Tipiskie kiberdrošības incidenti un labās prakses bibliotēkām

10/09/2025

Evita Roponena, Elizabete Citskovska
RTU Datorzinātnes un informācijas tehnoloģijas fakultāte,
«Kiberdrošības izglītības» kursa pasniedzējas

Lekcijas saturs

- Kāpēc kiberdrošība ir aktuāla?
- Kiberdrošības incidenti
- Kiberhigiēna un labās prakses ikdienas darbā

Kas notiktu, ja šodien pēkšņi pazustu visi elektroniskie katalogi un dati?

Kāpēc kiberdrošība ir svarīga?

Digitalizācija un jaunās tehnoloģijas -> kļūstam arvien vairāk atkarīgi no tehnoloģijām

Kas ir kiberdrošība?

Ko saka Tezaurs...

kiberdrošība

kiberdrošība

Informācijas tehnoloģiju sistēmu īpašība, kam jānodrošina to uzticamība, pieejamība un integritāte, arī darbs ar tām; arī informācijas drošība.

Nedaudz vienkāršāk:

Kiberdrošība ir darbības, kas jāveic, lai **aizsargātu tīklu** un **informācijas sistēmas**, to **lietotājus** un **citas personas**, kuras skar kiberdraudi

https://tezaurs.lv/kiberdro%C5%A1%C4%ABba

Kiberdrošība rūpējas, ka mūsu informācija ir droša:

Konfidencitāte: Informācijai nepiekļūst nevēlamās personas.

Facebook-Cambridge Analytica skandāls 2018. gadā:

Politiskais uzņēmums «Cambridge Analytica» piekļuva FB datiem no vairāk kā 87 miljonu lietotāju **bez to piekrišanas**.
Dotie dati tika pielietoti, lai veidotu psiholoģiskus profilus politiskai reklamēšanai, ieskaitot 2016. gada ASV prezidenta vēlēšanām.

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Kiberdrošība rūpējas, ka mūsu informācija ir droša:

Integritāte: Informācija ir patiesa.

Bitcoin krāpšana.

2020. gadā hakeri ieguva piekļuvi Twitter un pārņēma kontroli pār daudziem augsta profila kontiem, ieskaitot Elon Musk, Barack Obama, Bill Gates, Jeff Bezos, Apple. Viņi ievietoja tvītus, kas nepatiesi apgalvoja, ka, ja lietotāji nosūtīs Bitcoin uz noteiktu adresi, viņi pretī saņems dubultu summu.

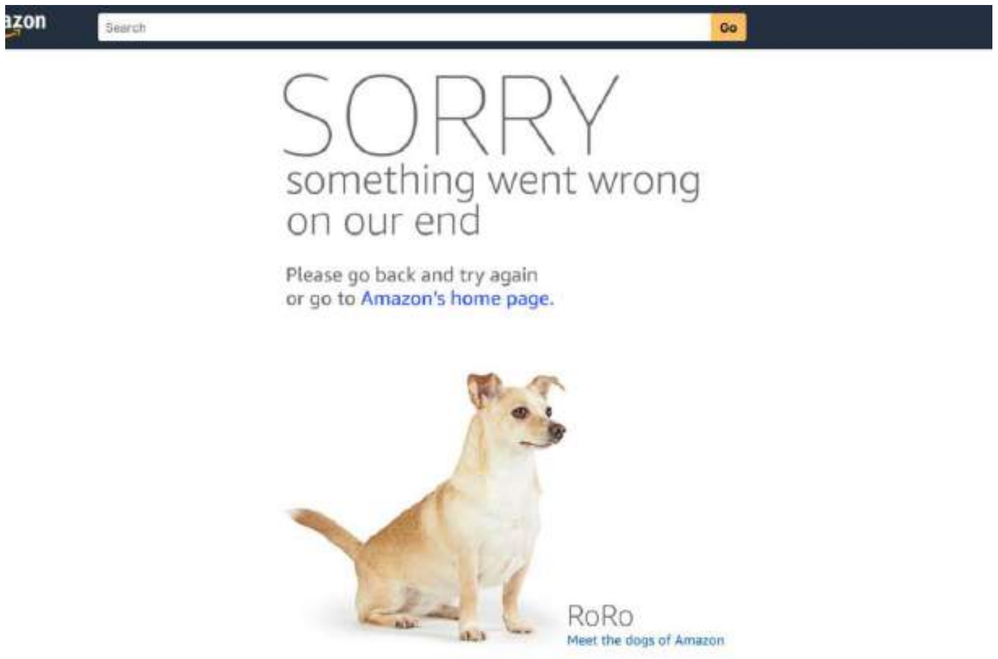
https://www.bbc.com/news/technology-53425822

Kiberdrošība rūpējas, ka mūsu informācija ir droša:

Pieejamība: Informācijai var piekļūt, kad nepieciešams.

Dyn DNS DDoS uzbrukums.

2016. gadā tika veikts masveida izkliedētā pakalpojuma atteikuma uzbrukums vērsts pret Dyn kopmānija, padarot servisus, kas izmantoja Dyn pakalpojumus, piem., Airbnb, Netflix, Amazon, nepieejamus klientiem.

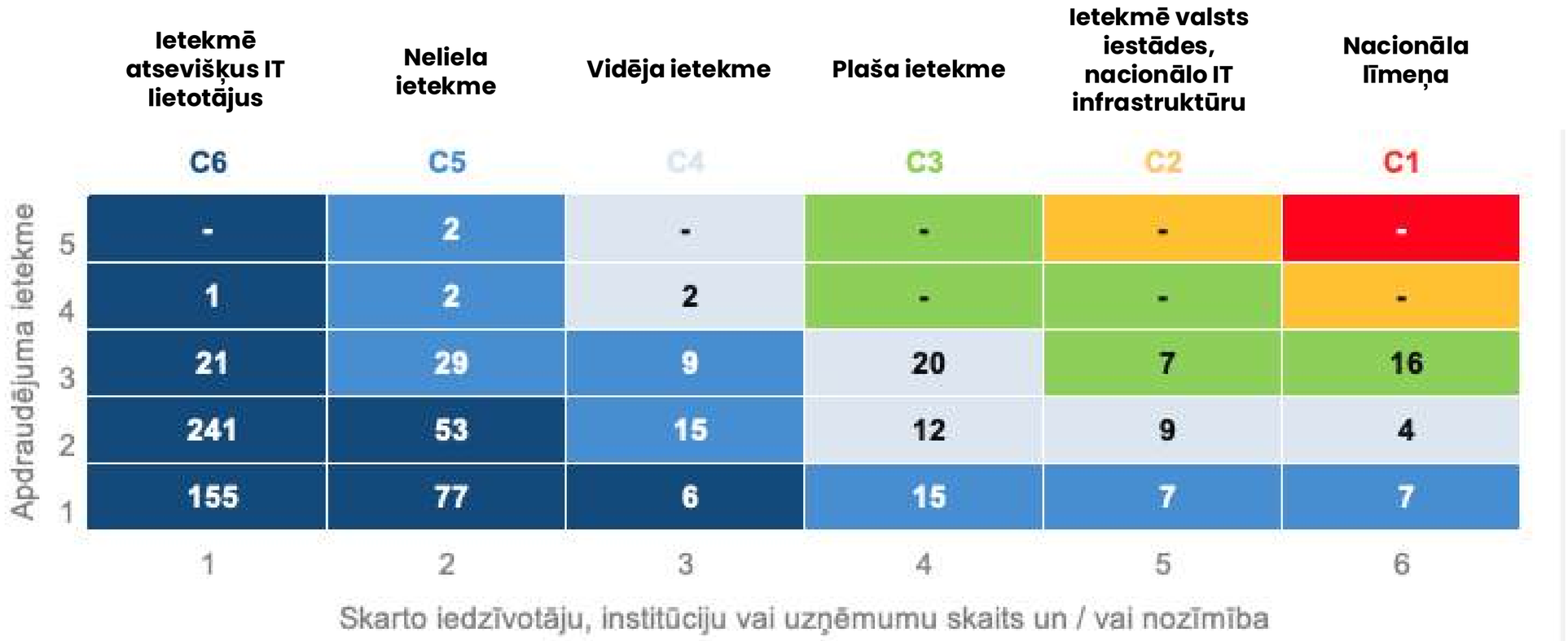


https://www.cloudflare.com/en-gb/learning/ddos/famous-ddos-attacks/

Neatļautas piekļuves gadījumā...

	Pieejamība	Konfidecialitāte	Integritāte
Neatļauta piekļuve	⚠	⚠	⚠
Informācijas izpaušana		⚠	
Informācijas sagrozīšana			⚠
Informācijas iznīcināšana	⚠		
Pakalpojuma atteikums	⚠		

2025. gada 2. ceturkšņa CERT.LV apstrādātie incidenti



https://cert.lv/lv/2025/07/pieejama-statistika-par-2025-gada-2-ceturksni

Ko vēl ir svarīgi atcerēties?

Ievainojamība + **Drauds** = **Risks**

Sistēmas vai programmas vājums

Bibliotēkas durvis netiek aizslēgtas uz nakti

Lietotājam ir vāja parole BIS ALISE

Iespējama darbība, kas var izraisīt kaitējumu

Kāds var ienākt un paņemt grāmatas bez atļaujas

Hakeris var viegli uzminēt lietotāja paroli

Iespējamība, ka drauds izmantos ievainojamību un būs kaitējums

Iespēja, ka grāmatas tiks nozagtas

Iespēja, ka hakeris piekļūs kontam un sagrozīs datus vai iegūs privātu informāciju

Ko vēl ir svarīgi atcerēties?

Risks

Iespējamība, ka drauds izmantos ievainojamību un būs kaitējums

Iespēja, ka hakeris piekļūs kontam un sagrozīs datus vai iegūs privātu informāciju

Kiberuzbrukums

Mēģinājums radīt kaitējumu kibertelpā (datorā, tīklā, IT sistēmā u.c.)

Hakeris mēģināja uzlauzt ALISE sistēmu un nozagt lietotāju paroles

Incidents

Noticis drošības gadījums, kas ir ietekmējis sistēmu vai lietotāju

Hakeris ir ielogojies ALISE sistēmā un nozadzis lietotāja personīgos datus

Ko vēl ir svarīgi atcerēties?

