TRANS eSCOUTS
Empowering eFacilitators for intergenerational dialogue

Lifelong Learning

# DROŠĪBA INTERNETĀ

2015

# Saturs

# IEVADS

Mācību materiāls “Drošība internetā” paredzēts izmantošanai mērķgrupu apmācībā projekta **TRANS E-Scouts** ietvaros.

Tajā ir atspoguļoti galvenie aspekti, kam būtu jāpievērš uzmanība, lai interneta lietošana būtu droša, t.i., e-drošībai un e-aizsardzībai.

Projekta ietvaros materiāls izmantojams 2. modulī: *M2 E-prasmju veicinātāji - jaunieši apmācība*, kurā jaunieši tiek sagatavoti darbam ar senioru auditoriju, kā arī 3. modulī: *M3 Jaunieši - seniori - IKT prasmju apmācība*, kurā jaunieši kā pasniedzēji darbojas ar senioru auditoriju.

**TRANS E-scouts** ir Eiropas Savienības atbalstīts projekts, kura ietvaros paredzēta starppaaudžu sadarbība un kompetenču un prasmju apmaiņa. Projekta ietvaros jaunieši gūst pieredzi, darbojoties kā IKT prasmju pasniedzēji senioru auditorijā. Savukārt seniori apgūst jaunas digitālās prasmes, kā arī nodod savu pieredzi jauniešiem, darbojoties kā padomdevēji.

Projektu līdzfinansē EK Mūžizglītības programma un tas tiek īstenots Horvātijā, Latvijā un Lietuvā.

Vairāk par projektu

*Šis projekts tika finansēts ar Eiropas Komisijas atbalstu. Šis materiāls atspoguļo vienīgi autora uzskatus, un Komisijai nevar uzlikt atbildību par tajā ietvertās informācijas jebkuru iespējamo izlietojumu.*

# DROŠĪBA INTERNETĀ

## E-drošība un e-aizsardzība

Mūsdienās ir grūti iztēloties savu dzīvi bez interneta. Internetā ikviens no mums lasīt ziņas, piekļūt dažādiem pakalpojumiem, sazināties viens ar otru, pārvaldīt savus finansu darījumus un meklēt gan profesionālu, gan izklaidējošu informāciju, taču, vai mēs protam lietot internetu droši un vai mākam pasargāt savus tuvos cilvēkus no iespējamiem draudiem?

Ar **drošību saprot** datoru tīklos un datoru sistēmās glabājamo datu aizsardzību pret to bojāšanu, zaudēšanu vai nesankcionētu piekļuvi.

Mūsdienās datortīklu un it īpaši interneta straujā izplatība un pieejamība liek šai problēmai pievērst arvien lielāku uzmanību. Drošības raksturošanai lietoti divi termini: **e-drošība un e-aizsardzība**.

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

## E-drošība

Ikdienā internetu lieto ne tikai cilvēki ar labiem nodomiem. Līdzīgi kā reālajā dzīvē, sastopami arī cilvēki ar sliktiem nodomiem, kas cenšas iegūt nelegālus labumus, maldinot un ļaunprātīgi iegūstot uzticību. Uzņēmumu pārstāvji bieži vien nekorekti lieto interneta pakalpojumus, lai izplatītu nevēlamus e-pastus un reklāmas. Pornogrāfijas bizness ir pārpludinājis internetu ar bērniem nepiemērotiem materiāliem. Komunikācija ar citiem cilvēkiem internetā ne vienmēr var izrādīties tik jauka, kā plānots. Anonīmi cilvēki var iespraukties sarunās, paust savu agresiju vai kā citādi aizvainot. Jūtīgāki pret pāridarījumiem ir nepilgadīgie, kas visbiežāk nevar vai negrib par to runāt ar pieaugušajiem, dažkārt pat arī ne ar saviem draugiem.

Ja internetā sūtītā informācija nav speciāli šifrēta, to ir iespējams aplūkot arī citiem cilvēkiem. Jūsu e-pastus un informāciju par apmeklētajām mājas lapām var iegūt jūsu darba devējs, interneta pakalpojumu sniedzējs un jūsu izmantoto datu kanālu pārvaldītāji. Speciālas programmas dažādās valstīs ieraksta un analizē gandrīz visu starptautisko interneta plūsmu.

