



Funded by the
Erasmus+ Programme
of the European Union

Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem

Proaktīvā rīcība

Safeguarding against Phishing in the age of 4th Industrial Revolution

www.cyberphish.eu

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Apmācību mērķis



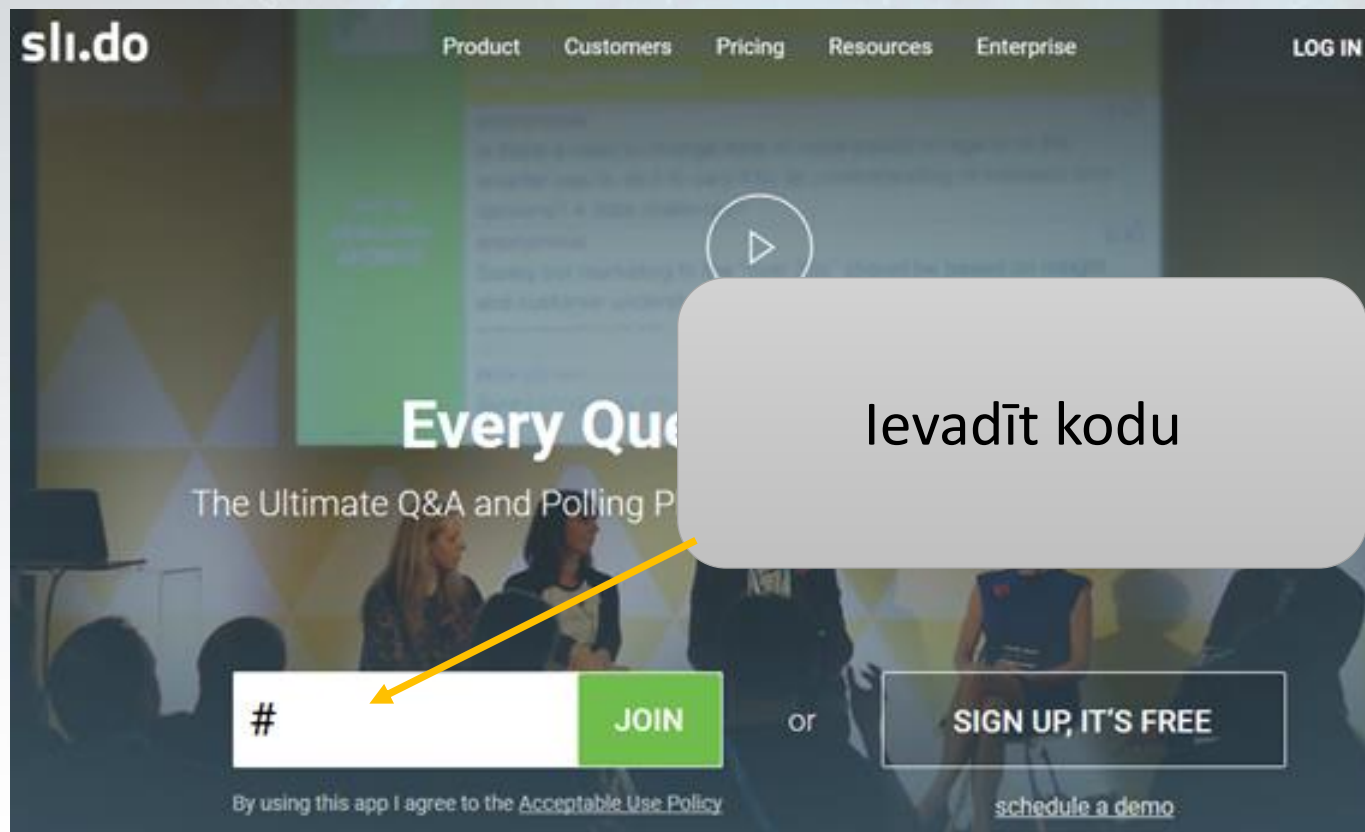
Kibernētiskā higiēna internetā
Kibernētiskā higiēna darba vietā
Tehnoloģiskie instrumenti un pasākumi

Kursantu darba slodze



Lekcija	2 st.
Audio un video materiāli	1 st.
Pētījumi	0,5 st.
Papildu lasīšana	1,5 st.
Sagatavošanās eksāmenam	1 st.

*Praktiskais vingrinājums: norādiet pēc iespējas vairāk īpašības vārdu vidē
sli.do saistībā ar interneta un digitālo ierīču drošību*





USERNAME:

Administrator

PASSWORD:

•••••

LOGIN

Interneta kibernetiskā higiēna

Digitālie pēdu nospiedumi

- Saglabātā informācija par jebkādām lietotāja darbībām: apmeklētajām vietnēm, skatītajiem profiliem vai fotoattēliem, aizpildītām veidlapām, reģistrācijām iepazīšanās vietnē, instalētajām lietotnēm utt.
 - **Aktīvie pēdu nospiedumi** — informācija, ko mēs brīvprātīgi un apzināti augšupielādējam un atstājam (fotoattēli, ziņas, komentāri)
 - **Pasīvie pēdu nospiedumi** – informācija, ko mēs atstājam neapzināti, bieži vien to pat nezinot vai nesaprotot (IP adrese, meklēšanas vēsture, ģeogrāfiskās atrašanās vietas dati)



Personas dati

Personiskā informācija ir informācija, kas nosaka attiecības starp konkrētu informāciju un personu.*



** Malinauskaite Van De Kastela, Inga [Malinauskaitē-van de Castel, Inga]. Datu subjektu tiesības virtuālajos sociālajos tīklos: promocijas darbs. – Viļņa, 2017. gads.*

Kas ir personas dati?

- Personas kontaktinformācija (t.i., vārds, uzvārds, mājas adrese, mobilā tālruņa numurs)
- Biometriskie dati
- Personas kods
- Personas ID vai pases kods
- Personas ienākumi
- Paroles
- Finanšu dati
- Klientu dati
- Intelektuālie dati bez īpašnieku atļaujas



Kas ir publiski dati?

- Publiski dati var būt:
 - Uzņēmuma reģistrācijas numurs
 - Uzņēmuma e-pasts, piemēram info@company.com
 - Depersonalizēti dati
 - Segvārds
 - Hobiji
 - Dabas fotogrāfijas
 - Emuāri (blogi)
 - ...



Kāpēc ir svarīgi nepublicēt personas datus?

- Identitātes zādzības
- Kibernoziegumi (zādzība, šantāža, uzmākšanās)
- Potenciāls kaitējums reputācijai:
 - Ikviens interneta lietotājs var piekļūt brīvi pieejamiem datiem
 - Publicētie dati tiek izmantoti pret personu
- Jo vairāk informācijas tiek publicēta internetā, jo lielākā mērā krāpnieki var nozagt personas identitāti, izmantot datus uzbrukumiem utt.