Risks

Iespējamība, ka drauds izmantos ievainojamību un būs kaitējums

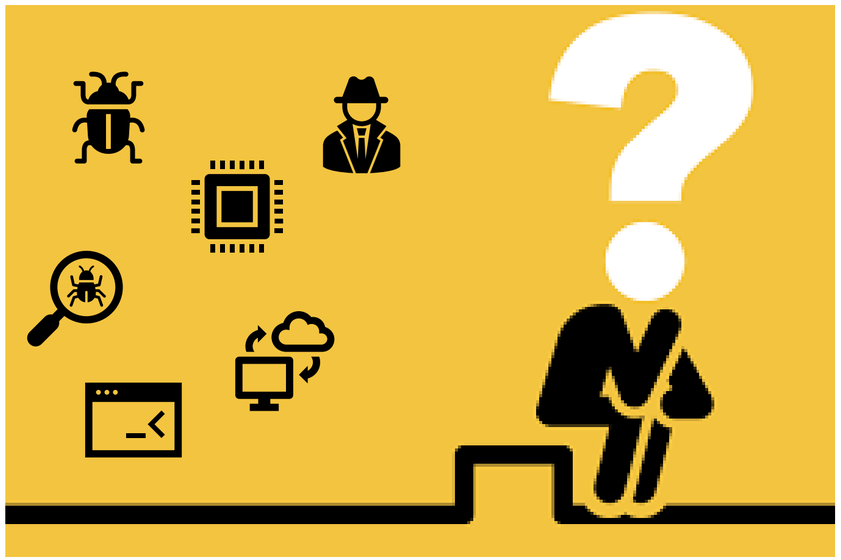
Iespēja, ka darbinieks nejauši izdzēsis lasītāju datu ierakstus pārstrādāšanās dēļ

Incidents

Noticis drošības gadījums, kas ir ietekmējis sistēmu vai lietotāju

Darbinieks ir saguris un netīšām izdzēsa 50 lasītāju kontus

Kādēļ bibliotēkas ir pakļautas riskam?



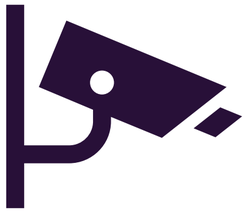
«Mazākas pašvaldību organizācijas kļūst par arvien pievilcīgākiem mērķiem tikai tāpēc, ka IT infrastruktūra šajos līmeņos nav tik labi nodrošināta.»

Aleksandr Essex, Rietumu Universitātes asociētais profesors un kiberdrošības eksperts

Dati – mūsdienu zelts

Darbinieku, bibliotēkas lietotāju **personas dati*** (vārds, uzvārds, dzimšanas dati, lasītāja kartes numurs, personas kods, dzīves vietas adrese, tālruņa numurs, e-pasta adrese, lasīšanas vēsture u.c.)

- Personas dati vēlāk var tik izmantoti krāpniecībā
- Privātuma aizskārums (lasītāja vēstures atklāšana)



Videoieraksti

- Izsekošanas, privātums pārkāpšanas risks

Informācija par pašvaldību un skolu bibliotēku krājumiem, novada resursu datu bāze un pašvaldību dokumentu datu bāze

- Informācijas manipulēšana, iznīcināšana
- Piekļuves iegūšana plašākai infrastruktūrai

***Jebkāda informācija, kas attiecas uz fizisko personu, kuru tiešā vai netiešā veidā var identificēt.

Kas apdraud bibliotēkas?

Ārējie draudi

Noticis kiberuzbrukums kultūras nozares informācijas sistēmām

Dalīties:

Ilustratīvs attēls. Freepik

Avots: https://www.lsm.lv/raksts/zinas/latvija/08.08.2025-noticis-kiberuzbrukums-kulturas-nozares-informacijas-sistemam.a609708/

Kādi vēl varētu būt ārējie draudi?

Viss, kas nāk no ārpuses

	Piemērs
Kiberuzbrukumi	Kāds mēģina uzlauzt bibliotēkas IT sistēmas
Vīrusi un ļaunatūra	Datorā nonāk kaitīga programmatūra, to inficējot
Pakalpojuma atteices uzbrukumi	Bibliotēkas mājaslapa tiek pārplūdināta ar pieprasījumiem un nav pieejama lasītājiem
Datu zādzība	Hakeris nozog lietotāju personas datus vai pieejas informāciju.
Publisko tīklu apdraudējumi	Bibliotēkas publisko Wi-Fi izmanto datu pārtveršanai

Ne visi ir rūdīti uzbrucēji..

Attēls: https://vividcomm.com/2019/04/15/threat-actors/

Iekšējās kļūmes

Notiek darbs pie Valsts vienotās bibliotēku informācijas sistēmas datu atjaunošanas

Atskaņot tekstu A Viegli lasīt

Publicēts pirms vairāk nekā 1 gada

Publicēts: 04.07.2024.

Avots: https://www.kis.gov.lv/lv/jaunums/notiek-darbs-pie-valsts-vienotas-biblioteku-informacijas-sistemas-datu-atjaunosanas

Kādi vēl varētu būt iekšējie draudi?

Viss, kas nāk no iekšpuses

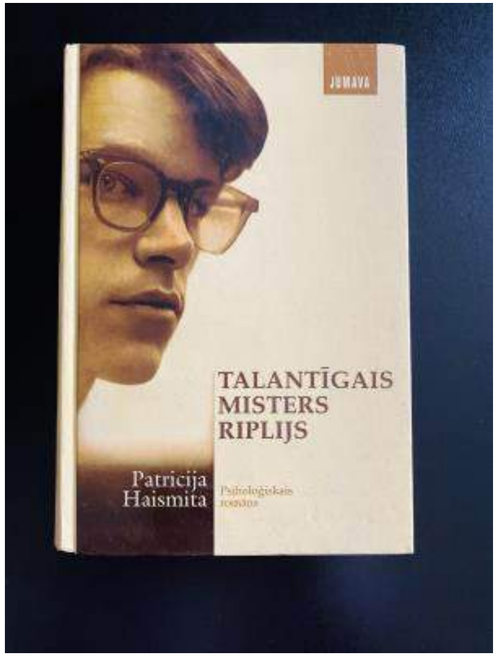
	Piemērs
Cilvēka kļūdas	Darbinieks nejauši izdzēš grāmatu no kataloga
Neapzināta rīcība	Lasītājs aizmirst izrakstīties no sava konta publiskajā bibliotēkas datorā
Apzināta rīcība	Neapmierināts darbinieks noplūdina lietotāju informāciju
Vājas paroles	
Nolaidība	Netiek uzstādīti sistēmu atjauninājumi

Testiņš – Cik drošs tu esi?

Identitātes zādzība un paroles drošība

Identitātes zādzība – kāds pretlikumīgi iegūst cita cilvēka personīgo informāciju un izmanto krāpnieciskiem mērķiem.

Piemēram, iegūstot lietotāja autentifikācijas datus, jo lietotāja parole ir gaužām vienkārša.



Jūs esat uzsācis darbu Talsu bibliotēkā. Darba uzsākšanai ir jāizveido parole bibliotēkas informācijas sistēmai ALISE. **Kā izvēlēties drošu paroli?**

Attēls: https://pixabay.com/photos/alzheimers-dementia-words-3068938/

Kuru paroli izvelēsimies?

A

soso123aljg

B

@apolo.lv

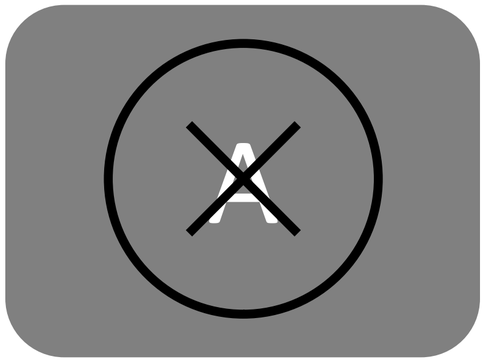
C

madara

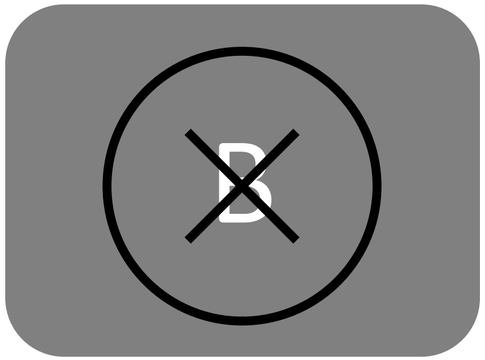
D

qwerty

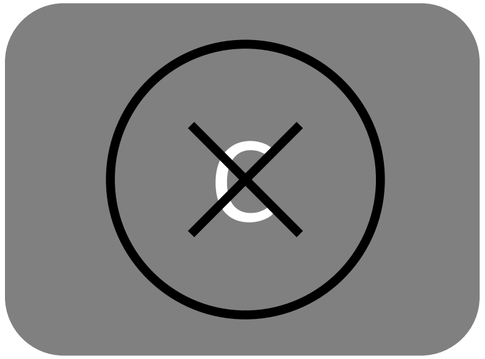
Kuru paroli izvelēsimies?



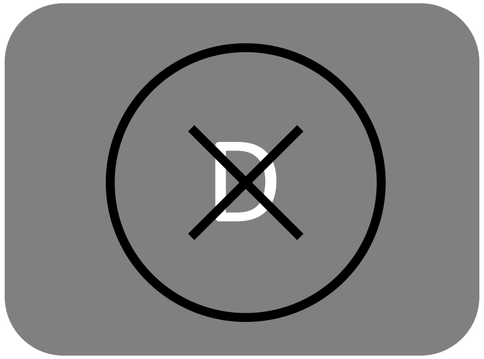
soso123aljg



@apolo.lv



madara



qwerty

Vai Jūsu parole ir sliktāko paroļu TOP100?

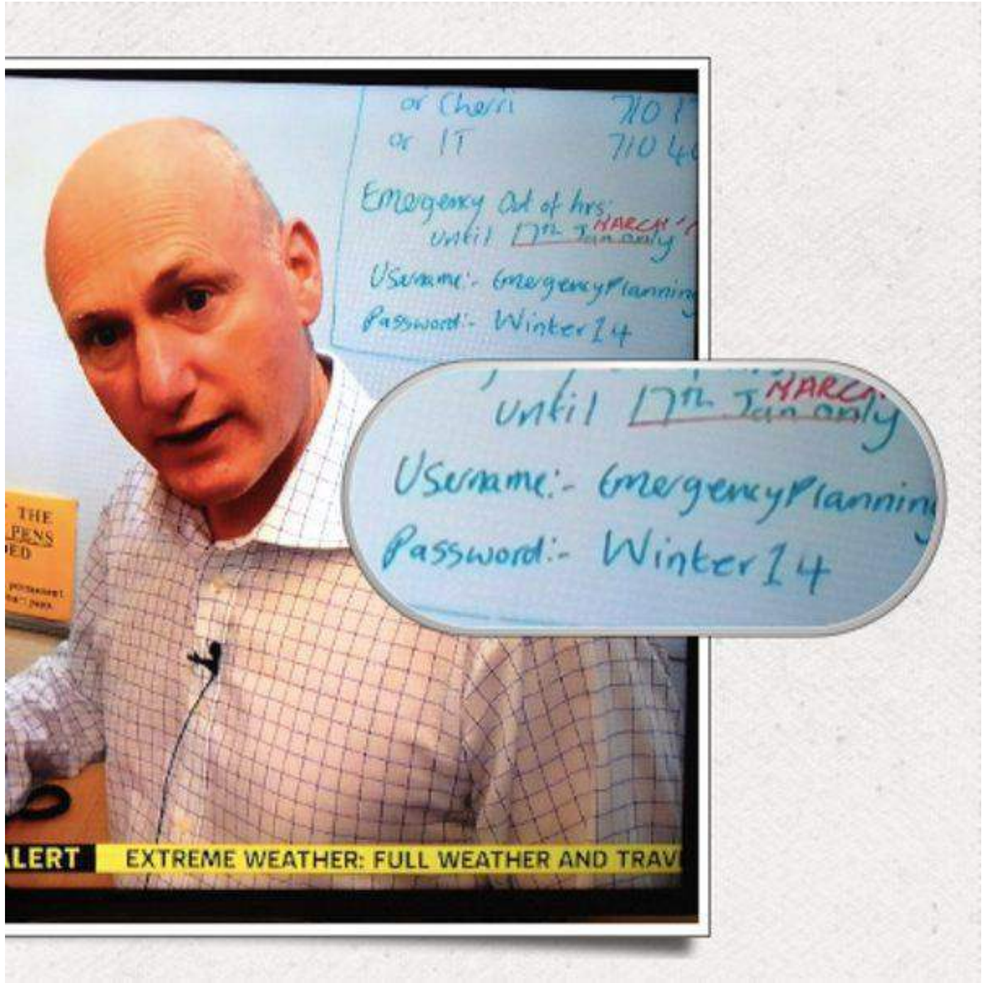
Avots: https://rokasgramata.esidross.lv/slikto-parolu-top-100/

