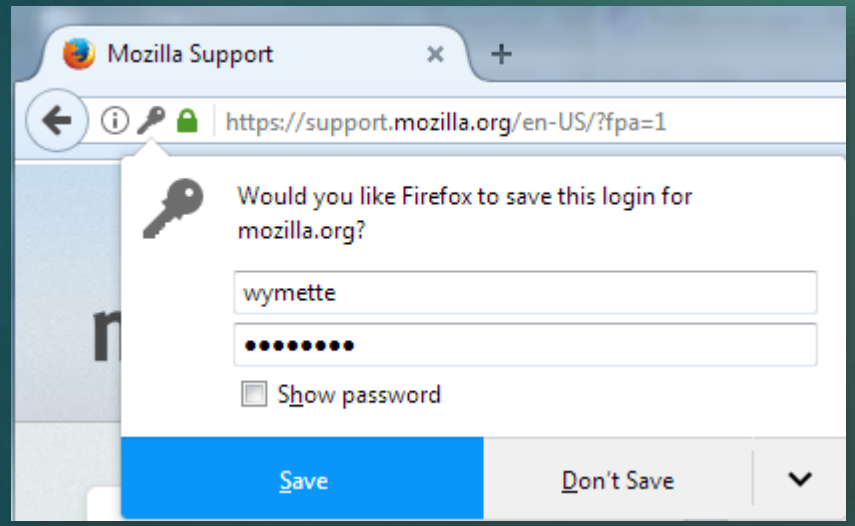
Ko darīt?

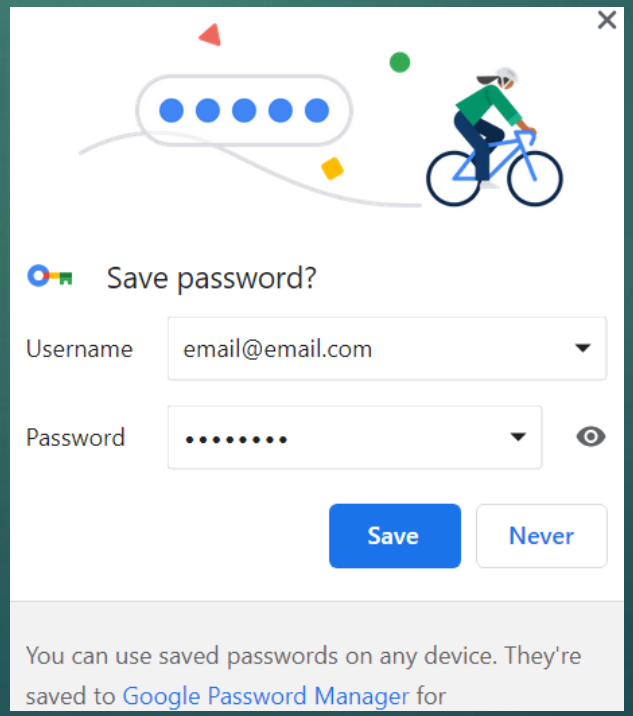
Izmantot paroļu glabāšanas programmas, aplikācijas

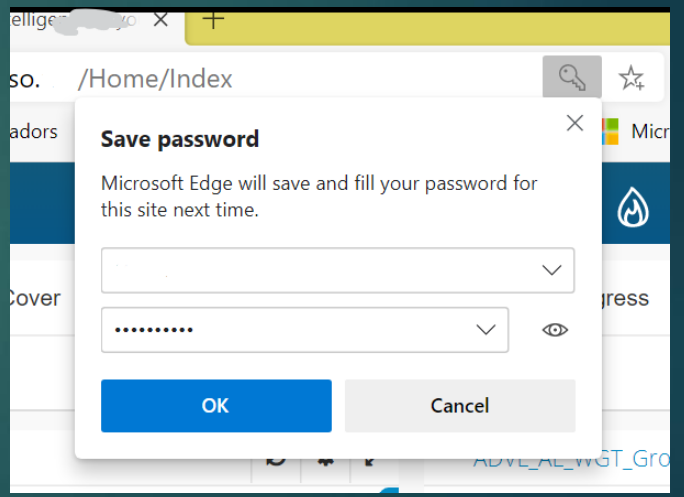
Programmatūras instalāciju jāsaskaņo ar drošības specialistu.

Paroļu politika

Izmantot paroļu ģenerēšanas un glabāšanas iespējas pārlūkā vai mobilajā ierīcē

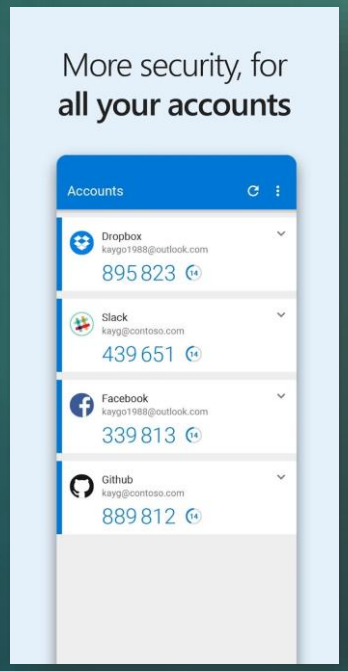


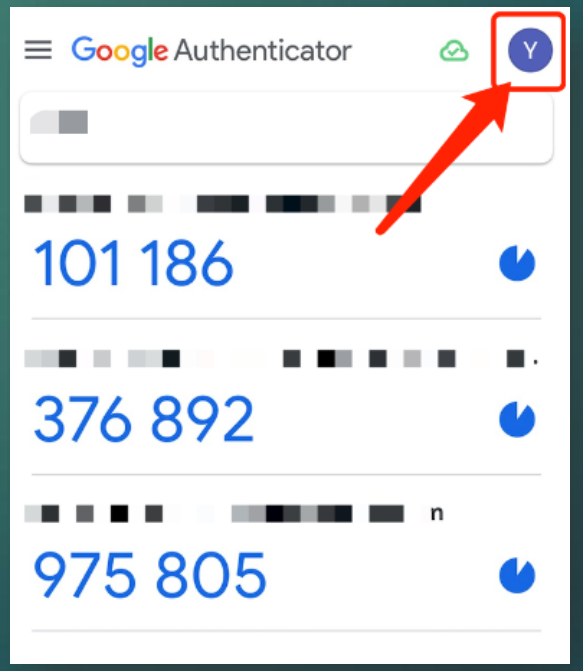




Paroļu politika

Izmantot paroļu ģenerēšanas un glabāšanas iespējas pārlūkā vai mobilajā ierīcē





Paroļu politika

Izmantot savu paroļu sistēmu

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

m@n@BANKA02@$

m@n@BANKA02)@

Paroļu politika

Izmantot savu paroļu sistēmu un kombinēt tās

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

m@n@BANKA02)@

Paroļu politika

Kur vien iespējams izmantot daudzfaktoru autentifikāciju, MFA

Paroļu politika

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

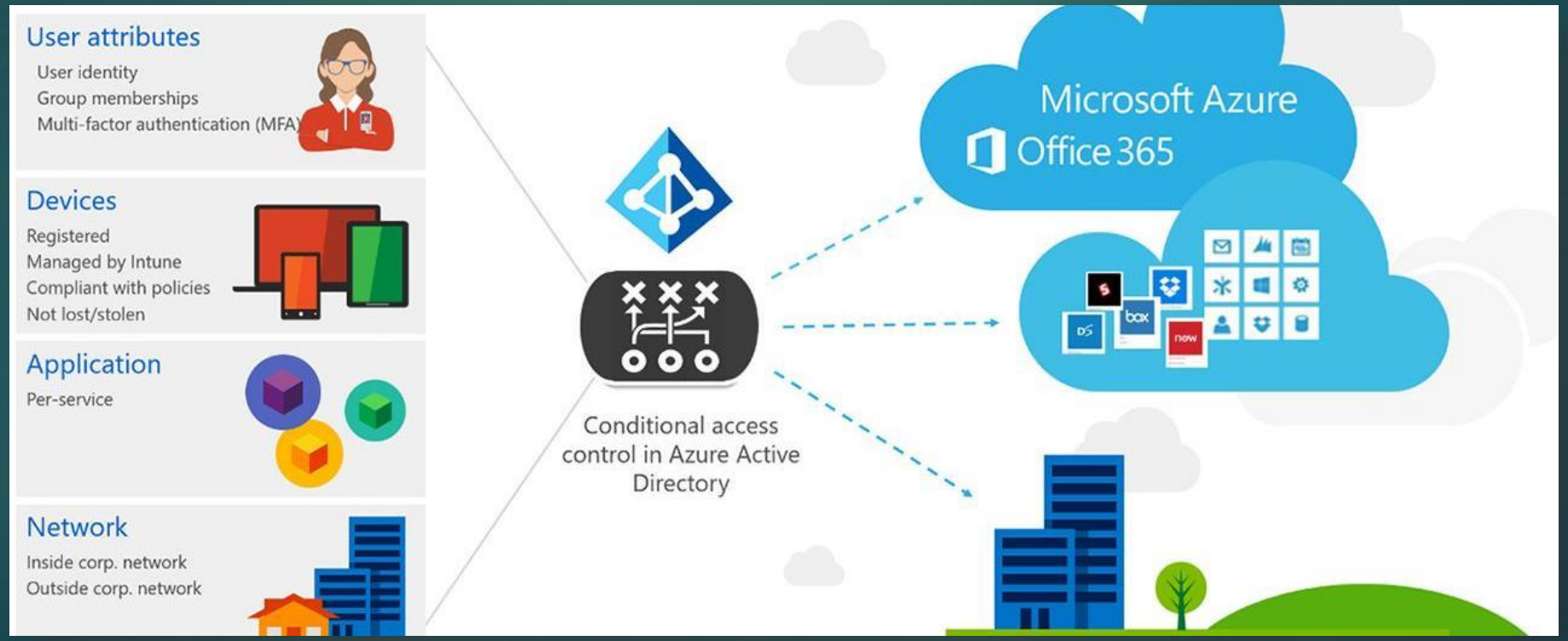
Paroļu politika

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

Nosacījumu piekļuve, Conditional access



Darbs attālināti

Darbs attālināti

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

Darbs attālināti

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

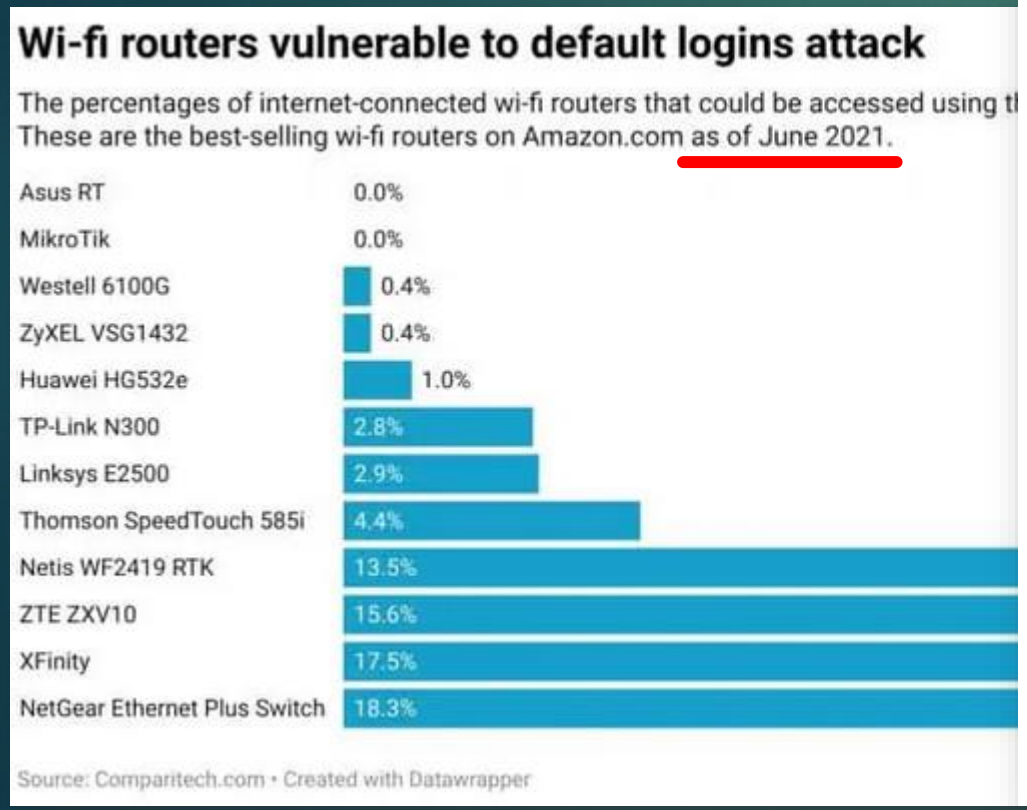
Izveidojiet drošu un atjauninātu tīkla savienojumu

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

Darbs attālināti

Izveidojiet drošu un atjauninātu tīkla savienojumu

- Nomainiet mājas rūtera noklu

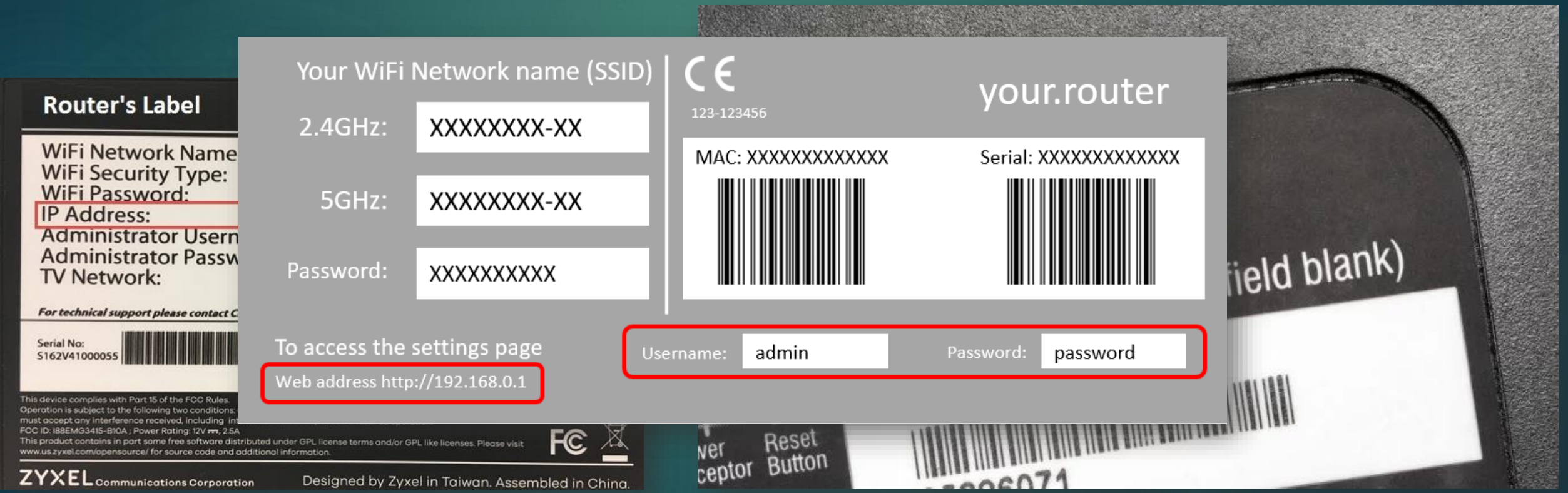


Router model	Successful logins	# Tested
Asus RT	0.00%	307
MikroTik	0.00%	463
Westell 6100G	0.40%	753
ZyXEL VSG1432	0.40%	1001
Huawei HG532e	1.00%	546
TP-Link N300	2.80%	1000
Linksys E2500	2.90%	1000
Thomson SpeedTouch 585i	4.40%	998
Netis WF2419 RTK	13.50%	1000
ZTE ZXV10	15.60%	859
XFinity	17.50%	1000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

Darbs attālināti

Izveidojiet drošu un atjauninātu tīkla savienojumu

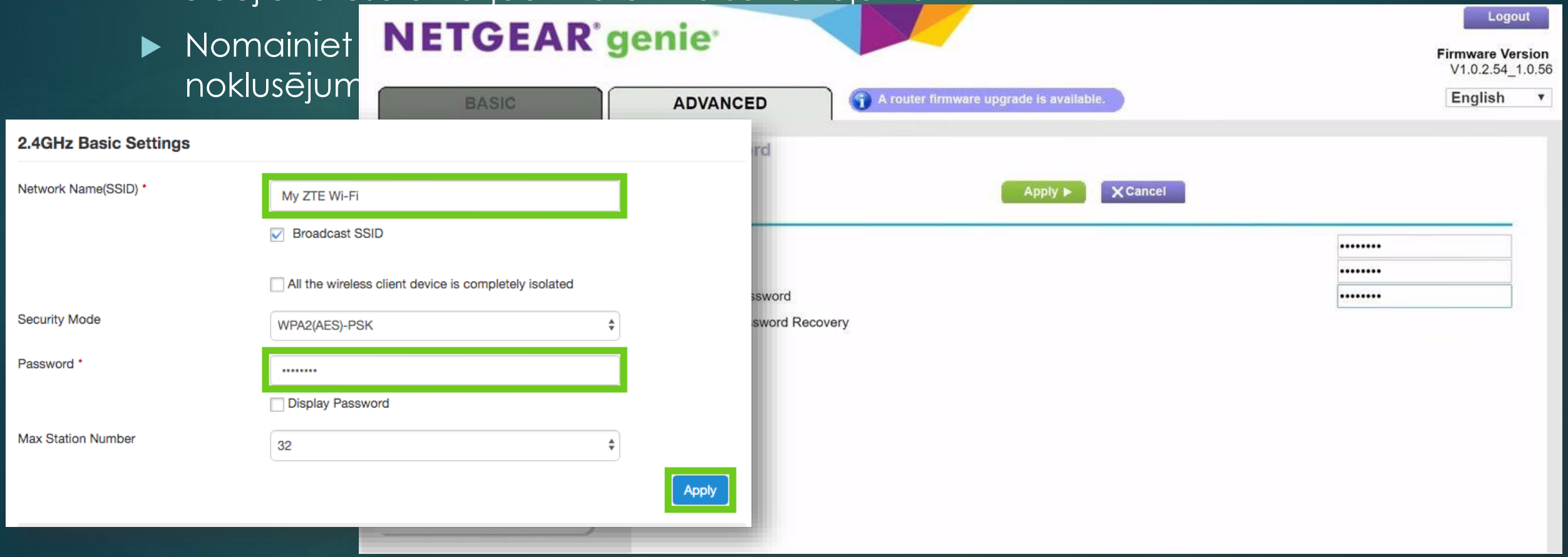
- Kā atjaunināt mājas rūtera programmatūru un nomainīt paroles



Darbs attālināti

Izveidojiet drošu un atjauninātu tīkla savienojumu

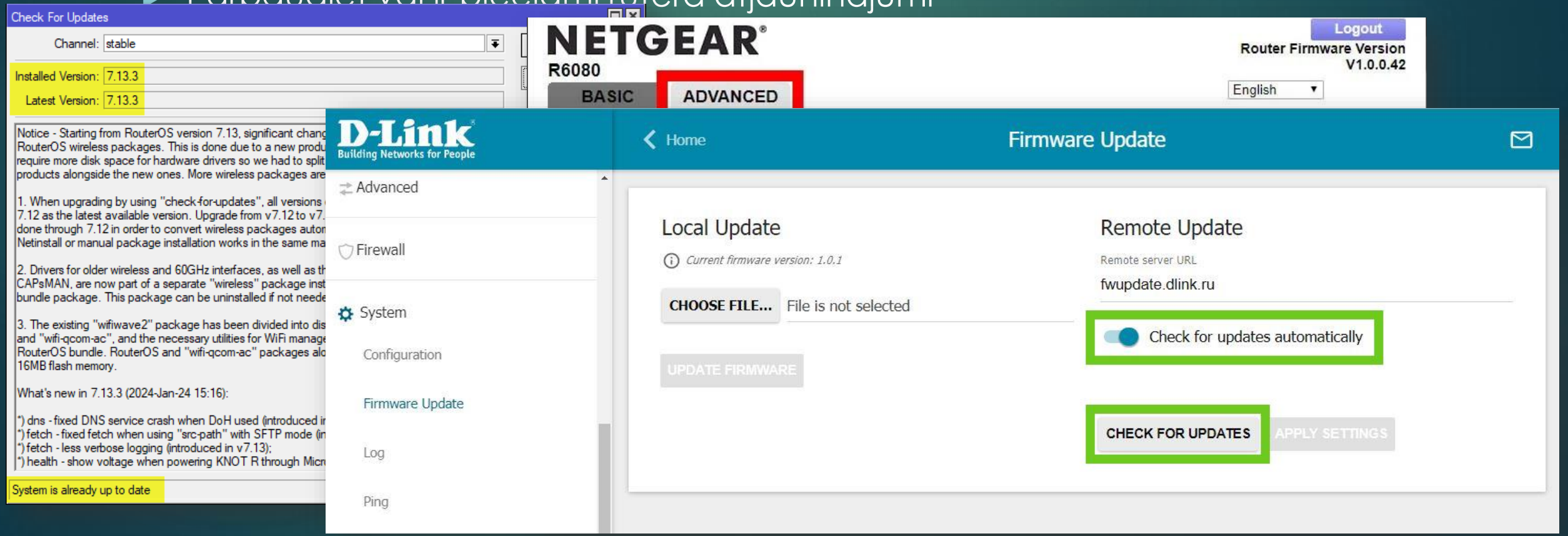
- Nomainiet
  noklusējum



Darbs attālināti

Izveidojiet drošu un atjauninātu tīkla savienojumu

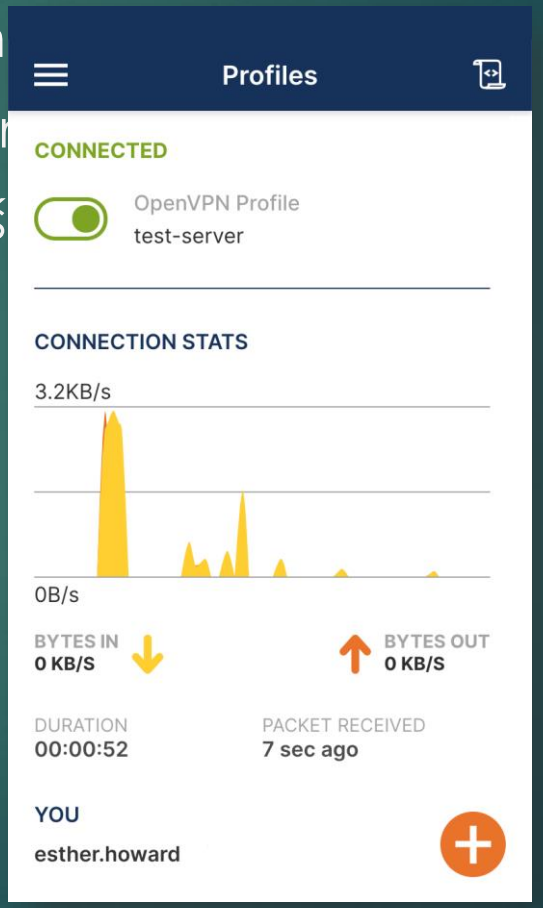
- Pārbaudiet vai ir pieejami rūtera atjauninājumi