Pārbaudiet, kāda informācija par jums ir pieejama

- Izmantojiet meklētājprogrammu, lai meklētu sevi tiešsaistē un redzētu, kādu informāciju varat atrast
- Pārbaudiet informāciju par sevi, izmantojot dažādas meklētājprogrammas
 - Google
 - Bing
 - DuckDuckGo
- Veicot meklēšanu, izmantojiet pēdiņas un citus simbolus, piemēri:
 - “Vārds, uzvārds” – iegūsiet informāciju par šo personu
 - “Vārds, uzvārds@” – iegūsiet e-pasta adreses, kas saistītas ar šo personu
 - “Vārds, uzvārds” faila tips: PDF – jūs iegūsiet PDF dokumentus, kuros šī persona ir pieminēta

Fotoattēlu publicēšana

- Vai esat domājis par:
 - kam ir piekļuve jūsu fotogrāfijām?
 - Vai fotogrāfijās ir citi cilvēki?
 - Vai fotoattēlā ir saglabāta GPS informācija par atrašanās vietu?
- Izmantojot meklētājprogrammu, varat mēģināt atrast fotoattēlus ar jums



Fotoattēlu un video kopīgošana

- Cieniet citu cilvēku privātumu
- Ja vēlaties kopīgot fotoattēlu vai videoklipu ar jums pazīstamiem cilvēkiem, labas manieres noteiktu atļaujas lūgšanu pirms tam.
- Neizplatiet citu cilvēku bērnu fotogrāfijas bez viņu vecāku atļaujas
- Neizmantojiet cilvēku fotogrāfijas savos reklāmas materiālos, ja vien viņi nav devuši atļauju
- Fotografējiet svešiniekus tikai publiskās vietās. Ja persona ir skaidri paziņojusi, ka nevēlas tikt fotografēta, jūs nedrīkstat viņu fotografēt
- Nekopīgojiet fotoattēlus un videoklipus kā līdzekli atriebībai vai izsmieklam
- Nekopīgojiet vardarbīgus, naidpilnus vai aizskarošus fotoattēlus un videoklipus. Tas attiecas arī uz gadījumiem, kad vēlaties nosodīt vardarbību vai naidu
- Nekopīgojiet fotoattēlus un videoklipus, kuros jūs vai jūsu draugi vai radnieki tiek pieķerti, pārkāpjot noteikumus, uzvedoties nepiedienīgi vai pat pārkāpjot likumu

Fotoattēlu un video kopīgošana

- Ja atrodat savu vai savu radnieku fotoattēlu un nevēlaties, lai tas tiktu kopīgots, varat veikt šādus pasākumus
 - Sazinieties ar izdevēju (vietni) un pieprasiet attēla noņemšanu
 - Sazinieties ar sociālā tīkla administratoru un lūdziet noņemt fotoattēlu, izskaidrojot situāciju
 - Ja iepriekš minētās darbības nav palīdzējušas, sazinieties ar Personas datu aizsardzības inspekciju

Draugi sociālajos tīklos

Esiet gudrs un izvēlīgs, pieņemot lietotājus par draugiem sociālajos tīklos



Uzmanieties un esiet apzinīgi, publicējot jebkādu informāciju par sevi

- Viss, ko ievieņojat internetā, var būt pastāvīgi tajā pieejams
- Informācija var būt pieejama arhīvos, piem., <https://web.archive.org>
- Citi cilvēki var
 - saglabāt informāciju savās ierīcēs,
 - izdrukāt vai
 - atkārtoti publicēt informāciju internetā

Pārraugiet, kāda informācija par jums tiek publicēta internetā

- Iespējams pārraudzīt, vai tīmekļa lapās, emuāros, zinātniskajos pētījumos, forumos, Youtube tiek publicēta jauna informācija par lietotāju, izmantojot izmaiņu noteikšanas un paziņošanas pakalpojumus, piemēram, Google Alerts
- Google Alert sistēmā ir iespējams norādīt atslēgvārdus
- Kad tiek atrasti jauni rezultāti, lietotājs saņems paziņojumu e-pastā, vai lietotājs var jebkurā laikā skatīt rezultātus vietnē www.google.com/alerts



Pieprasījums noņemt personas informāciju no Google pakalpojumiem

- iespējams ziņot, sniedzot pilnīgu informāciju, lai saturs par jums tiktu noņemts no Google pakalpojumiem
- iespējams pieprasīt satura noņemšanu no šādiem Google pakalpojumiem

- ☐  Google Search
- ☐  Blogger/Blogspot
- ☐  Google Maps and related products
- ☐  Google Play: Apps
- ☐  YouTube
- ☐  Google Images
- ☐  A Google Ad
- ☐  Drive and Docs
- ☐  Google Photos and Picasa Web Albums
- ☐  Google Shopping
- ☐ See more products

Pārbaudiet, vai jūsu dati nav uzlaukti

- Iespējams pārbaudīt, vai jūsu e-pastā vai tālruņa e-pastā ir datu aizsardzības pārkāpumi, izmantojot tiešsaistes rīkus, piemēram, Vai mani dati ir uzlaukti?
- Iespējams arī pārbaudīt, vai jūsu parole nav uzlauzta <https://haveibeenpwned.com/Passwords>. Uzlauztās paroles var meklēt tiešsaistē, un ikviens var tās lejupielādēt

'--have i been pwned?

Datu pārkāpumu uzraudzība

- iespējams reģistrēties īpašos portālos, kas informē, vai lietotāja konts ir uzlauzts, piem., <https://monitor.firefox.com>

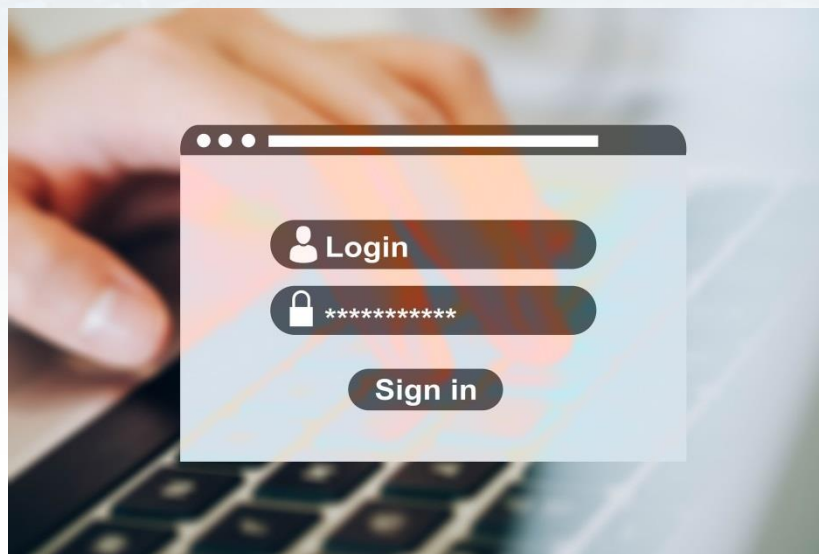


Vairāk informācijas: www.cnet.com/tech/services-and-software/firefox-monitor-shows-if-your-personal-information-was-lost-in-a-hack