Ja jūs izmantojat bezvadu internetu, šis risks ir vēl augstāks. Tādā gadījumā jūsu datus var pārtvert ikviens, kas atrodas interneta signāla izplatīšanās apgabalā.

Internets ir kā grūti kontrolējama bezmaksas informācijas aprites platforma, kurā ir arī daudz kaitīgas informācijas un nepieņemama satura. Dažādi pakalpojumi interneta satura uzturēšanai lielākoties cīnās pret jau pastrādātajiem elektroniskajiem noziegumiem, **tāpēc interneta lietotājiem arī pašiem jābūt uzmanīgiem**.

Atšķirībā no kādreizējām statiskajām interneta mājas lapām, šobrīd pastāvošās lapas ir dinamiskas. Galvenās izmaiņas nav veiktas lapu saturā, bet gan metodēs, kā tās tiek radītas. Mūsdienās interneta mājas lapas

lielākoties veido paši lietotāji, kurās tie pauž savas idejas, dalās ar pieredzi, publicē fotogrāfijas un filmas. Lai labāk atdalītu moderno tīmekli no tā kādreizējās formas, tas tiek saukts par **tīmekli 2.0**.

Visbiežāk sastopamie draudi pastāv sociālo tīklu lietotāju drošības un datu aizsardzības jomā. Tā kā sociālo tīklu mājas lapas atrodas uz datoriem „kaut kur tīklā", pastāv iespēja, ka īpašnieki tos var jebkurā mirklī izslēgt, mainīt pieejas noteikumus, pārdot datus trešajām pusēm vai arī paši izmantot mārketingam, reklāmai vai kam citam. Pastāv arī liela iespēja datus nozagt un pārdot. Bezmaksas mājas lapas negarantē datu drošību un atjaunošanu.

Dažas no modernā tīmekļa tehnoloģijām rada grūtības aplūkot visu interneta saturu pārlūkprogrammas vai operētājsistēmas ierobežojumu dēļ.

## Nepieciešamība pēc lietotājvārda un paroles

Informācijas drošība ir tieši saistīta ar datoru drošību, kas tiek realizēta veicot aizsardzību pret datorvīrusiem, urķiem (hakeriem) un datora bojājumiem, piešķirot **paroles** un ierobežojot piekļūšanas tiesības, kā arī regulāri **dublējot svarīgus datus**, tādējādi nodrošinot pilnvērtīgu datu aizsardzību.

**Datu aizsardzība** ir pasākumi, ko, izmantojot aparatūru un programmatūru, veic, lai izsargātos no datu zaudēšanas, bojāšanas vai nesankcionētas piekļuves.

Datoros esošās informācijas drošību var apdraudēt ne tikai cilvēki, bet arī datoru un atmiņas ierīču bojājumi, tāpēc jāveic arī apkārtējās vides nevēlamu apstākļu ietekmes samazināšanas pasākumi.

Izmantojot datoru, nepieciešams savu lietotāju padarīt privātu, t.i., nepieejamu citiem, lietojot paroli.

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

Paroles izmanto, lai pret nesankcionētu piekļuvi aizsargātu datoru, darbvirsmu, programmas, datnes, e-pastu un tiešsaistes iepirkšanās norēķinus. Paroles izmanto arī daudzlietotāju sistēmās, pirms lietotājs ar to var uzsākt darbu.

| **Nelietot** | **Ieteicams** |
|---|---|
| Ar sevi saistītus vārdus, piemēram, savu ģimenes locekļu vai mājdzīvnieka vārdu | Paroli izvēlēties vismaz 8 simbolus garu - jo tā ir garāka, jo grūtāk to uzminēt |
| Atsevišķu, jebkurā valodā loģiski saprotamu, vārdu | Izmantot kāda sakarīga teksta vārdu pirmos burtus, piemēram, Kur tu teci, kur tu teci, gailīti man'? - KttKttGm? |
| Zīmīgus skaitļus, piemēram, dzimšanas datumu vai tālruņa numuru | Parolei vajadzētu saturēt vismaz 2 lielos un divus mazos burtus un vismaz vienu ciparu un kādu simbolu, piemēram, 2xKttG} |

**Vairāk informācijas par paroļu lietošanas noteikumiem**, drošām parolēm, biežāk lietotajām parolēm, tas nozīmē, viegli uzminamām var atrast interneta vietnē: http://www.drossinternets.lv/page/203.

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.