Darbs attālināti

Izveidojiet (vienojum

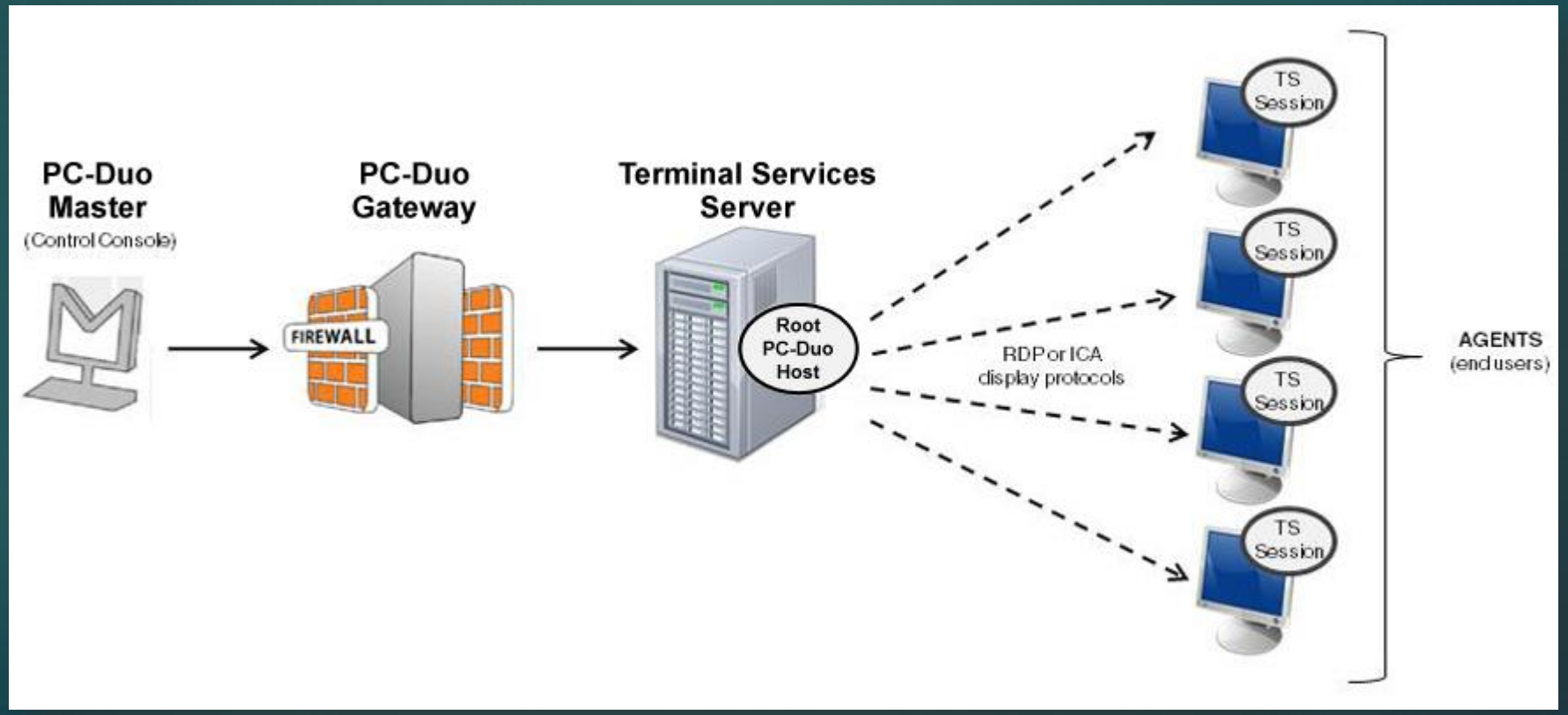
- Pieslēgš a paplašin
- Lietojiet epiecieš



Darbs attālināti

Izveidojiet drošu un atjauninātu tīkla savienojumu

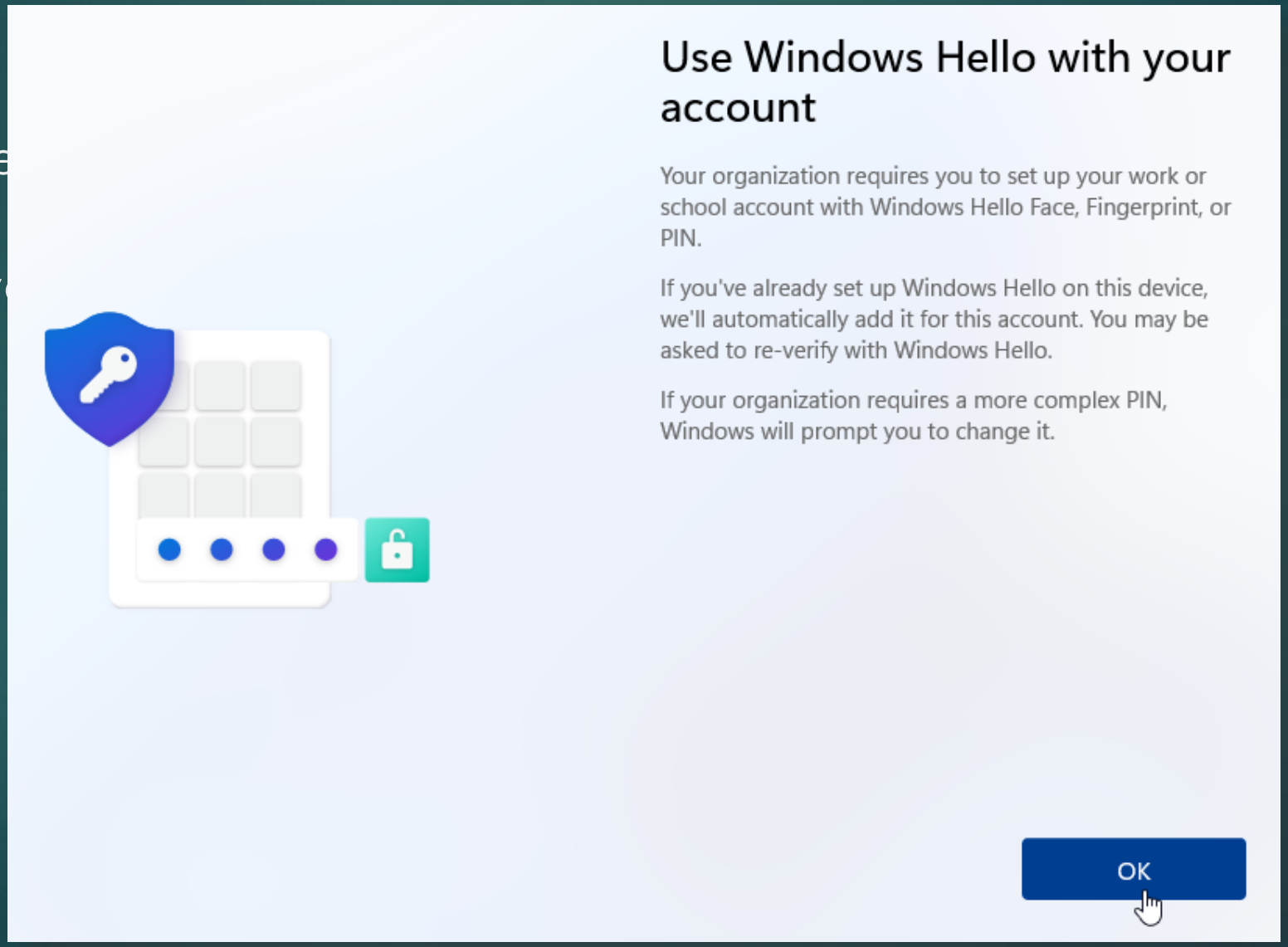
- Starpniekservera izmantošana



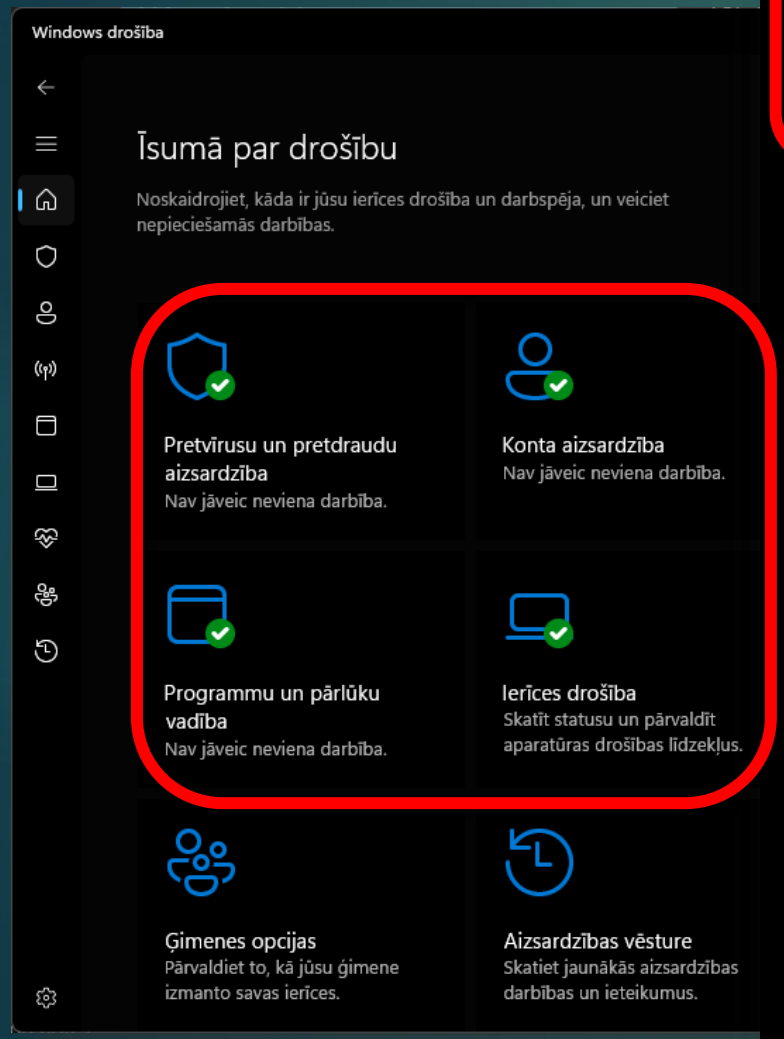
Darbs attālināti

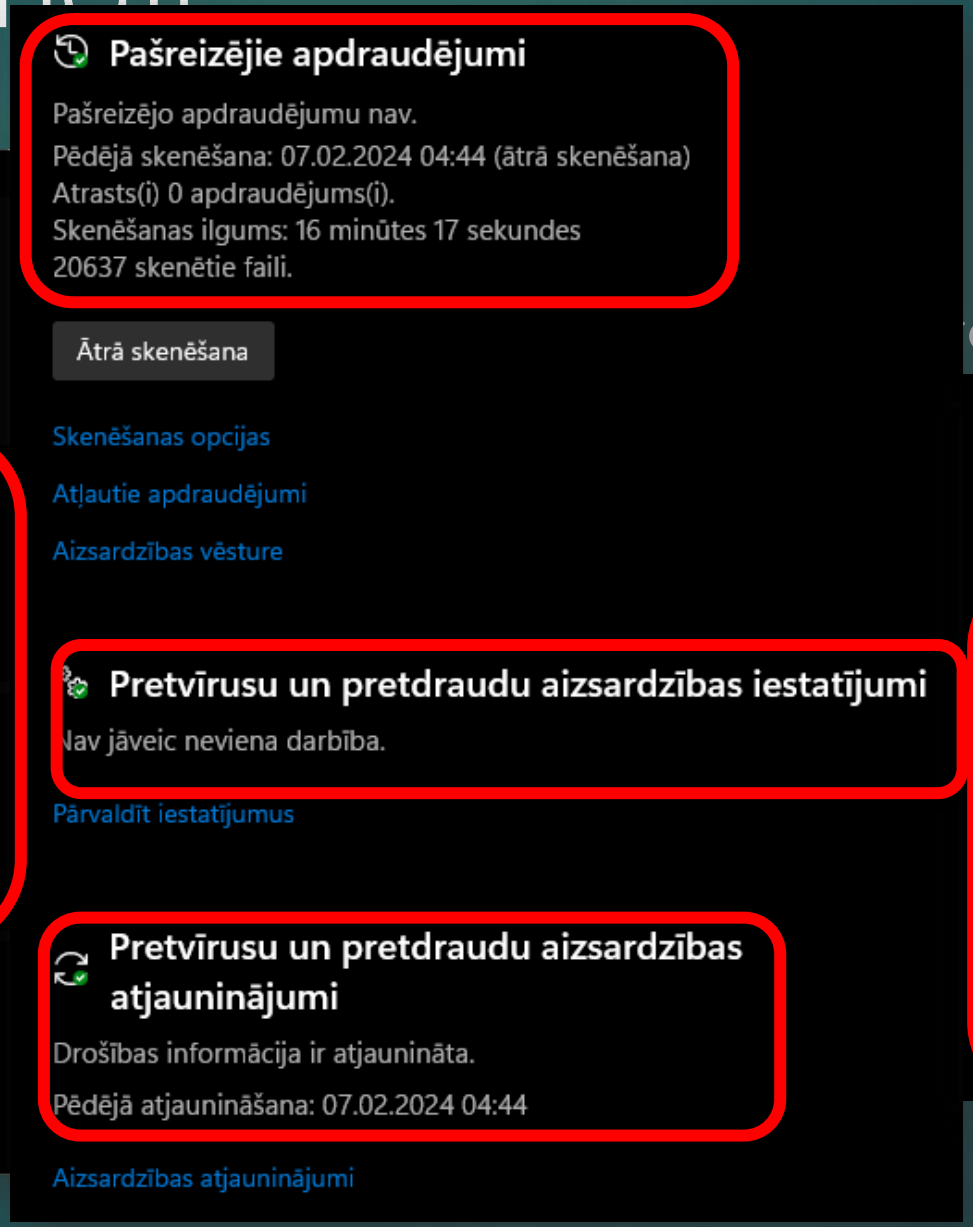
Aizsargājie

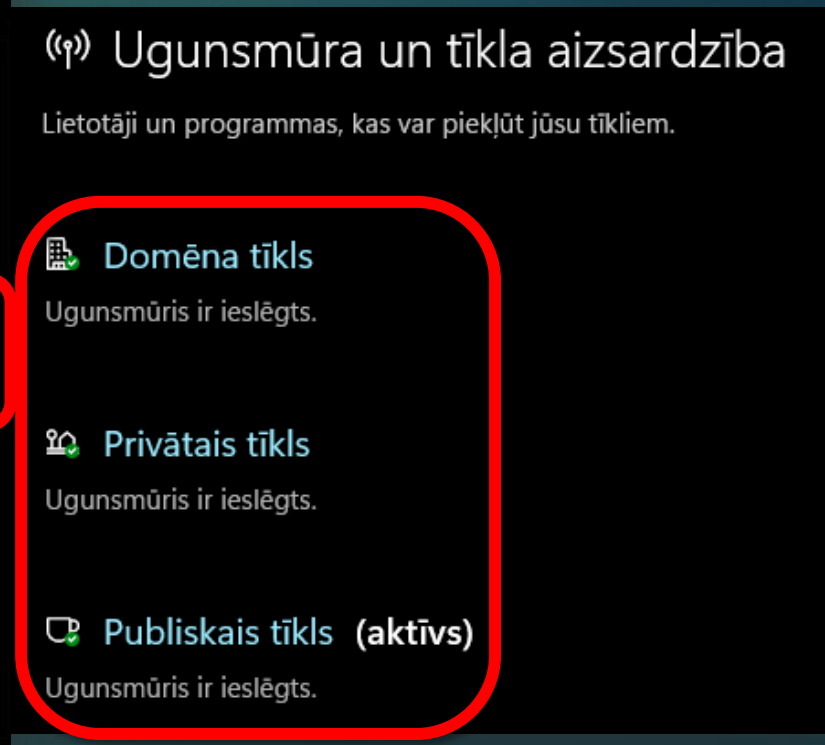
- datora
  piedāv



Darbs attālināti

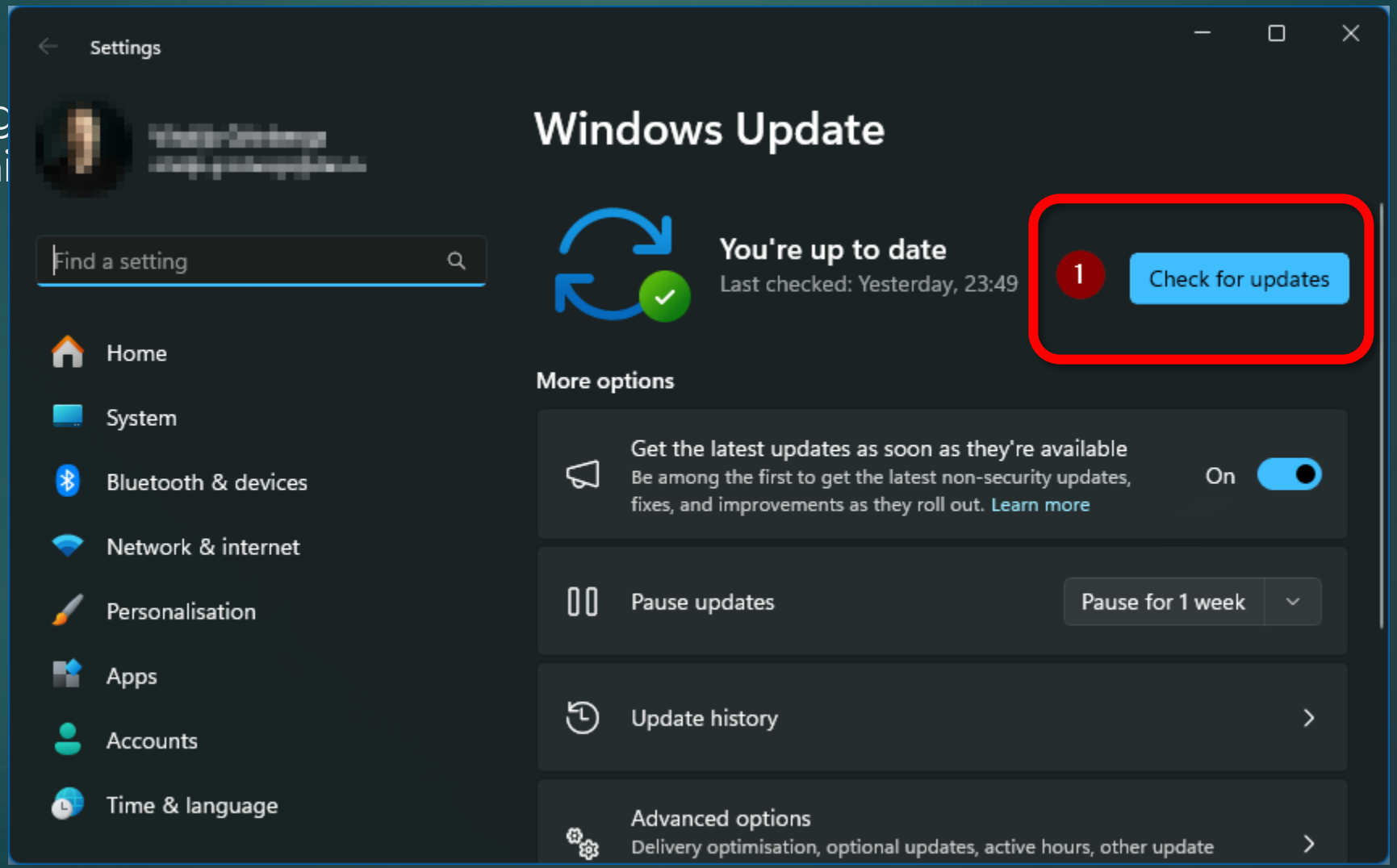






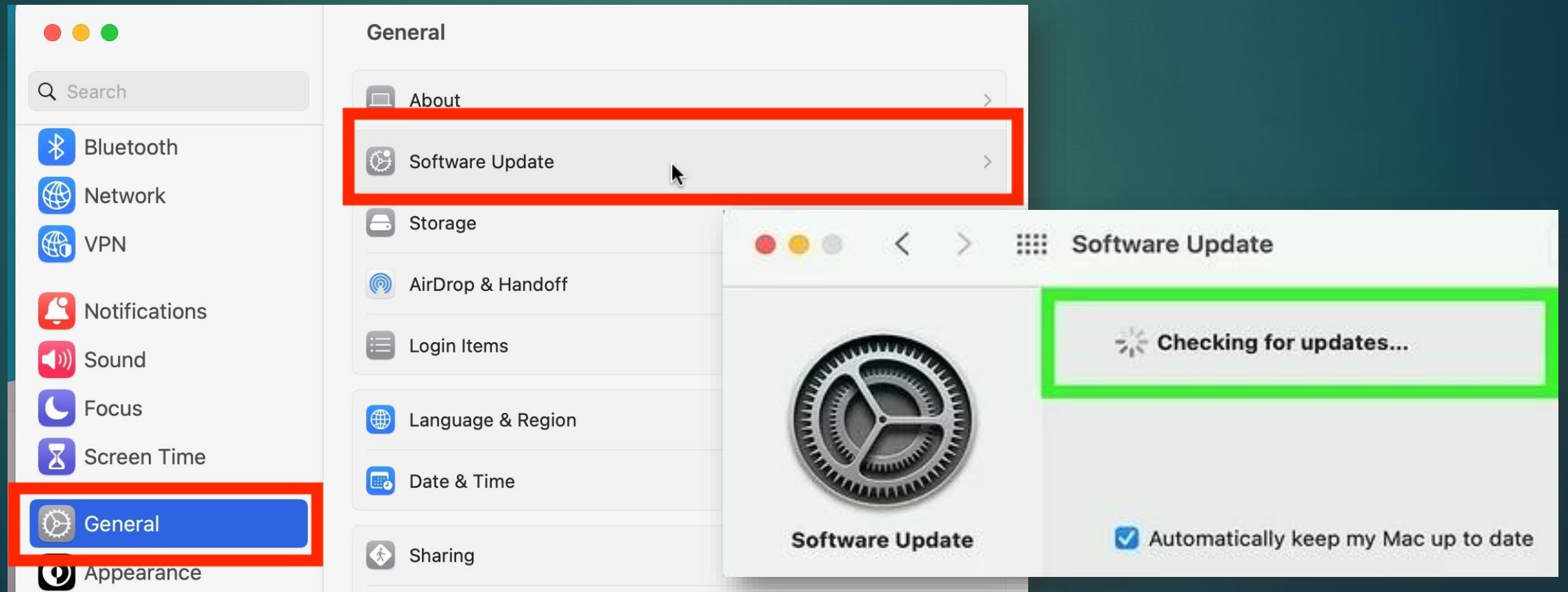
Darbs attālināti

Aizsarg
atjauni



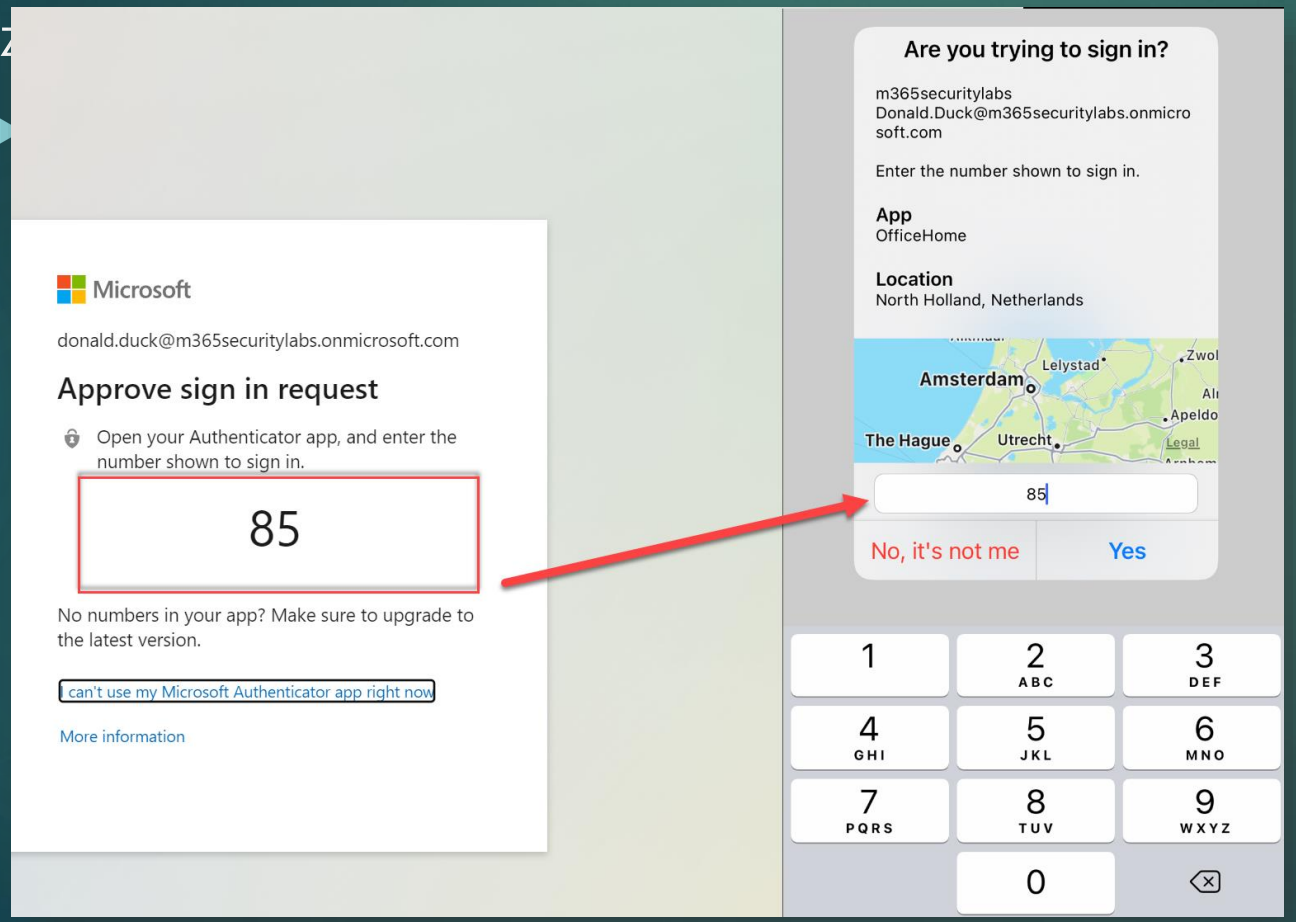
Darbs attālināti

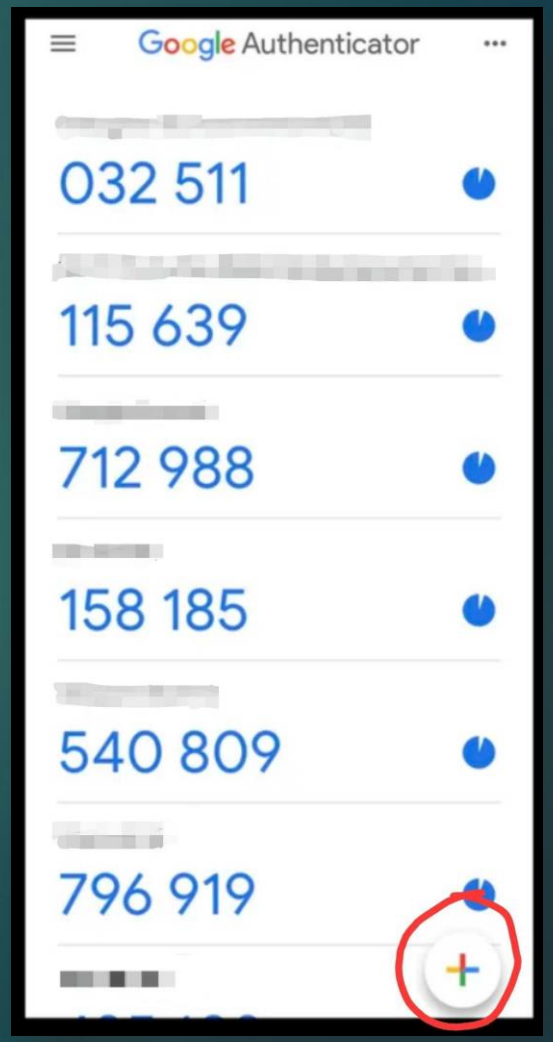
Aizsargājiet sava datora operaetājsistēmu veicot tās pieejamo atjauninājumu pārbaudi MAC OS