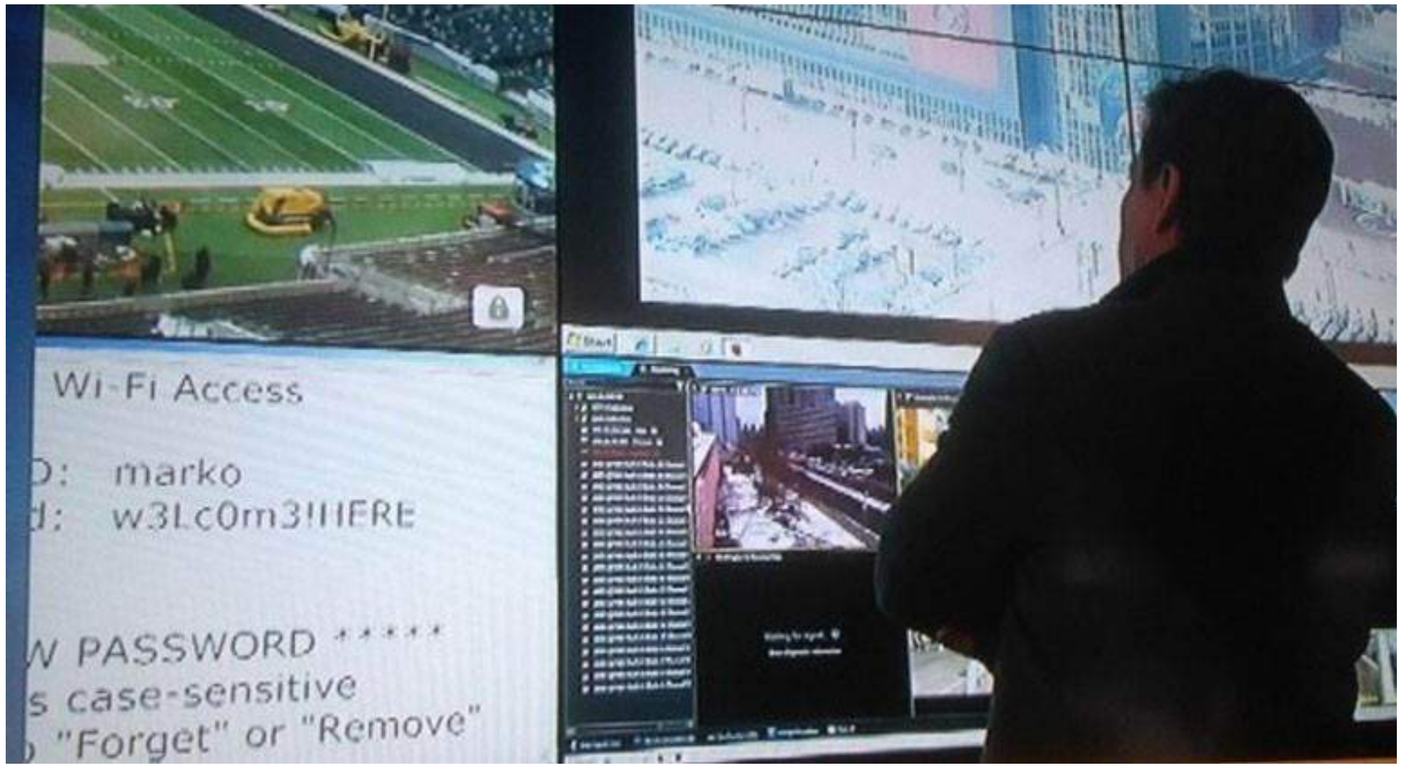
Par parolēm īsumā

- Vienas paroles atkārtota izmantošana
- Dalīšanās ar parolēm
- Personīgas informācijas iekļaušana parolē
- Vienkāršu paroļu izmantošana, piem., parole123
- Paroļu pierakstīšana uz lapiņām 😭

- Divu vai vairāku faktoru autentifikācijas izmantošana
- Paroļu pārvaldnieka izmantošana
- Drošu unikālu paroļu izmantošana 🤵
- Savu profilu pārbaude, vai to piekļuves dati nav izpausti kāda datu noplūdē

Kāpēc paroles nepierakstīt





Attēli: https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

Unikālas paroles un paroļu noteikumi

Parolēm bieži tiek ir uzstādīti sastāva noteikumi – cik daudz dažādām rakstzīmēm jābūt parolē. Pētījumi rāda, ka lietotāji ļoti paredzami veido “kompleksās paroles”.

Kā lietotāji veido paroles atbilstoši noteikumiem

nav noteikumu	**parole**
jābūt vismaz 1 lielam burtam un ciparam	**Parole1**
jābūt vismaz 1 lielam burtam, ciparam un simbolam	**Parole1!**

Kā veidot drošu paroli?

Garas, sarežģītas paroles vietā – frāzveida parole!

Piemēri:

- Laiks stiprai m3lnai k@fij@i!
- pazudis-gliemezis-lien-pludmal3
- Gudrība ir robezas-mulkība nav

Ļaundaris ir ieguvis Jūsu bibliotēku informācijas sistēmas ALISE paroli.

Kas viņu atturēs no pieslēgšanās sistēmai ?

Attēls: https://pixabay.com/photos/thief-burglary-break-into-1562699/

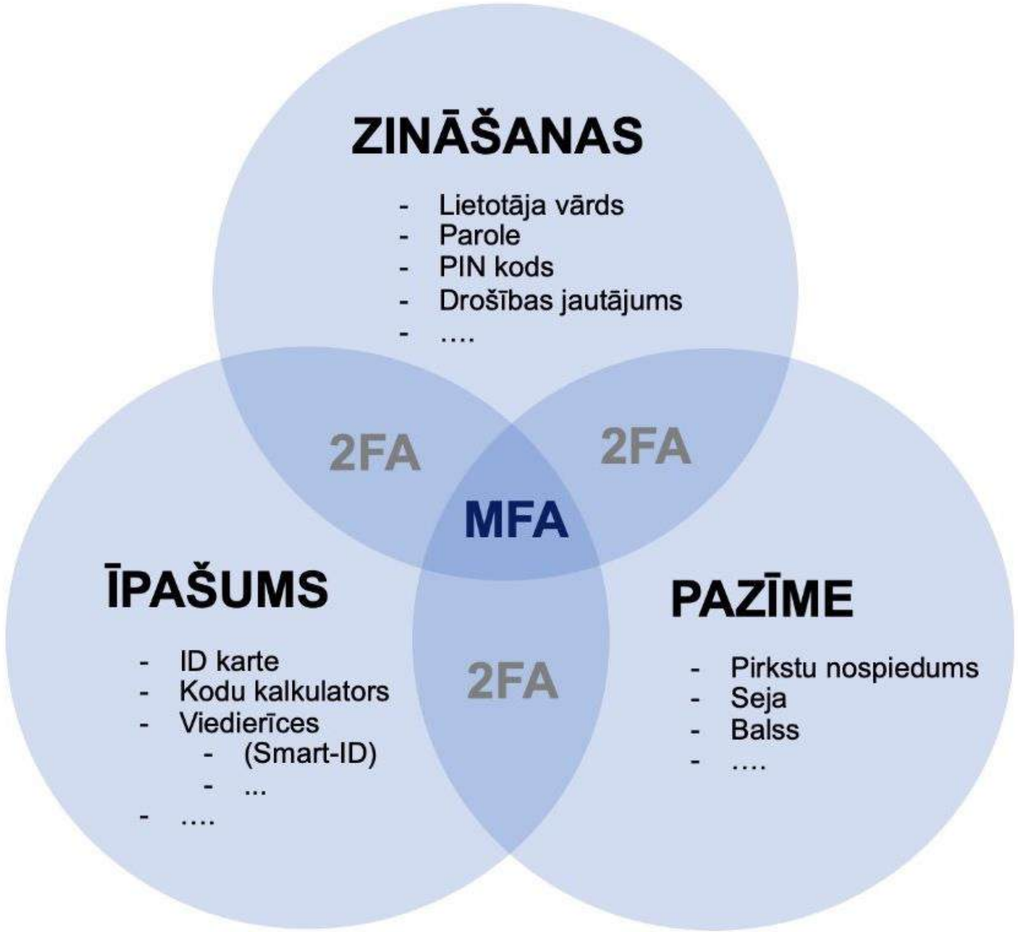
Daudzfaktoru autentifikācija!

Daudzfaktoru autentifikācija – kas tas tāds?

