Funded by the
Erasmus+ Programme
of the European Union

Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem

# Apiešanās ar kiberuzbrukumiem

**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.*

CyberPhish
Safeguarding your digital future

# *Apmācību mērķis*

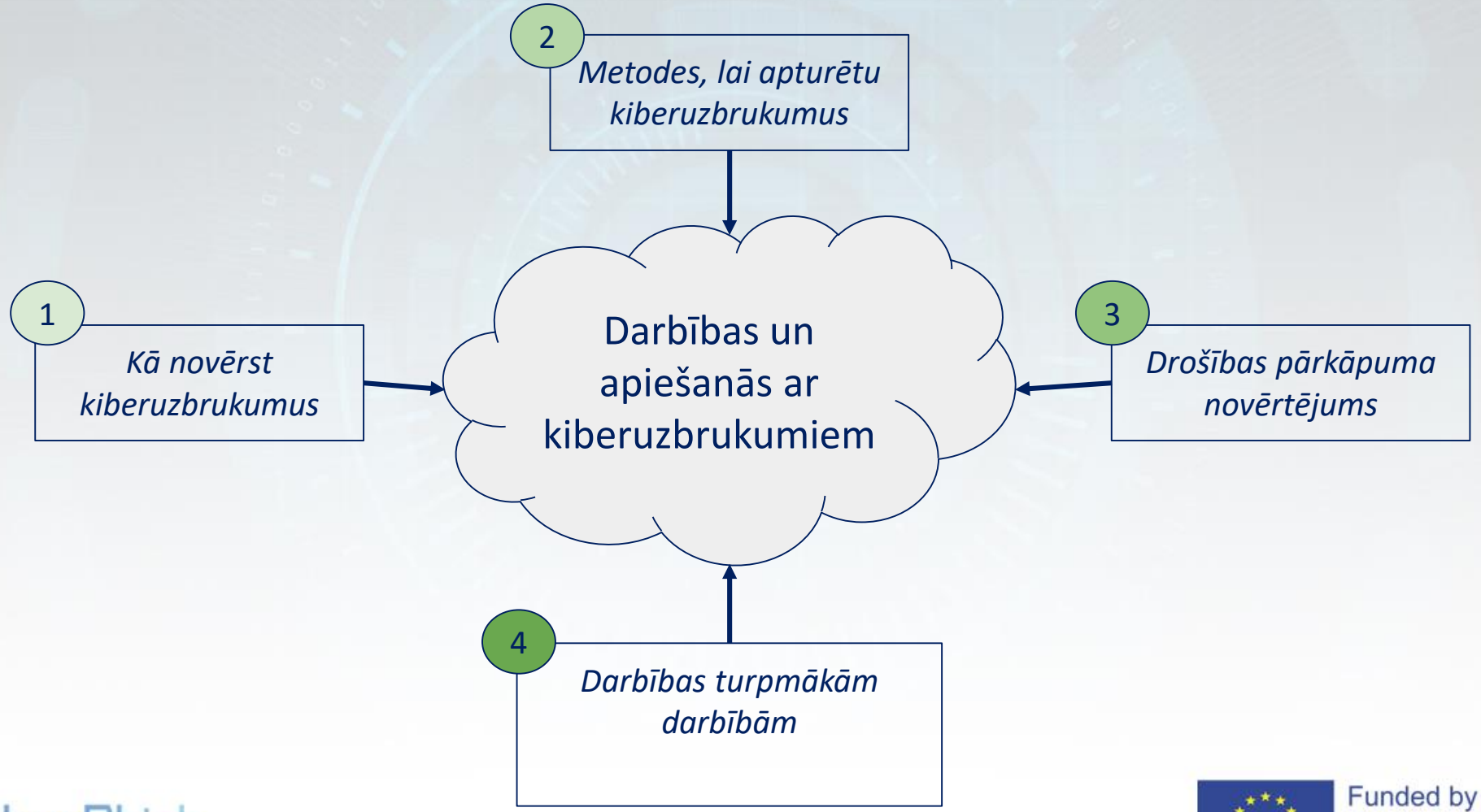
Izskaidrot un izprast veidus, kā varētu tikt galā ar kiberuzbrukumiem

Izprast, kā var izvairīties no kiberuzbrukumiem vai samazināt kaitējumu

# *Kursantu darba slodze*


| | |
|---|---|
| Lekcija | 5 st. |
| Audio un video materiāli | 2 st. |
| Pētījumi | 2 st. |
| Papildu lasīšana | 4 st. |
| Sagatavošanās eksāmenam | 2 st. |

# Saturs


2
Metodes, lai apturētu kiberuzbrukumus
1
Kā novērst kiberuzbrukumus
Darbības un apiešanās ar kiberuzbrukumiem
3
Drošības pārkāpuma novērtējums
4
Darbības turpmākām darbībām

# *Izvairīšanās no kiberuzbrukumiem*

- Visefektīvākais veids, kā apkarot kiberuzbrukumus, ir piemērot atbilstošus profilakses pasākumus
- *Nav veiksmīga uzbrukuma – nav zaudējumu.*

- Lai izvairītos no uzbrukuma vai to mazinātu, jums ir jāattīsta daži ieradumi, ko bieži sauc par drošības higiēnu vai kiberhigiēnu (kibernētisko higiēnu).

- *Ja jūs un jūsu darbinieki ievērosit drošības higiēnu, iespēja kļūt par kiberuzbrukuma upuri var tikt samazināta vismaz par 90 procentiem!*



Funded by the Erasmus+ Programme of the European Union

# *Izpratnes veidošanas trenēšana*

- Pirmais un viens no svarīgākajiem padomiem, kā rīkoties ar kiberuzbrukumiem, ir izpratnes veidošanas trenēšana.
- Tas nodrošinās, ka visi darbinieki atbilstoši amatam vai pilsoņi varēs tikt galā ar kiberincidentiem.

- Apmācība ir arī viens no galvenajiem riska samazināšanas instrumentiem.
- *Taču arī tie nevar garantēt 100% drošību, taču var samazināt risku*



Funded by the Erasmus+ Programme of the European Union

# *Paraugprakse, lai izvairītos no kiberuzbrukumiem*

1. No augšas uz leju vērstas politikas jūsu drošības stāvokļa uzlabošanai.

*Paraugprakse vienmēr ir jāatbalsta ar pareizo politiku. Tas nozīmē, ka kiberdrošībai ir jābūt korporatīvās pārvaldības neatņemamai sastāvdaļai.*

2. No apakšas uz augšu virzītas prakses kiberdrošības komandām.

*Pamatojoties uz labi izstrādātām politikām, var izmantot vairākas prakses, lai palīdzētu novērst, ierobežot vai mazināt kiberuzbrukumus.*

3. Veiciet proaktīvus pasākumus, lai atklātu progresīvus kiberdraudus un reaģētu uz tiem.

*Iespējams, vissvarīgākā labākā prakse ir proaktīva pieeja kiberdrošībai.*



Funded by the Erasmus+ Programme of the European Union

# *Pasākumi potenciālā uzbrukuma novēršanai*

- *1. solis: Uzziniet, kuri ir visizplatītākie kiberdraudi*
- *2. solis: Pārejiet uz kiberdrošības darbības režīmu*
- *3. solis: Novērtējiet risku un pakļautību tam*
- *4. solis: Izstrādājiet aizsardzības un atklāšanas pasākumus*
- *5. solis: Izveidojiet ārkārtas rīcības plānus*
- *6. solis: Atlabšana*



Funded by the Erasmus+ Programme of the European Union

# *Izvairīšanās no kiberuzbrukumiem*

- Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**1. Apmāciet savus darbiniekus.**

- Viens no efektīvākajiem veidiem, kā cīnīties pret kiberuzbrukumiem un visa veida datu pārkāpumiem, ir apmācīt savus darbiniekus.

