DIGITĀLĀ DROŠĪBA

E-PRASMJU NEDĒĻA
ULBROKAS BIBLIOTĒKA
2017.GADA 27.MARTS

E-drošība
E-aizsardzība

- **E-drošība** - viss, kas saistās ar drošu interneta izmantošanu, cilvēka rīcību un zināšanām, interneta ētiku.
- **E-aizsardzība** - tehnoloģiska aizsardzība, programmatūras, vīrusi utt.

Informācijas sabiedrība

Svarīgi atcerēties:

Digitālajā vidē:

Katrs no mums var būt informācijas radītājs.

Katrs no mums ir informācijas patērētājs.

Katrs no mums ir potenciāls uzbrukuma mērķis.

Svarīgi zināt:

Zināšanas par to, kā aizsargāt informāciju par sevi, veicina personīgo drošību.

Rīkojamies saprātīgi: internets

- Pārdomājam, pirms atvērt nezināmas saites
- Ja rodas šaubas, pārbaudām, vai tīmekļa vietne ir īsta
- Bez vajadzības neveram saites portālu komentāros

<u>Kā pasargāt sevi:</u>

- Nespiežam uz nezināmām saitēm e-pastā
- Nespiežam uz nezināmām saitēm pārlūkā
- Neatveram aizdomīgus pielikumus e-pastā
- Veidojam rezerves kopijas svarīgai informācijai

Drošas interneta vietnes

Rīkojamies saprātīgi: e-pasts

- Lietojam darba e-pastu darba vajadzībām
- Lietojam privāto e-pastu privātai sarakstei
- Pārbaudām e-pasta sūtītāju un adresātu
- Neatveram šaubīgas saites e-pastā
- Neatveram šaubīgus e-pasta pielikumus
- Izmantot filtrus, lai atdalītu vēlamu e-pastu no mēstulēm (nevēlamā e-pasta jeb «spama»)
- Elektroniskais pasts nav drošs saziņas līdzeklis (nekad nesūtam pa e-pastu personīgu informāciju: savus personas datus , bankas kontu numurus)

Interneta lietošana mājās: labā prakse

- uzstādīt ‘ugunsmūri’ (*firewall*);
- lietot antivīrusu programmas (regulāri atjaunināt);
- pārbaudīt ar antivīrusu programmu zibatmiņas, CD, DVD diskus;
- lietot licencētu programmatūru;
- nestrādāt ar konfidenciālu informāciju;
- lūgt ievērot noteikumus arī pārējiem datora lietotājiem.

Wi Fi (bezvadu internets): labā prakse

- Izvēlamies uzticamu piegādātāju
- Uzliekam atjauninājumus
- Bezvadu tīkla iekārtas pieejai uzstādīt drošu paroli
- Nomainām noklusētās paroles un lietotājus
- Izvērtējam pieslēgšanos pie publiskā interneta tīkla
- Izmantojot bezvadu datortīklus, jāatceras, ka ir nepieciešams papildus rūpēties par savu privāto datu drošību.

Antivīrusu (pretvīrusu) programmas

- Izmantojot speciālas programmas - interneta **ugunsmūri, antivīrusu** un **pret-spiegu programmas**, **e-pasta filtrus** u.c., jūs varat aizsargāt sevi no daudziem draudiem, kas rodas interneta vidē un izplatās ar datorvīrusu starpniecību. Visas minētās programmas ir nepieciešams regulāri atjaunināt, veidot datu rezerves kopijas, sekot noteiktām rekomendācijām, kā uzvesties internetā.
- Kas ir datorvīrusi un ko tie dara? **Datorvīruss** (*computer virus*) **ir programma**, kas patvaļīgi pievienojas citām datora programmām un to darba laikā veic dažādas nevēlamas darbības: bojā datnes, katalogus un skaitļošanas rezultātus, dzēš vai piesārņo atmiņu, kā arī citādi traucē datora darbību. **Datorvīruss** parasti pats sevi pavairo, inficējot diskos esošās datnes vai sistēmas apgabalus. Ja datorā netiek lietotas pretvīrusu programmas, par vīrusu esamību var pārliecināties tikai tad, kad tie ir sākuši aktīvu darbību.
- **Pretvīrusu programma ir** programma, ar ko pārbauda (skenē) datorā ievadāmās datnes un atmiņas ierīces, lai noskaidrotu, vai tās nav inficētas, kā arī, lai identificētu, izolētu un likvidētu tajās iekļuvušos vīrusus. Jāatceras, ka pretvīrusu programmas prot atklāt tikai tām pazīstamus vīrusus. Tāpēc **pretvīrusu programmām regulāri ir jāatjaunina pretvīrusu definīcijas**