Daudzfaktoru autentifikācija (MFA) apvieno
- zināšanas (angļu val. something you know)
- īpašumu (angļu val. something you have)
- pazīmi (angļu val. something you are)

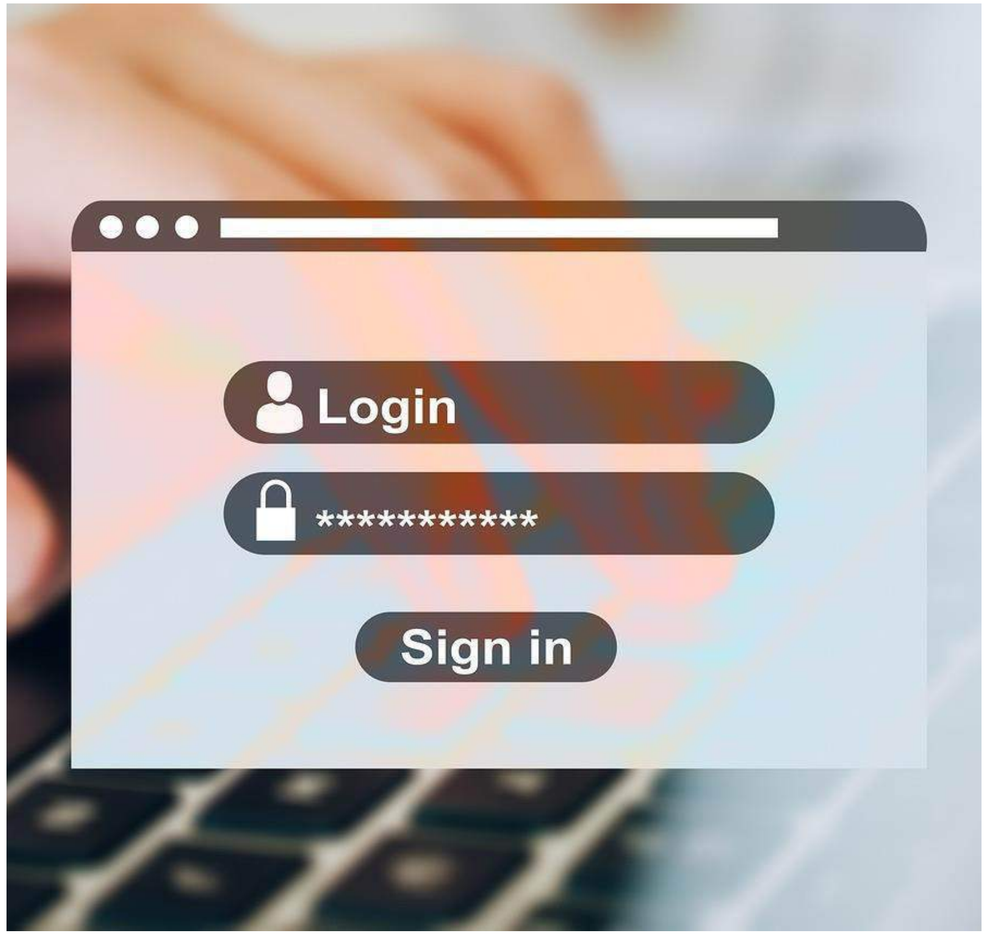
2FA jeb divu faktoru autentifikācijā tiek apvienoti tikai 2 no faktoriem.

❗ Iespējojam 2FA vai MFA opciju visur, kur iespējams ❗

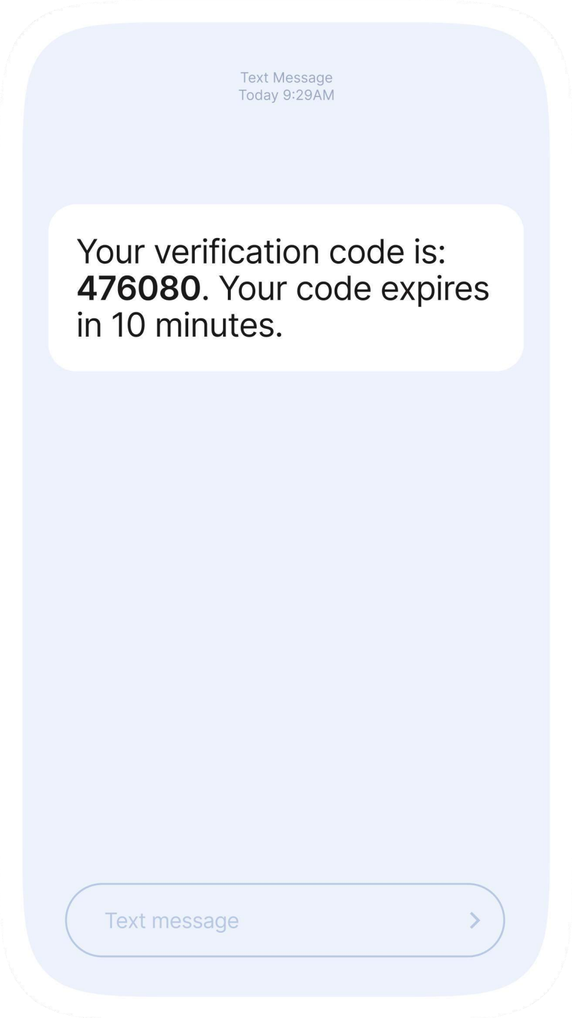


Attēls: https://www.esidross.lv/2021/03/25/papildu-drosiba-vairaku-faktoru-autentifikacija/

Parole un lietotājvārds



SMS kods



Attēls pa kreisi: https://pixabay.com/photos/registration-log-in-keyboard-hand-3938434/
Attēls pa labi: https://www.infobip.com/sms/2fa

Mazie MFA baušļi

Tas, ka izmantosiet divu vai vairāku faktoru autentifikāciju **nenozīmē**, ka Jūsu dati būs drošībā. Ļoti nozīmīgi ir tas, kā Jūs to izmantojat. **Pievērsiet uzmanību**:

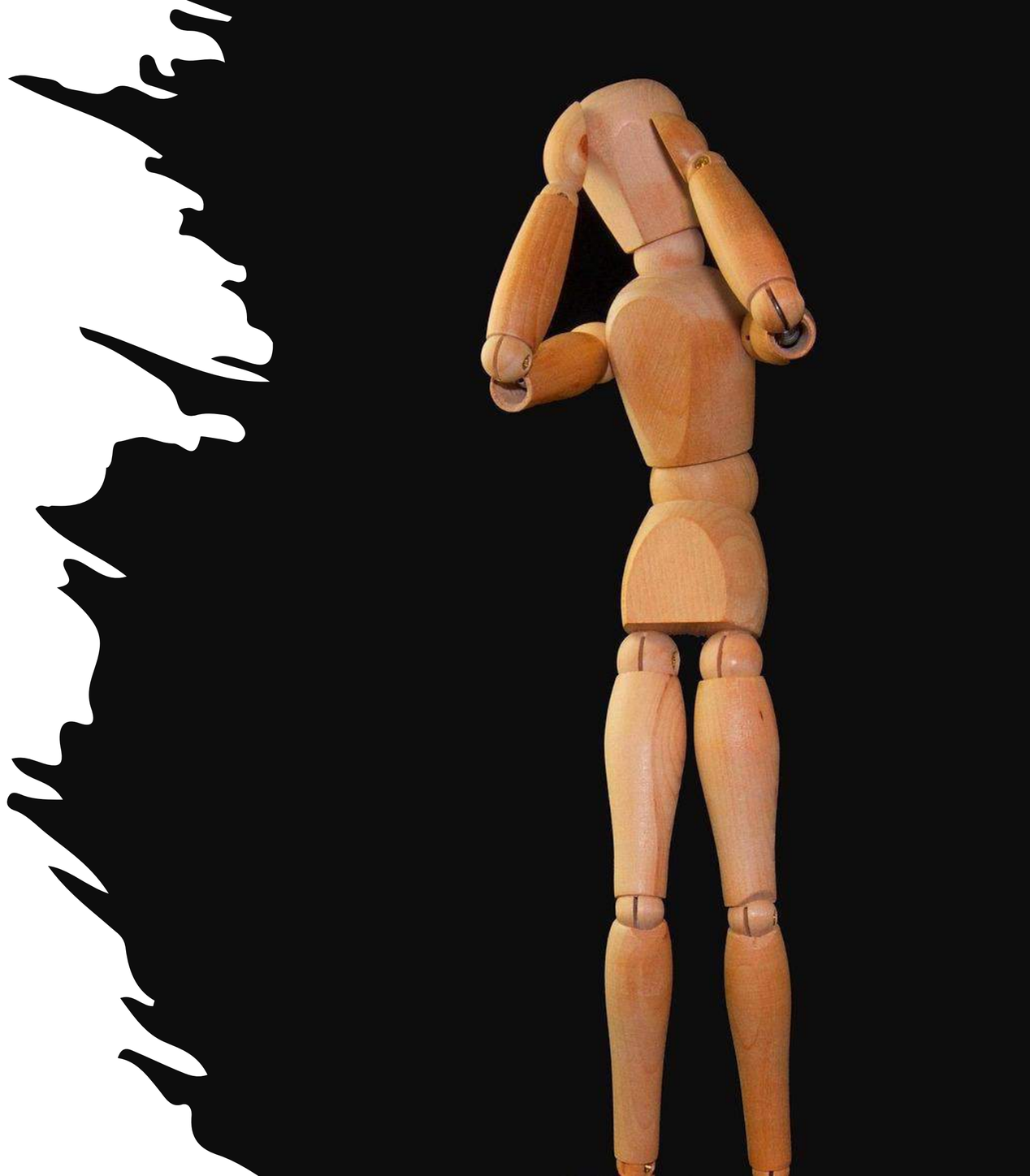
1. Ne visas otrā faktora opcijas ir vienlīdz drošas – SMS kodi ir nedrošāki par autentifikācijas lietotnēm
2. Nedalieties ar saviem SMS, autentifikācijas lietotņu kodiem ar citiem – tos ievadīt tikai paredzētajās vietās!

Jums tagad ir daudz drošu paroļu:

- M@zie-m1rkli-Iecava!
- L3ni l3ni gulbji sl1d
- strauja-x2-upe-T3cej
- …

Sistēmu un tīmekļu vietņu ir tik daudz. Katrai parolei ir savi ķeburi pievienoti, lielie burti dažādās vietās….

Kā tās visas atcerēties?



Attēls: https://pixabay.com/photos/figure-man-to-stand-headache-think-1703631/

Paroļu pārvaldnieks

Paroļu pārvaldnieks – kas tas tāds?

Tā ir specializēta programma Jūsu paroļu drošai glabāšanai.

Tas nozīmē, ka tā vietā, lai atcerētos visas paroles, Jums ir **jāzina tikai** viena **galvenā** (angļu val. *master*) **parole**.

Kuru izvēlēties?

Dažādi paroļu pārvaldnieki atšķiras:

- ar cenu (maksas/ bezmaksas)
- pieejamajām papildu funkcijām
- drošības līmeni (noteikti izpētiet, vai pārvaldniekam nav bijušas datu noplūdes vai citi skandāli, kā tas ir *LastPass* gadījumā)

1Password DASHLANE bitwarden KEEPER Proton Pass

Mazie paroļu pārvaldnieku baušļi

Tas, ka izmantosiet paroļu pārvaldniekus **nenozīmē**, ka Jūsu paroles būs drošībā. Paroļu pārvaldnieks ir tikai tik drošs, cik droši mēs to izmantojam! **Pievērsiet uzmanību**:

1. Jūsu paroļu pārvaldnieka galvenajai parolei jābūt drošai – ja tā būs «madara123», «biblioteka» vai ««qwerty», tad ātri vien ļaundari varēs piekļūt visām parolēm. Tāpat šo paroli nerakstām uz līmlapiņām un neatstājam labi redzamās vietās!
2. Apskatiet pārvaldnieku iestatījumus. Šobrīd ieteicams atspējot automātiskās aizpildes funkciju (angļu val. *autofill*). Tapāt izvērtēt pārvaldnieka noildzes iespējas, tas ir, pēc cik ilga laika krātuve aizslēdzas.

Lai Jūsu dati būtu drošībā, drošības pasākumi ir jāveic pareizi!

Par parolēm un paroļu pārvaldniekiem viss ir skaidrs.
Bet kas ir šie kaitinošie atgādinājumi?