- Lai novērstu pikšķerēšanu, viņiem ir:

*Pārbaudīt saites, pirms noklikšķināt uz tām*

*Pārbaudīt e-pasta adreses saņemtajā e-pastā*

*Pirms sensitīvas informācijas sūtīšanas izmantot veselo saprātu. Pirms izpildāt pieprasījumu, labāk ir pārbaudīt, sazinoties ar attiecīgo personu.*



Funded by the Erasmus+ Programme of the European Union

# *Izvairīšanās no kiberuzbrukumiem*

Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**2. Atjauniniet savu programmatūru un sistēmas pilnībā.**

*- bieži vien hakeri izmanto programmatūras nepilnības, par kurām kļuvis zināms hakeru kopienā;*

*- ir gudri ieguldīt programmnodrošinājumu ielāpu pārvaldības sistēmā;*

*- izskatiet piedāvājumus ielāpu pārvaldībai kā daļu no pārvaldītā drošības risinājuma.*



Funded by the Erasmus+ Programme of the European Union

# *Izvairīšanās no kiberuzbrukumiem*

Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**3. Nodrošiniet galapunktu aizsardzību.**

*- galapunktu aizsardzība aizsargā tīklus, kas ir attālināti savienoti ar ierīcēm. Mobilās ierīces, planšetdatori un klēpjdatori, kas ir savienoti ar korporatīvajiem tīkliem, nodrošina piekļuves ceļus drošības apdraudējumiem.*

**4. Instalējiet ugunsmūri.**

*- Tīkla novietošana aiz ugunsmūra ir viens no efektīvākajiem veidiem, kā aizsargāt sevi no jebkāda kiberuzbrukuma.*

# *Izvairīšanās no kiberuzbrukumiem*

Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**5. Dublējiet savus datus (veidojiet rezerves kopijas)**

*- katastrofas gadījumā (to var izraisīt kiberuzbrukums) jums ir jābūt jūsu datu kopijai.*

**6. Kontrolējiet piekļuvi savām sistēmām**

*- uzbrukumi var būt fiziski.*

*- Ir svarīgi kontrolēt, kas var piekļūt jūsu tīklam.*

# *Izvairīšanās no kiberuzbrukumiem*

Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**7. Wi-Fi drošība.**

*- neaizmirstiet ievadīt paroli katram izmantotajam Wi-Fi savienojumam.*

**8. Personīgie konti katram darbiniekam.**

*- katram darbiniekam ir jāizmanto personīgais konts;*

*- kontu koplietošana ir jāaizliedz.*

# *Izvairīšanās no kiberuzbrukumiem*

Lai izvairītos no kiberuzbrukumiem, stingri ieteicams veikt vairākas tālāk norādītās darbības.

**9. Piekļuves pārvaldība**

*- darbiniekiem jābūt instalētiem tikai autorizētai programmatūrai;*

*- ir jāaizliedz neautorizētas programmatūras izmantošana.*

# *Izvairīšanās no kiberuzbrukumiem*

**Padomi drošības palielināšanai:**

*1. Samaziniet datu pārsūtīšanu un nevajadzīgu saziņu;*

*2. Sekojiet līdzi kiberdrošības reljefam;*

*3. Veiciet aptaujas par datu noplūdi;*

*4. Izstrādājiet un ieviesiet incidentu reaģēšanas plānu.*

Nav viegli tiem visiem sekot katru dienu, bet jums par tiem ir jādomā.



Funded by the
Erasmus+ Programme
of the European Union

# *Izvairīšanās no kiberuzbrukumiem*

Ja ievērosit šos norādījumus, jūs ievērojami samazināsit kiberuzbrukuma risku.

Bet neaizmirstiet:

- *Var būt grūti zināt, kur ir vājākās vietas.*
- *Ir tik daudz informācijas, kas dažreiz ir pat pretrunīga.*
- *Ir nepieciešams jums piemērots risinājums.*



Funded by the
Erasmus+ Programme
of the European Union

# *Droša interneta pārlūkošana*

- Pārlūkojot tīmekli, iespējams, jūs uztverat spiegprogrammatūru, lejupielādējat ļaunprātīgu programmatūru vai pat apmeklējat krāpnieciskas vietnes.

- Bieži vien jūs varat nezināt, ka darāt kaut ko nedrošu.

- Tas nenozīmē, ka jums ir jābaidās katru reizi, noklikšķinot uz jebkuras saites.

- Daži vienkārši piesardzības pasākumi var palīdzēt jums būt ievērojami drošākam pārlūkošanas laikā.



Funded by the Erasmus+ Programme of the European Union

# *Droša interneta pārlūkošana*

- **Datora aizsardzība pret ļaunprātīgām vietnēm:** katrā pārlūkprogrammā ir drošības līdzekļi, kas aizsargā jūs pret ļaunprātīgu vietņu apmeklēšanu. Iespējojiet šīs funkcijas!

- **Pārlūkprogrammas atjaunināšana:** regulāri tiek radītas jaunas ļaunprātīgas programmatūras un pikšķerēšanas draudi. Ir svarīgi regulāri atjaunināt pārlūkprogrammu.

*- Pārliecinieties, vai jums ir jaunākā pārlūkprogrammas versija.*

*- Pārliecinieties, vai esat instalējis visus jaunākos atjauninājumus.*



Funded by the Erasmus+ Programme of the European Union

# Droša interneta pārlūkošana

- **Domēna pārbaude:** Ļaunprātīgas vietnes bieži izmantos maldinošus domēnus, lai liktu lietotājiem noticēt, ka viņi atrodas leģitīmā vietnē. Lielākajai daļai pārlūkprogrammu ir funkcijas, kas ļauj pārbaudīt domēnu, vai arī varat izmantot īpašas tīmekļa vietnes, lai pārbaudītu domēnu (mazāk ērti).

- **Lejupielādējiet tikai no uzticamām vietnēm:** viens no vienkāršākajiem veidiem, kā ļaunprātīga programmatūra, spiegu programmatūra un reklāmprogrammatūra var piekļūt jūsu datoram, ir lejupielādes.

- Esiet piesardzīgs pret bezmaksas programmatūru;
- Izvairieties no nelegālām lejupielādēm;
- Esiet piesardzīgs P2P failu koplietošanā.

# *Droša interneta pārlūkošana*

- **Regulāri iztīriet kešatmiņu**

- Pārlūkprogramma var paātrināt piekļuvi, ielādējot lapas no kešatmiņas.
- Izmantojot ātrgaitas interneta savienojumu, jūs, iespējams, nepamanīsit atšķirību.
- Kešatmiņa laika gaitā var aizņemt vietu, izraisot pārlūkprogrammas darbības palēninājanos.

**Ieteicams regulāri iztīrīt kešatmiņu, lai atbrīvotu vietu datorā un ... un noņemtu iespējamos ļaunprātīgos failus.**



Funded by the Erasmus+ Programme of the European Union

# *Droša interneta pārlūkošana*

- **Bloķējiet uznirstošos logus**
  - Uznirstošie logi ir nelieli pārlūkprogrammas logi, kas automātiski tiek parādīti, kad apmeklējat noteiktas vietnes.
  - Uznirstošie logi var būt daļa no vietnes likumīgas darbības.
  - Dažos uznirstošajos logos var būt ļaunprātīga programmatūra.

- **Ieteicams bloķēt uznirstošos logus**

Lielākajai daļai pārlūkprogrammu ir īpaši uznirstošo logu bloķētāji.