Ievadītās paroles rakstzīmju vietā parasti ir redzamas tikai viena veida rakstzīmes, piemēram, zvaigznītes, krustiņi vai punkti. Noteikts skaits nepareizi ievadītu paroļu var tikt uzskatīts par atminēšanas mēģinājumu, un pieejas tiesības var tikt liegtas. Lai nevarētu atminēt paroles un iegūtos datus izmantot ļaunprātīgi, ieteicams ievērot labu (drošu) paroļu veidošanas un lietošanas noteikumus.

**Tīmekļa vietne** ir informācijas un interaktīvu pakalpojumu sakopojums, kas uzbūvēts no tīmekļa lappusēm un cita veida datiem (attēliem, skaņām u. tml.).

**Tīmekļa vietnes iedala:**

- publiskajās, kam var piekļūt jebkurš tīkla lietotājs;
- privātās jeb aizsargātās, kam var piekļūt, lietojot lietotāja vārdu (user name) un paroli (password). Lietotāji var tikt dalīti grupās ar dažādām piekļuves tiesībām (access rights), kas nosaka lietotāja tiesības piekļūt tīkla resursiem, piemēram, serverim vai atsevišķām mapēm, kā arī atļautās darbības, piemēram, tikai lasīt vai lasīt un mainīt datnes saturu.

## Kredītkartes izmantošana interneta pirkumiem un rezervācijām

Galvenā drošības problēma datortīklos ir to aizsardzība pret nesankcionētu izmantošanu, piemēram, veicot elektroniskos maksājumus, pastāv iespēja, ka dati var tikt nozagti un ļaunprātīgi izmantoti.

Lietojot kredītkarti, rūpīgi jāizvēlas sadarbības partneri, kas ir labi zināmi un uzticami un lieto drošas datu pārraides metodes.

Lai pārliecinātos, ka **interneta maksājums tiek veikts droši**, pārliecinieties, ka mājas lapa ir aizsargāta un izmanto drošo protokolu. Mājas lapas adreses laukā ierastā protokola http://... vietā būs redzams **https://** drošais protokols.

Arvien biežāk bankas piedāvā papildus aizsardzību pirkumiem internetā jeb 3D Secure sistēmu. **3D Secure sistēma** aizsargā jūsu karti ar diviem papildu aizsardzības veidiem - pirmkārt, ar jūsu identifikācijas ziņojumu un, otrkārt, ar paroli. Katrā iepirkšanās reizē internetā jūsu reģistrētais identifikācijas ziņojums būs redzams darījuma apstiprināšanas logā, un jums būs jāievada parole.

Identifikācijas ziņojums būs redzams, un paroli pirms interneta pirkumu veikšanas vienmēr prasīs tikai tie tirgotāji internetā, kas paši izmanto 3D Secure drošības sistēmu un ir tajā reģistrējušies.

## Aizliegta un ierobežota informācija internetā

Informācija, kas tiek publicēta internetā, kļūst publiska. Diemžēl bieži vien ir iespējams publicēt arī informāciju, kuru likums paredz ierobežot vai pat pilnīgi aizliedz. Tāpēc **informāciju var klasificēt**, kā ierobežotu vai pilnīgi aizliegtu.

**Aizliegtu informāciju** ir aizliegts nopludināt vai izplatīt saskaņā ar Latvijas likumdošanu:

- pornogrāfiska satura informācija (tai skaitā, informācija, kas attēlo bērnu seksuālo izmantošanu (pedofilija);
- materiāli, kas vērsti uz cilvēka vai grupas pazemošanu, aizskaršanu, rosina uz nevienlīdzīgu attieksmi dzimuma, seksuālās orientācijas, rases, tautības, valodas, izcelsmes, sociālā statusa, reliģijas, uzskatu vai attieksmes dēļ;
- kā arī jebkura cita informācija, kas aizliegta Latvijas likumdošanā.

**Ierobežota informācija** tiek regulēta, lai tiktu aizsargāti nepilngadīgie. Tā ir informācija, kurai ir negatīva ietekme uz nepilngadīgo fizisko, psihisko vai morālo attīstību:

- informācija, kurā atspoguļota fiziska vai psihiska vardarbība, vai kriminālas darbības;
- informācija, kurā atspoguļota erotika, parādot vai imitējot dzimumaktu vai kāda cita veida seksuālo apmierinājumu, dzimumorgānus vai intīmpreces;
- informāciju, kurā parādīts miris vai smagi ievainots cilvēks (izņemot gadījumus, kad šāda informācija nepieciešama personas identificēšanai);
- informācija, kas rada bailes vai šausmas, kūdīšana uz pašsakropļošanos vai pašnāvību;
- cita informācija, kuru ierobežo likums.