Darbs attālināti

Iz

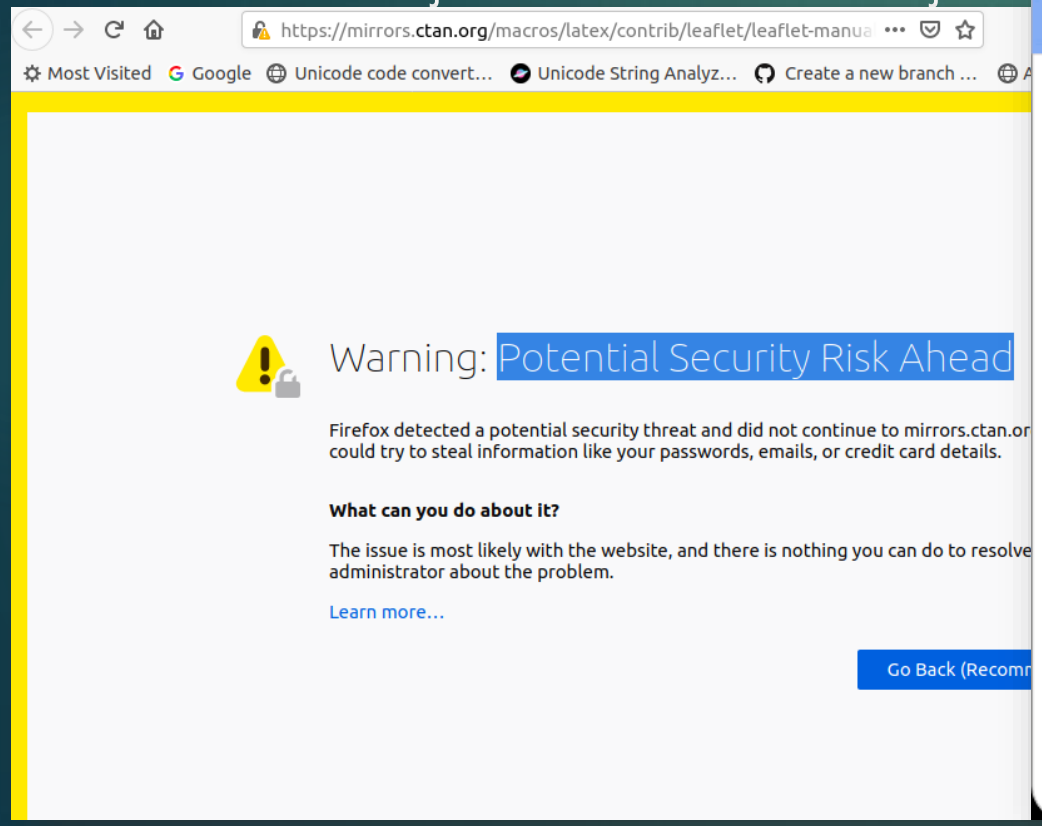


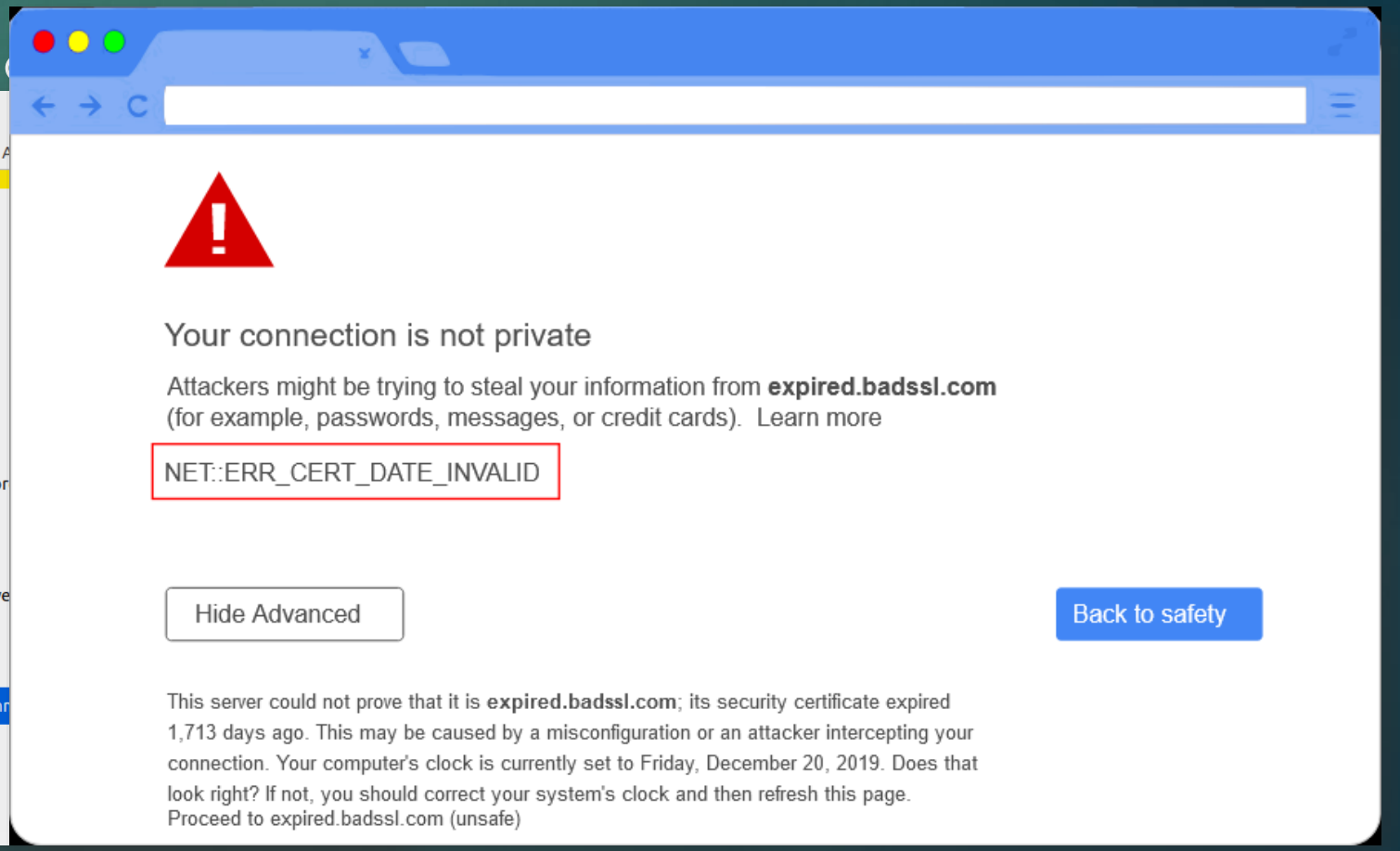


Darbs attālināti

Izmantojiet drošu pieslēgšanos

- Sekojiet drošam savienojum

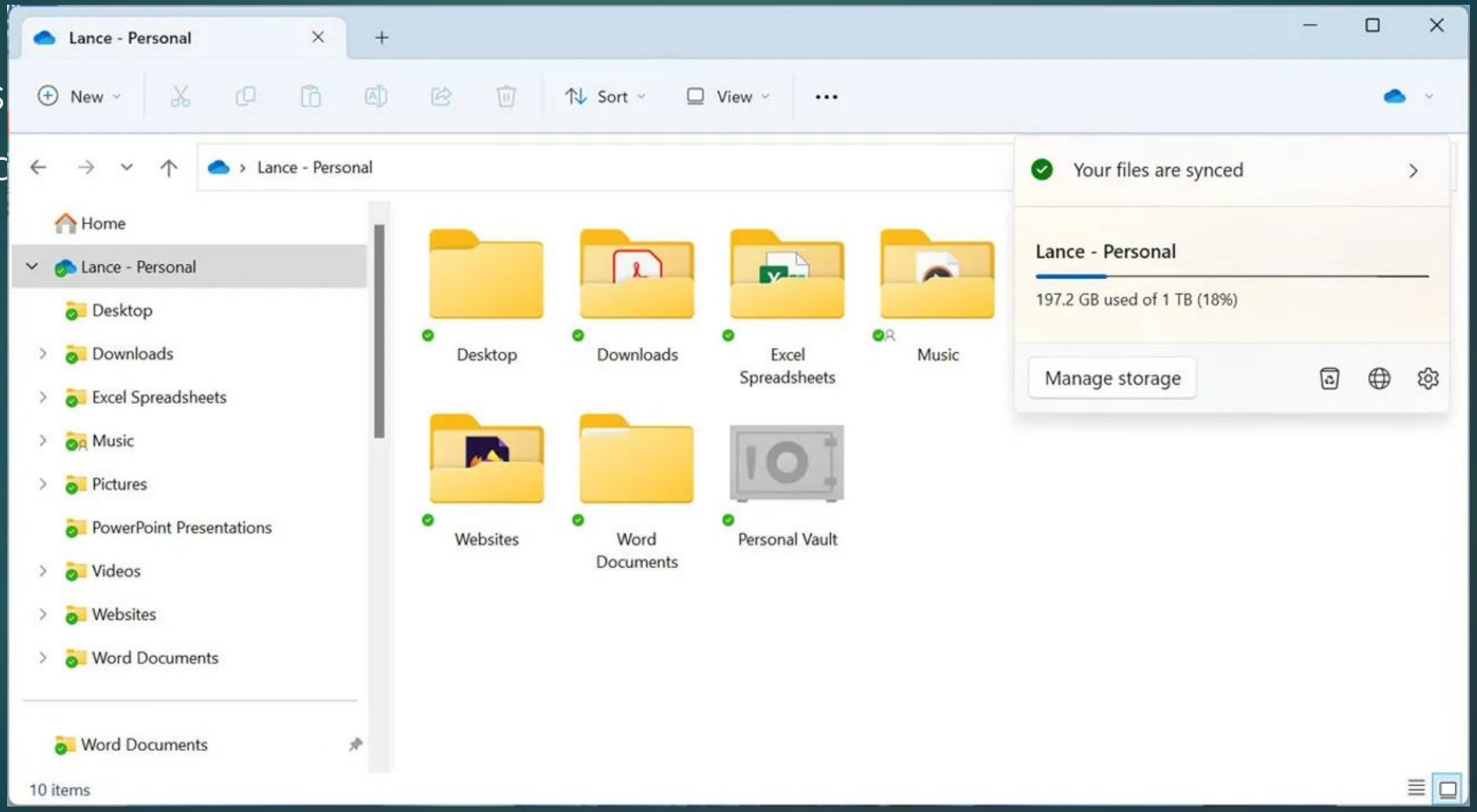




Darbs attālināti

Aizs

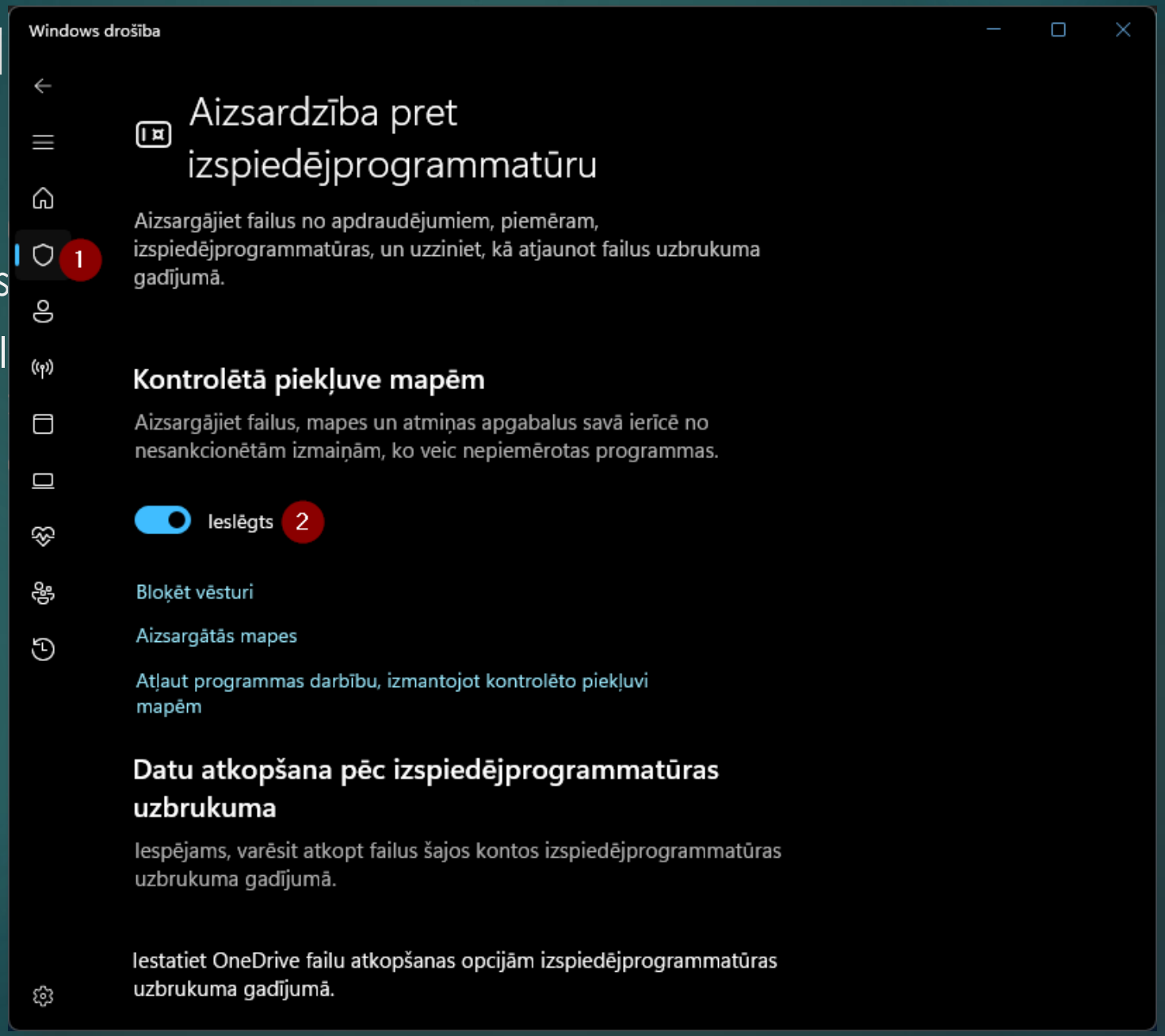
- C



Darbs a

Aizsargājiet s

- darba fail



Darbs attālināti

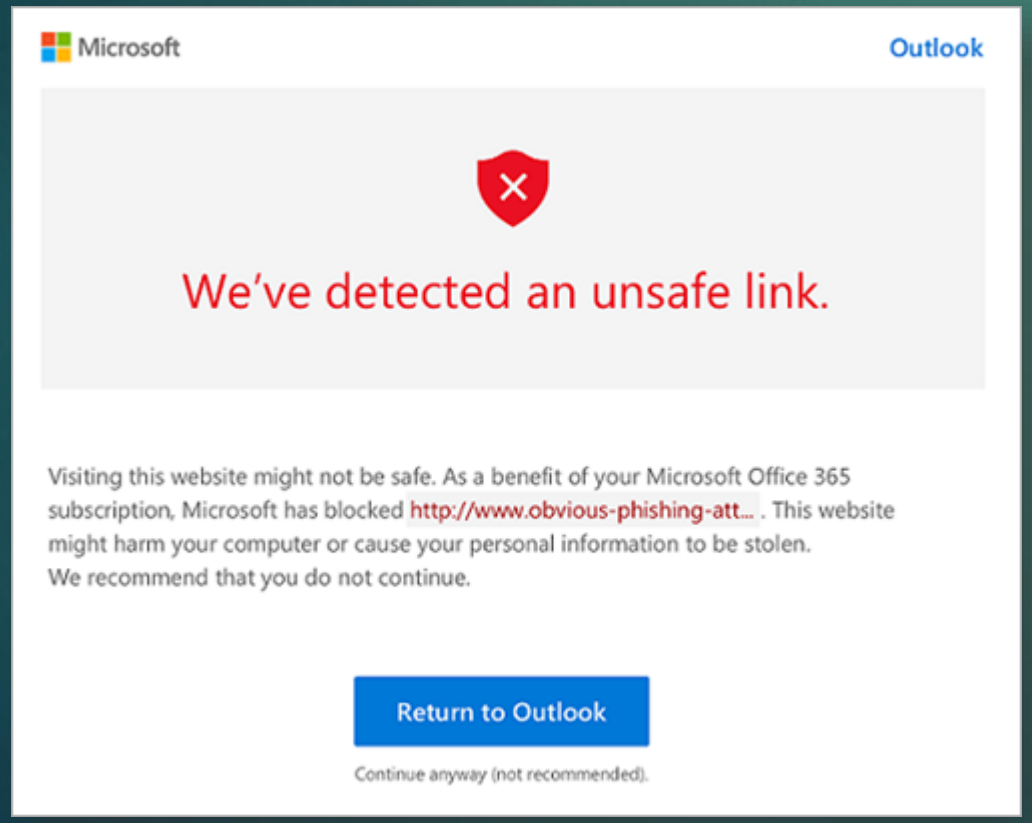
Uzmanieties no pikšķērēšanas uzbrukumiem

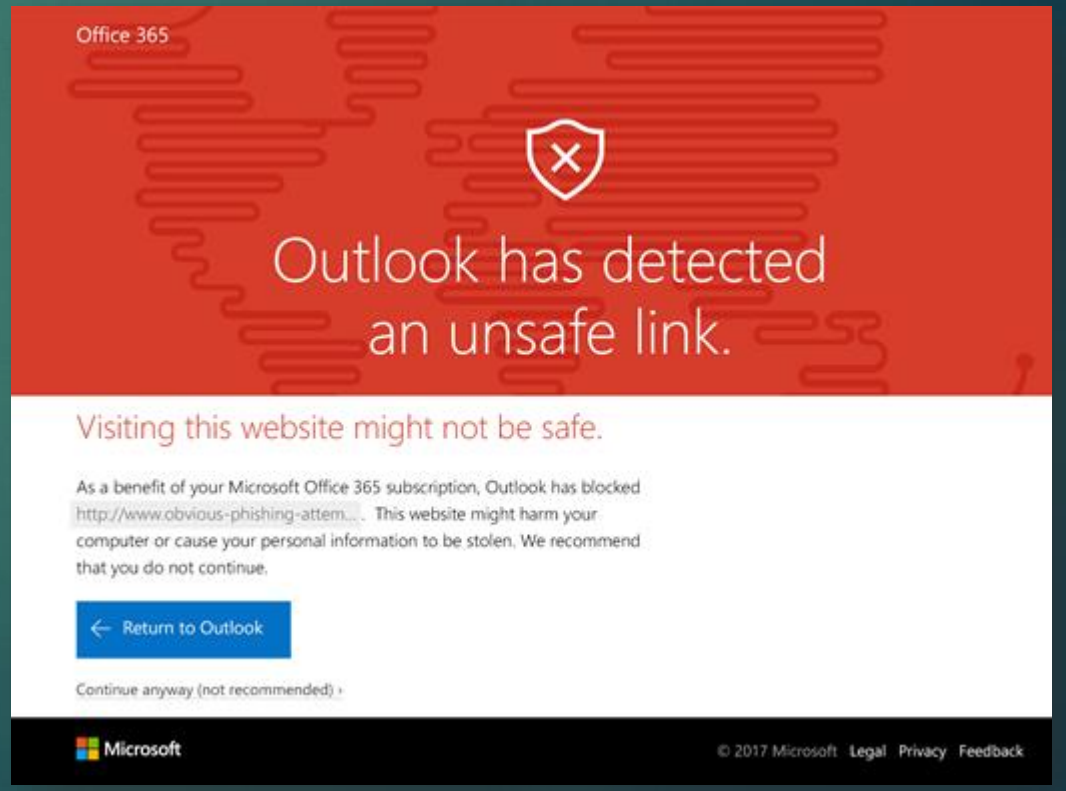
- Pārliecinieties, ka e-pasts ir no uzticama avota, pirms atveriet pielikumus vai sekojiet pievienotām saitēm