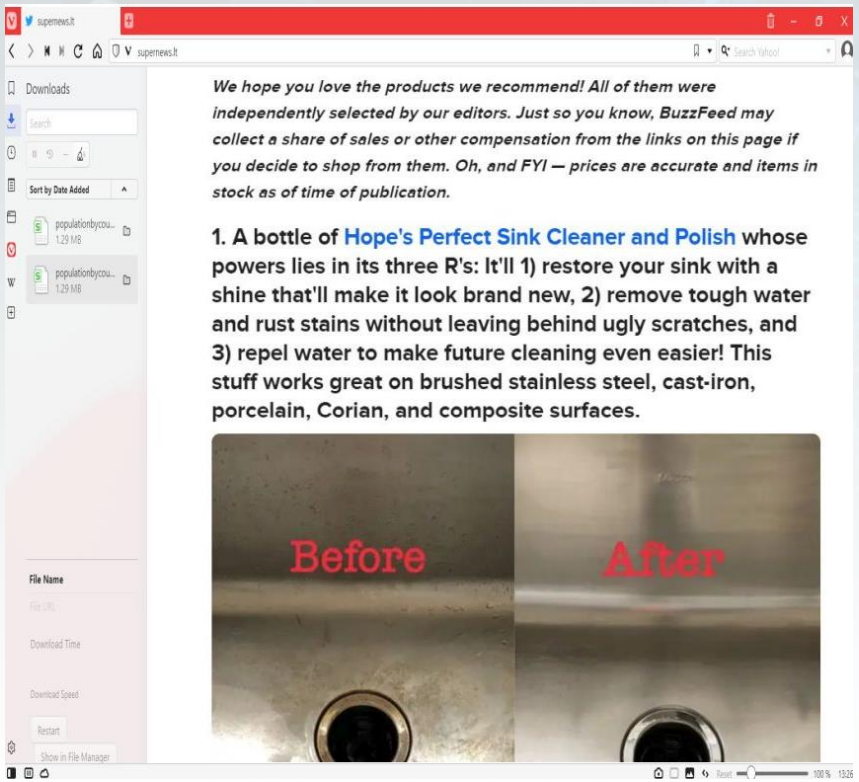


Funded by the Erasmus+ Programme of the European Union

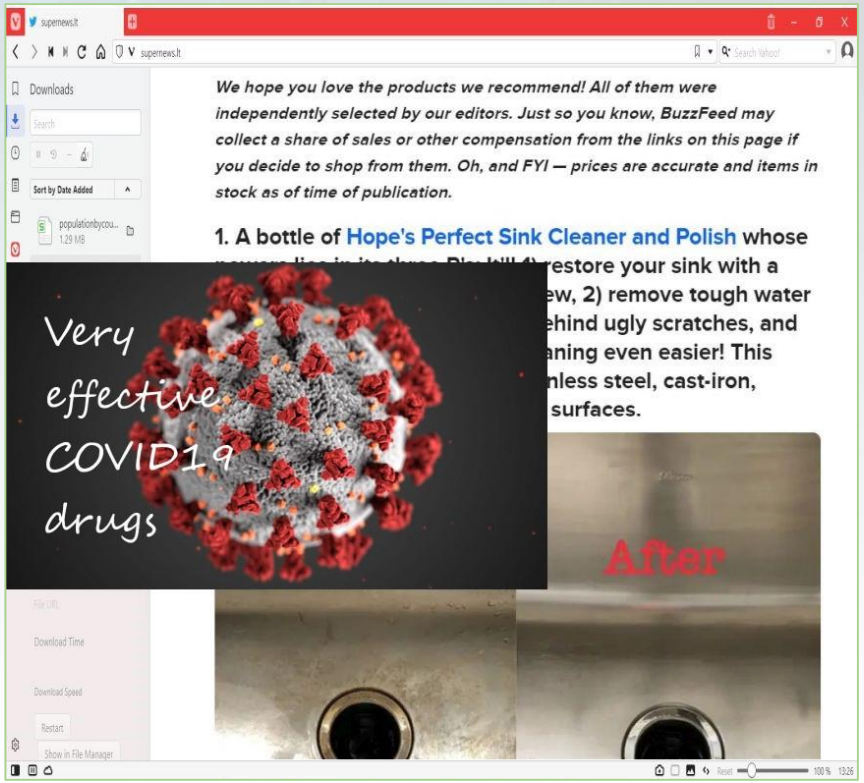
# *Droša interneta pārlūkošana:*

## *piemēri ar uznirstošiem logiem un bez uznirstošiem logiem*

**Mērija *[Mary]* nobloķēja uznirstošos logus**




**Džeina *[Jane]* – nē...**




CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Drošības programmatūras instalēšana*

- **Drošības programmatūra ir būtisks elements** droši strādājot kibertelpā.

- Pievērsiet uzmanību

*1. Instalējiet interneta drošības programmatūru;*
*2. Instalējiet ugunsmūri;*
*3. Izveidojiet startēšanas (palaišanas) disku;*
*4. Konfigurējiet stingrus tīmekļa pārlūkprogrammas un e-pasta drošības iestatījumus;*
*5. Neinstalējiet/nepalaidiet nezināmas programmas;*
*6. Atspējojiet slēptos faila nosaukumu paplašinājumus.*


Funded by the Erasmus+ Programme of the European Union

# *Kā tiek izsekota jūsu pārlūkošanas darbība*

- Dažas vietnes (Amazon, eBay, Netflix un daudzas citas) apkopo datus par jūsu vēlmēm: tās vēlas ieteikt produktus, kas jums varētu patikt.
- Google izseko un analizē darbības, lai uzņēmumiem sniegtu statistikas datus.
- Dažas valdības apkopo datus par jūsu darbībām tiešsaistē, ja tie ir nepieciešami kriminālizmeklēšanas vai valsts drošības nolūkos.
- **Arī daži noziedznieki var mēģināt izsekot jūsu darbībām.**

- Ir svarīgi apzināties šo izsekošanu, lai veidotu drošas pārlūkošanas paradumus.



Funded by the Erasmus+ Programme of the European Union

# *Spēcīgu paroļu izveide*

Parole – parasti galvenais rīks, kas nodrošina Jūsu drošību mūsdienu IT sistēmās.

Parolei ir jābūt spēcīgai, lai nodrošinātu augstu drošības līmeni.

Kas ir spēcīga parole?

***Spēcīga parole ir tāda, kuru jums ir viegli atcerēties, bet citiem grūti uzminēt.***



Funded by the
Erasmus+ Programme
of the European Union

# *Padomi spēcīgu paroļu izveidei*

**Slikta prakse:** izmantot vienu un to pašu paroli katram kontam.

Iemesls:  ja kāds atklās jūsu paroli vienam kontam, visi pārējie konti, iespējams, kļūs neaizsargāti.

**Padoms:** parolē izmantot ciparus, simbolus un gan lielos, gan mazos burtus. Tas apgrūtinās paroles uzlaušanu, izmantojot brutālu spēku uzbrukumu.



Funded by the Erasmus+ Programme of the European Union

# *Padomi spēcīgu paroļu izveidei*

**Slikta prakse:** personas informācijas, piemēram, jūsu vārda, dzimšanas dienas, lietotājvārda vai e-pasta adreses, izmantošana.

Iemesls: šāda veida informācija bieži ir publiski pieejama, tāpēc kādam ir vieglāk uzminēt jūsu paroli.

**Izmantojiet garāku paroli**
Standarta padoms: jo garāka parole, jo labāk (un to ir arī grūtāk atcerēties). Lai gan papildu drošībai tai vajadzētu būt vēl garākai.


Funded by the Erasmus+ Programme of the European Union

# *Padomi spēcīgu paroļu izveidei*

**Slikta prakse:** lietot vārdus, kas atrodami vārdnīcā.

Iemesls: daudzi hakeru rīki veic tā sauktos uz vārdu krājumu balstītus uzbrukumus. Vispirms hakeri mēģina pārbaudīt zināmos vārdus vārdu krājumā.

Piem., **speletajs2002** būtu vāja parole (vārds no vārdu krājuma un cipars, kas apzīmē dzimšanas gadu).

**Nejaušas, uz labu laimi veidotas paroles ir visspēcīgākās**. Padomājiet par paroļu ģeneratora izmantošanu.



Funded by the Erasmus+ Programme of the European Union

# *Biežākās paroļu problēmas*

Visbiežāk lietotās paroles ir balstītas uz uzvārdiem, vaļaspriekiem vai vienkāršiem modeļiem. Viegli atcerēties, bet arī viegli uzminēt.

Daži piemēri ar sliktām parolēm

**Parole:** *niks1995ketija1997*

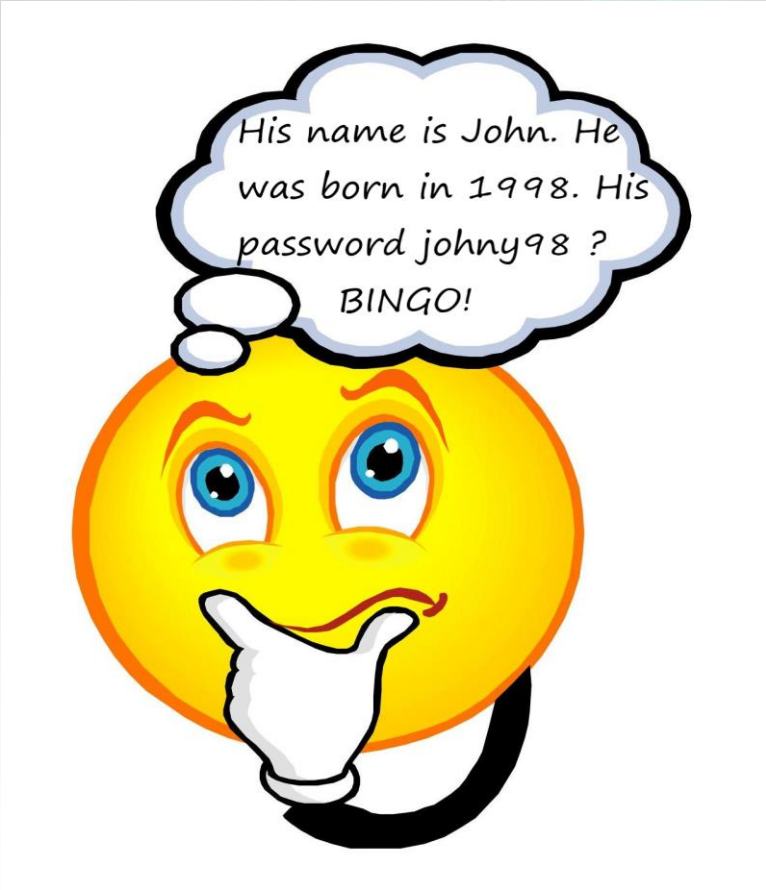
**Problēma:** izskatās gara, bet viegli uzminama, jo tiek izmantoti divi vārdi (draugs un draudzene) ar dzimšanas gadiem. Viegli uzminēt, ja zināt informāciju par mērķa personām.

Risinājums: ievietojiet nejaušus simbolus, izmantojiet lielo - mazo burtu kombinācijas, piem.***ni%k199oK$tie199x***



Funded by the Erasmus+ Programme of the European Union

# Padomi spēcīgu paroļu izveidei




# *Biežākās paroļu problēmas*

**Parole:** *w@kLx*

Problēma: izskatās nejauša un grūti uzminama, bet satur tikai 5 simbolus.
Pārāk īsa.