Bezmaksas antivīrusu programmas:

- **Avast**

https://www.avast.com/index

- **AviraAntiVirPersonalEditionClassic**

http://www.avira.com

- **AVG Anti-VirusFree**

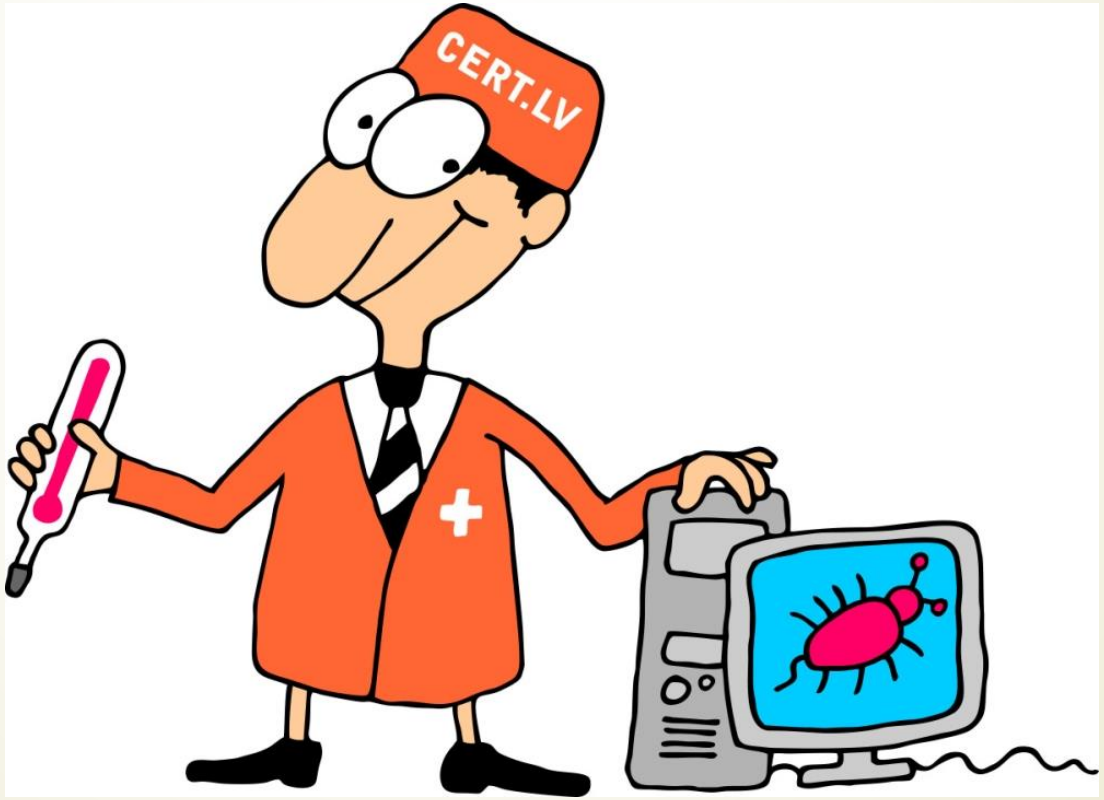
http://www.grisoft.com

- **ClamWin**

www.clamwin.com

- Protams, instalēt vienlaicīgi nepieciešams tikai vienu no tām. Dažkārt bezmaksas programmas aizsargā datoru ne sliktāk, kā maksas programmas. Viena no populārākajām bezmaksas antivīrusu programmām ir **Avast! Free Antivirus.**

Datorologs - ir IT drošības speciālists, kurš var diagnosticēt un, ja iespējams, novērst e-slimības un ļaunatūras datorā un sniegt konsultācijas kā pasargāt datoru nākotnē.