Darbs attālināti

Uzmanieties no pikšķērēšanas uzbrukumiem

- Saites no nezināmiem avotiem





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

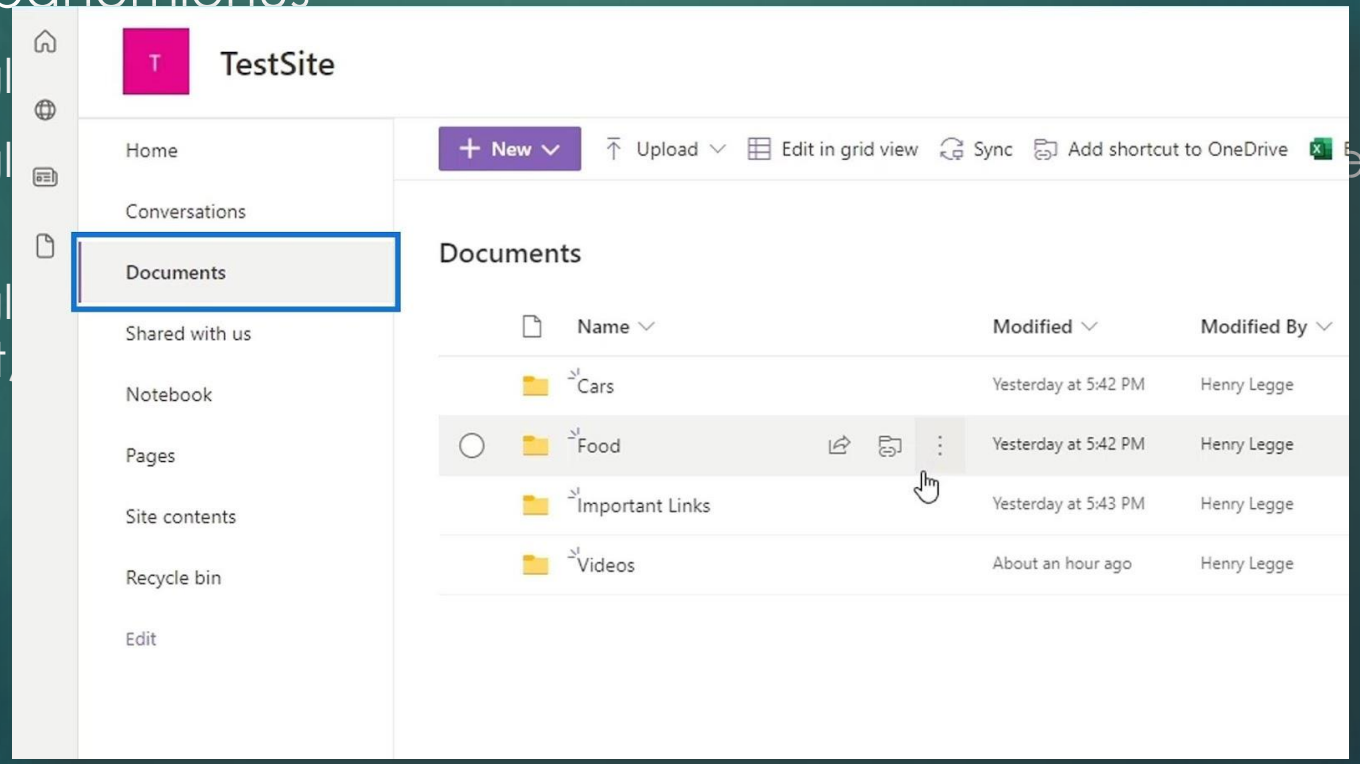
Nodrošiniet savu darba vietu

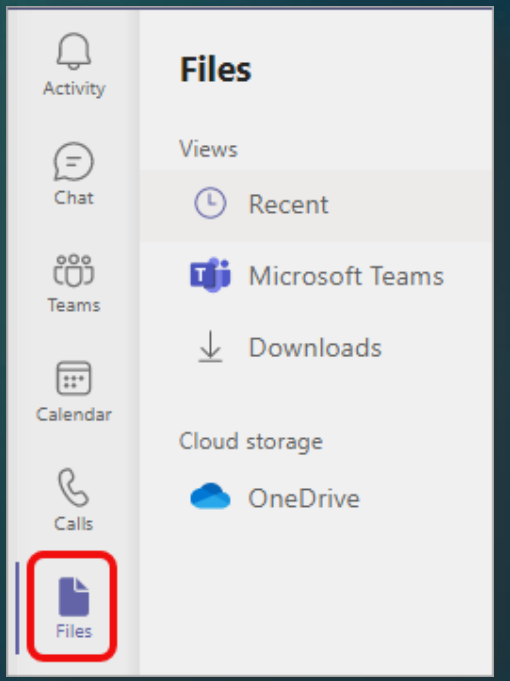
- Pārliecinieties, ka jūsu darba vide ir privāta
- Apmeklētāji nevar piekļūt jūsu darba datoram vai dokumentiem

Darbs attālināti

Regulāri veiciet datu dublēšanu

- Atkarībā no datu klasifikācijas tiem piemēro atbilstošos datu dublēšanas panēmienus
  - Dati, kuri gl
  - Dati, kuri gl kopijām
  - Dati, kuri gl SharePoint,



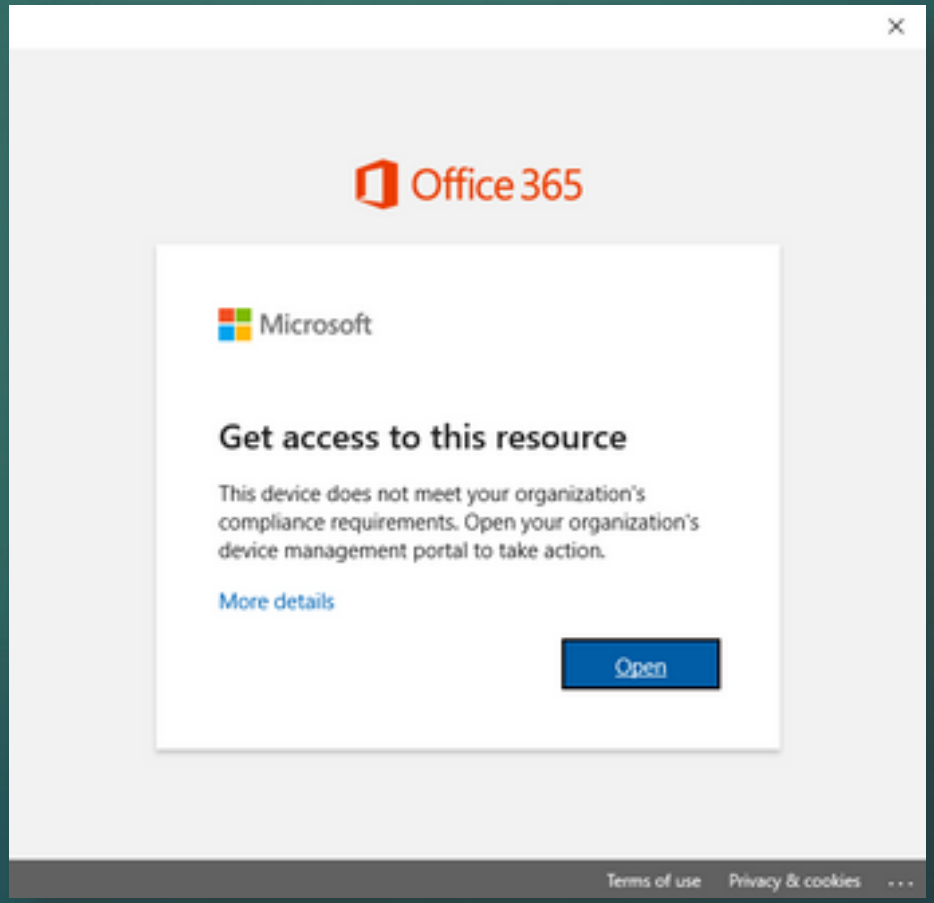


OneDrive for Business

Google Drive

Darbs attālināti

Nesaderīgas ierīces



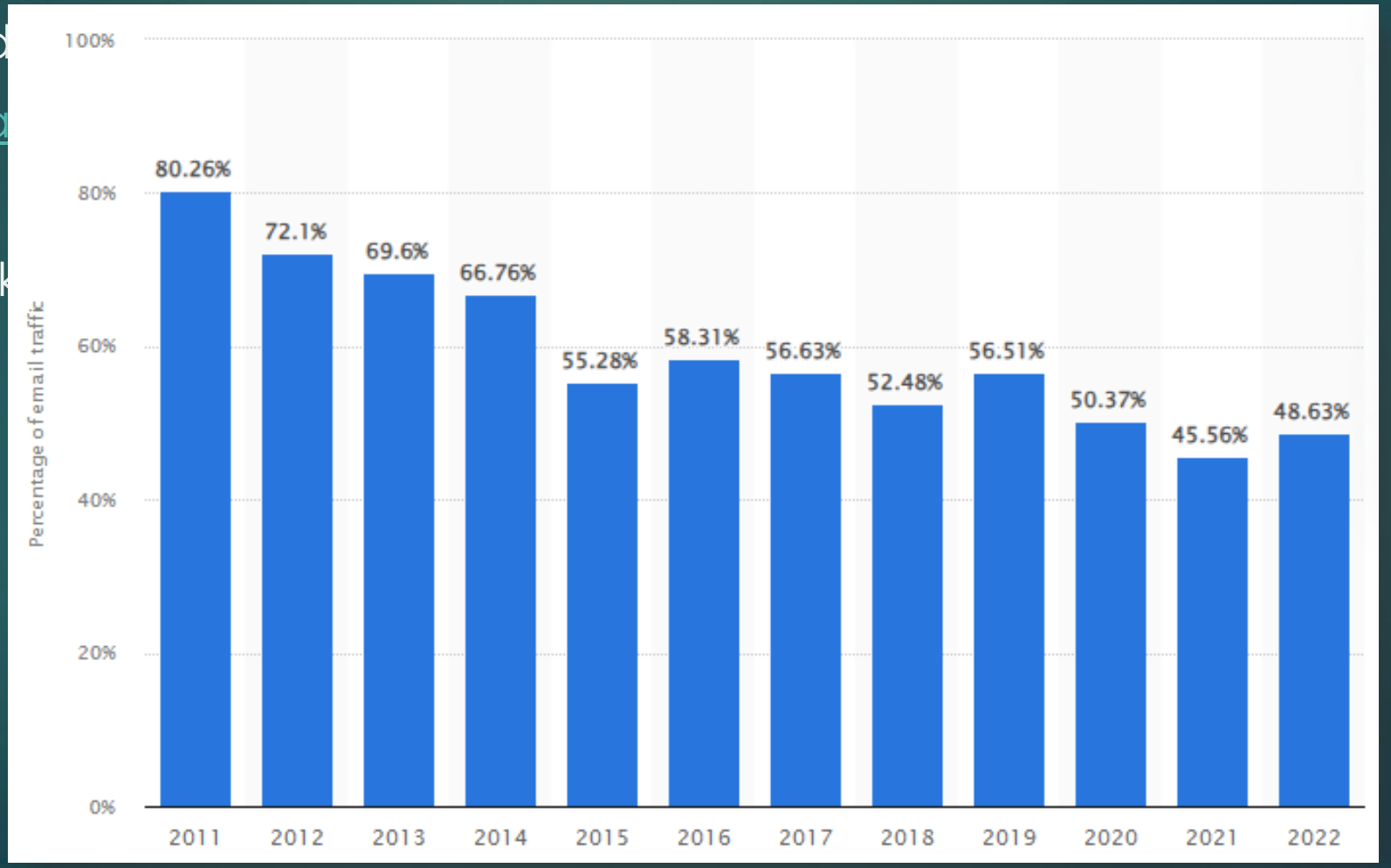
E-pasta drošība

E-pasta drošība

Mēstuļu d

Avots: sta

Kā jums šk



E-pasta drošība

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

Draudu mērķi:

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

E-pasta drošība

Microsoft Security

Microsoft Defender for Office 365

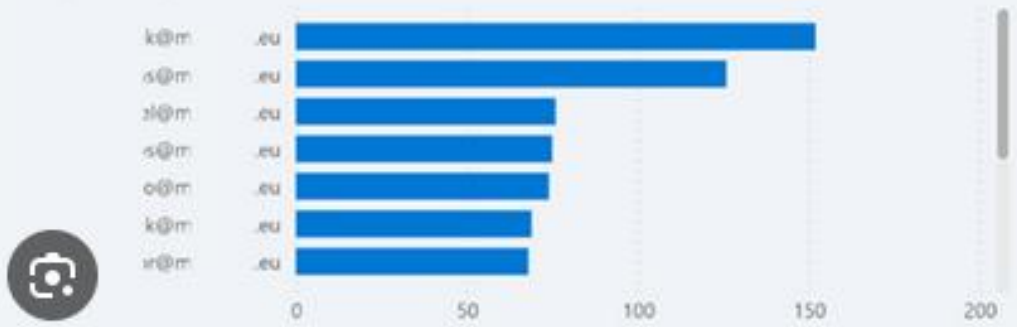
Detection Overview

10/09/2022 10/10/2022

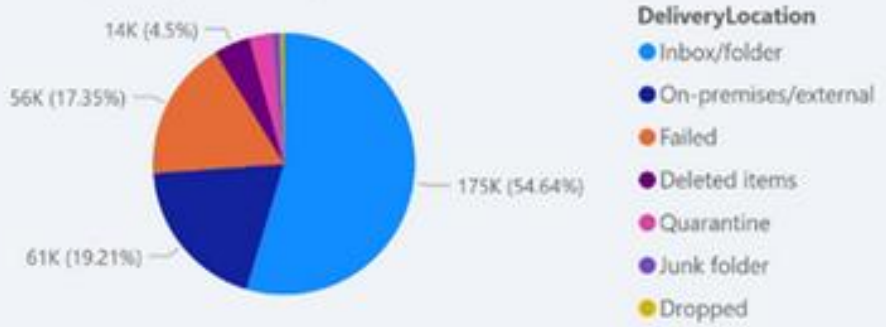
Back to ReadMe

Total Emails (Inbound)	Total Emails (Intra-Org)	Total Emails (Outbound)	Total Emails detected as Malicious
102K	99K	117K	16K
Total Emails Reported by Users	**Total Emails with Malware Threats**	**Total Emails with Phish Threats**	**Total Emails with Spam Threats**
223	1426	8160	14K
Total Emails removed by ZAP	**Total Emails Removed by Manual Remediation**	**Total Emails removed after Detonation Analyis**	**Malicious Emails Allowed due to Admin Configuration**
16	5799	127	363

Top 15 Targeted Users (Malware + Phish)

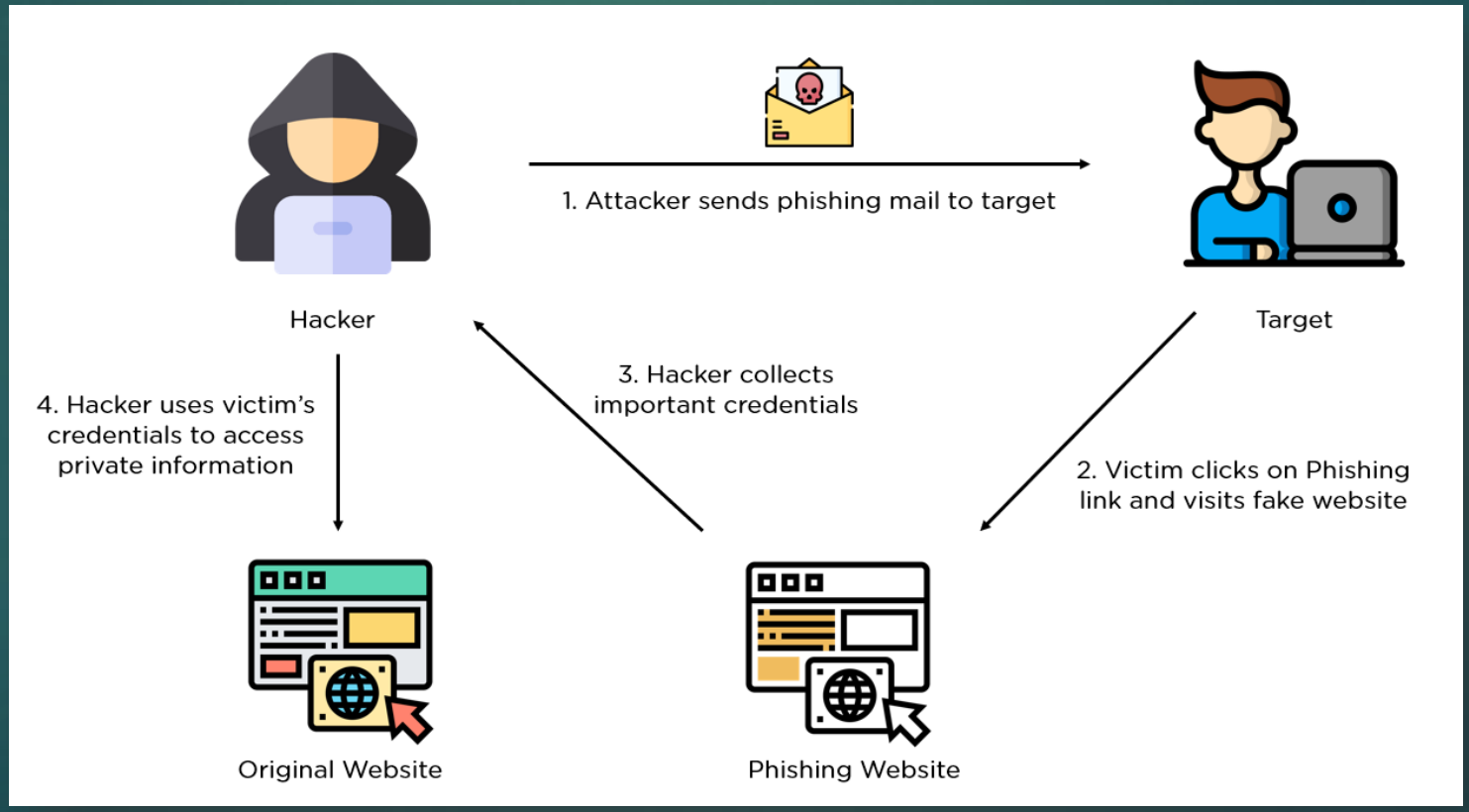


Total Emails by Original Delivery Location



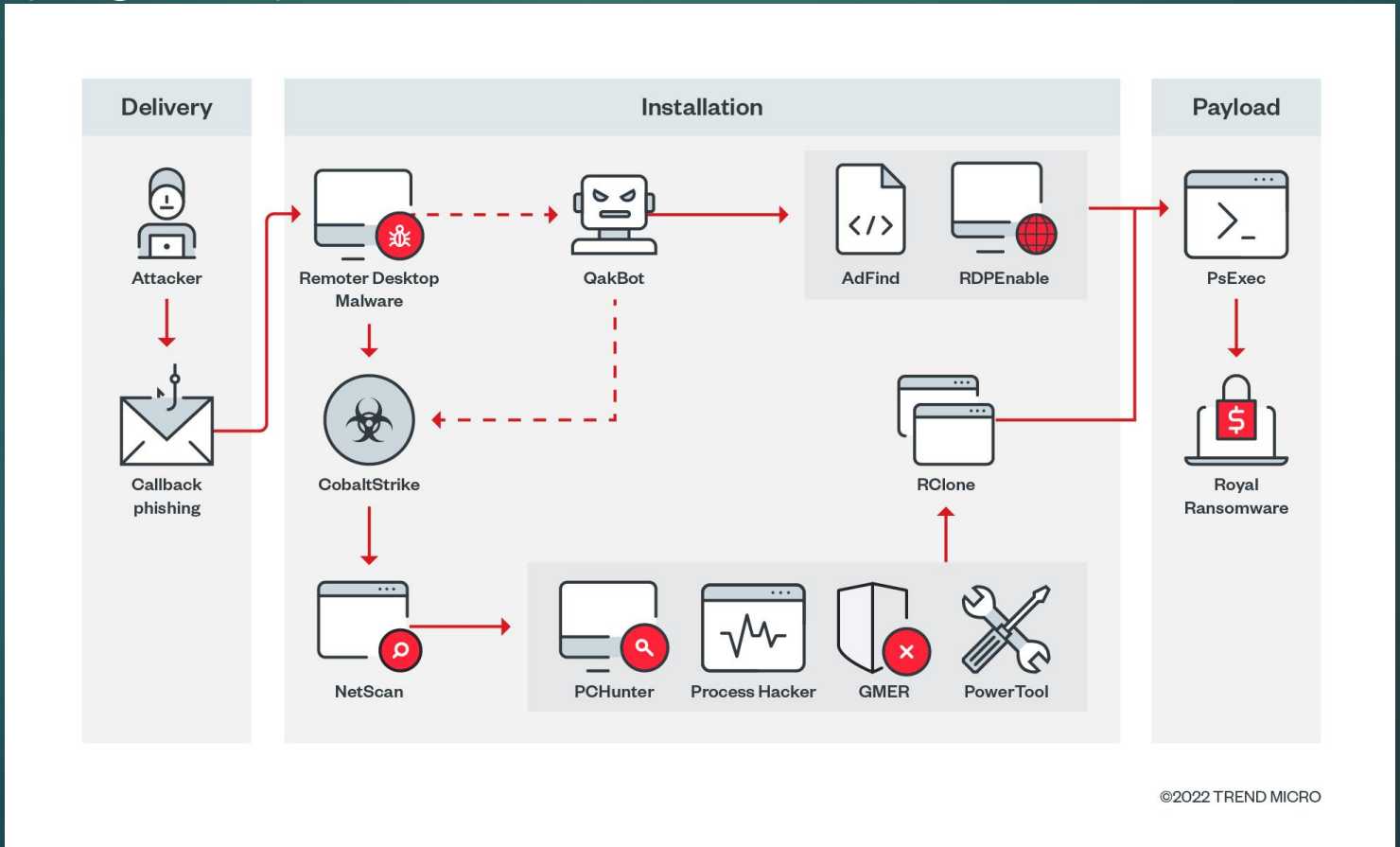
E-pasta drošība

Pikšķerēšanas piemērs



E-pasta drošība

Ļaunatūras piegādes piemērs



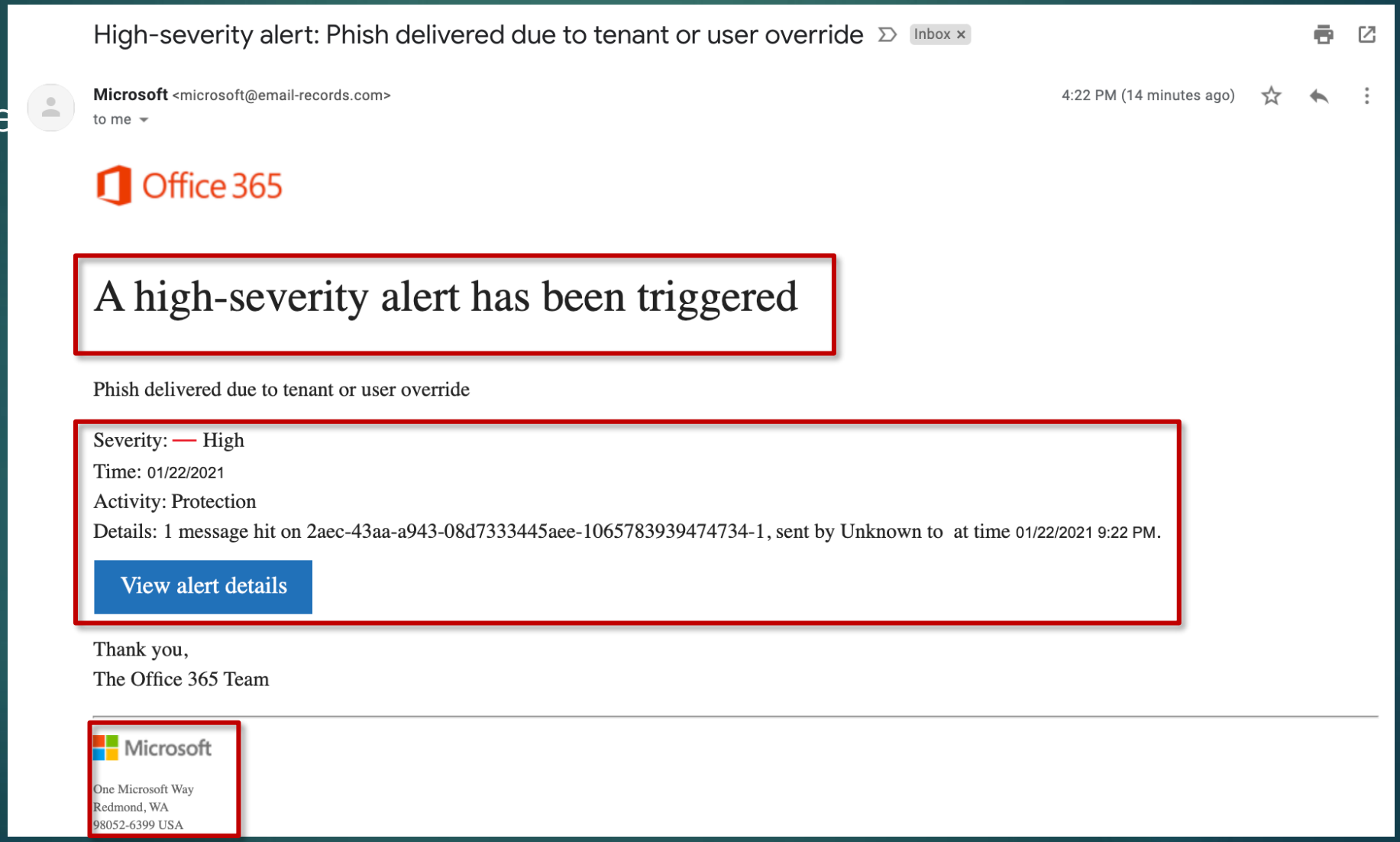
E-pasta drošība

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

pikšķe



High-severity alert: Phish delivered due to tenant or user override Inbox ×

Microsoft <microsoft@email-records.com>
to me

4:22 PM (14 minutes ago)

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.