<https://www.online-tech-tips.com/computer-tips/what-is-firefox-monitor-and-how-it-protects-your-login-details/>

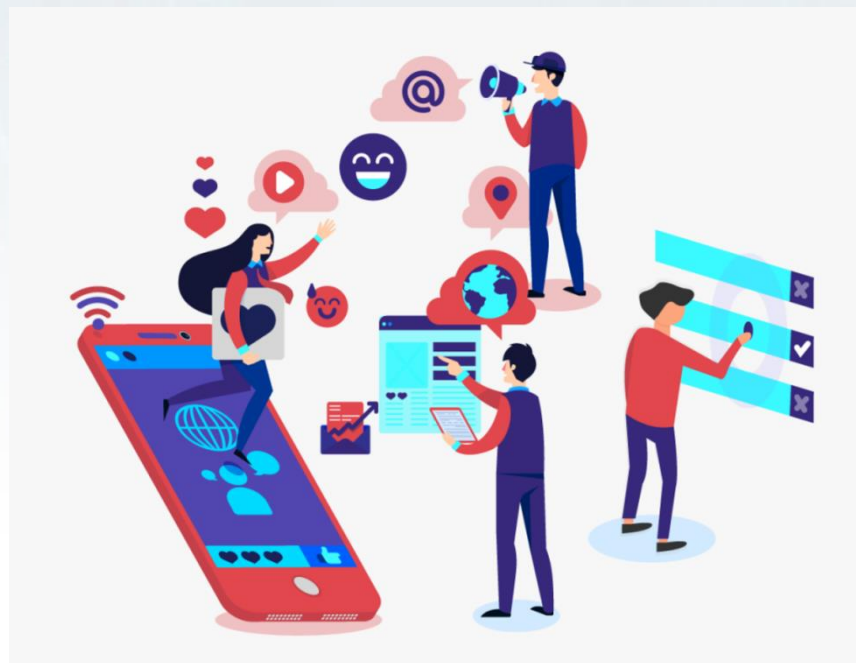
Pasākumi, ja jūsu konts ir uzlauzts

- Ja jūsu dati ir uzlauzti, tas nozīmē, ka jūsu e-pasts un parole varētu būt kibernoziēdnieku rokās. Tādā gadījumā jārīkojas sekojoši:
 - nekavējoties nomainiet uzlauztā konta paroli
 - nomainiet citu kontu paroles, ja izmantojāt to pašu paroli
 - iespējojiet divu faktoru autentifikāciju, ja pakalpojuma nodrošinātājs to atbalsta



Izvairieties no personas datu kopīgošanas

- Lietotājiem jābūt piesardzīgiem attiecībā uz sniegtās informācijas apjomu, jo parasti cilvēki vairāk informācijas dalās sociālajos tīklos
- Nepublicējiet savus plānus, mājas adreses, finanšu informāciju
- Pielāgojiet sava konta drošības iestatījumus un pārvaldiet, kas var redzēt jūsu ziņas un citu informāciju



Izmantojiet dažādas e-pasta kastītes dažādiem mērķiem

- E-pasts personīgajai dzīvei, piemēram name.surname@gmail.com
- E-pasts biznesa nolūkiem, piemēram name.surname@comapny-name.com
- E-pasts reģistrācijai dažādās vietnēs
 - iespējams izveidot kontu reģistrācijai bezmaksas e-pasta pakalpojumu portālos
 - iespējams izmantot pagaidu e-pasta pakalpojumu, piemēram [Guerrilla Mail](#), [Mailinator](#)

Neuzticieties, vienkārši pārbaudiet

- Esiet piesardzīgs, klikšķinot uz saitēm, kuras saņemat ziņās no draugiem
- Neticiet, ka ziņojums patiešām ir no personas, no kuras tas tiek apgalvots
- *IZLASIET, pirms noklikšķiniet uz kaut ko, lai lejupielādētu vai instalētu bezmaksas programmas*





Digitālo ierīču higiēna

Digitālo ierīču drošība

- Lietotājiem, izmantojot gan datorus, gan viedierīces, ir jāuzvedas atbildīgi un jāizmanto atbilstoši drošības pasākumi, jo viedierīcēm ir līdzīgas funkcijas kā galddatoriem vai portatīvajiem datoriem.
- Izmantojot šīs ierīces, var rasties tādas pašas drošības problēmas kā datoriem – datu zudumi utt.
- Viedierīces tāpat kā datorus var aizsargāt pret vīrusiem un citiem iespējamām tiešsaistes draudiem

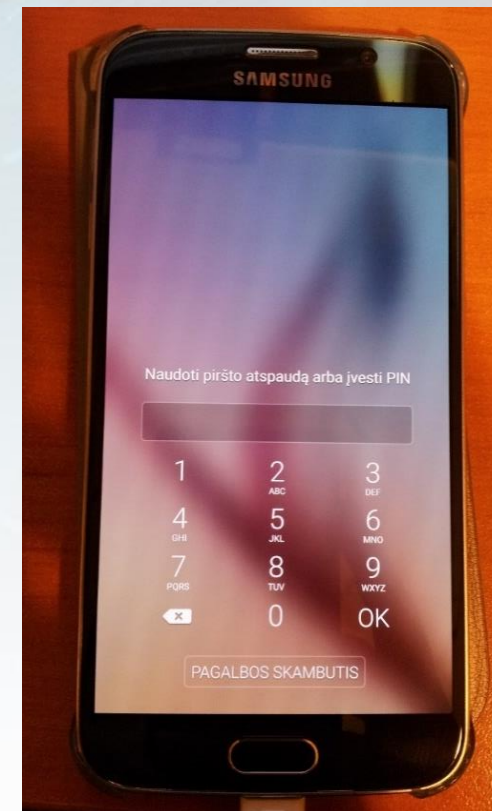
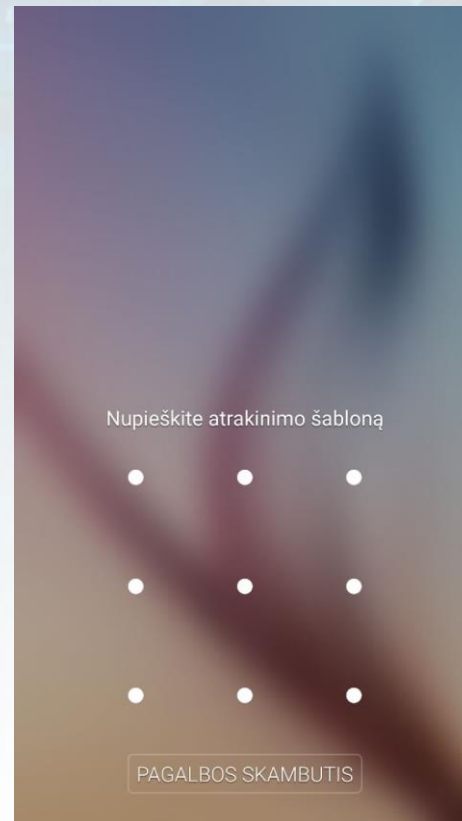