Risinājums: spēcīgākai versijai ir jābūt daudz garākai, vēlams vismaz 10 simboliem.

**Parole:** *123abc456cba789*

Problēma: viegli iegaumējama, bet izmantotā simbolu kombinācija tiks pārbaudīta starp pirmajiem

Risinājums: izlases paroļu ģenerators, e.g. *#eV$pIg&qf*



Funded by the
Erasmus+ Programme
of the European Union

# *Biežākās paroļu problēmas*

**Parole:** *Gmail Bd458$%Kl!df;  eBay Bd458$%Kl!df; Amazon: Bd458$%Kl!df*

**Problēma**: parole ir laba, taču tās izmantošana dažādās vietnēs ir slikta prakse.

Risinājums: izmantojiet dažādas paroles katrai vietnei.

Tā vietā, lai rakstītu paroles uz papīra, varat izmantot paroļu pārvaldnieku, lai tās droši uzglabātu.

Paroļu pārvaldnieki var atcerēties un ievadīt jūsu paroli dažādās vietnēs, kas nozīmē, ka jums nav jāatceras garākas paroles.



Funded by the
Erasmus+ Programme
of the European Union

# *Daudzfaktoru autentifikācija*

Daudzfaktoru autentifikācija (MFA) ir vēl labāks veids, kā aizsargāt jūsu sensitīvos datus.

Kas ir vairāku faktoru autentifikācija?

Daudzfaktoru autentifikācija ir verifikācijas metode, kurā ir nepieciešami vismaz divi dažādi pierādījuma faktori.

MFA dažreiz tiek saukta par 2FA (divfaktoru autentifikācija).

Principā tas pievieno papildu drošības līmeni.



Funded by the Erasmus+ Programme of the European Union

# *Daudzfaktoru autentifikācijas veidi*

Parasti ir trīs atzīti autentifikācijas faktoru veidi:

**1. tips:** Kaut kas, ko jūs zināt – ietver paroles, PIN, kodu vārdus utt.

**2. tips:** Kaut kas, kas jums ir – ietver visus priekšmetus, kas ir fiziski objekti (atslēgas, viedtālruņi, viedkartes, USB diski).

**3. tips:** Kaut kas, kas jūs esat — ietver biometriskos datus (pirkstu nospiedumus, plaukstu skenēšanu, sejas atpazīšanu, tīklenes skenēšanu, varavīksnenes skenēšanu, balss verifikāciju).



Funded by the Erasmus+ Programme of the European Union

# *Daudzfaktoru autentifikācija*

Apvienojot vismaz divus faktorus no šīm trim kategorijām, mēs iegūstam daudzfaktoru autentifikāciju.

Iebrucējam ir daudz grūtāk pārvarēt vairāku faktoru autentifikāciju.

Izmantojot vairāku faktoru autentifikāciju, uzbrucējam ir jābūt vairāk prasmēm un jāspēj veikt vairākus uzbrukumus vienlaikus.

Ļoti bieži tas ir ārkārtīgi grūti.

Labi zināms vairāku faktoru autentifikācijas piemērs, kas atbalsta tiešsaistes pakalpojumu, ir pakalpojumam PayPal.



Funded by the Erasmus+ Programme of the European Union

# *Populāri vairāku faktoru autentifikācijas rīki*

Ir pieejami daudzi vairāku faktoru autentifikācijas rīki.

Izplatītākās autentifikācijas lietotnes var atrast mobilās ierīces lietotņu veikalā:

- Google Authenticator;
- LastPass Authenticator;
- Microsoft Authenticator;
- Authy;
- un daudzi citi.


# *Failu šifrēšana*

- *Kas ir failu šifrēšana?*

  *Failu šifrēšana ir datu kodēšanas metode, lai droši pārsūtītu failus.*

- *Ko dara failu šifrēšana?*

  *Failu šifrēšana palīdz novērst manipulācijas vai nesankcionētu piekļuvi.*

- *Kā darbojas failu šifrēšana?*

  *Tā darbojas, izmantojot sarežģītus algoritmus, lai sajauktu nosūtītos datus.*



Funded by the
Erasmus+ Programme
of the European Union

# *Failu šifrēšana*

**Svarīgi:**

***ir jābūt atslēgai, lai varētu piekļūt failā esošajai informācijai!***



Funded by the
Erasmus+ Programme
of the European Union

# *Kā tiek šifrēti faili*

Divi no populārākajiem šifrēšanas standartiem ir:

- ***Open PGP*** - ļauj šifrēt un atšifrēt failus, izmantojot publiskās un privātās atslēgas.
- ***ZIP ar AES*** - saspiež un šifrē failus ar AES šifrēšanu, izmantojot ZIP un GZIP standartus.


Funded by the Erasmus+ Programme of the European Union

# *Kāpēc izmantot failu šifrēšanas programmatūru*

- Slāņaina datu aizsardzība

- Drošība daudzās ierīcēs

- Datu pārsūtīšana nodrošināta

- Datu integritāte (veselums) saglabāts

- Nodrošināta atbilstība



Funded by the
Erasmus+ Programme
of the European Union

# *Kā izvēlēties kodēšanas programmatūru*

- Kādi šifrēšanas standarti ir jāatbalsta?

- Cik sensitīvi ir dati?

- Vai notiek lielu failu apmaiņa?

- Vai ir jāšifrē faili vai savienojums?

– Kā tiks pārsūtīti dati?



Funded by the
Erasmus+ Programme
of the European Union

# *Kodēšanas programmatūra*

- AxCrypt Premium
- Folder Lock
- CryptoForge
- NordLocker
- Steganos Safe

# *Padomi kiberuzbrukuma identificēšanai*

Ja jau esat atvēris aizdomīgu e-pastu vai saiti, pārbaudiet tālāk norādītās lietas.

- *Neparastas darbības jūsu ierīcē vai tīklā.*
- *- aizdomas par paroles izmantošanu jūsu kontā.*
- *Identificējiet aizdomīgus uznirstošos logus.*
- *Pārraugiet tīklu, kas darbojas lēnāk nekā parasti.*
- *Atjauniniet programmatūru.*
- *Negaidītas vai pēkšņas izmaiņas diskā vai atmiņā.*


Funded by the Erasmus+ Programme of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- Iepirkšanās tiešsaistē ir ļoti ērts un bieži vien ekonomisks veids, kā kaut ko iegādāties.
- Bet tas var būt arī ļoti bīstams: FBI *Interneta noziegumu sūdzību centrs* (IC3) atklāja, ka puse kibernoziegumu 2019. gadā bija saistīti ar iepirkšanos tiešsaistē.
- Situācija citur nav labāka.
- Dažādi nepareizas uzvedības avoti:

*- nesaņemtas preces;*

*- nav samaksāts par precēm;*

*- aktīvisti zog sensitīvos datus, jo īpaši finanšu datus, e. g. kredītkaršu dati.*



Funded by the Erasmus+ Programme of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **1. padoms: izmantot tikai pazīstamus vai uzticamus tiešsaistes veikalus**

*- Šis ir drošības pasākums numur viens;*

*- Meklējiet klientu viedokli par tiešsaistes veikalu;*

*- Paskatieties, cik ilgi veikals ir aktīvs (parasti jo ilgāk tas ir aktīvs, jo ticamāks tas ir);*

*- Centieties neizmantot veikalus, par kuriem dzirdējāt no uznirstošajām reklāmām vai e-pasta reklāmām;*

*- Ja kļuvāt par upuri, ziņojiet par kibernoziegumiem!*



Funded by the Erasmus+ Programme of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **2. padoms: nekad nepērciet neko tiešsaistē, izmantojot savu kredītkarti no vietnes, kurā nav instalēta SSL (drošligzdu slāņa) šifrēšana.**

*- vietnei ir SSL, ja vietnes URL sāksies ar HTTPS — nevis tikai HTTP;*

*- parādīsies bloķētas piekaramās atslēgas ikona, parasti pa kreisi no URL adreses joslā vai statusa joslā zemāk;*

*- HTTPS tagad ir gandrīz standarts pat vietnēs, kas nav iepirkšanās vietnes*.

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **3. padoms. Nepārsniedziet dalīšanos ar personisko informāciju**

*- nevienai tiešsaistes iepirkšanās vietnei nav vajadzīgs jūsu personas kods, pases dati utt.;*

*- jūsu kredītkartes dati ir jāapstiprina jūsu bankai tiešsaistē;*

*- iespējojiet drošas iepirkšanās iespēju savā e-bankā;*

*- nereģistrētam pircējam bieži vien ir priekšrocības no drošības viedokļa.*

Atcerieties: jo mazāk krāpnieks par jums zina, jo grūtāk jūsu datus uzlauzt.