Atjauninājumi

Ļaunatūra

Jebkura veida ļaunprātīga programmatūra, kas paredzēta, lai kaitētu vai iegūtu nesankcionētu piekļuvi datoram, tīklam vai ierīcei.

Vīrusi	Programma, kas ir piesaistīta likumīgai programmatūrai un izplatās ar lietotāja mijiedarbību
Trojieši	Ļaunprātīga programma, kas maskējas kā likumīga programmatūra
Tārpi	Pāšizplatāmas ļaunatūras, kas inficē sistēmas bez lietotāja iejaukšanās
Spiegprogrammatūra	Slepeni uzrauga lietotāja darbības un nozog informāciju

Vēl viena ļaunatūra:
Izspiedējvīruss

Tipiski tiek šifrēti uzņēmuma dati, par to atšifrēšanu prasot atlīdzību.

Ļaunatūras izplatīšana

Inficētas tīmekļa vietnes un ievainojamas programmatūras

E-pasta pielikumi

Lejupielādes

Regulāri atjaunojumi

- Visu – operētājsistēmu, programmatūru, telefona lietotnes – regulāri atjaunināt

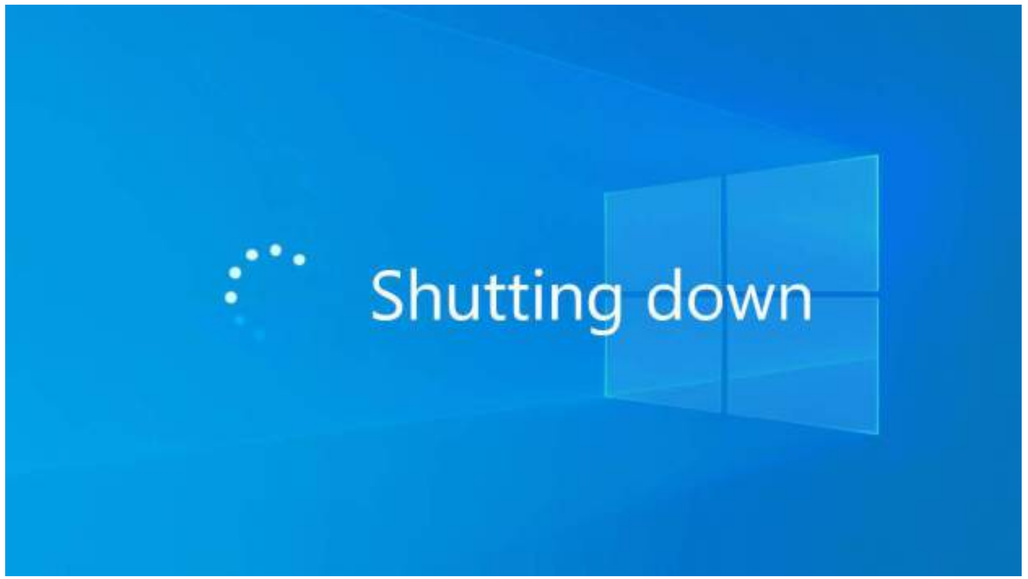
- Izmantot automātiskos atjauninājumus, kur šāda iespēja pastāv

Attēls: https://www.pugetsystems.com/support/guides/how-to-manually-install-windows-10-updates-1171/

Pievēršam uzmanību

! 2025. gada 14. oktobrī tiek **pārtraukts atbalsts Windows 10** (Windows 10 vairs nesaņems drošības atjauninājumus un Microsoft nenodrošinās tehnisko palīdzību)! !

Vairāk: https://www.microsoft.com/en-us/windows/end-of-support



Attēls: https://www.laptopmag.com/laptops/windows-laptops/windows-10-end-of-support-app-extension

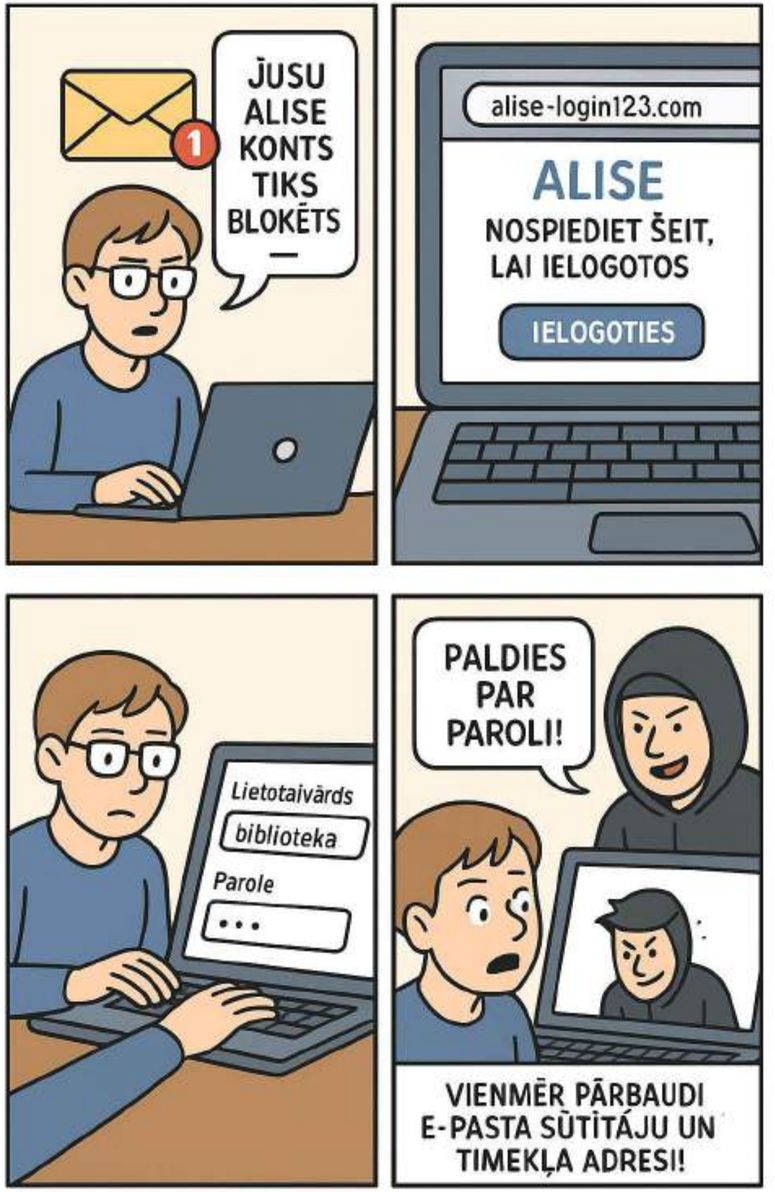
Dators ir atjaunināts. Tagad noskan signāls – ir pienākusi jauna vēstule.
Kāpēc man ir uzrakstījis prezidents?

E-pastu un komunikācijas drošība

Pikšķerēšana un sociālā inženierija

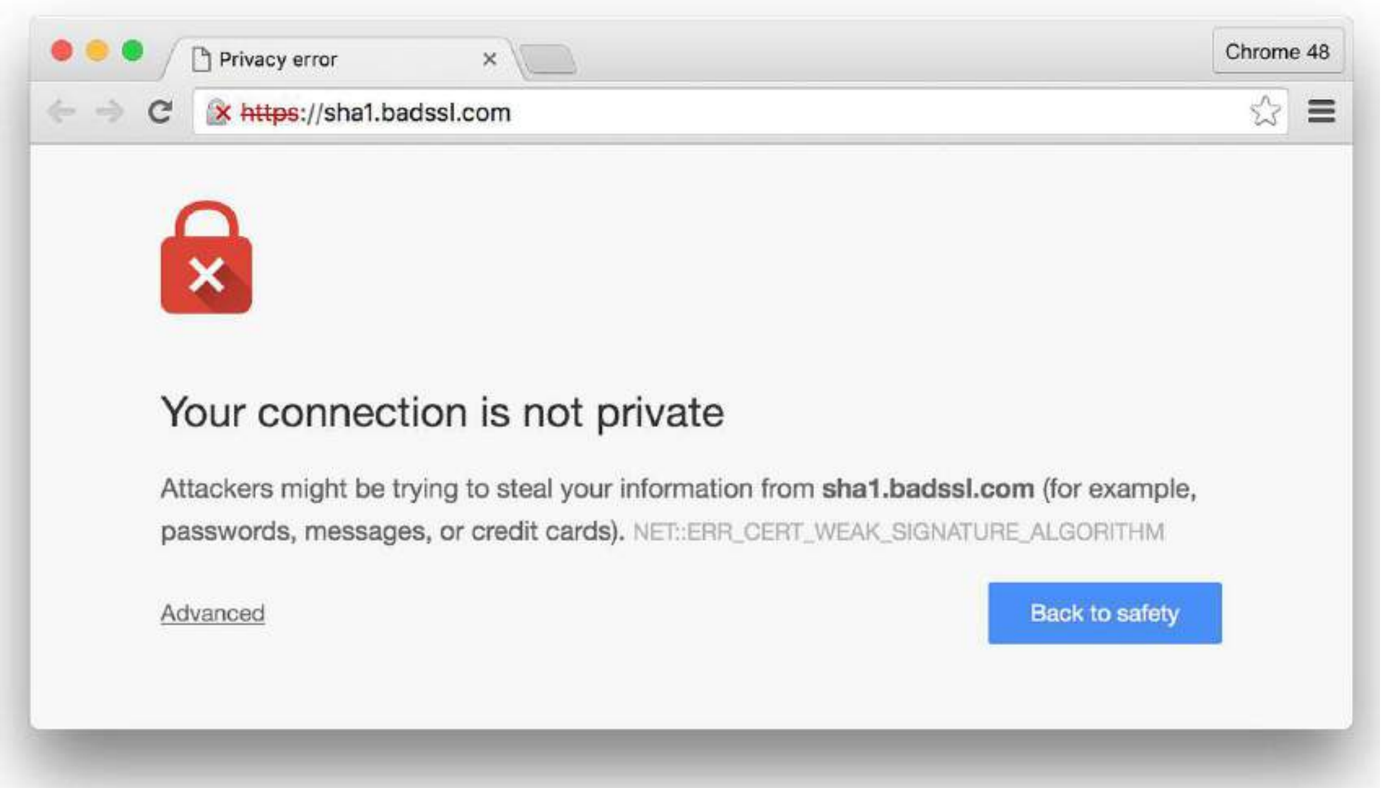
Sociālā inženierija – psiholoģiska manipulācijas metode ar mērķi apmānīt cilvēku.