*Izmantojiet pieteikumvārdus un paroles, lai
izveidotu savienojumu ar digitālajām
ierīcēm*



Aktivizējiet PIN vai citas drošās pieteikšanās metodes

- Mobilajām ierīcēm ieteicams katru reizi pirms ierīces lietošanas aktivizēt savu PIN, lai nepieļautu, ka nepilnvarotas personas pārlūko jūsu ierīci, skata jūsu personas datus, fotoattēlus utt.
- Dažām ierīcēm ir citas drošas pieteikšanās funkcijas, piemēram, pirkstu nospiedumu skenēšana, acu zīlīšu skenēšana
- Iespējojiet automātiskās bloķēšanas funkciju, kad esat pabeidzis darbu ar ierīci



Privātā interneta pārlūkošana

- Atspējojiet trešo pušu sīkfailus (*angl. cookies*)
- Izmantojiet privātās pārlūkošanas režīmu
- Izmantojiet pārlūkprogrammas spraudņus (pluginus), piemēram, [HTTPS Everywhere](#)
- Izmantojiet virtuālā privātā tīkla VPN risinājumus, ja nepieciešams paslēpt datu plūsmu
- Pārbaudiet, ko Google par jums zina
<https://myactivity.google.com/myactivity>

Paroļu pārvaldības vadlīnijas

- Neizpaudiet savus lietotājvārdus un paroles citām personām, pat saviem kolēģiem
- Nekad neuzglabājiēt paroles piezīmēs, zīmītēs vai failos datorā vai mobilajā ierīcē
- Neizmantojiēt paroles, kas sastāv no vārdiem, adresēm, tālruņu numuriem un citiem viegli uzminamiem vārdiem
- Dažādiem kontiem izmantojiēt dažādas paroles
- Lai nodrošinātu labāku drošību, periodiski mainiēt paroles
- Izmantojiēt paroļu pārvaldniekus, lai aizsargātu savas paroles, piemēram, [Firefox Lockwise](#), [NordPass](#), [KeePass](#)

Pārbaudiet paroļu sarežģītību

The Password Meter

www.passwordmeter.com

safest9

Test Your Password	
Password:	●●●●●●
Hide:	☒
Score:	23%
Complexity:	Weak

MyPassword!5SafeAndStrong

Test Your Password	
Password:	12345678901234567890
Hide:	☒
Score:	100%
Complexity:	Very Strong

Padomi, atstājot darba vietu

- Pabeidzot darbu, atvienojieties (atslēdzieties) no informācijas sistēmām
- Pārlūka aizvēršana ne vienmēr nozīmē, ka jūs izrakstījāties
- Bloķējiet savu digitālo ierīci, kad atrodaties prom no ierīces pat neilgu laiku. Ja atstājat ierīci atbloķētu, citas personas var:
 - piekļūt jūsu informācijai bez atļaujas;
 - piekļūt konfidenciālai informācijai vai datiem;
 - Nosūtīt e-pastus no jūsu konta;
 - Izdzēst jūsu failus;
 - Veikt citas ļaunprātīgas darbības.

Ja izmantojat citas personas ierīci

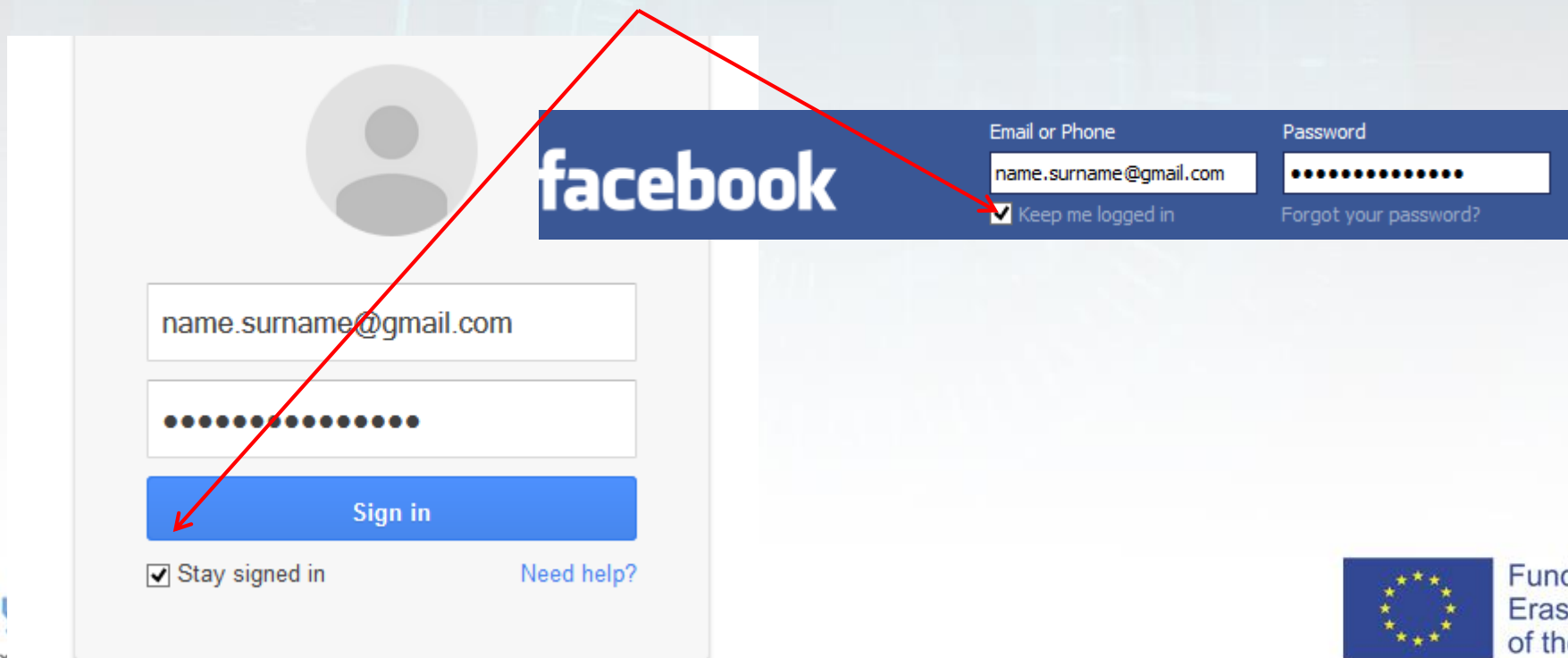
- Nomainiet izmantotā pakalpojuma paroli no uzticama datora un tīkla, ja izmantojāt kāda cita ierīci un jums ir aizdomas par neparastām darbībām
- Lai ievadītu paroles, izmantojiet "virtuālo" tastatūru
- Izrakstieties (izejiet) no vietnēm, kurām nepieciešama autorizācija
- Nesaglabājiēt savu pieteikšanās informāciju
- Izdzēsiet savu interneta "vēsturi" un lejupielādētos failus