Funded by the Erasmus+ Programme of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **4. padoms: pareizi aizsargājiet savu kontu**

*- izmantojiet spēcīgas paroles (skatiet iepriekš);*

*- regulāri mainiet paroles (tikai 25% cilvēku to dara, ja tas netiek prasīts);*

*- izmantojiet dažādas paroles dažādās iepirkšanās platformās;*

*- ja iespējams, izmantojiet vairāku faktoru autentifikāciju;*

*- izmantojiet pret ļaunās programmatūras nodrošinājumu;*

*- izvairieties no iepirkšanās, izmantojot datoru, kas nav privāts.*



Funded by the
Erasmus+ Programme
of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **4. padoms: domājiet mobili**

*- nebaidieties pirkt, izmantojot mobilās lietotnes: tās nav mazāk drošas kā iepirkšanās galddatorā;*

*- izmantojiet tikai mazumtirgotāja vai citas tiešsaistes iepirkšanās platformas nodrošinātās lietotnes;*

*- paslēpiet ierīces ekrānu, veicot maksājumu publiskā vietā;*

*- pareizi aizsargājiet savu mobilo ierīci.*

Atcerieties: veicot drošu iepirkšanos vai maksājot publiski, jums ir jādomā nedaudz kā gangsterim.



Funded by the Erasmus+ Programme of the European Union

# *Daži padomi drošai iepirkšanās veikšanai tiešsaistē*

- **5. padoms: neizmantojiet karti, izmantojiet tālruni**

*- norēķināties par precēm, izmantojot viedtālruni, ir standarta pakalpojums;*

*- šāda veida pirkumi patiesībā ir vēl drošāki nekā kredītkartes izmantošana;*

*- mobilo maksājumu lietotnes, piemēram, Apple Pay, pirkumam ģenerē vienreiz lietojamu autentifikācijas kodu, ko neviens cits nekad nevarētu nozagt un izmantot.;*

*- kredītkartei nav jābūt līdzi: arī tas ir piesardzības pasākums!*

# *Apiešanās ar sīkfailiem (angl. cookies)*

- Sīkfaili ir būtisks mūsdienu interneta elements, taču tie ir neaizsargātība pret jūsu privātumu.
- Sīkfaili palīdz tīmekļa izstrādātājiem nodrošināt jums personiskākus un ērtākus vietnes apmeklējumus.
- Sīkfaili ļauj vietnēm atcerēties jūs, jūsu vietnes pieteikšanās datus, iepirkumu grozus un daudz ko citu. Taču tie var būt arī privātas informācijas dārgumu krātuves, ko noziedznieki var izspiegot.

- Pat pamatzināšanas par sīkfailiem var palīdzēt novērst nevēlamas jūsu darbības internetā.


Funded by the Erasmus+ Programme of the European Union

# *Kas ir sīkfaili?*

- To pamata formā: sīkfaili ir teksta faili ar datu daļām (piemēram, lietotājvārdu un paroli).
- Tie tiek izmantoti, lai jūs identificētu to, kā jūs izmantojat internetu.
- HTTP sīkfaili tiek izmantoti, lai identificētu konkrētus lietotājus un nodrošinātu lielākas pārlūkošanas ērtības.

- Sīkdatnē saglabātos datus serveris izveido jūsu savienojuma laikā. Šie dati ir apzīmēti ar jums un jūsu datoram unikālu identifikatoru (ID).
- Serveris nolasa šo ID un zina, kādu informāciju jums vajadzētu sniegt.


Funded by the Erasmus+ Programme of the European Union

# Sīkfailu veidi

Divi pamata veidi:

- Maģiskie sīkfaili
- **HTTP sīkfaili**

- Maģiskie sīkfaili ir termins, kas attiecas uz informācijas paketēm, kas tiek nosūtītas un saņemtas bez izmaiņām.
- Visbiežāk tos izmanto, lai pieteiktos datoru datu bāzu sistēmās, piemēram, uzņēmuma iekšējā tīklā.



Funded by the Erasmus+ Programme of the European Union

# Sīkfailu veidi

Divi pamata veidi:

- Maģiskie sīkfaili
- **HTTP sīkfaili**

- HTTP sīkfaili ir modificēta “Maģisko sīkfailu” versija, kas paredzēta interneta pārlūkošanai.
- HTTP sīkfails tiek izmantots, lai pārvaldītu mūsu tiešsaistes pieredzi.
- Ļaunprātīgi cilvēki var tos izmantot, lai izspiegotu jūsu tiešsaistes aktivitātes un pat nozagtu jūsu personisko informāciju.



Funded by the Erasmus+ Programme of the European Union

# *Kam tiek izmantoti sīkfaili?*

- **Interneta sesijas pārvaldība**. Piemēram, sīkfaili var ļaut vietnēm atpazīt lietotājus un atcerēties viņu individuālo pieteikšanās informāciju un preferences, piemēram, sporta ziņas pret politiku.

- **Personalizēšana**. Pielāgota reklāma ir galvenais veids, kā sīkfaili tiek izmantoti, lai personalizētu jūsu sesijas.

- **Izsekošana**. Iepirkšanās vietnes izmanto sīkfailus, lai izsekotu lietotāju iepriekš apskatītās preces, ļaujot vietnēm ieteikt citas preces, kas viņiem varētu patikt, un paturēt preces iepirkumu grozos, kamēr viņi turpina iepirkties.



Funded by the Erasmus+ Programme of the European Union

# *Dažādi HTTP sīkfailu veidi*

- **Sesijas sīkfaili** tiek izmantoti tikai pārlūkošanas laikā vietnē. Tie tiek glabāti brīvpiekļuves atmiņā un nekad netiek ierakstīti cietajā diskā. Kad sesija beidzas, sesijas sīkfaili tiek automātiski dzēsti.

- **Pastāvīgie sīkfaili** paliek datorā neierobežotu laiku, taču bieži vien daudzās sīkdatnēs ir norādīts derīguma termiņš un tās tiek izdzēstas pēc iepriekš noteikta laika.



Funded by the
Erasmus+ Programme
of the European Union

# *Pastāvīgie sīkfaili*

- Pastāvīgie sīkfaili tiek izmantoti diviem galvenajiem mērķiem:

- **Autentifikācija:** izsekot, vai lietotājs ir pieteicies, un ar kādu vārdu. Tie arī racionalizē pieteikšanās informāciju, lai lietotājiem nebūtu jāatceras vietņu paroles.

- **Izsekošana:** izsekot vairākus vienas vietnes apmeklējumus laika gaitā.



Funded by the
Erasmus+ Programme
of the European Union

# *Kā sīkfaili var būt bīstami?*

- Tā kā sīkfailos esošie dati nemainās, sīkfaili paši par sevi nav kaitīgi.
- Tomēr daži kiberuzbrukumi var nolaupīt sīkfailus un nodrošināt piekļuvi jūsu interneta pārlūkošanas sesijām.
- Briesmas slēpjas viņu spējā izsekot personu pārlūkošanas vēsturei.
- Dažreiz tos var izmantot, lai inficētu datoru ar ļaunprātīgu programmatūru.


Funded by the Erasmus+ Programme of the European Union

# Pirmās puses un trešo pušu sīkfaili

- Pirmās puses sīkfailus tieši izveido jūsu izmantotā vietne. Šie faili parasti ir drošāki, ja vien pārlūkojat respektablas vietnes vai vietnes, kas nav apdraudētas.

- Trešo pušu sīkfailus ģenerē vietnes, kas atšķiras no tīmekļa lapām, kuras lietotāji pašlaik sērfo, parasti tāpēc, ka tās ir saistītas ar reklāmām šajā lapā.
- Apmeklējot vietni ar 10 reklāmām, var tikt ģenerēti 10 sīkfaili, pat ja lietotāji nekad nenoklikšķina uz šīm reklāmām.
- Trešās puses sīkfaili ļauj reklāmdevējiem vai analītikas uzņēmumiem izsekot personas pārlūkošanas vēsturei visā tīmeklī jebkurā vietnē, kurā ir viņu reklāmas.


Funded by the Erasmus+ Programme of the European Union

# *Pirmās puses un trešo pušu sīkfaili*

- Zombiju sīkfaili ir trešās puses sīkfaili, kas ir pastāvīgi instalēti lietotāju datoros, pat ja viņi izvēlas neinstalēt sīkfailus.
- Tie pat mēdz parādīties atkārtoti pēc dzēšanas.
- Tāpat kā citus trešo pušu sīkfailus, tīmekļa analīzes uzņēmumi var izmantot zombiju sīkfailus, lai izsekotu unikālu personu pārlūkošanas vēsturi.
- Vietnēs var izmantot arī zombiju sīkfailus, lai aizliegtu konkrētus lietotājus.