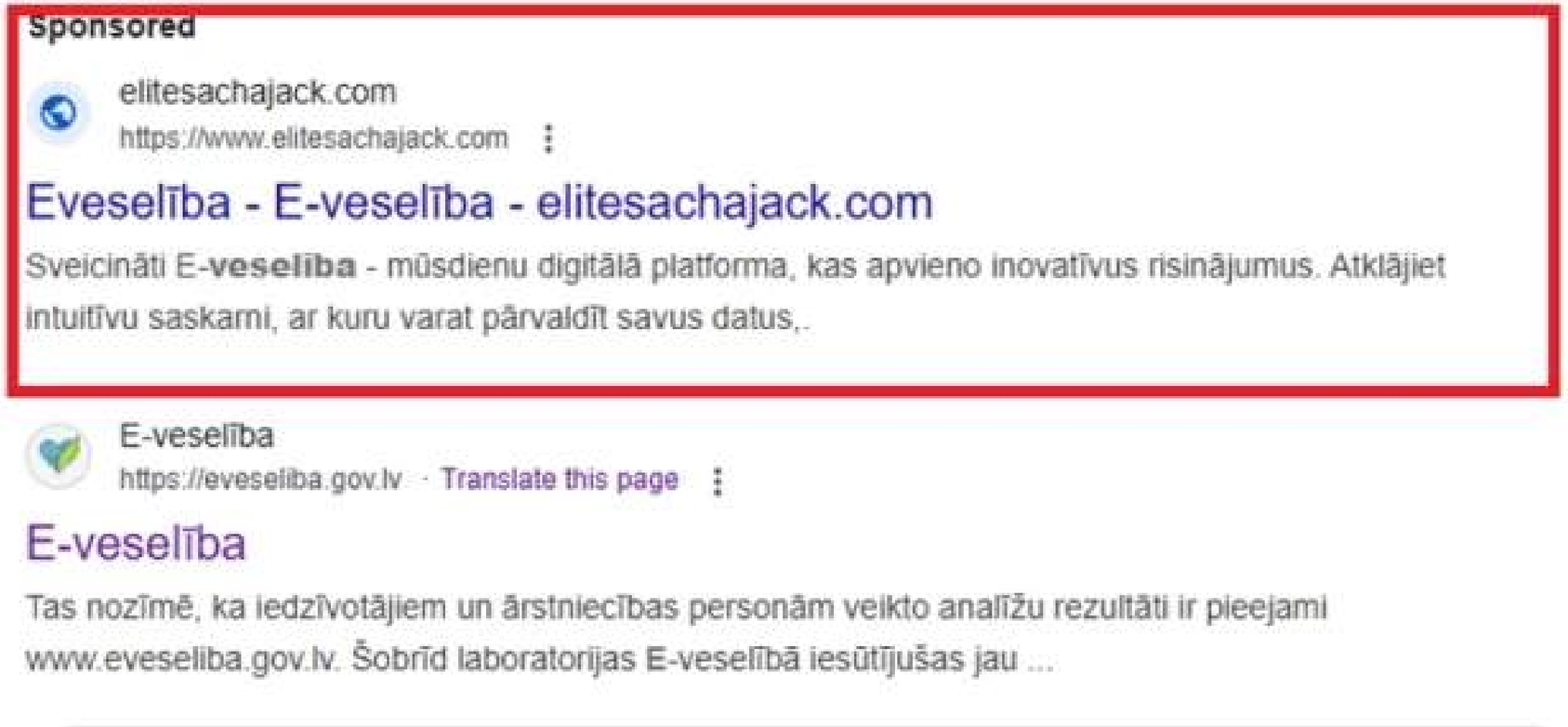
Pikšķerēšana - Informācijas zādzība, uzdodoties par uzticamu servisu



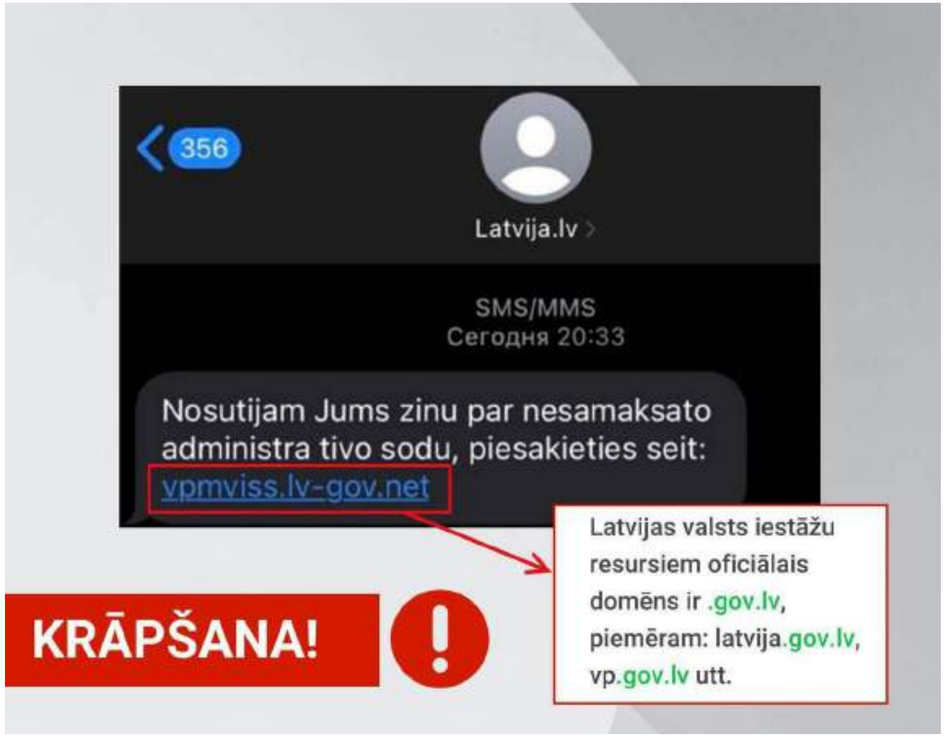
Nedrošas mājaslapas

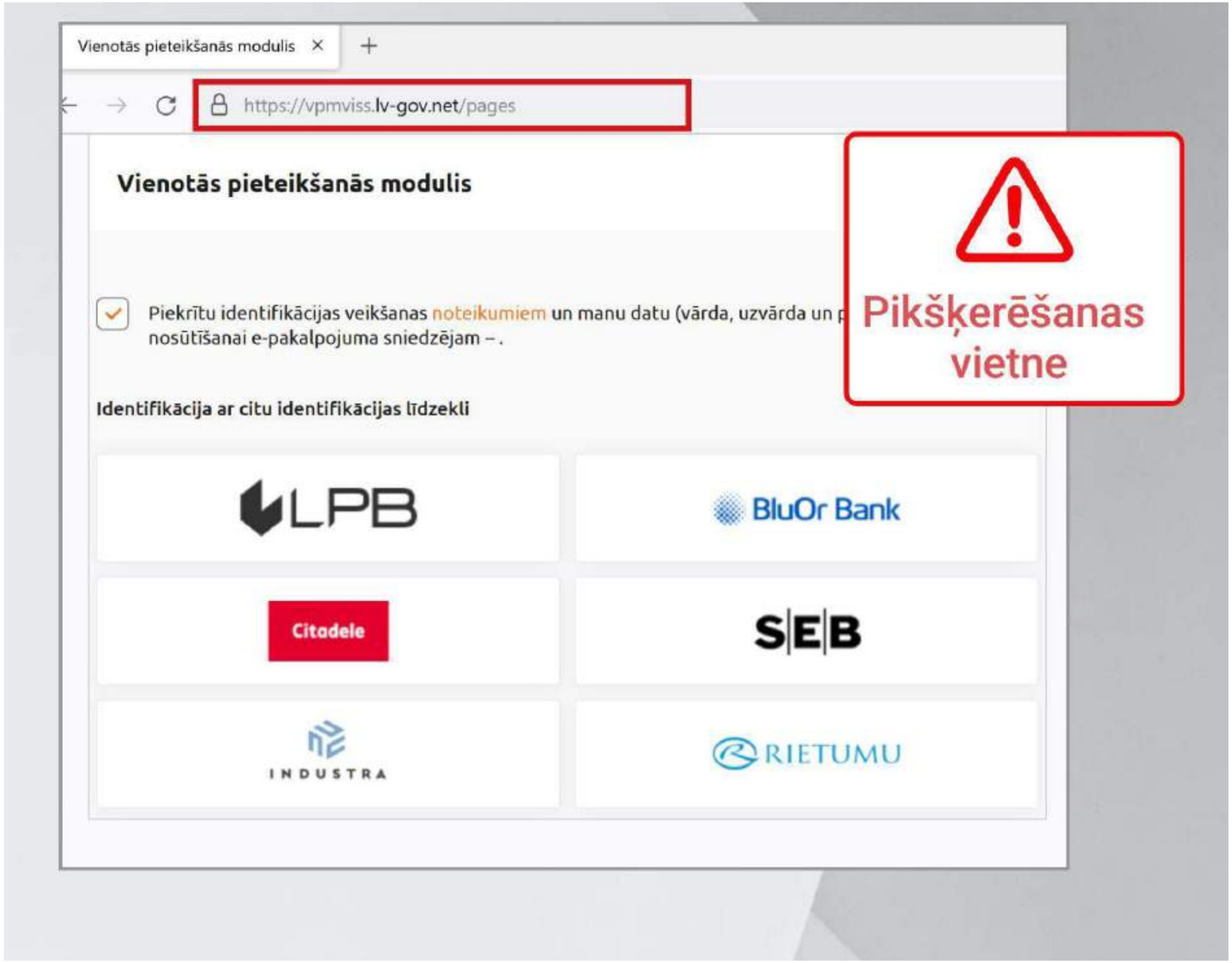
- Viens no veidiem kā iegūt ļaunatūru savā ierīcē
- Kā arī pārlūkprogrammas pārtveršana (nevēlamas reklāmas, jauni logi)
- Identitātes zādzība personiskās informācijas zagšanai





Avots: https://jauns.lv/raksts/zinas/648147-neiekriti-krapnieku-nagos-aktivizejusies-krapnieki-kuri-veido-viltus-majaslapas