Aizsargājiet sevi pret datu noskatīšanos pār plecu (sērfošanu pār plecu)

- Kad strādājat ar digitālām ierīcēm, piemēram, datoru, klēpj datoru, viedtālruni, kāds var novērot, skatoties pār plecu, ko lietotājs dara ekrānā, kāda veida informāciju vai paroles ievada, lai iegūtu informāciju un izmantotu to ļaunprātīgām darbībām.
- Lai pasargātu sevi no datu noskatīšanās pār plecu (sērfošanu pār plecu)
 - atrodiet vietu, kur varat sēdēt vai stāvēt ar muguru pret sienu
 - Vienmēr esiet informēts un apzinīgs attiecībā uz savu apkārtni, ne tikai cilvēkiem, bet arī video kamerām, kas varētu uzņemt video par jūsu darbībām

Pieteikšanās un atteikšanās (ieiešana pakalpojumos/vietnēs un iziešana no tiem)

- Izmantojot publisku datoru (vai kāda cita ierīci), noņemiet atzīmi no izvēles rūtiņas “Saglabāt manu pieteikšanos” vai “Palikt pierēģistrētā režīmā”
- Neļaujiet tīmekļa pārlūkprogrammai atcerēties jūsu paroli, lai jūs automātiski varētu pieteikties pakalpojumā



The image shows the Facebook login interface. A red line with arrows points to two specific elements: the 'Keep me logged in' checkbox and the 'Sign in' button. The interface includes a profile picture placeholder, the Facebook logo, and input fields for 'Email or Phone' and 'Password'. Below the input fields are checkboxes for 'Keep me logged in' and 'Stay signed in', and a 'Sign in' button. A 'Need help?' link is also present.

facebook

Email or Phone
name.surname@gmail.com

Password
.....

☒ Keep me logged in

Forgot your password?

name.surname@gmail.com

.....

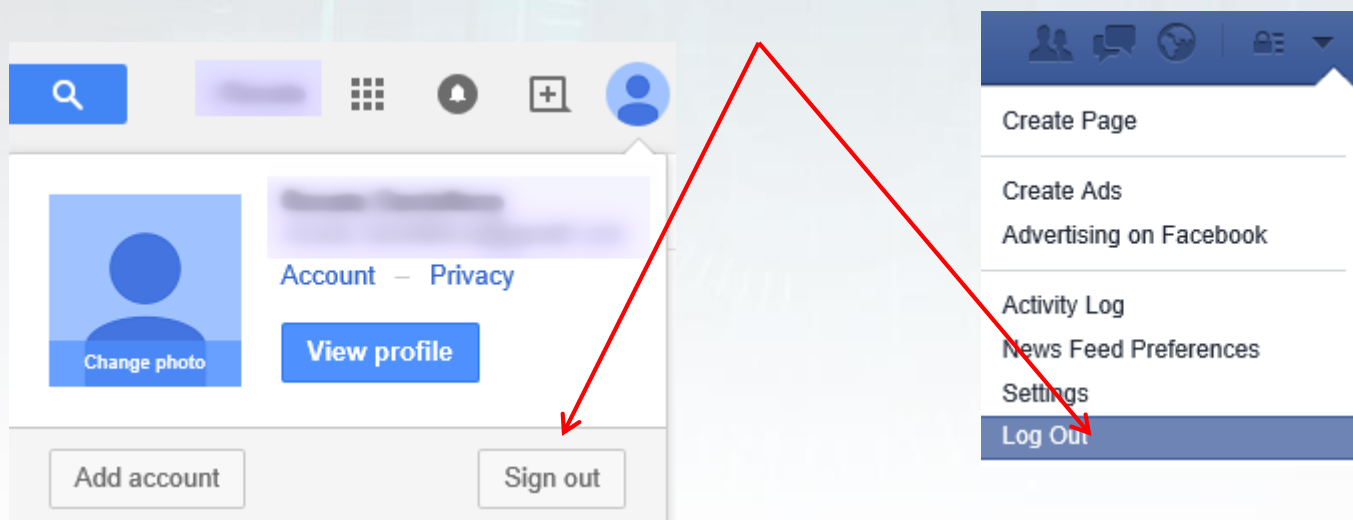
Sign in

☒ Stay signed in

Need help?

Pieteikšanās un atteikšanās (ieiešana pakalpojumos/vietnēs un iziešana no tiem)

- Izmantojot publisku datoru (vai kāda cita ierīci), izrakstieties (izejiet) no visiem kontiem un lietotnēm



Atvienošanās no sistēmām attālināti

- Iespējams izrakstīties (iziet) attālināti, ja esat aizmirsis izrakstīties no sava konta, strādājot ar publisku vai kāda cita datoru, vai gadījumā, ja esat pazaudējis savu digitālo ierīci
- Jums jāpārbauda, vai pakalpojums nodrošina attālinātās izrakstīšanās funkciju, piemēram, Google, Facebook, Dropbox, Netflix, Microsoft, Instagram, Amazon utt.

Piemēram:

Izrakstīties no Google

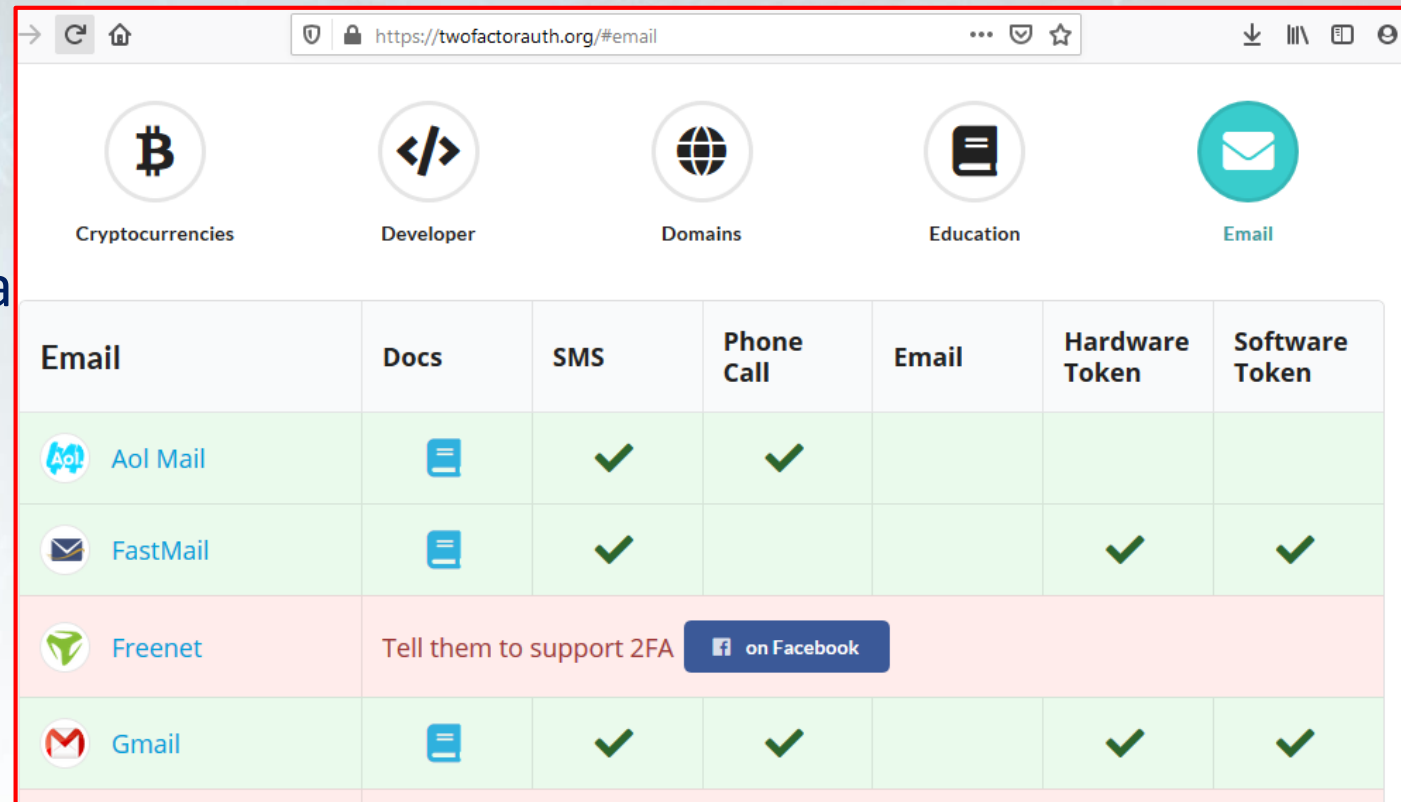
pakalpojumiem <https://support.google.com/mail/answer/8154?hl=en&co=GENIE.Platform%3DDesktop>

Izrakstīties no Netflix <https://help.netflix.com/en/node/18>

Izrakstīties no Dropbox <https://help.dropbox.com/accounts-billing/settings-sign-in/device-list-remote-sign-out>

Divu faktoru autentifikācija

- Ieteicams iespējot divu faktoru autentifikāciju, ja pakalpojumu sniedzējs to atbalsta
- Pārbaudiet, kuras vietnes atbalsta divu faktoru autentifikāciju, t.i., <https://twofactorauth.org>



The screenshot shows the website <https://twofactorauth.org/#email>. At the top, there are five category icons: Cryptocurrencies (Bitcoin), Developer (code symbol), Domains (globe), Education (book), and Email (envelope). Below these is a table with columns for different authentication methods: Email, Docs, SMS, Phone Call, Email, Hardware Token, and Software Token. The table lists several email services and their support status for these methods.

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail		✓	✓			
FastMail		✓			✓	✓
Freenet	Tell them to support 2FA on Facebook					
Gmail		✓	✓		✓	✓



Tehnoloģiskās problēmas

Instalējiet legāli iegūtu programmatūru un lietotnes tikai no uzticamiem avotiem

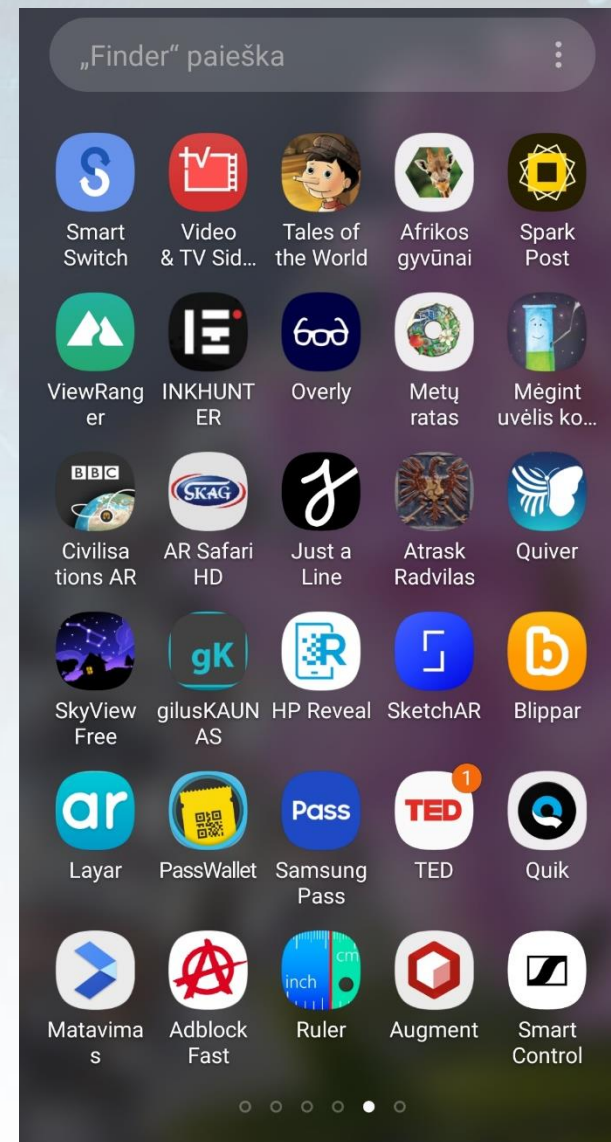
- Instalējiet tikai legālu programmatūru un lietotnes
- Neinstalējiet neuzticamu programmatūru
- Instalējiet lietotnes tikai no uzticamiem avotiem, piemēram:
 - Google Play
 - Apple App Store
 - Microsoft Store
 -