Funded by the Erasmus+ Programme of the European Union

# *Padomi, kā rīkoties ar sīkfailiem*

- ES tiesību aktos ir noteikta nepieciešama lietotāja piekrišana sīkfailu lietošanai.
- Lai ievērotu noteikumus, kas reglamentē sīkfailus saskaņā ar GDPR un e-privātuma direktīvu, jums ir:
- *jāsaņem lietotāju piekrišanu pirms jebkādu sīkfailu izmantošanas, izņemot noteikti nepieciešamos sīkfailus.*
- *pirms piekrišanas saņemšanas jāsniedz precīza un konkrēta informācija par katra sīkfaila izsekotajiem datiem un to mērķi vienkāršā valodā.*
- *jādokumentē un jāuzglabā no lietotājiem saņemtā piekrišana.*
- *jāļauj lietotājiem piekļūt jūsu pakalpojumam pat tad, ja viņi atsakās atļaut noteiktu sīkfailu izmantošanu*
- *jānodrošina, lai lietotājiem būtu tikpat viegli atsaukt savu piekrišanu, kā tas viņiem bija sākotnēji to sniegt.*


Funded by the Erasmus+ Programme of the European Union

# *Padomi, kā rīkoties ar sīkfailiem*

- Lielākā daļa mūsdienu pārlūkprogrammu ļauj pārvaldīt datorā saglabātos sīkfailus.
- Piemēram, iespējams, vēlēsities pieņemt visus sīkfailus, dzēst noteiktas vietnes sīkfailus vai noraidīt visus sīkfailus.
- Jums ir jāmeklē pārlūkprogrammas rokasgrāmata vai palīdzības sistēma, lai atrastu pārlūkprogrammas sniegtās iespējas sīkfailu pārvaldībai.


Funded by the Erasmus+ Programme of the European Union

# *Apiešanās ar ļaunprātīgu programmatūru*

- Ļaunprātīga programmatūra ir ļaunprātīgi kodēta programmatūra, kas ļauj uzbrucējam pilnībā vai ierobežoti kontrolēt mērķa sistēmu, tiklīdz tā ir ienākusi tajā.
- Tā var sabojāt vai modificēt informāciju sistēmā un nozagt informāciju no sistēmas.
- Ir dažādi ļaunprātīgas programmatūras veidi, piemēram, vīrusi, Trojas zirgi, tārpi, sakņu komplekti, spiegprogrammatūra un izpirkuma programmatūra.

- Ļaunprātīga programmatūra var iekļūt sistēmā, izmantojot e-pastu, failu pārsūtīšanu, nejaušas trešās puses programmatūras instalēšanu, kvalitatīvas pretvīrusu programmatūras neizmantošanu.


Funded by the Erasmus+ Programme of the European Union

# *Atšķirība starp vīrusu un tārpu*

## Vīrusi

- tas tiek pievienots programmai vai failam un turpina izplatīties no vienas sistēmas uz otru.
- atkārto (replicē) un izpilda sevi.
- maina sistēmu bez lietotāja ziņas.
- izplatās tādā ātrumā kā ieprogrammēts.

## Tārpi

- vīrusu apakšklase, kuru uzbūve ir līdzīga, atkārtojas no viena datora uz citu.
- izmanto operētājsistēmas (OS), kurām ir vāja drošība.
- liek sistēmai vai tīklam pārstāt reaģēt.
- izplatās ātrāk nekā vīruss.



Funded by the Erasmus+ Programme of the European Union

# *Pretvīrusu noteikšanas programmatūra*

- Antivīruss vai pretļaunprogrammatūra tiek izmantota, lai identificētu, novērstu vai noņemtu sistēmā esošo ļaunprātīgo programmatūru.
- Var veikt sistēmas pārbaudes un regulāri atjaunināt sistēmas drošību.
- Tirgū ir pieejamas dažādas pretvīrusu programmatūras bez maksas vai par maksu.

- Pretvīrusu programmatūras neizmantošana ir "kibernoziedzības veids"! Jūs varat ne tikai kļūt par uzbrukuma upuri, bet arī jūsu datoru var izmantot kā kiberuzbrukuma rīku.


Funded by the Erasmus+ Programme of the European Union

# *Padomi ļaunprātīgas programmatūras novēršanai*

- Līdzīgi tam, ko mēs runājām iepriekš, taču tas jebkurā gadījumā ir jāatceras:

- *Atjauniniet datoru un programmatūru.*
- *Kad vien iespējams, izmantojiet kontu, kas nav administrators.*
- *Padomājiet divreiz, pirms noklikšķināt uz saitēm vai kaut ko lejupielādējat.*
- *Esiet piesardzīgs, atverot e-pasta pielikumus vai attēlus.*
- *Neuzticieties uznirstošajiem logiem, kuros tiek prasīts lejupielādēt programmatūru.*
- *Ierobežojiet failu koplietošanu.*



Funded by the
Erasmus+ Programme
of the European Union

# *Novērtējiet drošības pārkāpumu*

Divi svarīgi jautājumi:

- **Sekojiet uzticamiem avotiem:** *Ja esat viens upuris plašākam uzbrukumam, kas skāris vairākus uzņēmumus vai personas, sekojiet rīcības atjauninājumiem no uzticamiem avotiem, kuru uzdevums ir pārraudzīt situāciju.*

- **Nosakiet pārkāpuma cēloni:** *neatkarīgi no tā, vai esat daļa no plašāka uzbrukuma vai esat vienīgais upuris, jums būs arī jānosaka pārkāpuma cēlonis jūsu konkrētajā iestādē, lai jūs varētu palīdzēt novērst tāda paša veida uzbrukuma atkārtošanos..*



Funded by the Erasmus+ Programme of the European Union

# *Novērtējiet drošības pārkāpumu*

Mēģiniet atrast atbildes uz sekojošiem jautājumiem:

- Kā tika uzsākts uzbrukums?
- Kam ir piekļuve inficētajiem serveriem?
- Kuri tīkla savienojumi bija aktīvi, kad notika pārkāpums?



Funded by the
Erasmus+ Programme
of the European Union

# *Novērtējiet drošības pārkāpumu*

- Piemēram, jūs varat precīzi noteikt, kā tika uzsākts pārkāpums vai uzbrukums, pārbaudot drošības datu žurnālus (reģistrācijas failus), izmantojot ugunsmūri vai e-pasta pakalpojumu sniedzējus, pretvīrusu programmu vai citā veidā.
- Iespējams, jums būs jālūdz kiberdrošības speciālistu atbalsts.
- Nevilcinieties meklēt padomu, ja jūtat zināšanu trūkumu.


Funded by the Erasmus+ Programme of the European Union

# *Novērtējiet drošības pārkāpumu*

Nosakiet personas, kuras ietekmējis pārkāpums:

- Ir ļoti svarīgi noskaidrot, kuras personas, iespējams, ir ietekmējis pārkāpums, tostarp jūsu darbiniekus, klientus un trešo pušu pārdevējus/piegādātājus.

- Novērtējiet, cik nopietns bija datu pārkāpums, nosakot, kādai informācijai tika piekļūts vai kāda informācija tika izvēlēta (atlasīta), piemēram, dzimšanas dienas, pasta adreses, e-pasta konti un kredītkaršu numuri.

# *Novērtējiet drošības pārkāpumu*

Uzsāciet savu kiberuzbrukuma protokolu:

- Jūsu darbiniekiem ir jāzina jūsu politika attiecībā uz datu pārkāpumiem.

- Pēc pārkāpuma iemesla noteikšanas pielāgojiet un paziņojiet savus drošības protokolus, lai nodrošinātu, ka neatkārtojas tāda paša veida incidenti..

- Apsveriet iespēju ierobežot savu darbinieku piekļuvi datiem, pamatojoties uz viņu darba pienākumiem.

# *Pārvaldiet kiberuzbrukuma radītās sekas*

Ja uzbrukums bija uzņēmumam: paziņojiet par pārkāpumu vadītājiem un darbiniekiem, kā arī visiem citiem, kurus var ietekmēt uzbrukums jums.

Tas ietver sekojošo:

*- Sazinieties ar saviem kolēģiem, lai viņi zinātu, kas noticis.*

*- Definējiet komandas locekļiem skaidras pilnvaras saziņai par šo problēmu gan iekšēji, gan ārēji.*

*- Atkopjoties no datu pārkāpuma, ir ļoti svarīgi uzturēt ciešu kontaktu ar savu komandu.*

*- Jums var būt nepieciešama juridiska konsultācija par incidenta juridiskiem aspektiem.*



Funded by the Erasmus+ Programme of the European Union

# *Pārvaldiet kiberuzbrukuma radītās sekas*

Ja uzbrukums bija uzņēmumam: paziņojiet par pārkāpumu vadītājiem un darbiniekiem, kā arī visiem citiem, kurus var ietekmēt uzbrukums jums.