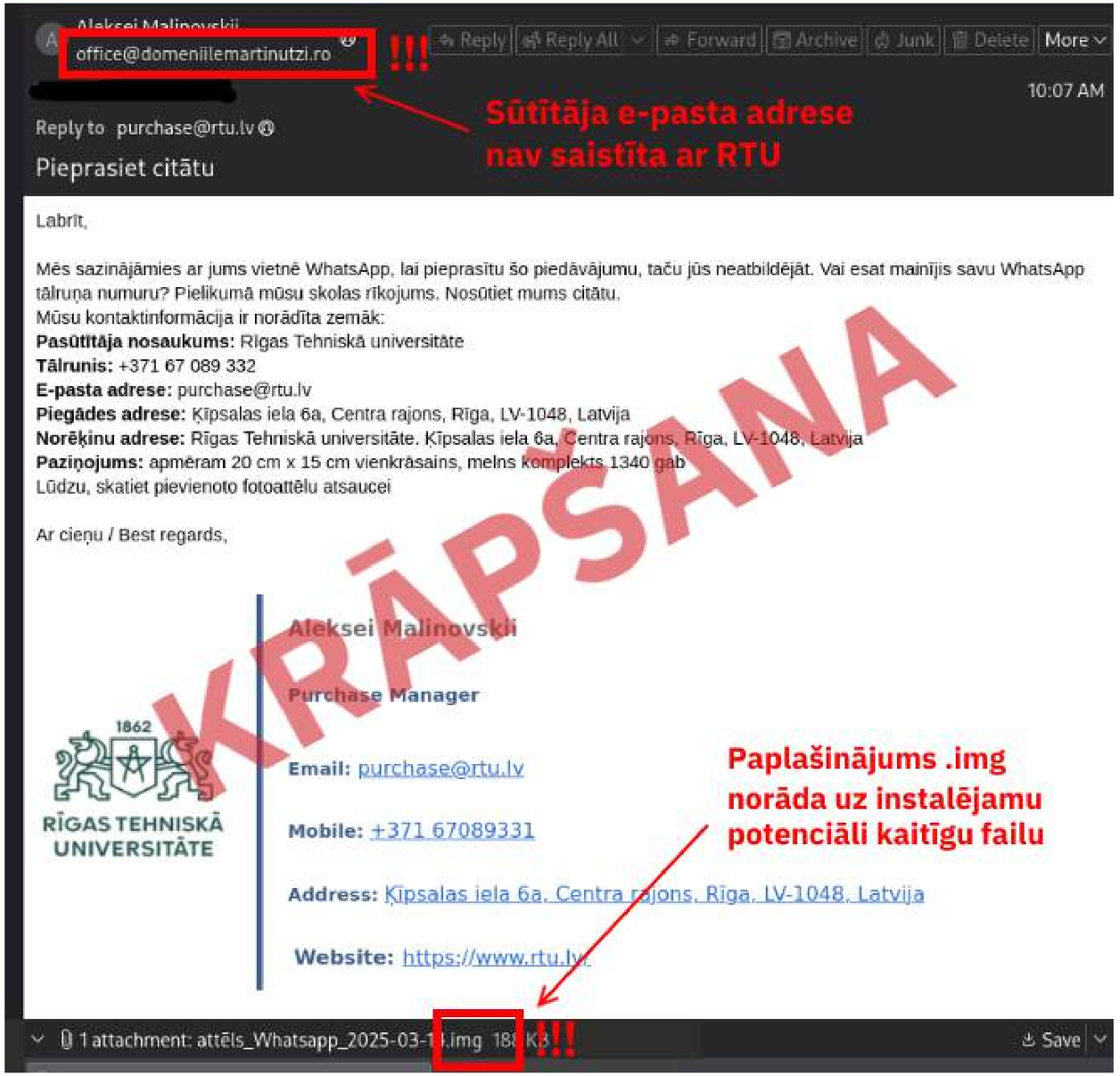




Avots: https://www.facebook.com/photo/?fbid=631131799056163&set=pcb.631133282389348

E-pastu drošība

- Izvairīties no saišu un pielikumu atvēršanas no nezināmiem un aizdomīgiem e-pastiem (bieži krāpnieki uzdodas par zināmām organizācijām!)
- Pārbaudīt sūtītāja identitāti, pirms tiek nosūtīta sensitīva informācija



Avots: https://cert.lv/lv/2025/03/launatura-rtu-varda

Kā atpazīt pikšķerēšanu

Dažas **kopīgās iezīmes**:

- E-pasta vai ziņas saturs parasti rada steidzamības sajūtu, aicina rīkoties nekavējoties
- Bieži novērojamas gramatikas un valodas stila kļūdas
- Aizdomīgs e-pasta izsūtīšanas laiks, piemēram, plkst. 2.00 naktī
- E-pastā norādīta saite, kurā tiek aicināts reģistrēties vai ievadīt datus
- Vēstule tiek sūtīta nevis no oficiāla darba e-pasta, bet privātā, piemēram, swebank@gmail.com vai info@rtu.ru
- Pikšķerēšanas uzbrukumiem ļaundari izmanto ne tikai e-pastu, bet arī telefona zvanus un citus komunikācijas kanālus – Facebook, WhatsApp utt.
- Negaidīti e-pasti ar pielikumiem
- Neierasti pielikumu paplašinājumi, piem., .exe, .rar., .zip, .img, .iso, .rdp

Sociālās inženierijas tehnikas

Cilvēki bieži pieņem lēmumus, balstoties uz emocijām. Tāpēc uzbrucēji cenšas ierosināt:

- **Steidzamību** (tūlīt samaksājiet sodu, citādi jums būs lielākas nepatikšanas)
- **Dusmas** (parasti saistītas ar politikas, vides, sociāliem jautājumiem)
- **Ziņkārību** (jūsu sūtījums nav piegādās, nospiediet šo saiti, lai uzzinātu vairāk..)
- **Uzticību** (uzdodoties par zināmām organizācijām, cilvēkiem)
- **Patīkamu satraukumu** (Jūs esat saņēmis balvu!)
- **Empātiju** (palīdziet Kalifornijas ugunsgrēkos cietušajiem, ziedojot naudu Ukrainai)

Rezerves kopiju veidošana

Kāpēc veidot rezerves kopijas?

Ja nevēlies, lai Jūsu dati neatgriezeniski zūd, veidojiet rezerves kopijas.

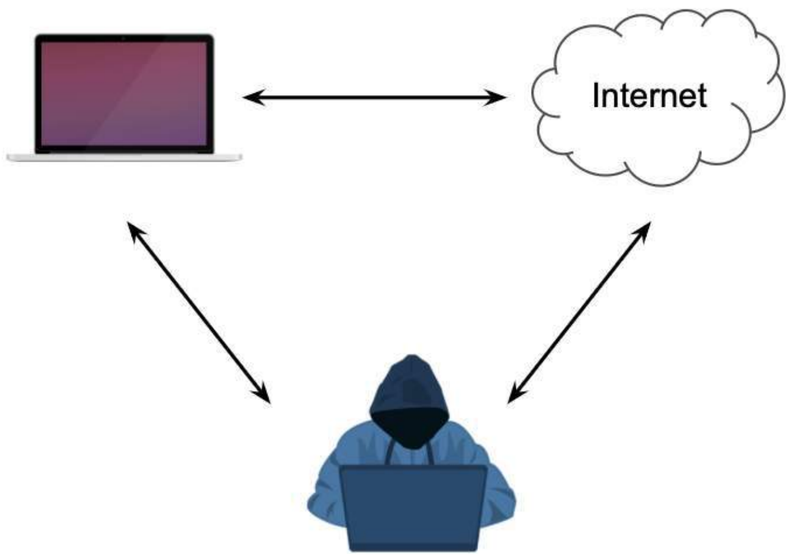
Pievērs uzmanību:

- Regulāri veidojiet rezerves kopijas (ārējā diskā vai mākonī)
- Pārliecinies, ka rezerves kopijas tiek glabātas droši
- Ārējos diskus un citus datu nesējus iespējams šifrēt

Publisko tīklu izmantošana

Draudi publiskajos tīklos

Oriģinālais savienojums



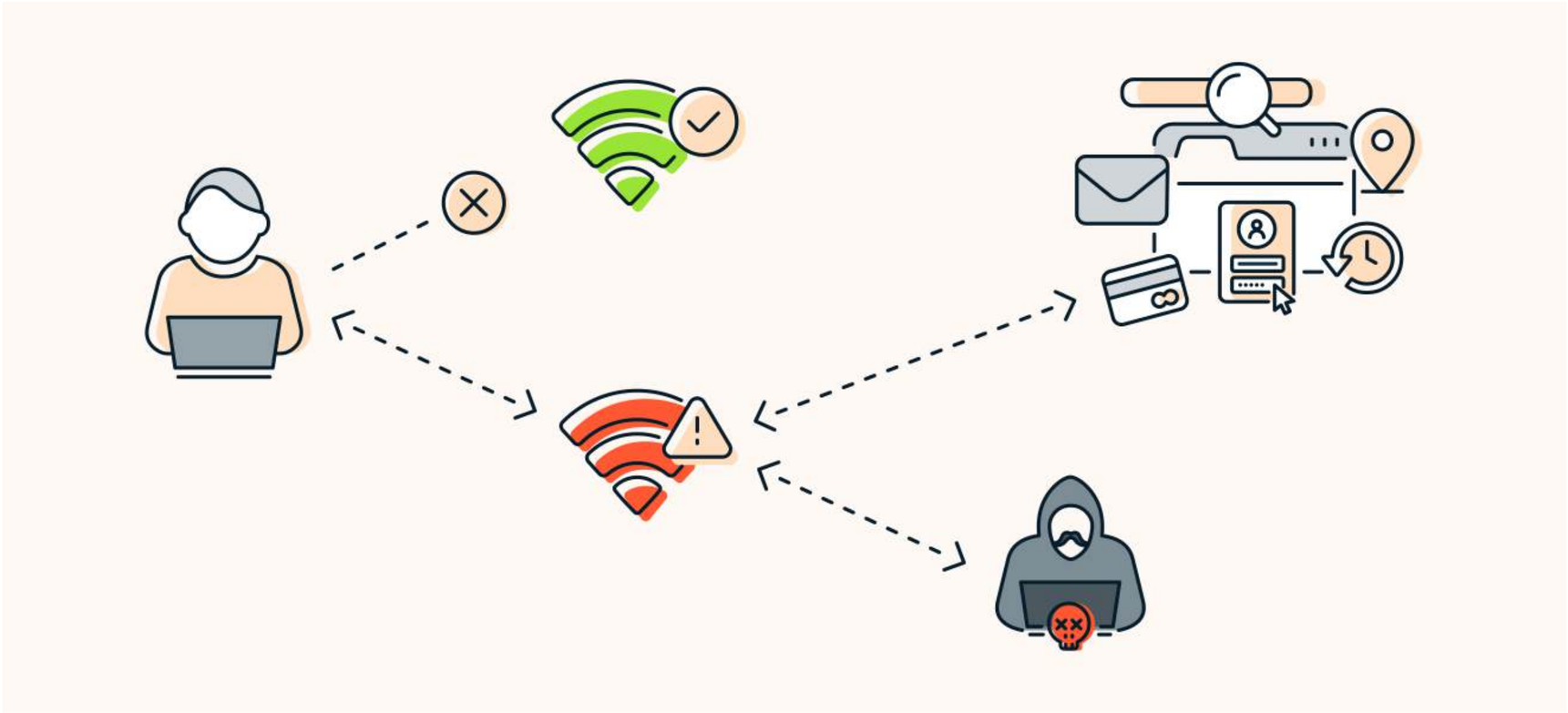
Uzbrucējs pārvirza plūsmu caur savu ierīci un var tos novērot

Datu pārtveršana
Uzbrucējs redz darbības tīklā un, ko dara lietotājs (piem., ievada paroli)

Sesijas pārtveršana
Uzbrucējs var nozagt sesiju, piem., e-pasta, un iekļūt lietotāja kontā

Draudi publiskajos tīklos

Viltus Wi-Fi punkti
Uzbrucējs izveido savu Wi-Fi punktu un redz visu, ko dara lietotājs



Ko ievērot izmantojot publiskos tīklus?