## 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.

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.

Īpaši izplatīta ir e-pasta adrešu pārdošana. Tās iegādājās surogātpasta izplatītāji. Papildus informācija par **surogātpastu** atrodama mājas lapā: https://www.esidross.lv/2012/08/22/surogatpasts-jeb-spams/

**Lietojot internetu, jāievēro sekojoši noteikumi:**

- neatklājiet savu identitāti: vārdu, uzvārdu, adresi, e-pasta adresi un citu personīgo informāciju;
- internetā ieteicams neizmantot savu īsto vārdu - pieņemiet segvārdus;
- esiet uzmanīgi internetā sarunājoties ar tiem, kas prasa jums nekavējoties atklāt jūsu personas datus vai vēlas satikt jūs;

- informācija par darbu, tuviem cilvēkiem vai jūsu personīgā mājas lapa arī ietilpst personas datos, neizpaudiet to nevienam;
- neiesniedziet savus datus neskaidru mājas lapu reģistrācijas formās. Ja reģistrācija ir nepieciešama, lai lejupielādētu dokumentu vai programmu no šīs mājas lapas, lietojiet vienreizēju e-pasta adresi. Īslaicīgas e-pasta adreses ir saņemamas bez reģistrēšanās, piemēram, vietnē http://10minutemail.com/10MinuteMail/index.html. Ja esat pārliecināts, ka uz e-pastu netiks sūtīta nekāda svarīga informācija, jūs varat ievadīt nederīgu adresi xlietotajs@piemers.lv
- Ja jūs kādā mājas lapā paziņojat savu īsto e-pasta adresi, rakstiet to tā, lai robots to nespētu atpazīt. Piemēram, tā vietā, lai rakstītu vards.uzvards@likta.lv, jūs varat rakstīt *vārds punkts uzvārds at likta punkts lv*.
- Kad vēlaties iegādāties preces vai pakalpojumus, pārliecinieties vai mājas lapa ir uzticama. Mājas **lapai ir jābūt šifrētai un drošai**, par to liecina mājas lapas adreses sākumā **https://.** Interneta **pārlūkprogrammas adreses joslā ir jābūt atslēdziņas simbolam** vai slēdzenei.

**Izmantojot bezvadu datortīklus**, ir nepieciešams papildus rūpēties par savu privāto datu drošību.

- Dati, kas nosūtīti no publiskiem interneta pieejas punktiem, ne vienmēr ir šifrēti, kā tas tiek darīts lielākajā daļā māju tīklos. Informācija par datu kodēšanu ir atrodama pieejas punkta mājas lapas sadaļā ***Privātums***. Ja jums pieejamajā interneta zonā nav pieejama kodēšana, un jūs glabājat svarīgus un konfidenciālus dokumentus savā datorā, labāk nepieslēgties šim tīklam vai arī šifrēt svarīgus datus.
- Jums ir jāpārliecinās vai saziņa ir droša gadījumos, kad veicat finansu operācijas internetā: ir jāpārliecinās vai interneta pārlūkprogrammā parādās slēdzenes simbols un vai mājas lapas adrese sākas ar https://.
- Šie līdzekļi jūs pasargās no nejaušiem interneta noziedzniekiem, taču profesionāls noziedznieks spēs apmānīt jebkuru drošības sistēmu. Tāpēc, ja vēlaties pilnībā nodrošināt savu datu drošību, jums jāizvairās izmantot bezvadu tīklu svarīgu datu, piemēram, kredītkartes numuru, finansu datu un citu nozīmīgu datu sūtīšanai.

## Privātums, izmantojot publiskos datorus

Ja tomēr ir nepieciešamība izmantot datorus kafejnīcā, 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.

Kā neaizmirst **izdzēst pārlūkošanas vēsturi?**

Ieteicams ir **pārnēsāt savu personīgo pārlūkprogrammu, e-pastu un citas nepieciešamās programmas USB zibatmiņas diskā**. Interneta vietnēs http://portableapps.com un http://www.liberkey.com pieejamas programmas, kas speciāli sagatavotas instalācijai zibatmiņā.