Tas ietver sekojošo:

*- Ja jums ir kiberatbildības apdrošināšana, informējiet savu apdrošināšanu. Ja nē, mēģiniet apsvērt, vai apdrošināšanas iegūšana var būt noderīga.*

*- Kiberatbildības apdrošināšana ir paredzēta, lai palīdzētu jums atgūties pēc datu pārkāpuma vai kiberdrošības uzbrukuma.*

*- Sazinieties ar savu mobilo sakaru operatoru, cik drīz vien iespējams, lai uzzinātu, kā viņš var jums palīdzēt noteikt, kā rīkoties pēc kiberuzbrukuma.*



Funded by the Erasmus+ Programme of the European Union

# *Pārvaldiet kiberuzbrukuma radītās sekas*

**Ja uzbrukums bija uzņēmumam:**

Informējiet klientus

Tas ietver sekojošo:

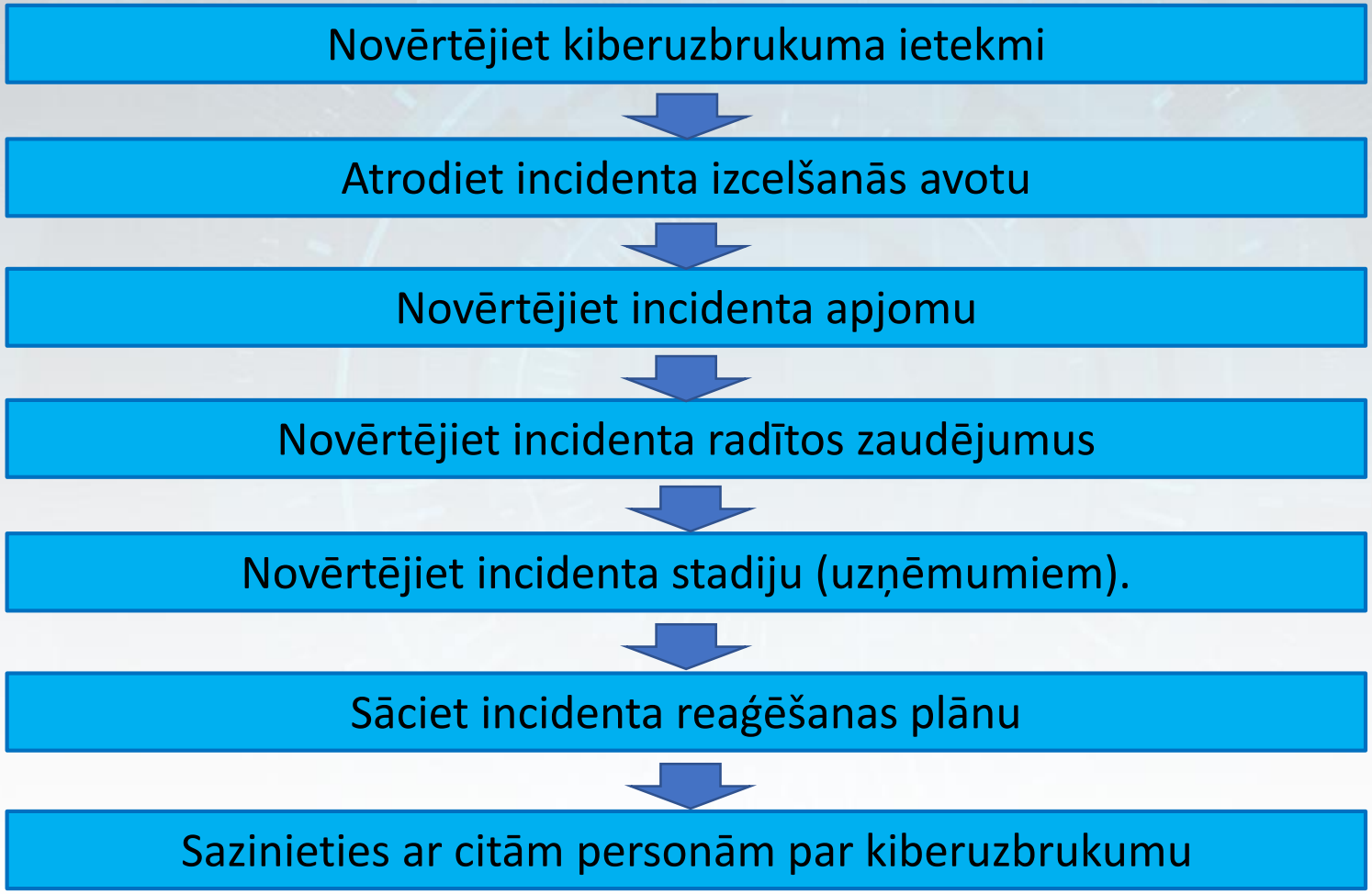
*- Uzsveriet savu vēlmi būt pārskatāmiem attiecībās ar klientiem, apsverot īpašu palīdzības tālruņa līniju, lai atbildētu uz skarto personu jautājumiem.*

*- Saziņa var būt galvenais faktors, lai uzturētu pozitīvas, profesionālas attiecības ar saviem klientiem un samazinātu iespējamos zaudējumus.*



Funded by the
Erasmus+ Programme
of the European Union

# Kiberuzbrukuma novērtējums



# *Ziņošana par kibernoziegumiem*

- Ziņojiet par uzbrukumu atbildīgajai iestādei:
    - - katrai valstij ir atbildīga iestāde, piemēram, CERT.
- Atkarībā no kiberuzbrukuma veida un vietējiem un starptautiskajiem noteikumiem, iespējams, jums būs jāinformē tiesībaizsardzības iestādes.
- Ja baidāties, ka var tikt apdraudēti sensitīvie finanšu dati, jums, iespējams, būs jāsazinās ar kredītkartes izsniedzēju.
- Paskaidrojiet finanšu organizācijai, ka apstrīdat krāpnieku veiktās neautorizētās maksas par jūsu karti vai ja jums ir aizdomas, ka kartes numurs ir apdraudēts.
- Apspriediet turpmākās darbības ar finanšu organizāciju.


Funded by the Erasmus+ Programme of the European Union

# *Ziņošana par kibernoziegumiem*

- Tas ir īpaši svarīgi, ja novērojāt darbības, kas saistītas ar kriminālām darbībām:

- jūs redzat, ka tas nebija ego hakerisma/uzlaušanas gadījums (piemēram, jauns hakeris mēģināja pārbaudīt sevi).

- Ja atklājat, ka esat krāpnieciska incidenta upuris:

*- Sazinieties ar savu IT/drošības nodaļu, ja tāda jums ir;*

*- Nekavējoties sazinieties ar savu finanšu iestādi, lai pieprasītu līdzekļu atsaukšanu;*

*- Sazinieties ar savu darba devēju, lai ziņotu par pārkāpumiem ar algas noguldījumiem.*

# *Darbības pēc tūlītējo draudu novēršanas*

- Atjauniniet savu programmatūru. Instalējiet nepieciešamos ielāpus.
- Nomainiet paroles visā sistēmā.
- Piesardzības nolūkos nomainiet paroles citās sistēmās.
- Divpakāpju verifikācijas metožu ieviešana, lai piekļūtu neaizsargātiem kontiem.

- WAF (tīmekļa lietojumprogrammu ugunsmūra) ievietošana, lai aizsargātu jūsu vietni, ja esat vietnes administrators vai jums ir sava vietne.
- Pārliecinieties, vai jūsu e-komercijas platforma ir savietojama ar 1. līmeņa PCI-DSS (*Maksājumu karšu nozares datu drošības standarts*)


Funded by the Erasmus+ Programme of the European Union

# *Kādas ir turpmākās darbības?*

- “Sešdesmit procenti mazo uzņēmumu un personīgo pārkāpumu pēdējo 3 gadu laikā bija ārēju faktoru rezultāts. Līdz ar to arī darbinieku izglītošanas apmācībām jābūt regulāri notiekošām un visaptverošām. Nodrošiniet, lai darbinieki identificētu brīdinājuma zīmes par aizdomīgiem e-pasta ziņojumiem un pielikumiem un zinātu, kā ziņot par saņemtajiem. Apmāciet viņus arī šifrēt personisku vai sensitīvu informāciju."

- *Maiks Tanenbauks [Mike Tanenbaum], Chubb Ziemeļamerikas izpildviceprezidents un kibernozares vadītājs.*



Funded by the Erasmus+ Programme of the European Union

# *Ja jūsu Gmail vai Youtube konts ir uzlauzts*

- Ja savā Google kontā, Gmail vai citos Google produktos pamanāt nepazīstamas darbības, iespējams, kāds cits to izmanto bez jūsu atļaujas.

**1. solis:** Pierakstieties savā Google kontā

**2. solis:** Pārskatiet darbības un palīdziet aizsargāt savu uzlauzto Google kontu

**3. solis:** Veiciet vairāk drošības pasākumu

*Sīkāku informāciju skatiet: https://support.google.com/accounts/answer/6294825?hl=en*



Funded by the Erasmus+ Programme of the European Union

# *Ja jūsu Facebook konts ir uzlauzts*

Saskaņā ar Facebook ieteikumiem jūsu konts, iespējams, ir uzlauzts, ja pamanāt sekojošo:

- Jūsu e-pasts vai parole ir mainīta.
- Jūsu vārds vai dzimšanas diena ir mainīti.
- Draudzības uzaicinājumi ir nosūtīti cilvēkiem, kurus jūs nepazīstat.
- Ir nosūtītas ziņas, kuras jūs neesat rakstījis.
- Ir izveidotas ziņas, kuras jūs neesat veidojis.