Paroles

Parole ir virtuāla atslēga, ar kuras palīdzību var piekļūt noteiktiem informācijas resursiem.

Ko ievērojam:

Sastāv no lielo un mazo latīņu alfabēta burtu un ciparu kombinācijas, un tās garums nedrīkst būt īsāka par deviņiem simboliem

Nedrīkst izmantot personu identificējošus datus: (piemēram: lietotāja vārdu, uzvārdu, dzimšanas gadu)

Mainīt reizi X mēnešos

Neizmantot iepriekšējās 2 paroles

Dažādiem resursiem lietot atšķirīgas paroles

Piemēri:

Sliktas paroles: Janis1956 Auto9724 Instituta19 Ivita14

Ieteicamas paroles: mz_17gD!o Z36b87lh zo0@amRx

Kā izveidot drošu paroli

1. Izvēlamies tekstu, ko viegli atcerēties – **limuzīns jāņu nakts krāsā**
2. Izvēlamies metodi – pirmais un pēdējais burts
3. Iegūstam paroli – limuzīns jāņu nakts krāsā lsjunska
4. Pastiprinām paroli

- Aizvietošana – l nomainam uz 1 – 1sjunska
- Aizvietošana – a nomainam uz @ - 1sjunsk@
- Pievienošana – lielie burti – 1sjunsk@LI

1sjunsk@LI

Paroli nedrīkst nevienam uzticēt, jo nav iespējams kontrolēt, kam vēl tā var kļūt zināma, un to nav vēlams pierakstīt un pierakstu novietot citiem viegli pieejamā vietā. Kā arī nav vēlams apstiprināt piedāvājumu saglabāt paroli datorā, jo lietpratējam to ir viegli izgūt no tīmekļa pārlūkošanas programmām. Paroli ieteicams regulāri mainīt. Tāpat vajadzētu ar paroli aizsargāt datoru (aizslēgt), ja tas paliek ieslēgts bez uzraudzības.

Privātums, izmantojot publiskos datorus

- Ja ir nepieciešamība izmantot datorus bibliotēkas lasītavā, datorklasē vai kādā citā publiskā vietā, ieteicams **ievērot dažus vienkāršus noteikumus**:
- **atvienojieties no** drošām un ar paroli aizsargātām **mājas lapām** tiklīdz beidzat darbu. Pēc e-pasta, interneta bankas vai kādas citas drošas mājas lapas lietošanas atvienojieties (mājas lapā spiediet uz pogas "iziet", "atvienoties", "izlogoties" u.tml.) un tad aizveriet interneta pārlūkprogrammas logu. Ja tas netiek izdarīts, citam lietotājam ir iespēja pieslēgties mājas lapā jūsu darba videi un darboties jūsu vārdā.
- **neļaujiet pārlūkprogrammai atcerēties jūsu ievadīto lietotājvārdu un paroli**. Ja tas notiek, citam lietotājam ir iespēja piekļūt jūsu datiem. Dažas pārlūkprogrammas var pielāgot, ka tās saglabā datus bez vaicāšanas. Tāpēc pārliecinieties, ka esat izdzēsuši visus privātos datus, ko par jums ir ievākusi pārlūkprogramma, tiklīdz esat beiguši darbu.
- **izdzēsiet pārlūkošanas ierakstus**, ko ir saglabājusi pārlūkprogramma, un pagaidu interneta dokumentus.
- **neatstājiet datorā lejupielādētos un pārvaldītos dokumentus**, kā arī neaizmirstiet paņemt pārnēsājamos datu nesējus.

Sociālā inženierija

Sociālā inženierija – manipulēšana ar cilvēku, lai tas veiktu zināmas darbības vai izpaustu konfidenciālu informāciju.