Cilvēki ar sliktiem nodomiem uz datoriem interneta kafejnīcās vai uz citiem publiskajiem datoriem bieži atstāj **spiegprogrammatūras**. Šīs programmas reģistrē visus nospiestos taustiņus un ieraksta lietotājvārdus un paroles, ko jūs esat ievadījuši. Iespējams, ka vienīgais veids, kas neprasa ilgu atklāšanu un atbrīvošanos no spiegprogramatūras, ir izmantot paroļu pārvaldības programmas, kas tiek glabātas USB zibatmiņas diskos un automātiski savada paroles reģistrācijas formās.

Ja nevēlaties, lai pārlūkā tiktu saglabāta informācija par apmeklētajām vietnēm un lejupielādēto saturu, varat pārlūkot tīmekli **inkognito režīmā.**

| Pārlūkprogramma | Informācija par privātā (inkognito) režīma lietošanu |
|---|---|
| **Google Chrome** | https://support.google.com/chrome/answer/95464?hl=lv |
| **Internet Explorer** | http://onlinehelp.microsoft.com/lv-lv/bing/ff808346.aspx |
| **Mozilla Firefox** | https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history |

## Privātums un datu aizsardzība

Vairums valstu mēģina kontrolēt internetā publicēto informāciju ar likumdošanas aktiem, taču interneta videi, salīdzinājumā ar citiem medijiem, tos ir grūtāk piemērot.

Viens no galvenajiem likumiem, kas regulē informāciju Latvijas masu medijos, ir **likums „Par presi un citiem masu informācijas līdzekļiem”**. Lai arī šis likums tieši neattiecas uz internetā publicēto, tajā tiek apskatīti galvenie aspekti informācijas publicēšanā.

Fiziskas personas datu apstrādes kārtību nosaka **„Fizisko personas datu aizsardzības likums”** (FPDAL). Tā 2. panta 4. punkts nosaka, ka personas datu apstrāde ir jebkuras darbības ar personas datiem. Personas datu apstrādes piemēri:

- aptaujas anketas aizpildīšana internetā;

- preces pasūtīšana internetā;
- e-pasta nosūtīšana uz adresi vards.uzvards@darbavieta.lv,
- e-pasta adreses vards.uzvards@darbavieta.lv nodošana sadarbības partnerim.

**FPDAL 2. panta 3. punkts** nosaka, ka **personas dati ir** jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisku personu.

Jāņem vērā, ka nav nozīmes informācijas formātam (elektroniska, papīra formātā ietverta, skaņa, attēls). Nav arī nozīmes tam, vai informācija ir sakārtota noteiktā sistēmā vai datu bāzē, šie visi ir personas dati.

**Personas datu apstrādes noteikumi:**

- personas datu apstrādes tiesisks pamats (FPDAL 7., 11., 12., 13. un 13.1. pants);
- personas datu apstrādes tiesisks mērķis (FPDAL 10. panta pirmās daļas 2. punkts);
- personas datu tehniska un organizatoriska aizsardzība (FPDAL 26. pants);
- personas datu apstrādes reģistrācija (FPDAL 21. pants);
- datu subjekta tiesību ievērošana (FPDAL 15. - 19. pants).

## Draudi privātumam

Internetā izplatītā informācija ceļo cauri daudziem datoru tīkliem, un to var redzēt visā pasaulē. Ja netiek ievērotas nepieciešamās drošības normas, cilvēki ar sliktiem nodomiem var uzzināt ne tikai jums zināmas privātas lietas, bet arī izmantot jūsu identitāti (uzdoties par jums).

Runājot par ļaunumu, ko var radīt datu zaudēšana, jāpiemin darbs ar internetbankām. Nolaidības dēļ atklājot savus piekļuves datus, varat zaudēt naudu.

Ja tiešsaistes sarunu laikā atklājat savu mājas, darba adresi, telefona numuru vai personīgās fotogrāfijas, vai publicējat tās mājas lapā, riski ir tikpat augsti.

Latvijā ir **institūcijas, kas atbild par datoru tīklu drošību un internetu**, to atbildības līmeņi ir dažādi.

**Eiropas informācijas tīklu drošības aģentūra** (*Europe Network Information Security Agency)* ir vienīgā Eiropas Komisijas institūcija, kas atbild par informācijas tīklu drošību. Tās uzdevums ir palīdzēt un dot ieteikumus Eiropas Komisijai un dalībvalstīm par informācijas drošību, lai risinātu dažādas ar drošību saistītas problēmas.