- Ja uzskatāt, ka jūsu konts ir uzlauzts vai pārņemts, jums ir jāapmeklē lapa: https://www.facebook.com/hacked



Funded by the Erasmus+ Programme of the European Union

# *Kā rīkoties, ja jūsu citi konti ir uzlauzti*

- Ir ļoti daudz dažādu sistēmu, kuras var uzlauzt
- Nav iespējams sniegt sīkāku informāciju par jebkuru sistēmu

- Vispārīgi ieteikumi ir:

- meklējiet padomus palīdzības sistēmā
- mēģiniet sazināties ar uzņēmumu, kas ir atbildīgs par produktu



Funded by the
Erasmus+ Programme
of the European Union

# Kopsavilkums

Ir iespējams izvairīties no kiberuzbrukumiem.

- Trenējiet un attīstiet izpratni;
- Attīstiet nepieciešamos ieradumus;
- Izmantojiet piemērotus instrumentus;
- Izveidojiet plānu, kā rīkoties kiberuzbrukuma gadījumā.

# *Uzdevums*

## Novērtējiet kiberdrošības stāvokli uzņēmumā

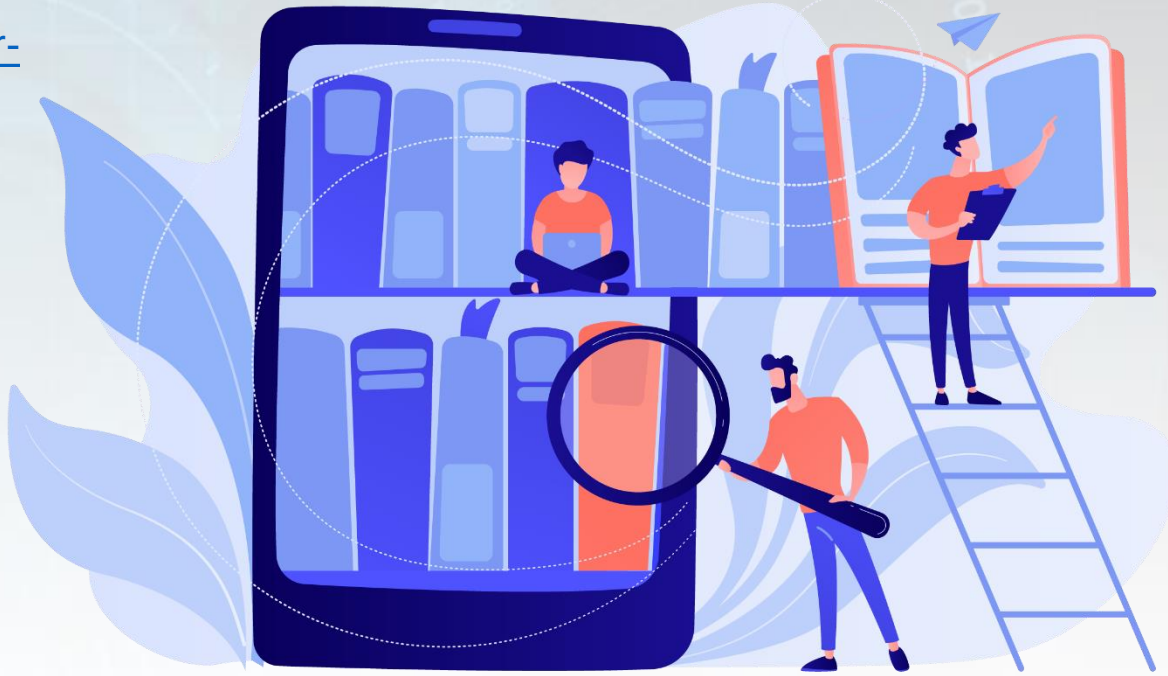
- Gatavības stāvoklis
- Izmantoto instrumentu un rīku kvalitāte
- Paroļu kvalitāte
- Reakcijas
- Izmaiņas pēc uzbrukumiem



Funded by the Erasmus+ Programme of the European Union

# Papildu lasīšana

- Aizsargājiet savu biznesu no kiberdraudiem. Austrālijas valdības vadlīnijas. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats
- Jučongs Li *[Yuchong Li]*, Šinhī Ljū *[Qinghui Liu]*. Visaptverošs pārskata pētījums par kiberuzbrukumiem un kiberdrošību; Jaunākās tendences un jaunākie notikumi. Enerģētikas pārskati, 2021. gada septembris
- Eituls S. Čaudherijs *[Atul S Choudhary]*; Pankadžs P. Čaudherijs *[Pankaj P Choudhary]*; Šrikants Seilve *[Shrikant Salve]*. Pētījums par dažādiem kiberuzbrukumiem un piedāvātā viedā sistēma šādu uzbrukumu uzraudzībai. Proc. IEEE 2018 3. starptautiskā konference par izgudrojošajām skaitļošanas tehnoloģijām

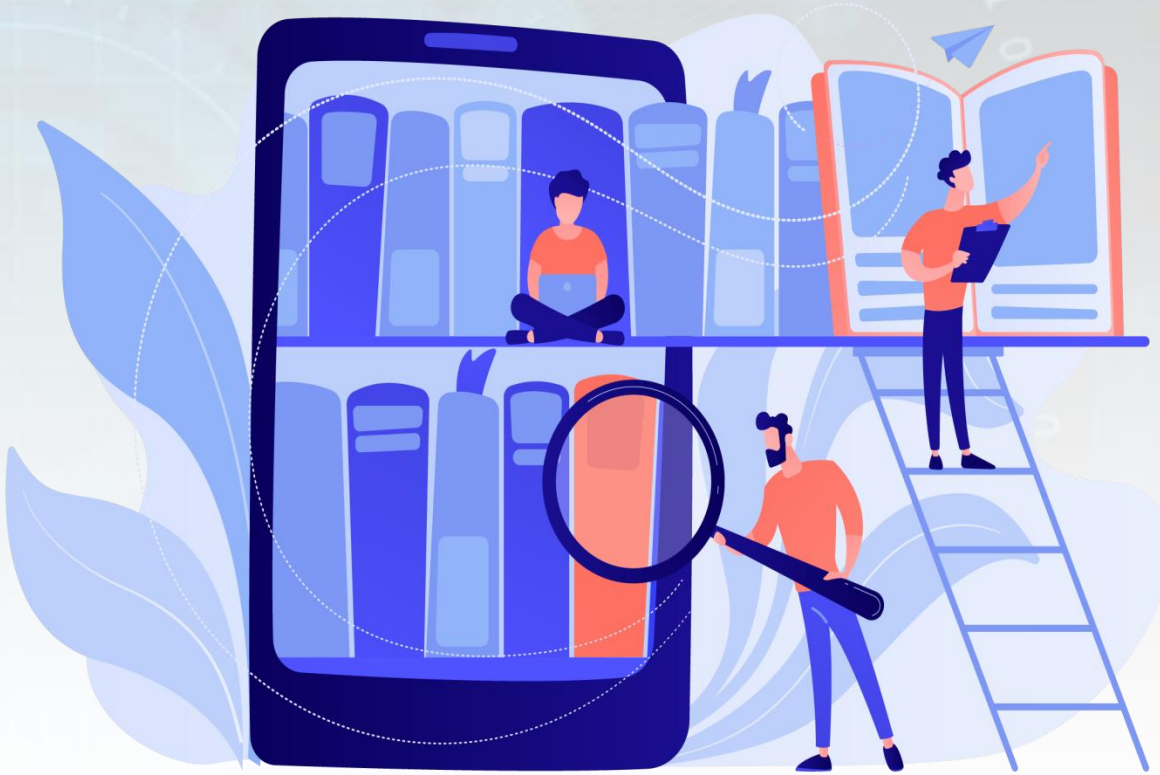




Funded by the Erasmus+ Programme of the European Union

# *Papildu lasīšana*

- Federālā sakaru komisija. Kiberdrošība mazajiem uzņēmumiem. https://www.fcc.gov/general/cybersecurity-small-business
- Kiberdrošības stāvoklis vietējā, štata un federālajā valdībā. Ponemon institūta pētniecības darbs. https://www.ponemon.org/local/upload/file/State%20of%20Cybersecurity%20in%20Government%20FINAL2.pdf
- NCSS labas prakses rokasgrāmata. Eiropas Savienības Kiberdrošības aģentūra. https://www.enisa.europa.eu/publications/ncss-good-practice-guide



# Pateicamies!