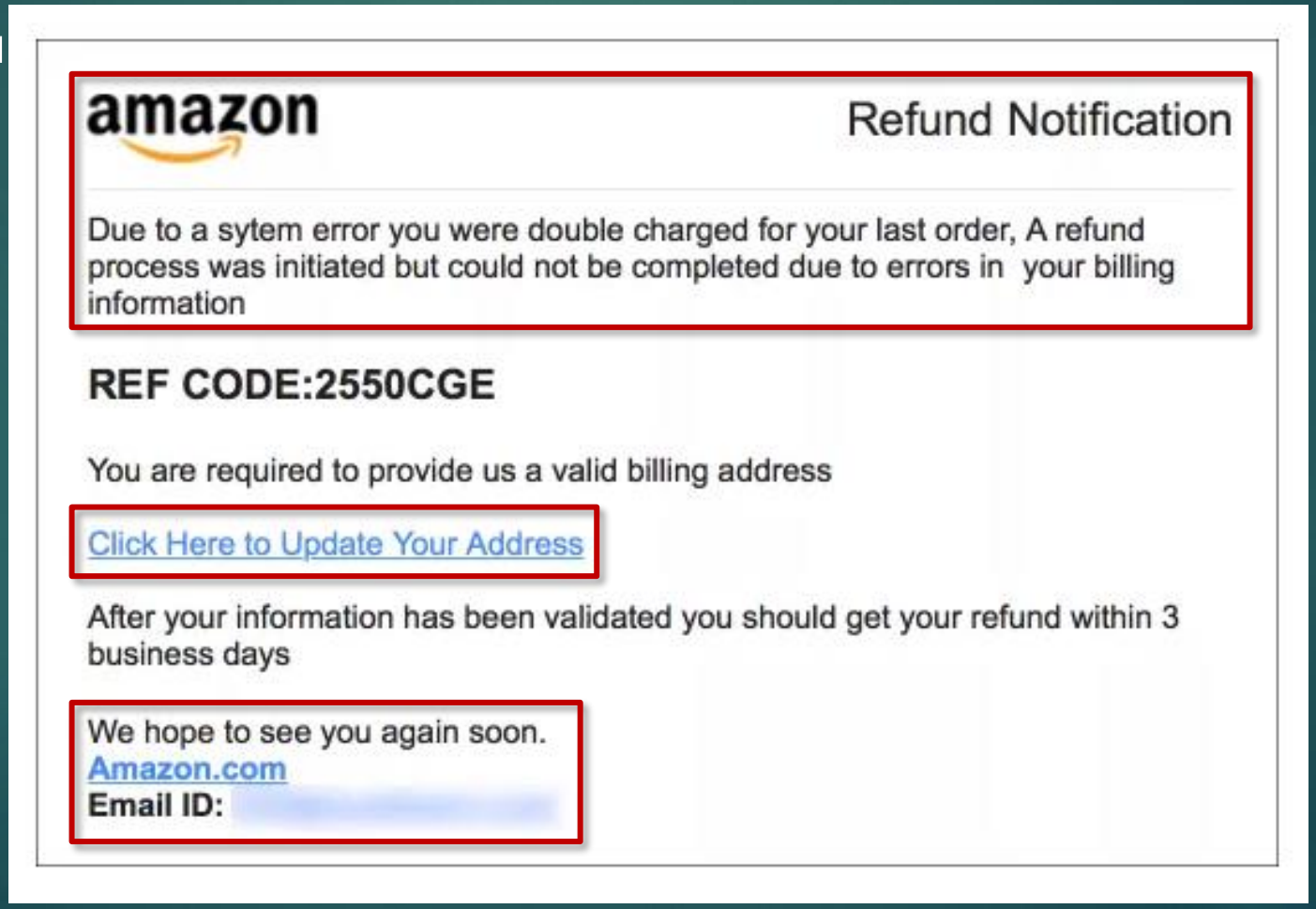
View alert details

Thank you,
The Office 365 Team

Microsoft
One Microsoft Way
Redmond, WA
98052-6399 USA

E-pasta drošība

pikšķerēšana



amazon

Refund Notification

Due to a sytem 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

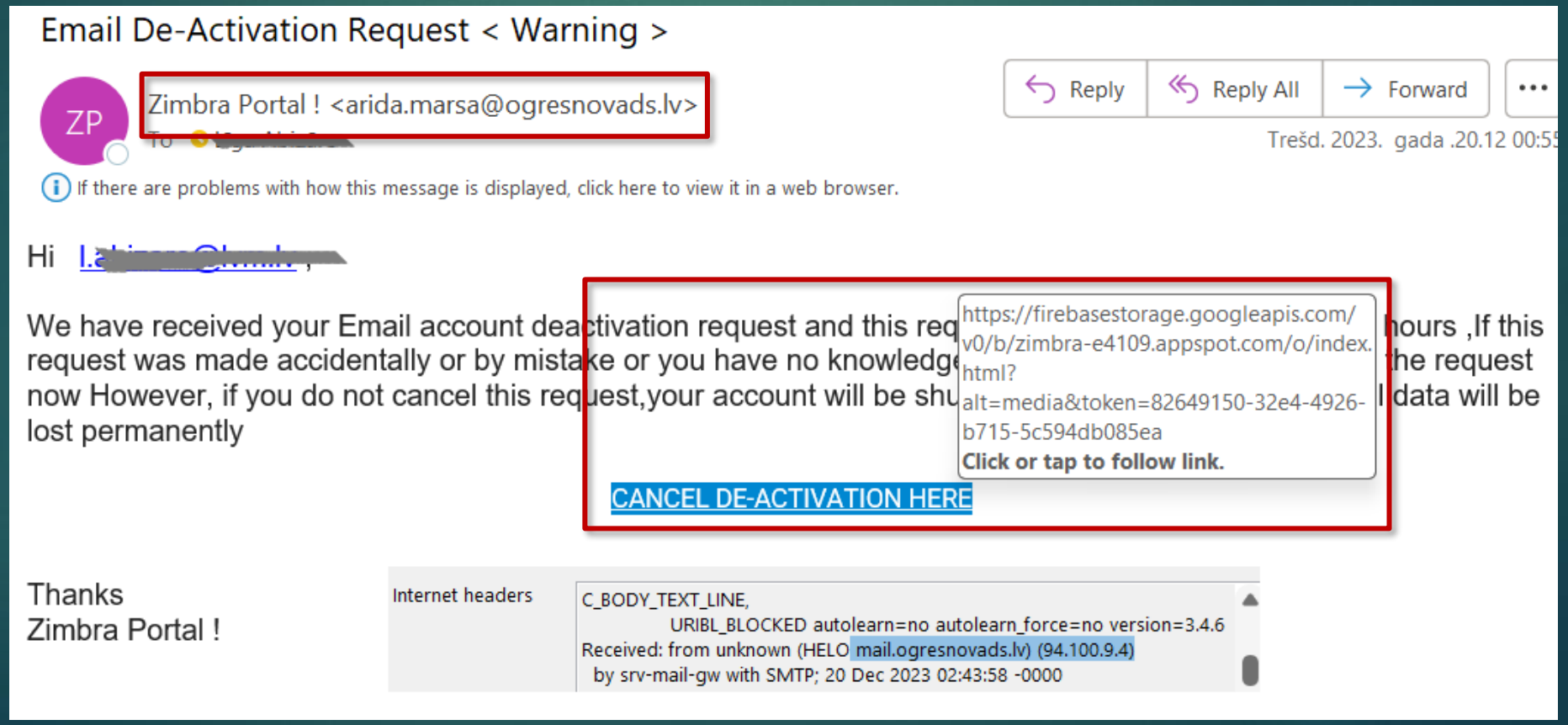
Click Here to Update Your Address

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

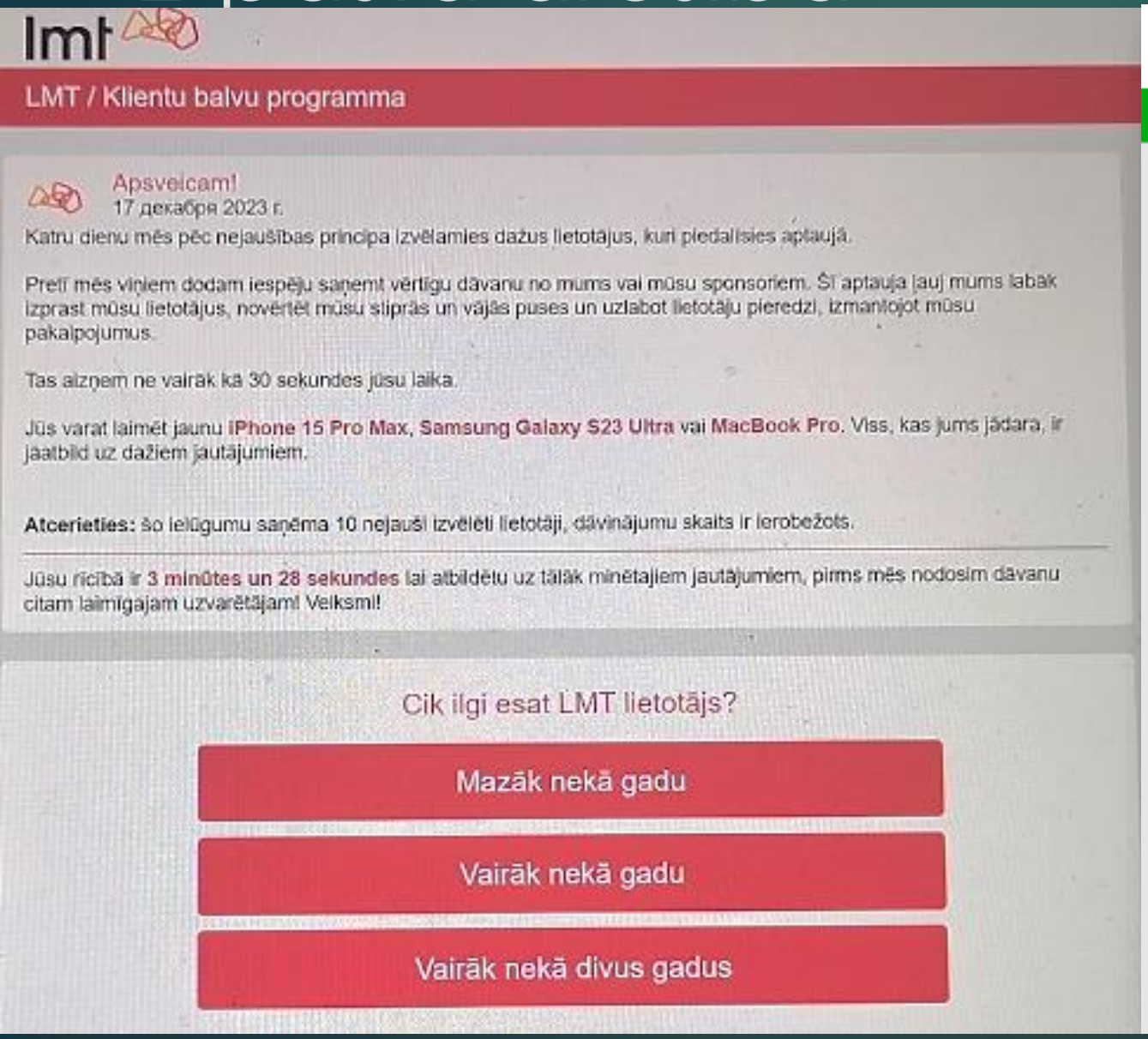
We hope to see you again soon.
Amazon.com
Email ID:

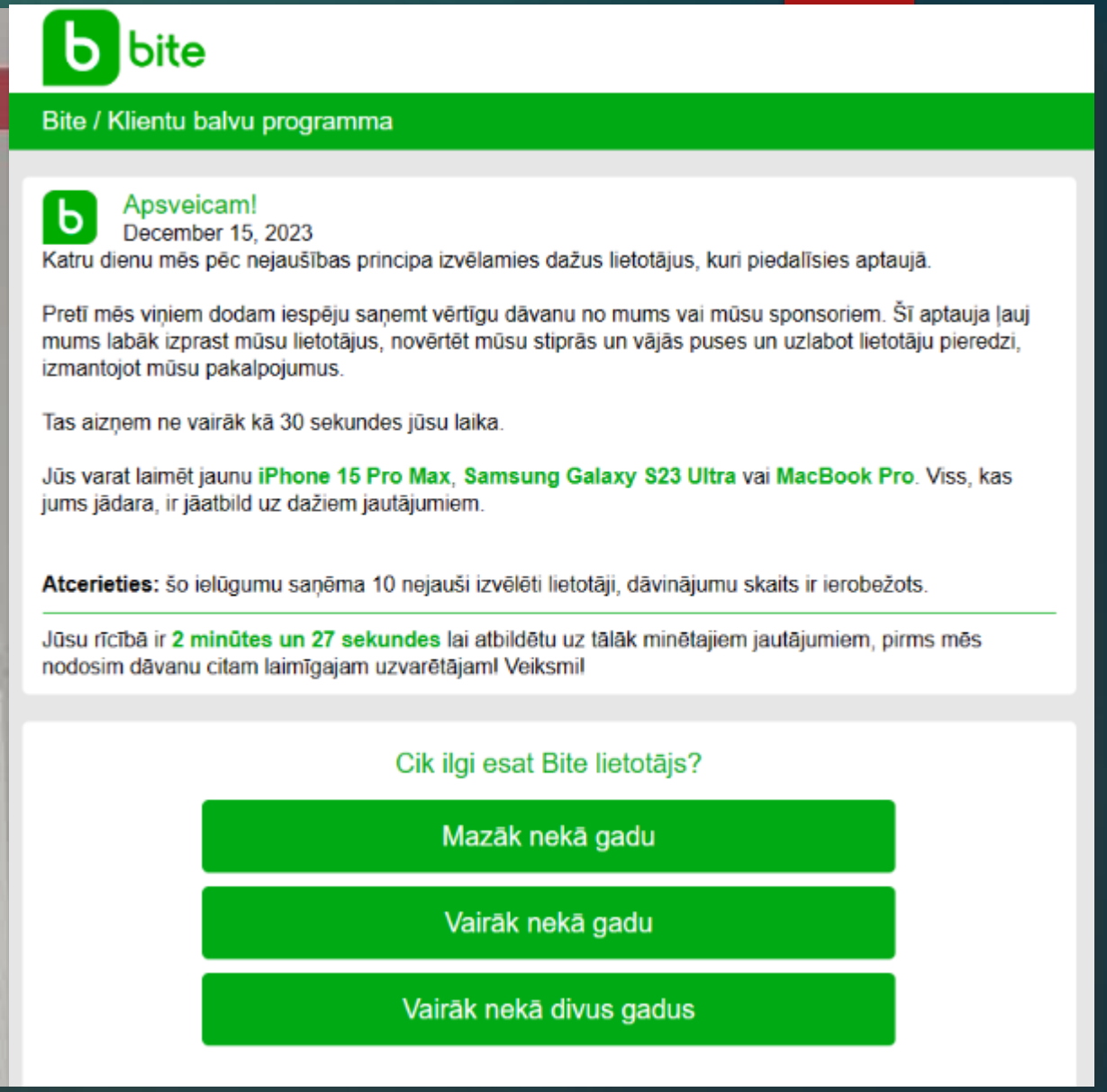
E-pasta drošība

pikšķerēšana



E-pasta drošība





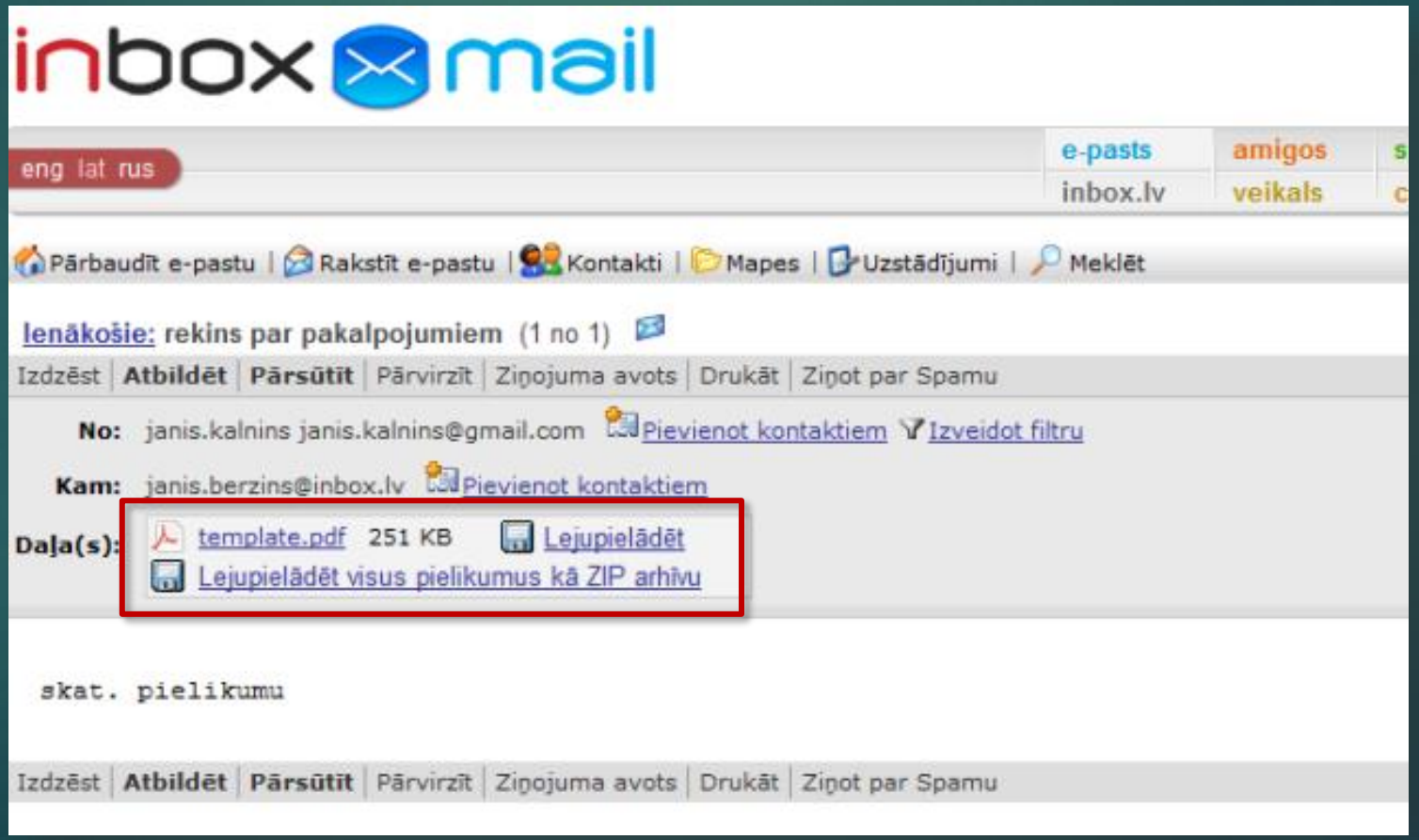
Darbs attālināti

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

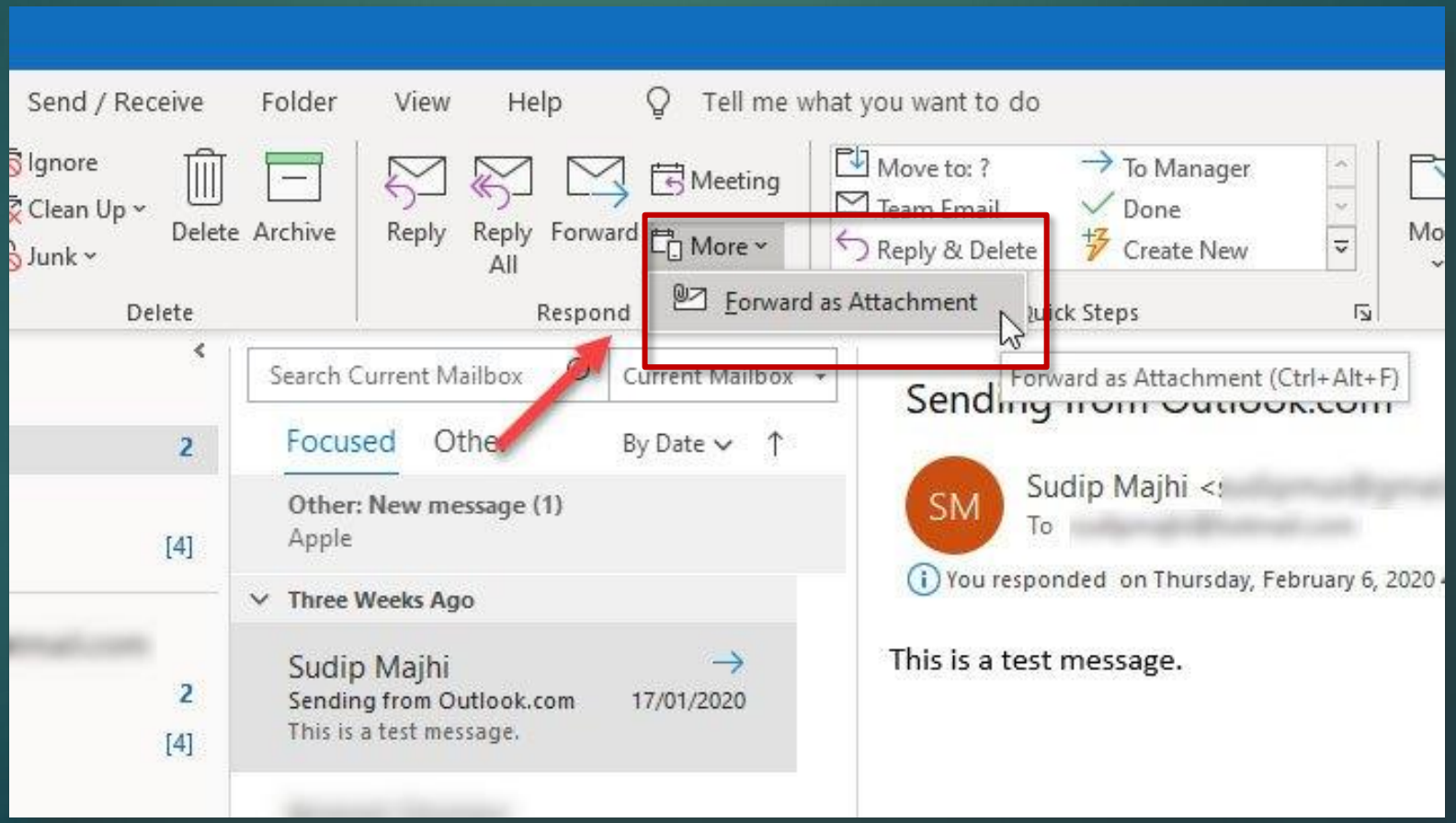
E-pasta drošība

Ļaunatūras piemēri



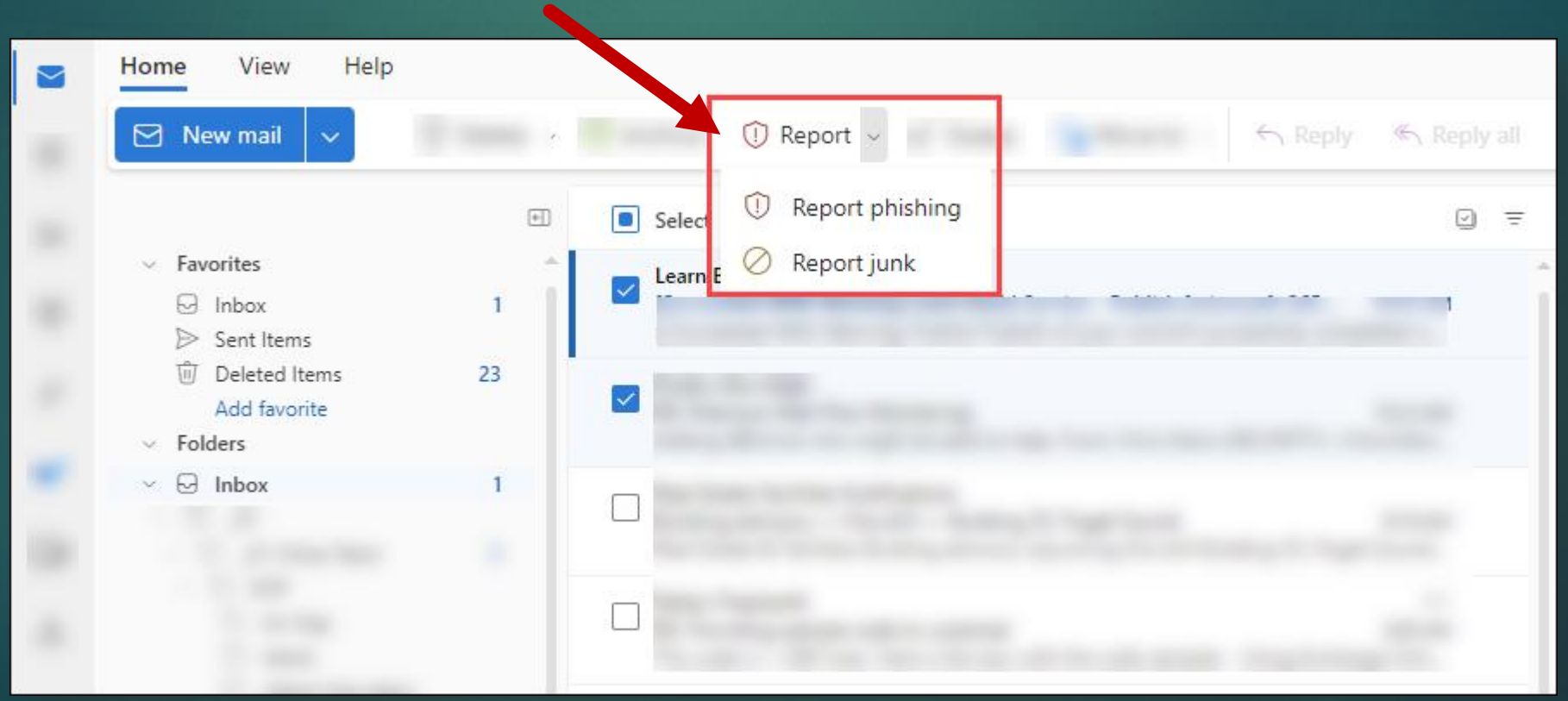
E-pasta drošība

Ko darīt ja saņemts «slikts» e-pasts:



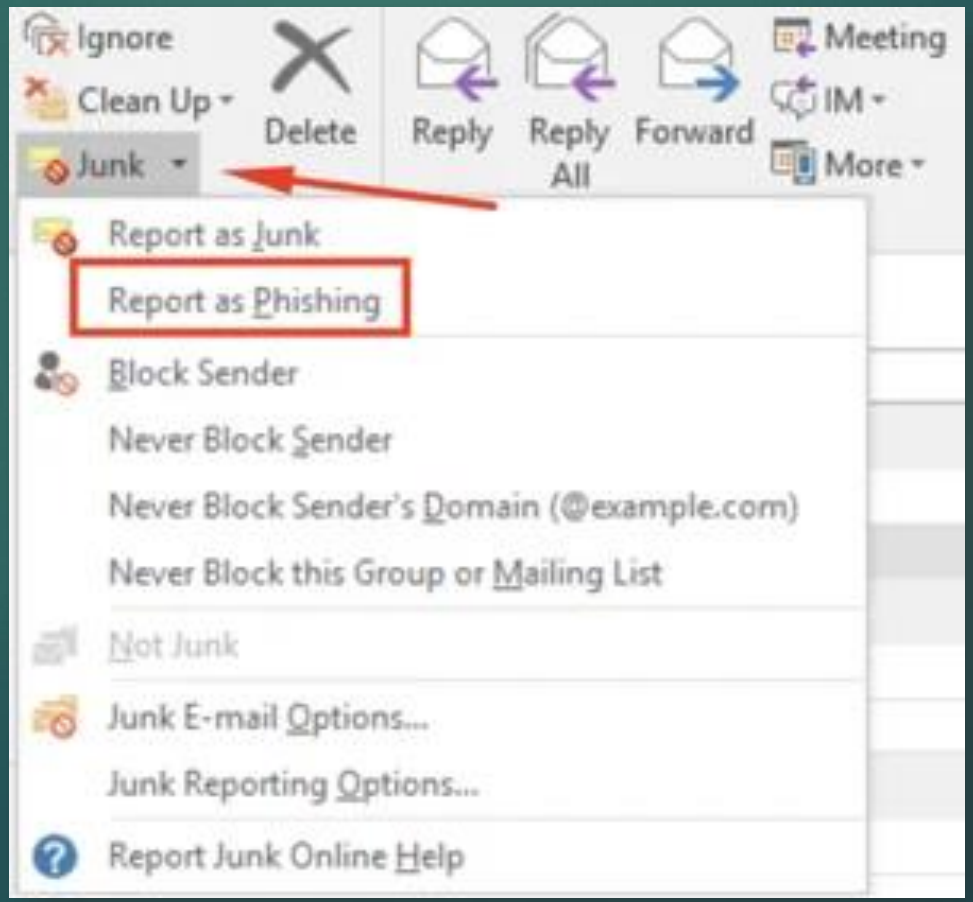
E-pasta drošība

Ko darīt ja saņemts «slikts» e-pasts:



E-pasta drošība

Ko darīt ja saņemts «slikts» e-pasts:

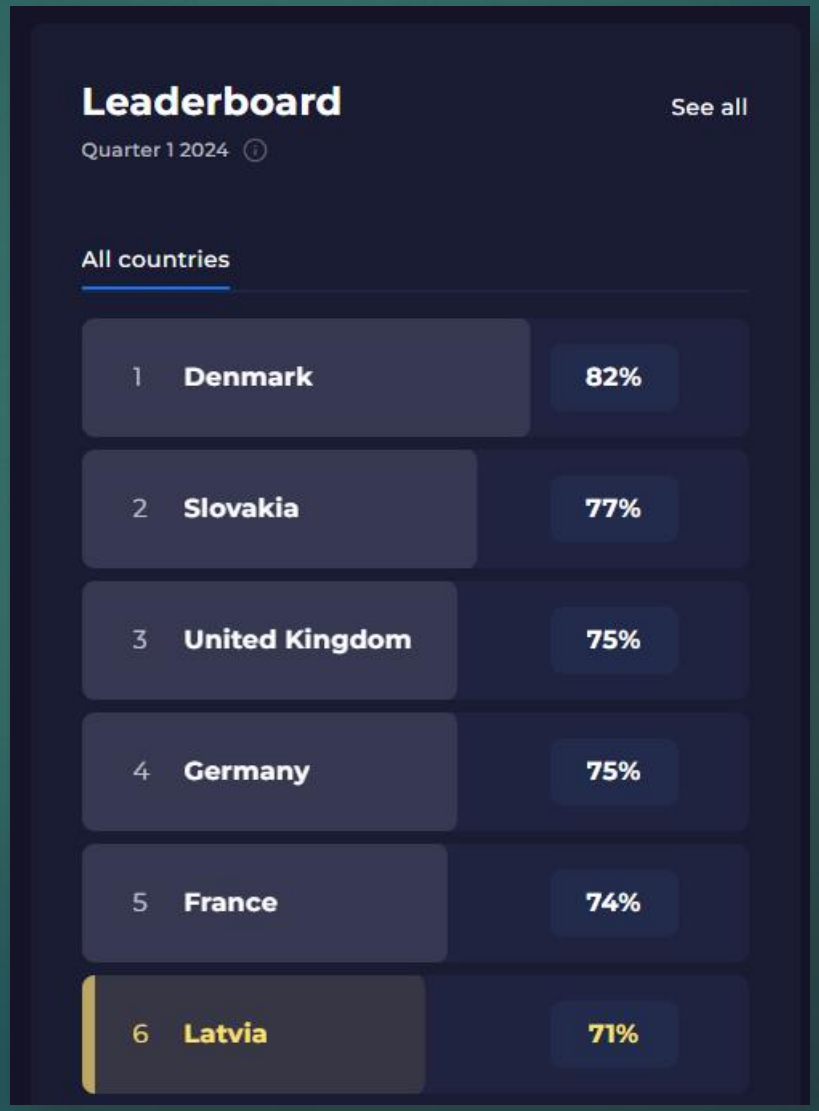


E-pasta drošība

Apmācību platformas

E-pasta drošība

Apmācību platformas



HOXHUNT

E-pasta drošība

Apmācību platformas

Draudu pārskats

Draudu veidi

- Iekšējie
- Ārējie

Draudu pārskats

Draudu veidi. Iekšējie

Darbinieks apzināti veic destruktīvas vai neatļautās darbības

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

Draudu pārskats

Draudu veidi. Iekšējie

Darbinieks neapzināti veic destruktīvas vai neatļautās darbības

- Zināšanu trūkums
- Neuzmanība

Draudu pārskats

Draudu veidi. Iekšējie. Kā pasargāties

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

Draudu pārskats

Draudu veidi. Ārējie.

- Sistēmu ievainojamības
- Konfigurāciju pārvaldība
- Destruktīvās darbības

Draudu pārskats

Sistēmu ievainojamības. Nepietiekama ievainojamību pārvaldība

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

Draudu pārskats

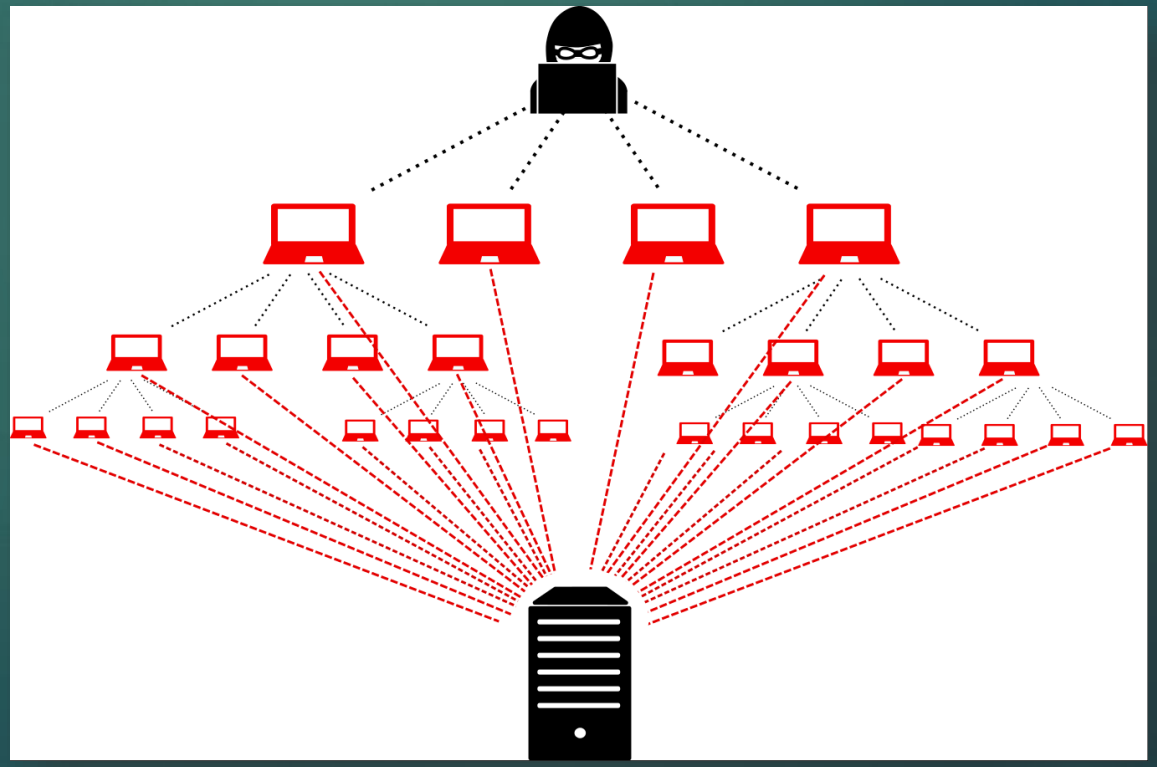
Sistēmu ievainojamības. Konfigurāciju pārvaldība

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

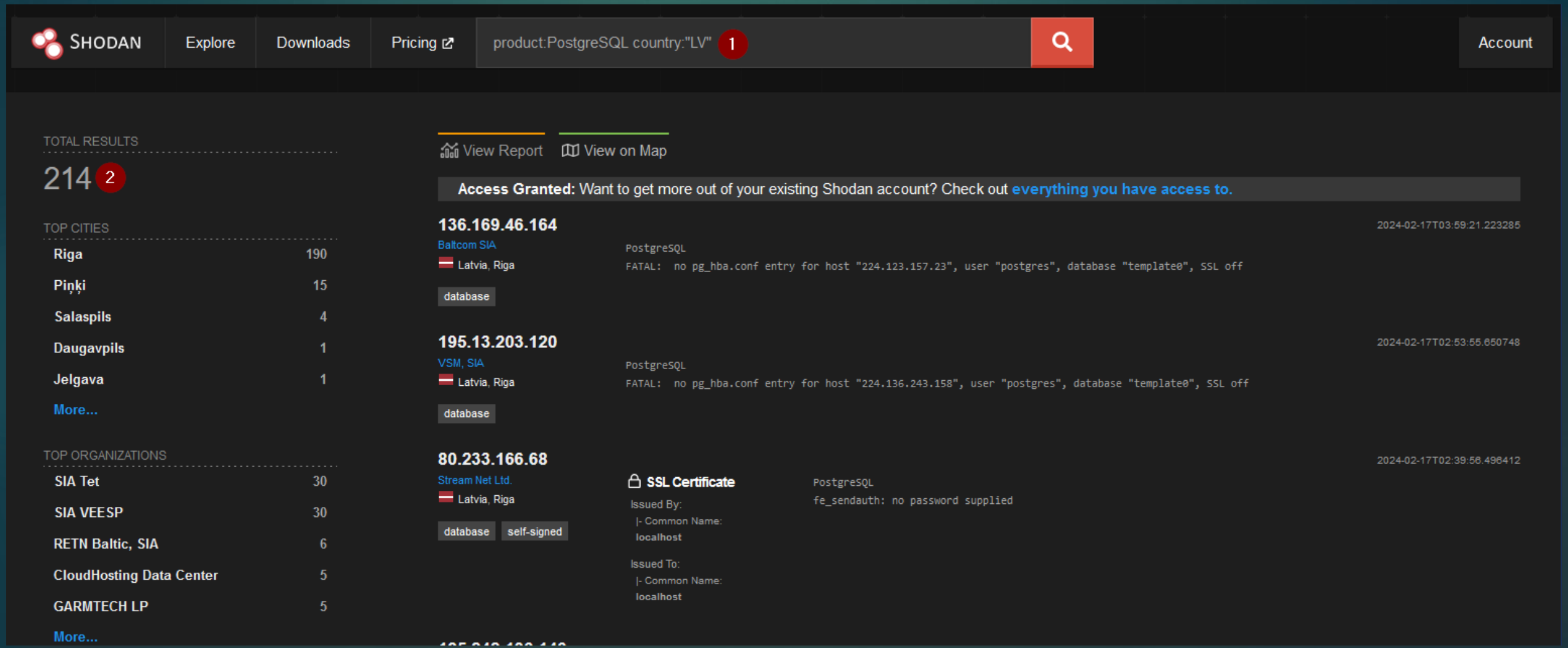
Draudu pārskats

Sistēmu ievainojamības. Destruktīvās darbības

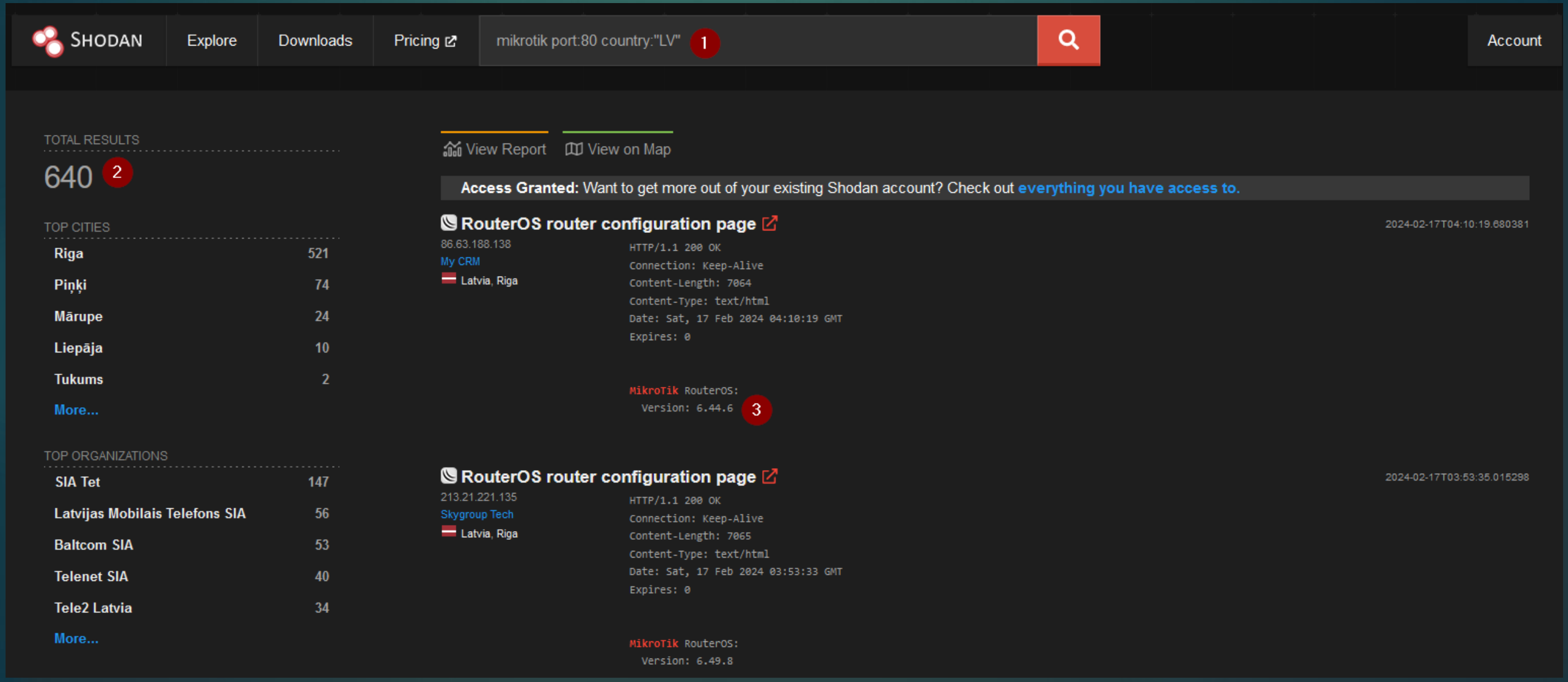
- DDoS uzbrukumi



Draudu pārskats



Draudu pārskats



Draudu pārskats

Ļaunprātīgās programmatūras piemēri

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

Draudu pārskats

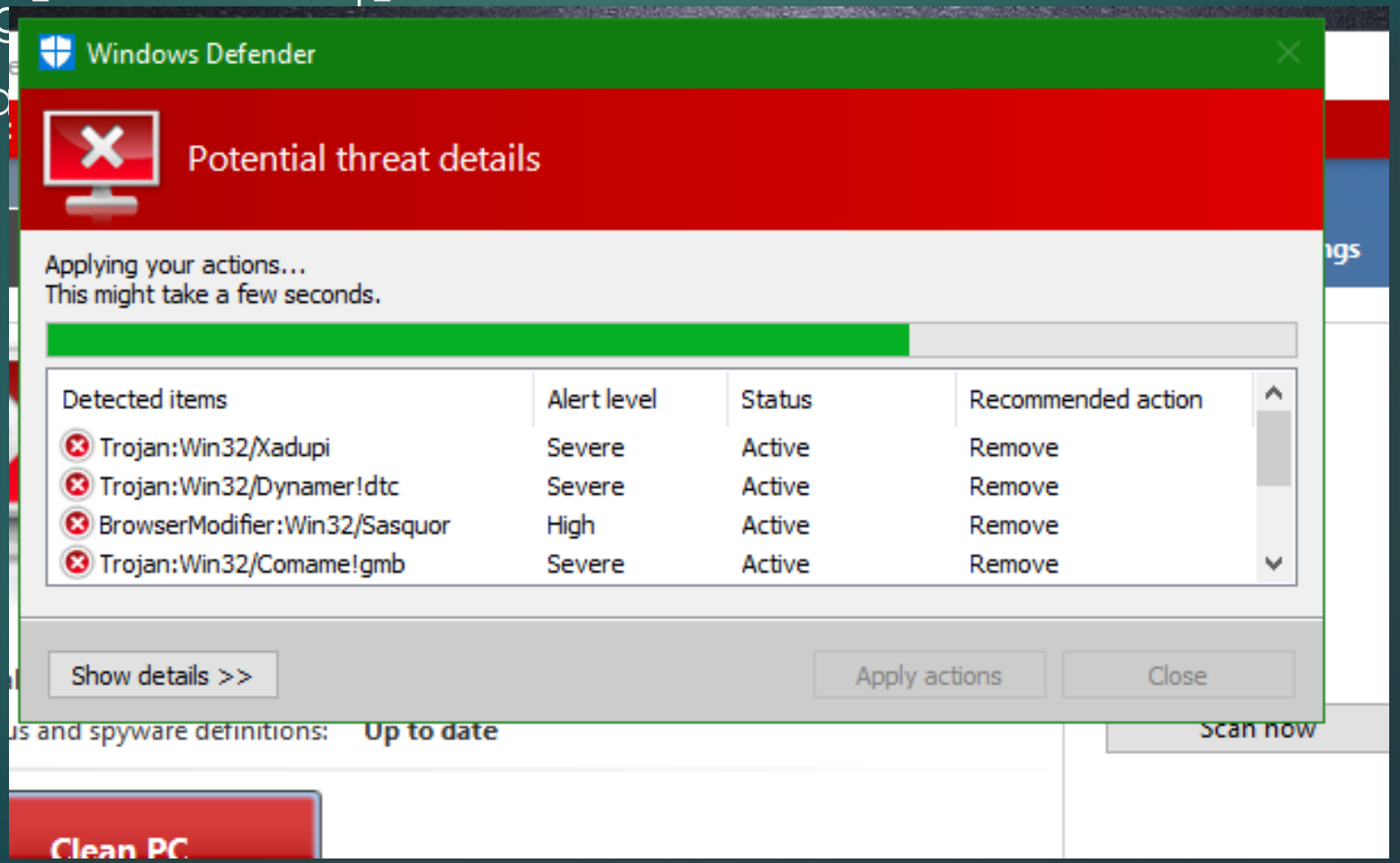
Ļaunprātīgā programmatūra

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

Draudu pārskats

Ļaunprātīg

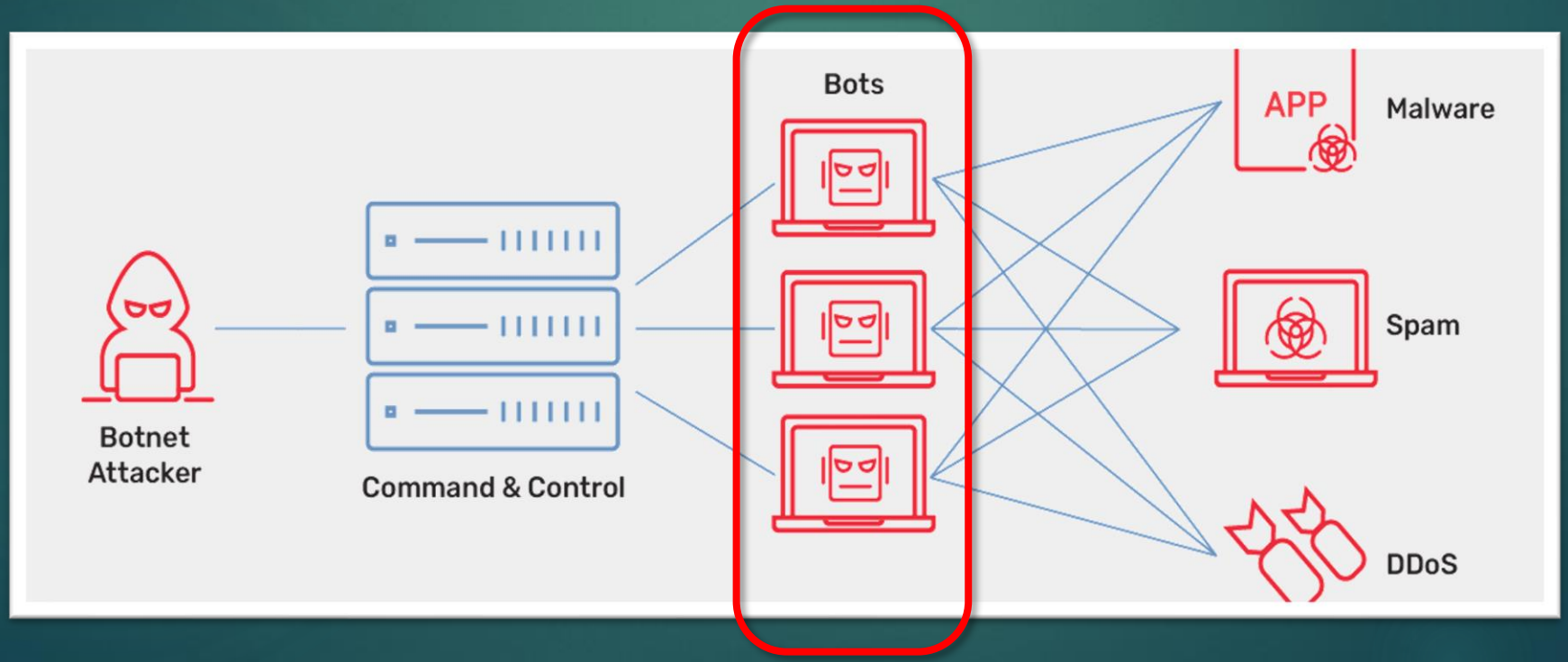
Nodarīt ko



Draudu pārskats

Ļaunprātīgā programmatūra.