Google Play

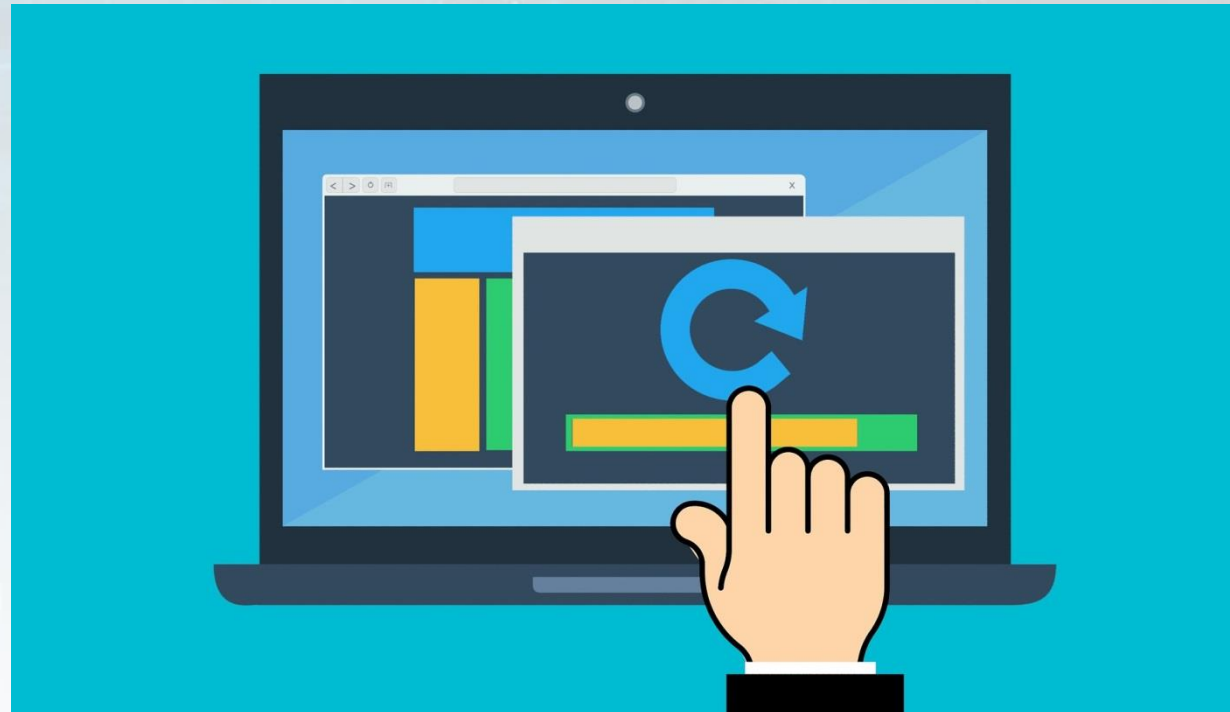
Jautājums

- Vai zināt visu savā ierīcē esošo lietotņu mērķi?



Regulāri atjauniniet programmatūru

- Nodrošiniet, lai ierīcēs, lietojumprogrammās un informācijas sistēmās tiktu regulāri instalēti visi nepieciešamie atjauninājumi un ielāpi
- Iespējojiet automātiskos operētājsistēmas un programmatūras atjauninājumus



Izmantojiet pretvīrusu un interneta aizsardzības rīkus

- Lielākā daļa pretvīrusu programmatūras ir komerciālas, un par tām ir jāmaksā
- Personīgai lietošanai ir pieejamas vairākas bezmaksas pretvīrusu programmas. Piemēri:
 - Avira Free Antivirus
 - AVG
 - Avast
 - Bitdefender Antivirus Free Edition
 - Windows Defender

Izmantojiet surogātpasta un e-pasta filtrus

- Surogātpasta filtri analizē, atklāj un aptur nevēlamus vai bīstamus e-pastus. Surogātpasta filtri var analizēt e-pastus pēc dažādiem kritērijiem
 - Tēmas filtrs
 - Satura filtrs
 - Bloķēšanas saraksts filtrs
 - Uz noteikumiem balstīts filtrs
- Surogātpasta filtrs novērš serveru pārslodzi un neļauj surogātpastam sasniegt darbiniekus to e-pastos
- Jāapzinās, ka surogātpasta filtrs pilnībā nenovērš nevēlamus un krāpnieciskus e-pastus

Izmantojiet sistēmas šifrēšanas funkciju

- Sistēmas šifrēšanas funkcija šifrē visus datus, tostarp lietojumprogrammu datus, lejupielādētos failus un visu pārējo, jūsu tālrunī vai planšetdatorā.
- Ikreiz, kad ieslēdzat tālruni, jums būs jāievada PIN vai parole



Dublējiet savus datus

- Datu dublēšana vai rezerves kopiju veidošana pasargā jūs datora avārijas vai elektrības padeves pārtraukuma vai pārsprieguma gadījumā, piemēram, zibens vai vētras gadījumā.
- Rezerves kopijām izmantojiet ārējo cieto disku vai citu datu nesēju
- Dublējuma vai rezerves kopijas var glabāt:
 - ārējās atmiņas ierīcēs;
 - tiešsaistes datu glabātuvēs, piemēram, Dropbox,
 - Apple iCloud, Google Drive u.c.



Identitātes aizsardzības rīks

- Izmantojiet brīdinājuma zīmes, kas liecina, ka jūsu dati ir apdraudēti, vai ka jūsu konts ir uzlauzts, piemēram, [Canary tokens](#)
- *Canarytokens* ir bezmaksas rīks, kas palīdz atklāt, ka jūsu dati ir uzlaukti, liekot uzbrucējiem tikt pamanītiem
- Canary token ir fails, URL, API atslēga vai cits resurss, kuram tiek nodrošināta piekļuve. Kad resursam ir piekļūts, tiek aktivizēts brīdinājums, informējot objekta īpašnieku par minēto piekļuvi



Vairāk informācijas:

<https://canarytokens.org/generate> www.lacework.com/blog/canarytokensandransomwareoperations

Identitātes aizsardzības rīks

- Canary token rīks var būt
 - Tīmekļa kļūda, URL marķieris (brīdinājums, kad URL tiek apmeklēts)
 - DNS marķieris (brīdinājums, kad tiek pieprasīts resursdatora nosaukums)
 - Unikāla e-pasta adrese (brīdinājums, kad e-pasts tiek nosūtīts uz unikālu adresi)
 - Marķieri programmām MS Word, MS Excel, PDF failiem (brīdinājums, kad dokuments tiek atvērts)
 - Windows mape (brīdinājums, kad mape tiek atvērta)
 - u.t.t.