- **Svarīgi atcerēties:**
  - šķietami visnenozīmīgākā komunikācija ar nepazīstamu cilvēku nedrīkst saturēt sevī informāciju par darbu, dzīves vietu, radiniekiem, personīgu informāciju par sevi.
  - Šos datus var izmantot ļauniem mērķiem: cilvēki ar sliktiem nodomiem var imitēt jūs, izvilinot informāciju no jums vai jūsu ģimenes, jūsu vārdā internetā iegādāties preces vai pakalpojumus. Šādiem datiem ir sava cena, tie tiek pirkti un pārdoti. Šādus noziedzniekus sauc par identitātes zagļiem.
- **Personas dati internetā**
- Arvien vairāk elektroniskajos pakalpojumos ir nepieciešama identifikācija, un mobilajām tehnoloģijām paliekot arvien populārākām, elektroniskais privātums kļūst arvien lielāka problēma. Katru reizi, kad internetā veicat maksājumus ar kredītkarti, autorizējaties mājas lapā vai vienkārši sērfojat publiskā bezvadu internetā, jūs riskējat ar to, ka kāds var piekļūt jūsu datiem.

Sociālie tīkli

- Sociālie tīkli ir tīmekļa vietnes, kur, reģistrējoties un izveidojot savu individuālo profilu, ir iespējams sazināties ar citiem cilvēkiem (draugiem, radiem, skolas biedriem, paziņām)
- Mūsdienās pastāv daudz dažādi sociālie rīki dažādām mērķauditorijām un interešu grupām. Lai tajos nodrošinātu savu datu un informācijas drošību, ieteicams uzmanīgi iepazīties ar sociālā rīka drošības uzstādījumiem.
- Pirms veidot profilu kādā sociālajā tīklā, pacentieties atbildēt uz šādiem jautājumiem:

✓ Kādam nolūkam es veidoju profilu?

✓ Kādu informāciju es vēlos publicēt par sevi?

✓ Kas varēs izlasīt šo informāciju?

✓ Cik labi es pazīstu cilvēkus, kuri lasīs šo informāciju?

✓ Vai šo informāciju varēs izlasīt tikai sociālajā tīklā reģistrēti cilvēki?

Facebook

- Visi dati, ko ievadām Facebook, saglabājas tur (Facebook serveros) uz visiem laikiem: publicētie ieraksti, foto, visi «laiki» un ieteikumi draugiem (share)
- Saglabājas ziņas, cik bieži apmeklējam savu profilu un no kādām ierīcēm, kad un ko pievienojam vai dzēšam no savu draugu saraksta un citas tehniskas detaļas
- Analizē mūsu darbības, ievāc datus par to, kādas valodas pārvaldām, par kādām precēm interesējamies, kur atrodamies, tādējādi veido tādu kā lietotāja alternatīvo profilu
- Seko līdzi tam, kuras mājaslapas apmeklējam, kas atrodas ziņu lentē vai reklāmās
- Pat tad, ja dzēšam kādu komentāru vai ierakstu, tas uz visiem laikiem paliks Facebook serveros.

Viedtālruņi un citas vied ierīces

Viedtālrunis - miniatūrs dators, kurš spēj:

- pieslēgties bezvadu internetam;
- fotografēt un filmēt;
- automātiski apmainīties ar datiem ar pakalpojuma sniedzēju;
- noteikt atrašanās vietu;
- kalpot kā datu nesējs;
- būt radiouztvērējs un mūzikas/video atskaņotājs;
- ... un visbeidzot spēj pildīt arī telefona funkcijas.

Viedo ierīču apdraudējumi:

- Nav atjaunota operāciju sistēma
- nedrošs wifi
- viltotas lietotnes
- Ierīces nozagšana vai pazaudēšana

Vied ierīces: labā prakse

- Aizsargā ar paroli (autentifikācija un autorizācija)
- Izmantojam tikai tās iespējas, kuras konkrētajā brīdī nepieciešamas
- Ieslēdzam auto-lock funkciju
- Instalējam drošas lietotnes, neinstalēt apšaubāmas izcelsmes lietotnes
- Vienmēr zinām, kur atrodas ierīce
- Neglabājam svarīgu un aizsargājamu informāciju
- Savu ierīci lietojam tikai pats/pati

Kopsavilkums

- Jaunas tehnoloģijas – jauni riski
- Katram pašam ir jāizvērtē iespējamais apdraudējums
- Labākā aizsardzība – **SAPRĀTĪGA** rīcība