Pārņemt kontroli tālākai izmantošanai



Draudu pārskats

Ļaunprātīgā 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

Ļaunprātīgā programmatūra.

Pārņemt kontroli tālākai izmantošanai

Draudu pārskats

Ļaunprātīgā programmatūra.

Šifrēt datus

Draudu pārskats

Ļaunprātīgā programmatūra. Šifrēt datus

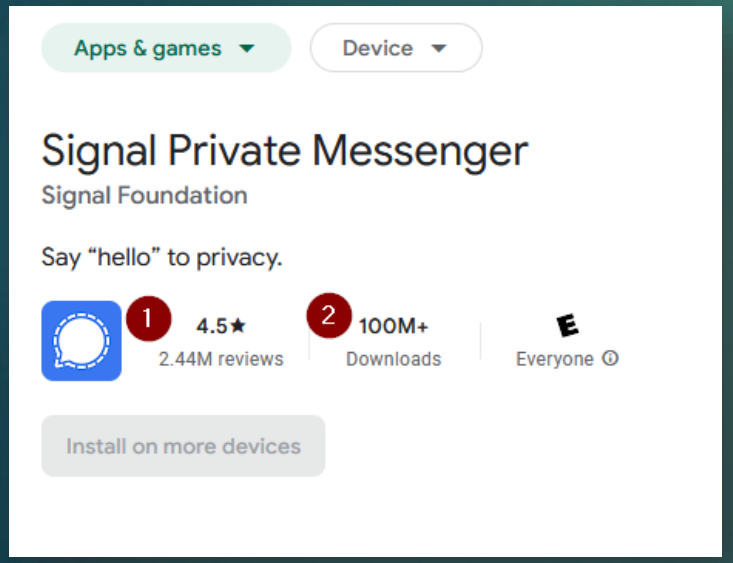
Uzņēmuma politika nepieļauj maksāt jo:

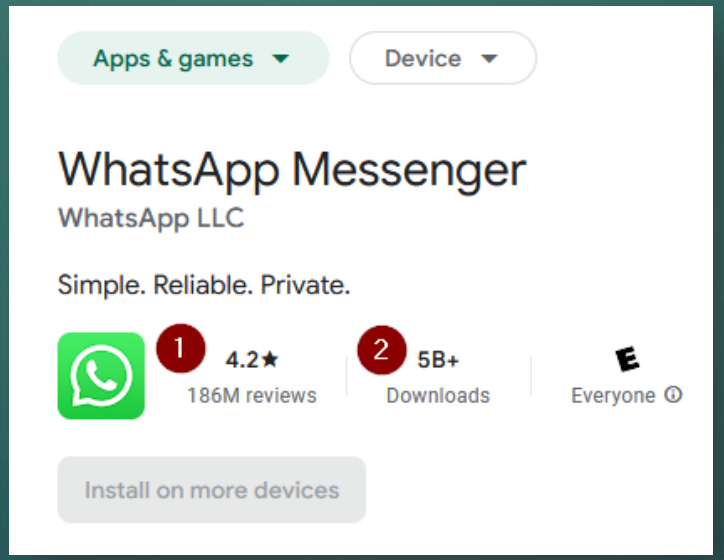
- Nav nekādas garantijas ka atgūs datus
- Nav garantijas ka summa nepalielināsies
- Reputācijas zaudēšana

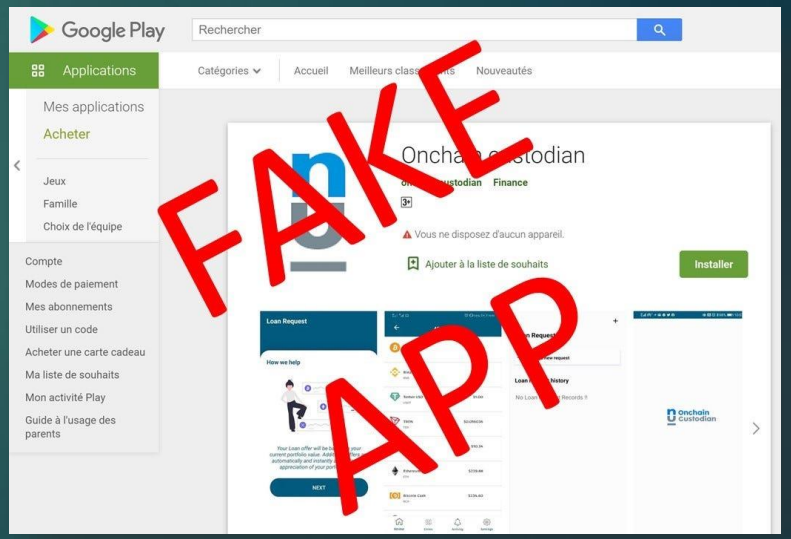
Draudu pārskats

Ļaunprātīgās programmatūra

- Nozagt datus
- Iegūt kontroli par ierīci







Rīcība drošības incidenta un pārkāpumu gadījumos

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

Rīcība drošības incidenta un pārkāpumu gadījumos

Viedierīces ir tik gudras cik gudrs ir to lietotājs

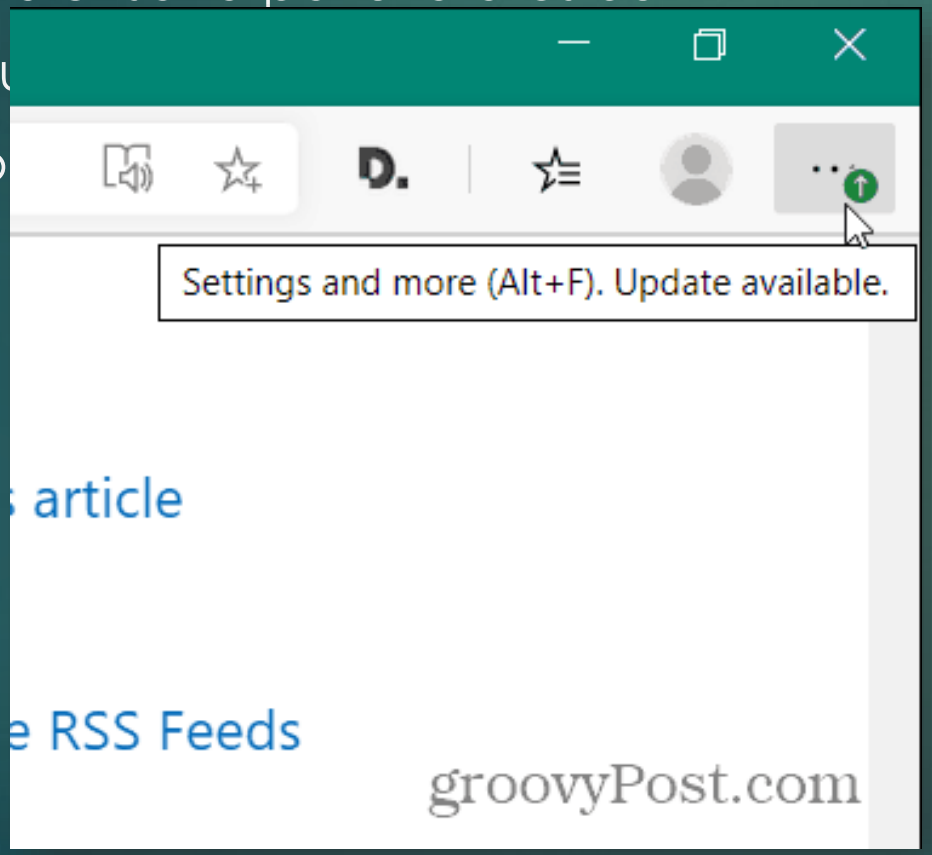
Apzināties savu vidi

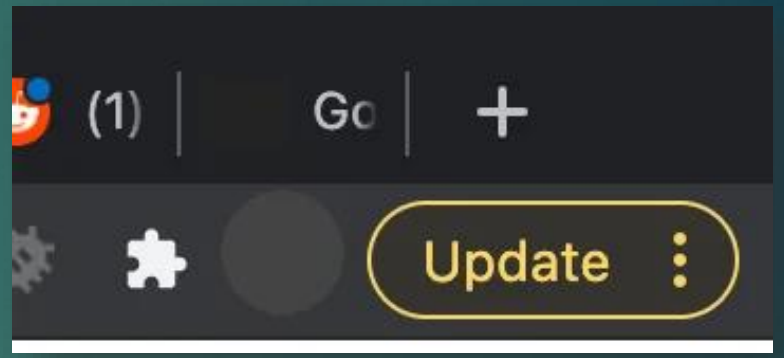
- Pamata darba komunikācijas vide: e-pasts, tālrunis, internets, Informācijas sistēmas
- Izmantot darbam IT ieteicamo pārlūku, pārējām lietām citu pārlūku
  - Darbam – MS Egde
  - Pārējam – Chrome, Firefox, Opera, u.c.

Rīcība drošības incidenta un pārkāpumu gadījumos

Pārbaudiet sava pārlūka drošību

- Atjau
- Atsp



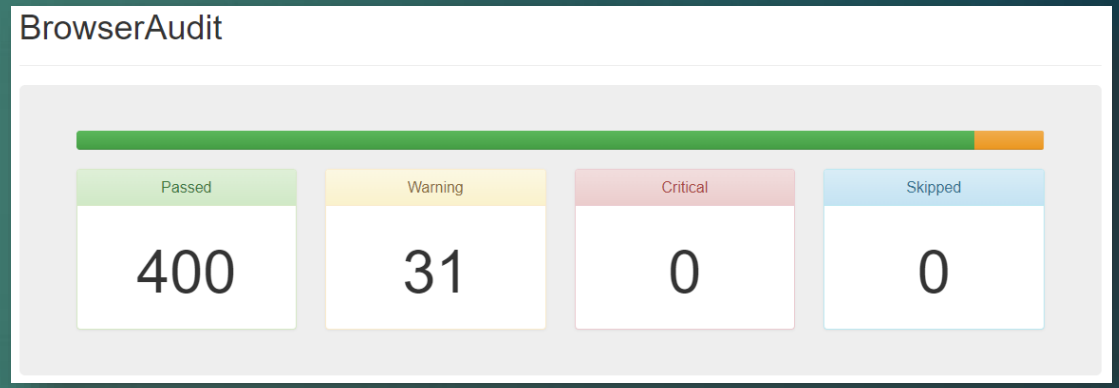


Rīcība drošības incidenta un pārkāpumu gadījumos

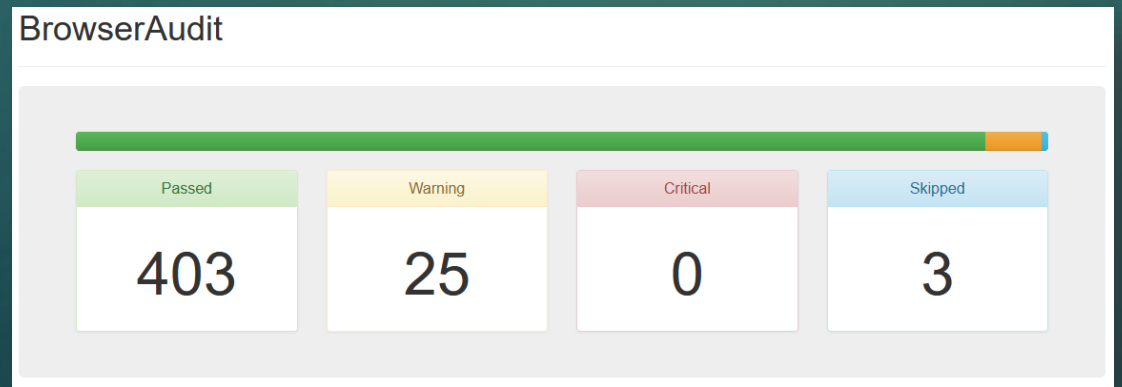
Pārbaudiet sava pārlūka drošību

- Pārbaudiet cik drošs ir pārlūks:
  - https://browseraudit.com/, apraksts
  - https://browserleaks.com/

MS Edge:



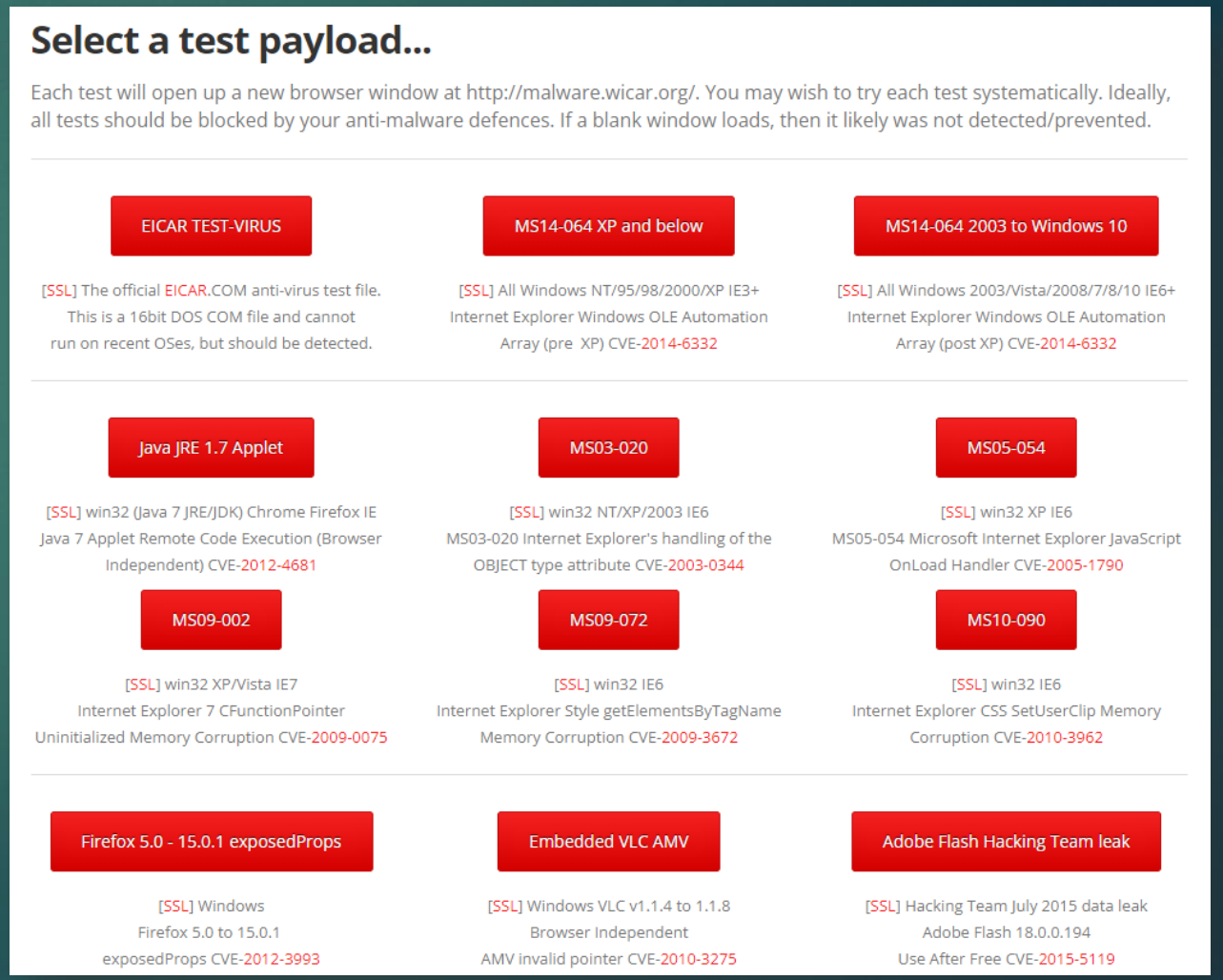
Firefox:



Rīcība drošības incidenta un pārkāpumu gadījumos

Pārbaudiet sava pārlūka drošību

[Test Malware! - WICAR.org - Test Your Anti-Malware Solution!]



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

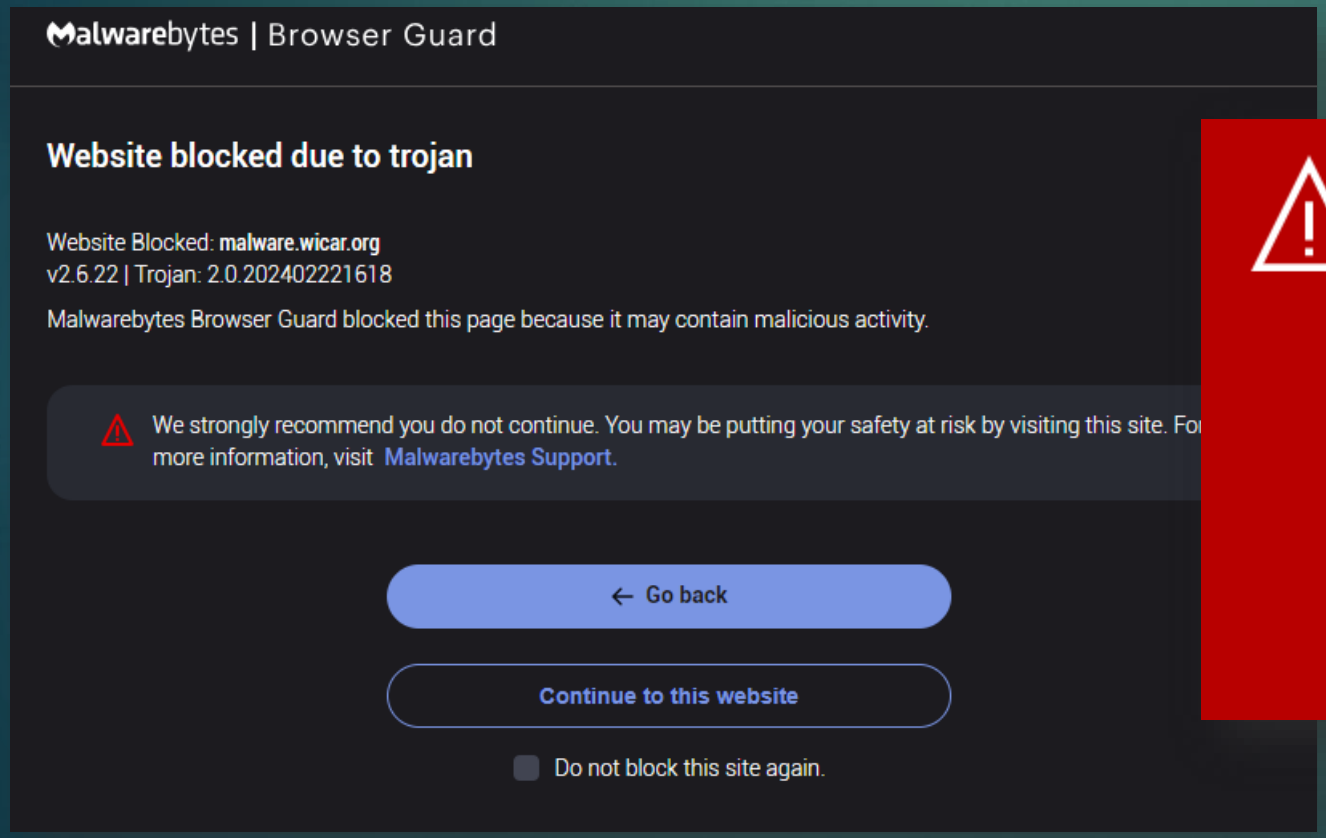
[SSL] Windows VLC v1.1.4 to 1.1.8 Browser Independent AMV invalid pointer CVE-2010-3275

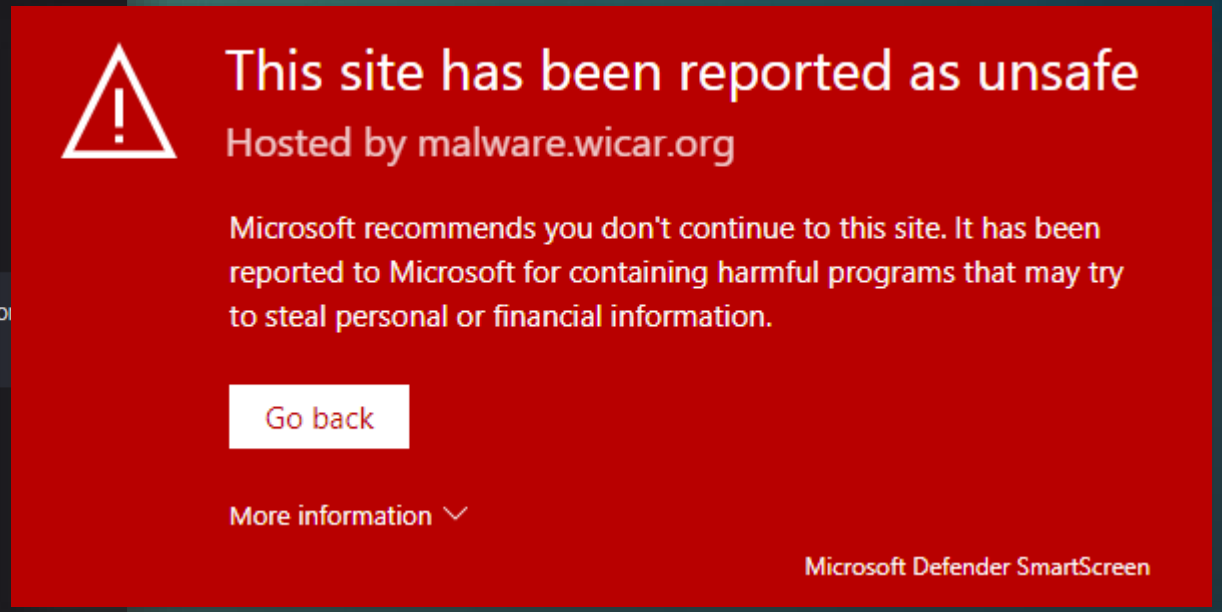
Adobe Flash Hacking Team leak

[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

Pārbaudiet sava pārlūka drošību





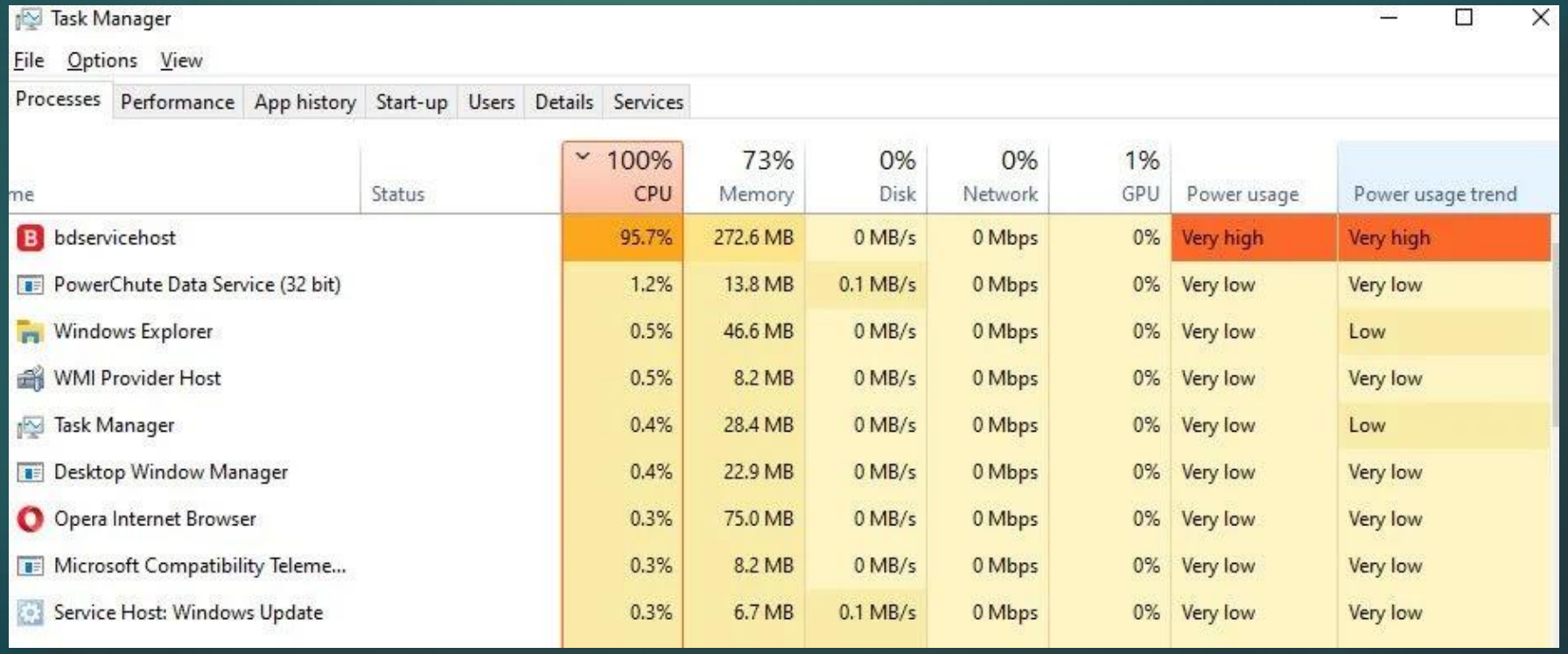
Rīcība drošības incidenta un pārkāpumu gadījumos

Kā pamanīt. Acīmredzami

Rīcība drošības incidenta un pārkāpumu gadījumos

Kā pamanīt. Slēptie procesi.