Vairāk informācijas marķieru ģenerēšanu:

<https://canarytokens.org/generate>

Viedierīču drošība

- Pārbaudiet un konfigurējiet visu lietotņu atļaujas un konfidencialitātes iestatījumus
- Iespējot attālināto vadību un datu iznīcināšanu
- Dublējiet savas mobilās ierīces datus
- Izslēdziet Bluetooth, kad to neizmantojat
- Esiet piesardzīgs, apskatot informāciju tālrunī publiskās vietās
- Pirms ierīces pārdošanas atiestatiet tās rūpnīcas iestatījumus

Ierīču un tīkla aizsardzība

- Iznīciniet ierīces vai atmiņas kartes, kuras vairs neizmantojat.
- Ieteicams izveidot savienojumu tikai ar uzticamiem bezvadu tīkliem, kas ir aizsargāti ar parolēm
- Šifrējiet USB un citus datu nesējus
- Pareizi izdzēsiet dokumentus, kuros ir personas informācija

Other Recommendations

- Izvairieties no P2P (vienlaicīgas ielādes vai vairākiem datu turētājiem) un kopīgotas failu koplietošanas
- Lejupielādējiet failus tikai legālā ceļā
- Izvairieties no sērfošanas vietnēs, kuras nezināt
- Izvairieties no piedāvājumiem, kas ir pārāk labi, lai būtu patiesi

Vissvarīgākais pretsvars kibernoziedzniekiem: patērētāju informētība un modrība!

Noderīgas ar tēmu saistītas saites

Kas ir personiskā informācija? | Personas dati

<https://www.cloudflare.com/en-gb/learning/privacy/what-is-personal-information/>

Video par to, cik viegli notiek personas datu uzlaušana: https://youtu.be/1hpU_Neg1KA

Kas ir kibernetiskā higiēna? Kiberhigiēnas definīcija, ieguvumi, paraugprakse un daudz kas cits

<https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>

Kas ir digitālie pēdu nospiedumi? Un kā tos pasargāt no hakeriem <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

Kā pasargāt savu digitālo privātumu?

<https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy>

Kā noņemt personisko informāciju no interneta

<https://www.lifelock.com/learn-identity-theft-resources-remove-personal-information-from-the-internet.html>

Kopsavilkums

Proaktīvā rīcība

- Kibernētiskā higiēna internetā
- Digitālo ierīču higiēna
- Tehnoloģiskās problēmas



Piešķiršana

Aizpildiet formulāru:

- Vārds, uzvārds,
- e-pasta adrese,
- tās skolas nosaukums, kuru pabeidzāt,
- jūsu dzīvnieku vārdi



PADOMS: Varat izmantot Google Form, bet pārliecinieties, vai uzdevums ir precīzs, piemēram

<https://forms.gle/uckbLqBmY2mkFs93A>

Piešķiršana



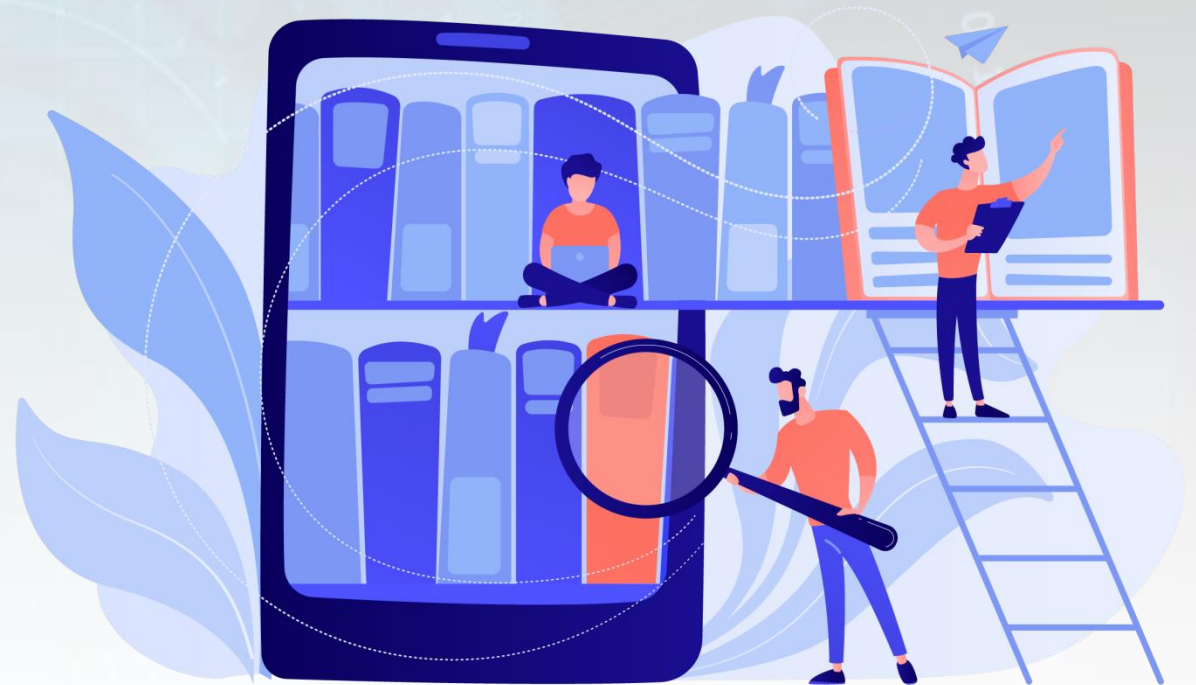
Apspriediet:

- Kāda veida pēdu nospiedumus jūs atstājat internetā?
- Kā jūs aizsargājat savus personas datus?
- Kā jūs aizsargājat savas digitālās ierīces?
- Kas ir divu faktoru autentifikācija un kur to izmantot?

Veiciet Google meklēšanu par sevi.
Ko iespējams atrast?

Papildu lasīšana

- **Eiropas Savienība. Tīklu un informācijas drošības aģentūra** Kiberhigiēnas prakses apskats, 2016. gads
- **Žerārs Blokdiks** [*Gerardus Blokdyk*], Kiberhigiēna, trešais izdevums, 2018. gads
- **Žerārs Blokdiks** [*Gerardus Blokdyk*] Kiberhigiēna — pilnīga rokasgrāmata – 2020. gada izdevums



Īsi video

- Cik viegli notiek personas datu uzlaušana?
 - https://youtu.be/1hpU_Neg1KA
- Kas ir digitālie pēdu nospiedumi?
 - <https://youtu.be/CfICOt2ul80>
- Kā aizsargāt savus datus tiešsaistē?
 - <https://youtu.be/XjJZoHOlgu4>
- Kas ir divu faktoru autentifikācija (2FA)?
 - <https://youtu.be/mMKo-fG89jQ>
- Mani dati ir uzlausti, ko man darīt?
 - <https://youtu.be/k5rIMr-u0Jw>
- Mobilās drošības izpratne
 - <https://youtu.be/ahNb6kA0Lms>



Pateicamies!



Prezentācijā izmantoto attēlu resursi no:

- www.pixabay.com
 - Personīgiem arhīviem
- Ekrānuzņēmumi no vietnēm