- Atvērtos publiskos WiFi tīklus izmanto tikai izklaides mērķiem, nepiereaksties svarīgos profilos vai kontos
- Ja ir iespējams, izmanto VPN pieslēgumu, lai aizsargātos no datu pārraides pārtveršanas /iejaukšanās
- Pievērs uzmanību, vai **HTTPS** darbojas, un web adrese tiek korekti atspoguļota
- Strādājot attālināti, izmantot VPN, lai pieslēgtos darba resursiem, un vairāku faktoru autentifikāciju
- Neveic finanšu darbības publiskajos tīklos!

Antivīrusi

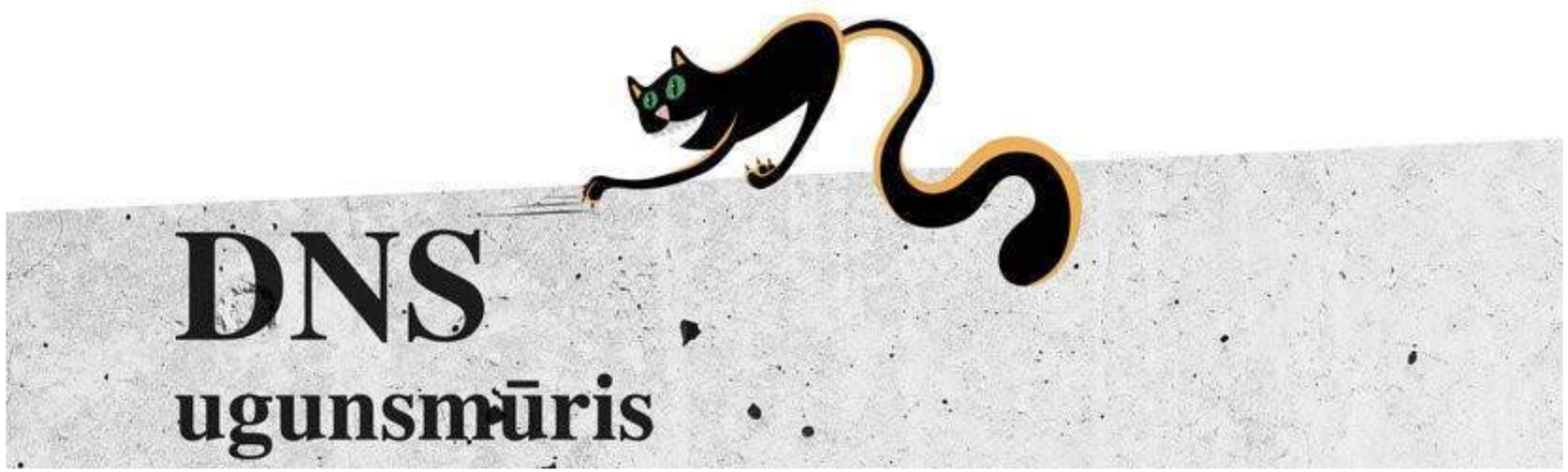
Kas jāzina par antivīrusiem?

- Instalē atzītas antivīrusu un pretļaunatūras programmas
- Regulāri skenē ierīces, lai identificētu un noņemtu draudus (Windows datoru noklusējuma antivīrusu programma pati regulāri skenē datoru)

Kā vēl sevi aizsargāt?

https://dnsmuris.lv

Iespējams uzstādīt uz gan konkrētām iekārtām, gan mājas maršrutētājā.
Pieejamas arī lietotnes Android un iOS telefoniem.
Aizsargā pret viltus banku lapām, krāpnieciskām tirdzniecības platformām, vīrusu izplatošām vietnēm u.c.



Personīgās informācijas izpaušana

Cik daudz informācijas par mani ir citiem?

- Apdomā, kādu informāciju par sevi izplati sociālajos tīklos un citur tiešsaistē
- Apskati privātuma iestatījumus sociālajos tīklos un citos tiešsaistes pakalpojumos

Ierīču un kontu uzraudzība

Kam jāpievērš uzmanība?

- Regulāri apskaties savus finanšu kontus un citus tiešsaistes profilus, pievēršot uzmanību aizdomīgām darbībām
- Pievērs uzmanību paziņojumiem par jaunu pieteikšanos savos kontos

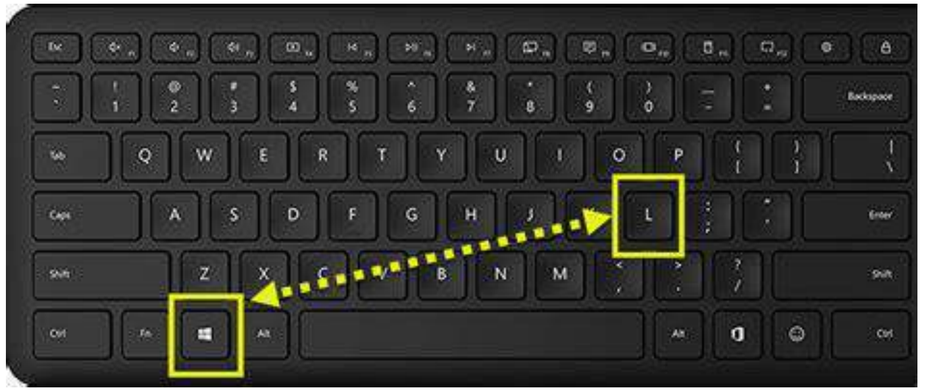
! Esiet vērīgi, ļaundari veido pikšķerēšanas e-pastus, kas līdzinās drošības paziņojumiem !

Īsts

Citi svarīgi aspekti

- Ierīču fiziskā drošība:
  - datora ekrānu nepieciešams aizbloķēt (**Control-Command-Q** MacBook un **Windows + L** Windows datoriem)
  - savas ierīces neatstāt publiskā vietā bez uzraudzības
  - telefoniem iespēja uzlikt privacy screen (aizsargā no tā, ka kāds pāri plecam noskatās, kā ievadāt paroles utt.)
- Droši atbrīvoties no ierīcēm, nodzēšot visus datus (veicam *factory reset*)
- Pārskatīt privātuma iestatījumu dažādām lietotnēm (*vai kameras lietotnei ir nepieciešama mana atrašanas vieta?)*
- Nesaglabāt paroles pārlūkā
- Uzmanīgi apieties ar svešiem USB zibatmiņām (tās var saturēt vīrusus)
- Pēc iespējas nodalīt darbu no privātās dzīves (darba aprīkojumu neizmantojam privātām vajadzībām, nenododam savas darba ierīces izmantot citiem)
- ...

Taustiņu kombinācijas datora aizslēgšanai:



Windows datoriem

MacBook datoriem

Ziņošana par incidentu

- Ja incidents noticis uzņēmumā/ organizācijā – ziņot atbildīgajai IT personai vai vadībai

- Ja incidents skāris konkrētu personu – ziņot **CERT.LV** rakstot uz cert@cert.lv vai zvanot uz +371 67085888
- CERT.LV speciālisti var palīdzēt saprast, kā incidents ir noticis un ko darīt, lai tas vairs neatkārtotos
- Krāpniecības gadījumā (atklājāt krāpniekiem savus internetbankas datus, krāpnieki izmanto Jūsu internetbanku pārskaitījumu veikšanai u.c.) – pēc iespējas ātrāk **sazinies ar banku**
- Finansiālu zaudējumu gadījumā nepieciešams rakstīt iesniegumu **Valsts policijai**, kas veiks izmeklēšanu

MI izmantošana

- Nedalieties ar personīgo informāciju un informāciju, kas nav brīvi pieejama tīmeklī.
- Izvērtē privātuma iestatījumus (piem., izslēgt tērzētavas saglabāšanu)
- Uzmanies no viltus MI rīkiem un pārlūka spraudņiem (angļu val. *browser extensions*)

Attēls: https://www.intuz.com/blog/guide-to-building-an-ai-chatbot

Kvikšķerēšana!?

Kvikšķerēšana ir krāpšanas shēmā, kurā tiek izmantots **QR kods**.

Skenējot QR kodu:

- Pievērs uzmanību, kur QR kods atrodas (QR kods bez paskaidrojumiem un gaismas staba vai QR kods aptaujai kādā pasākumā).
- Pievērs uzmanību, uz kādu mājaslapu noved QR kods
- Ja tiek prasīts lejupielādēt jaunu lietotni, tad to noteikti nedarīt
- Ja tiek prasīts ievadīts bankas datus, paroles, PIN kodus, citu sensitīvu informāciju, tad noteikti to nedarīt

Avots: https://www.cert.lv/lv/2024/04/krapnieki-aktivi-izmanto-qr-kodus-kas-jazina-par-kvikskeresanu

Viss it kā apgūts.
Ko darīt tālāk?

Turpiniet izglītoties!

https://www.esidross.lv/

- Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

“Saldas” runas un tukšs maciņš: Romantiskas investīciju krāpšanas OUCH! 02/2025

Turpiniet izglītoties!

https://cert.lv/lv

- Ieteikumi lietotājiem
- Ikmēneša kiberlaikapstākļu pārskats par aizvadītā mēneša spilgtākajiem notikumiem Latvijā
- Statistika par kiberuzbrukumiem
- Informāciju par pasākumiem
- Brīdinājumus par ievainojamībām, krāpšanām

Turpiniet izglītoties!

Dažādi īsformas video par kiberdrošību, krāpšanu un tehnoloģijām

Elvis Strazdiņš: video par kiberdrošību un tehnoloģijām:

- https://www.youtube.com/@elnormous
- https://x.com/elnormous
- https://www.tiktok.com/@elnormous

Ambex.lv:

- https://www.tiktok.com/@ambex.lv

Zināšanu nostiprināšana

Pieejami dažādi tiešsaisti testi zināšanu pārbaudei:

Latviešu valodā:

- LMT un CERT.LV izglītojošais tests: https://lmt.lmt.lv/drosiba
- CERT.LV kiberdrošības rokasgrāmata (aprakstīta laba prakse + jautājumi izpratnes pārbaudei): https://rokasgramata.esidross.lv/rokasgramata/darbiniekiem/darbiniekiem-interneta-lietotajiem/
- Seb kiberkvests: https://www.seb.lv/kiberkvests

Angļu valodā:

- ENISA pikšķerēšanas tests: https://cybersecuritymonth.eu/quiz
- Google kiberhigiēnas testu: https://phishingquiz.withgoogle.com/
- Google «Interland» spēle bērniem: https://beinternetlegends.withgoogle.com/en_ie/interland

10 kiberdrošības pamatprincipi

1. Drošu paroļu izmantošana
2. Divu faktoru autentifikācijas izmantošana
3. Regulāra programmatūras atjaunināšana
4. Piesardzība ar e-pastiem un saitēm tajos
5. Rezerves kopiju veidošana svarīgiem datiem
6. Droša WiFi tīkla izmantošana
7. Antivīrusu un pretļaunatūras programmatūru izmantošana
8. Sevis un citu izglītošana
9. Ieturēta personīgās informācijas izplatīšana
10. Savu ierīču un kontu uzraudzīšana

Laiks pārbaudīt Jūsu gatavību drošam darbam!

Jautājumi?

KIBER Academy Of Cybersecurity

1862 RĪGAS TEHNISKĀ UNIVERSITĀTE

Google