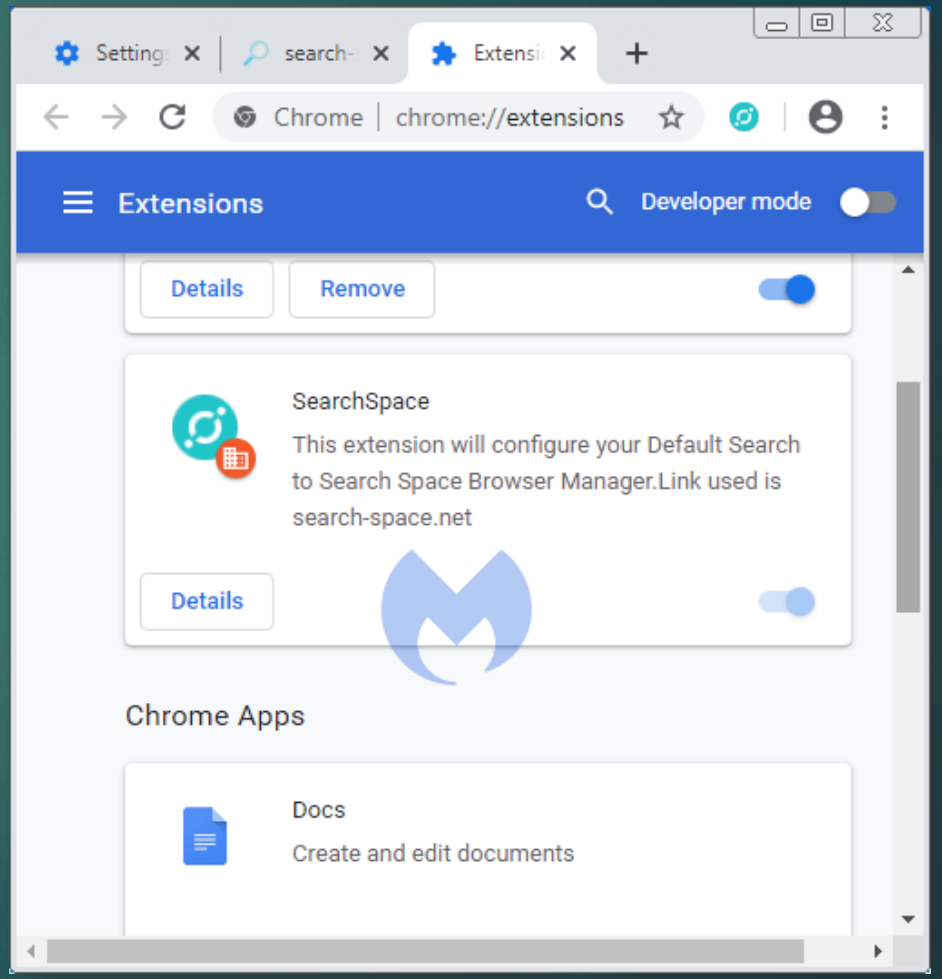
- Pazemājās datora veiktspēja, netipiskie procesi



Rīcība drošības incidenta un pārkāpumu gadījumos

Kā pamanīt. Slēptie procesi.

- Parādījās neierasta datora uzvedība



Rīcība drošības incidenta un pārkāpumu gadījumos

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

Izmantot uzticamu pretvīrusu programmatūru

Consumer antivirus software providers for Windows

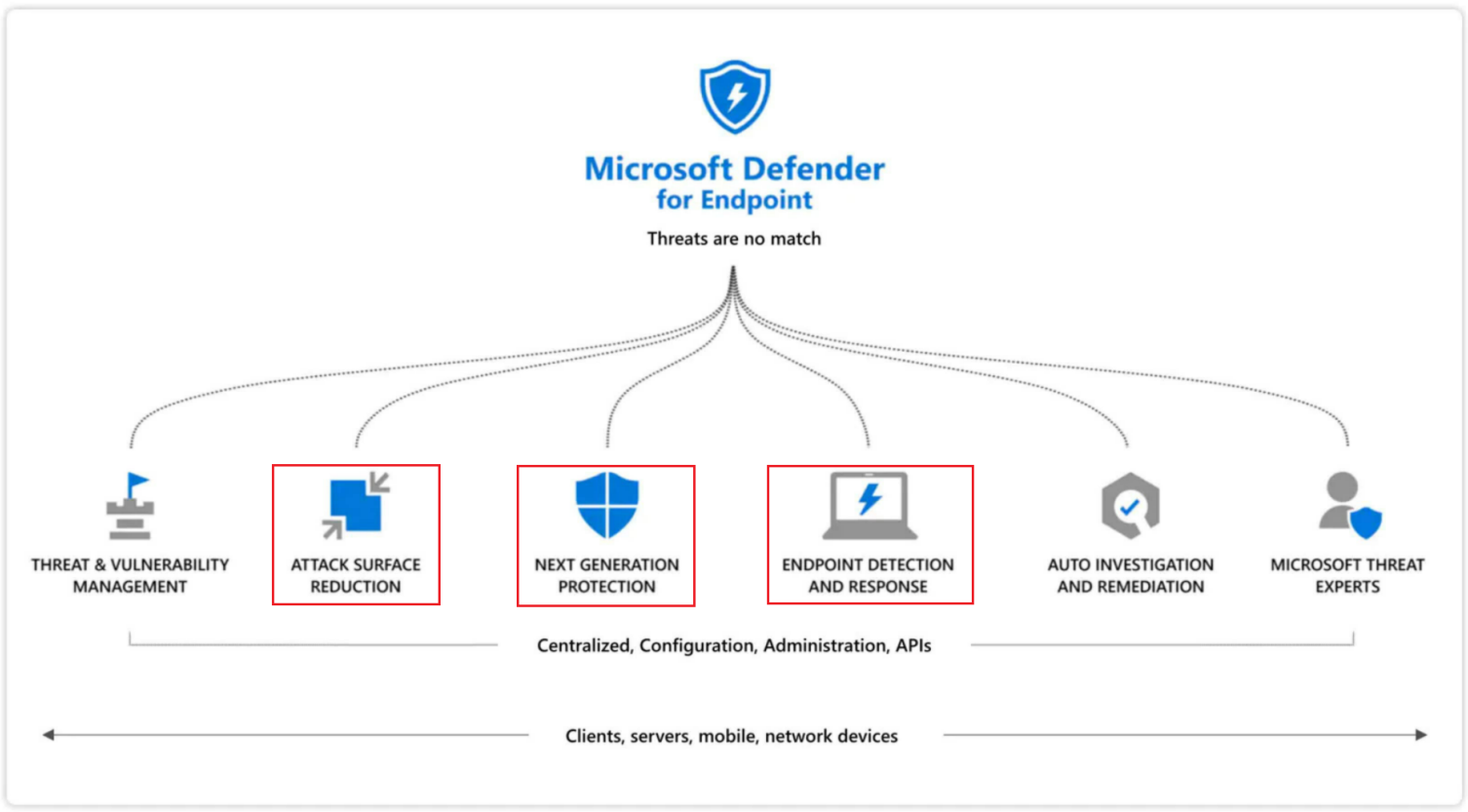
If you're running a supported version of Windows, you've already got Microsoft Defender Antivirus built in, helping to protect you against viruses, spyware, and other malware.

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

Izmantot uzticamu pretvīrusu programmatūru

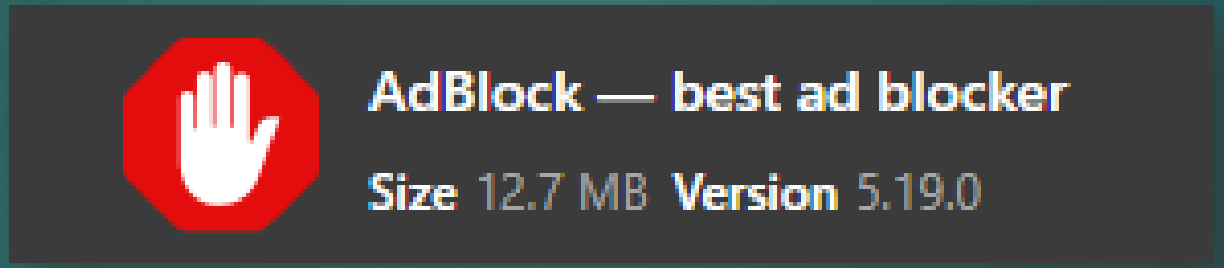


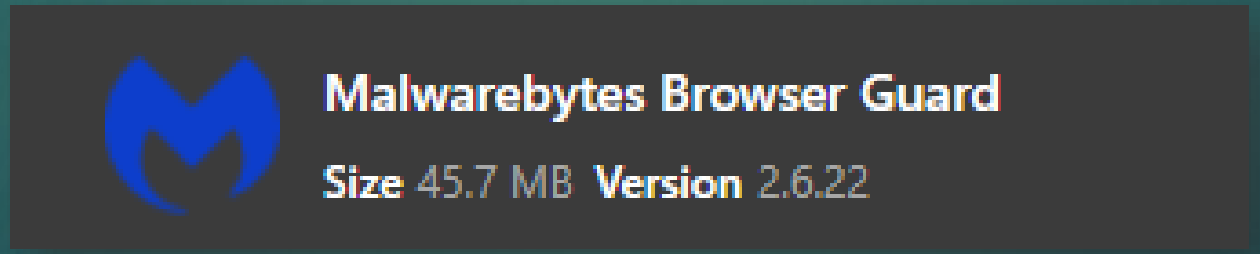
Rīcība drošības incidenta un pārkāpumu gadījumos

Izmantot uzticamu pretvīrusu programmatūru

Rīcība drošības incidenta un pārkāpumu gadījumos

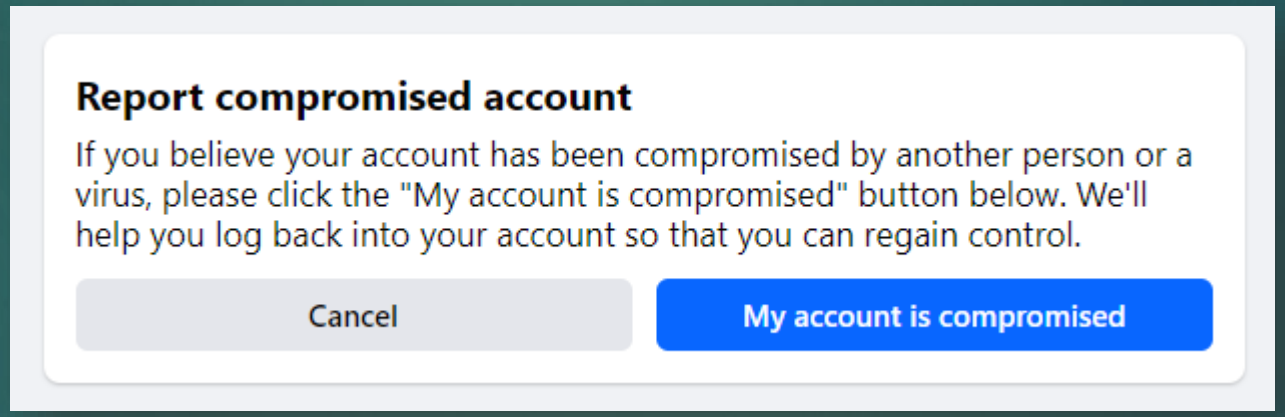
Izmantot drošības spraudņus pārlūkos





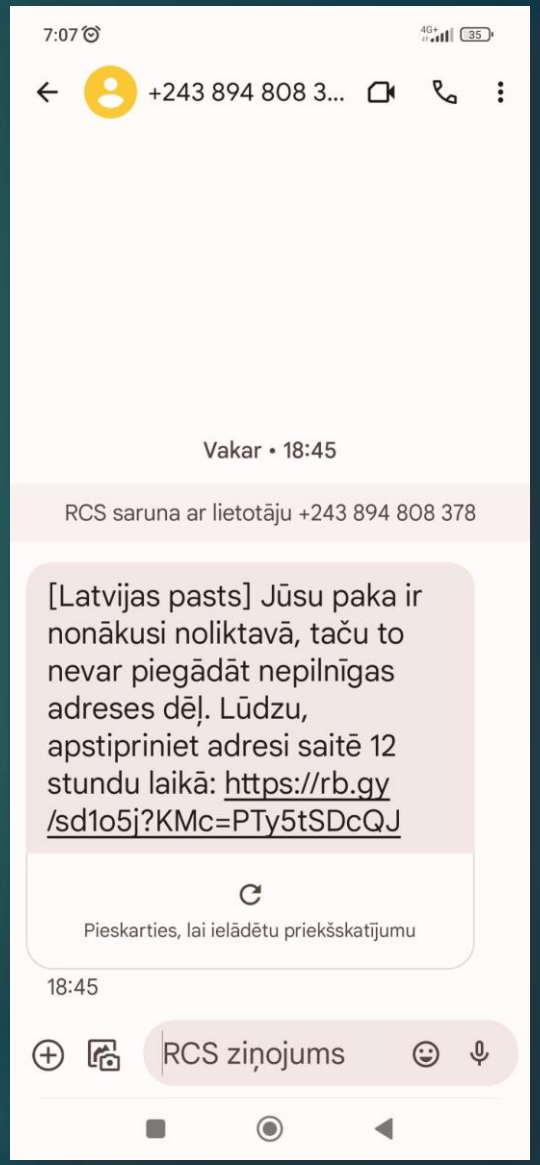
Rīcība drošības incidenta un pārkāpumu gadījumos

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



Rīcība drošības incidenta un pārkāpumu gadījumos

SMS krāpnieki



Rīcība drošības incidenta un pārkāpumu gadījumos

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:

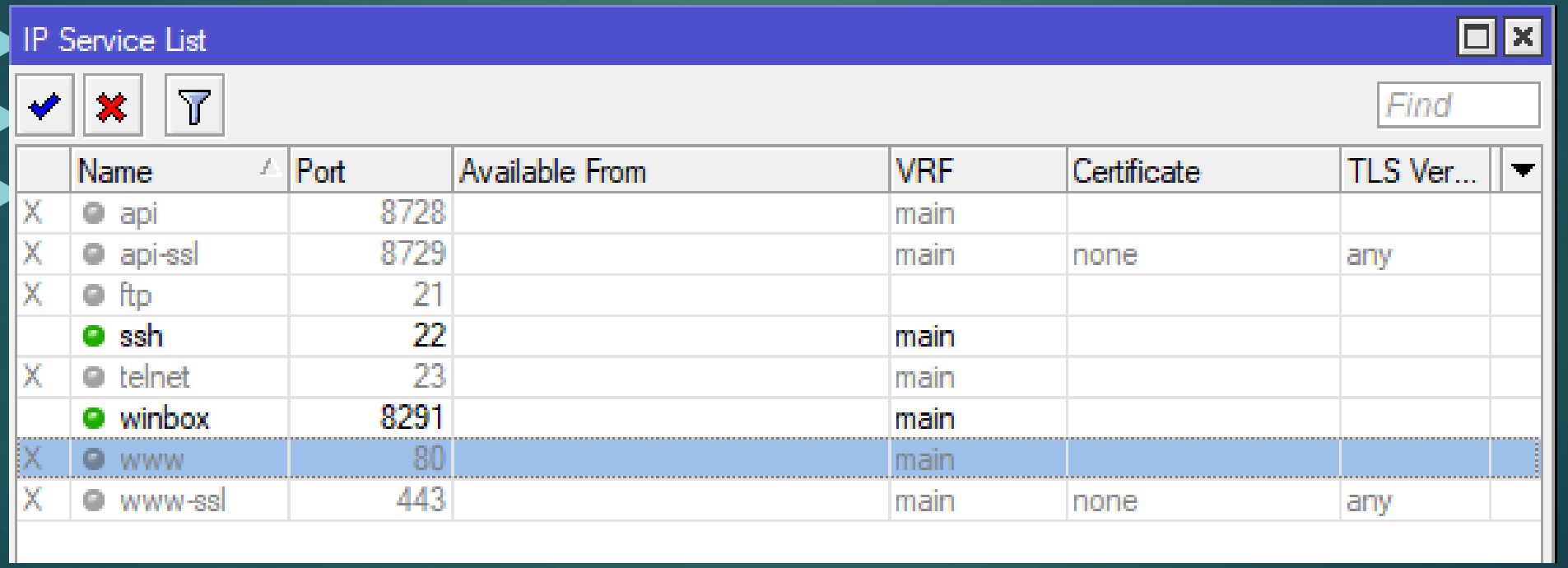
ziņot par incidentu: cert@cert.lv, cert@cert.gov.lv
par mēstuļu (SPAM) gadījumiem: abuse@cert.lv, abuse@cert.gov.lv
par atbildīgo personu: kontakti@cert.lv
sabiedriskās attiecības: prese@cert.lv
lai ziņotu par ievainojamību: cvd@cert.lv

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

Audotorijas Jautājumi

Mikrotik ugunsmūra ieteeicamā konfigurācija:

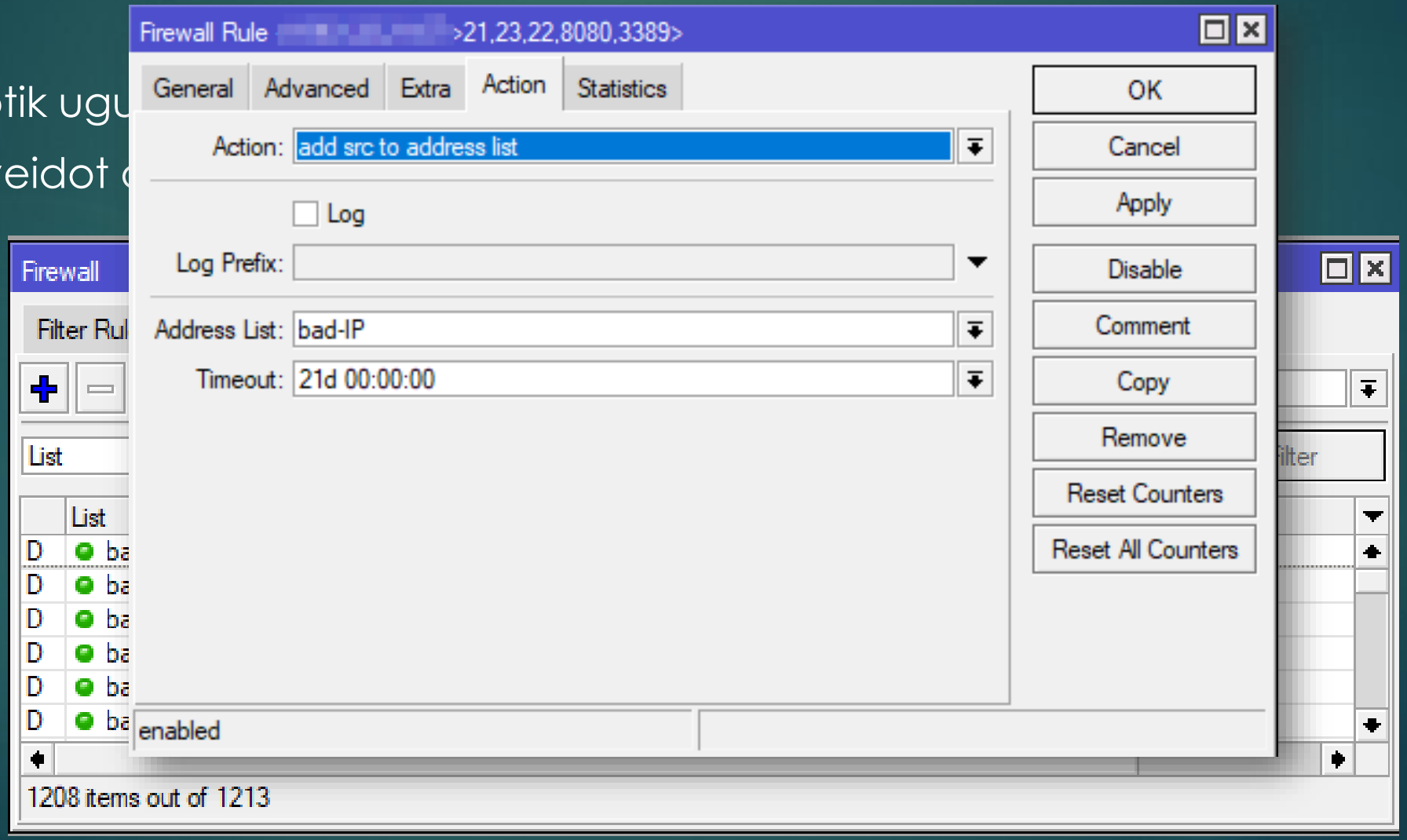
- Aizliegt noklusējuma Mikrotik servisus, SSH, HTTP, TELNET



Audotorijas Jautājumi

Mikrotik ugu

- Izveidot



Audotorijas Jautājumi

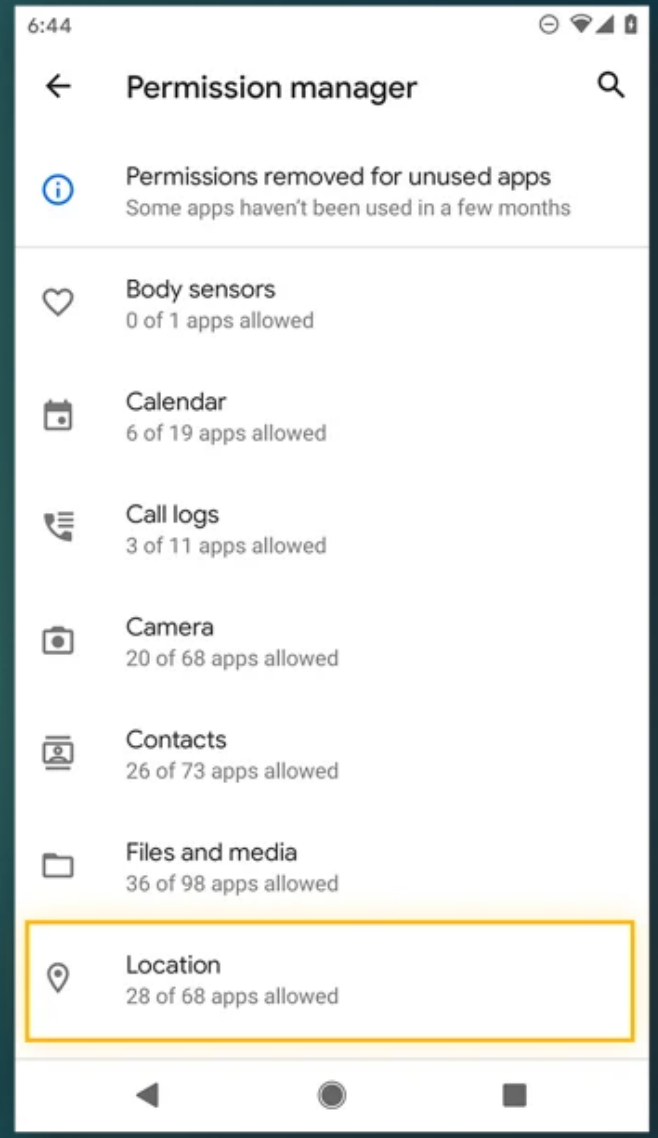
Uzmācīgie zvanītāji, ko darīt:

- 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

Viedierīču aizsardzība:

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



Finansē Eiropas Savienība

2027 Nacionālais attīstības plāns

Vides aizsardzības un reģionālās attīstības ministrija

CERT.LV

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

Aktivitāte tiek īstenota projekta "Pašvaldības kapacitātes stiprināšana to darbības efektivitātes un kvalitātes uzlabošanai, projekta Nr. 1.1.2.i.0/1/22/I/VARAM/001 ietvaros