**Datu valsts inspekcija** uzrauga personas datu aizsardzību Latvijā. **Projekts „Drošība tiešsaistē"** (http://www.draudzigsinternets.lv) Latvijā ir *Microsoft* iniciatīva. Tā tiek īstenota kopā ar atbalstītājiem - *Valsts bērnu tiesību inspekciju, Net-Safe Latvia* projektu, kā arī virkni nevalstisko organizāciju. Kampaņas vietnē var atrast viegli saprotamus, uzticamus un praktiskus padomus par drošību internetā, kas palīdz arī visneaizsargātākajiem lietotājiem, strādājot tiešsaistē, justies droši.

**Latvijas Drošāka interneta centra** darbību nodrošina Latvijas Interneta asociācija kopā ar partneri - Valsts bērnu tiesību aizsardzības inspekciju. Darbības nodrošināšanai un aktivitāšu īstenošanai ir piešķirts

līdzfinansējums 75% apmērā no Eiropas Komisijas Drošāka Interneta programmas. Centra darbības virziens ir bērnu, jauniešu, skolotāju un vecāku informēšana un izglītošana interneta satura drošības jomā - par iespējamajiem riskiem un apdraudējumiem internetā (naida kurināšana, rasisms, bērnu pornogrāfija un pedofilija, emocionāla pazemošana internetā, personas identitātes zagšana un datu ļaunprātīga izmantošana, uzvedības noteikumi internetā, tīmekļa etiķete utt.).

**CERT.LV** ir informācijas tehnoloģiju drošības incidentu novēršanas institūcija, kuras uzdevumi - uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu IT drošības incidentu novēršanā, sniegt atbalstu valsts institūcijām IT drošības jomā, organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem un citiem interesentiem. Vairāk informācijas par **CERT.LV** atrodama institūcijas mājas lapā.

**ZIŅOJUMU LĪNIJA:** mājas lapā *http://drossinternets.lv/page/3* sabiedrībai ir iespēja elektroniski ziņot par atklātajiem pārkāpumiem un nelegālu saturu internetā. Ziņojumi tiek apstrādāti atbilstoši LR normatīvajiem aktiem ar Valsts policijas atbalstu.

**UZTICĪBAS TĀLRUNIS 116111:** iespēja bērniem/jauniešiem ziņot par pārkāpumiem internetā un saņemt psihologa atbalstu un konsultāciju dažādu situāciju risināšanai. Ziņojumu līnijas darbu nodrošina Valsts bērnu tiesību aizsardzības inspekcija.

## Autortiesības

**Autortiesības ir** autora personisko nemantisko un mantisko tiesību kopums uz paša radītu intelektuālo darbu tā materiālajā formā (Veikša). Šīs tiesības veido divas daļas: personiskās jeb morālās un mantiskās jeb ekonomiskās tiesības.

Latvijas Republikas teritorijā tās nosaka **Autortiesību likums** un primārais to uzdevums ir aizsargāt autora darbu pret neatļautu lietošanu.

Gan intelektuālo īpašumu (Intelektuālais īpašums sastāv no patentiem, autortiesībām un preču zīmēm), gan datoros un datu nesējos glabāto informāciju pret neatļautu izmantošanu un izplatīšanu aizsargā likumi.

**Autortiesības (Copyright)** ir Starptautiskajā Ženēvas autortiesību konvencijā (Universal Copyright Convention - UCC) 1952. gadā noteikts autora tiesiskais stāvoklis, kas nosaka sevišķas tiesības publicēt, reproducēt un izplatīt literatūru, muzikālu, mākslas u. tml. darbu.

Tiek aizstāvētas tikai to autoru tiesības, kuru publikācijās iespiesta **autortiesību zīme ©.** Latvijā darbojas Autortiesību likums un Vispasaules intelektuālā īpašuma organizācijas (WIPO) līgums par autortiesībām. Atbildība par likumu pārkāpumiem ir paredzēta Administratīvo pārkāpumu kodeksā (155. pants), un Krimināllikumā (148. un 149. pants). Datoru lietotājiem jāievēro Autortiesību likuma normas, kas attiecas uz grāmatām, video un mūzikas diskiem un kasetēm, kā arī programmatūru. Datorprogrammu kopēšanu, izplatīšanu vai izmantošanu bez autortiesību īpašnieka atļaujas sauc par datorprogrammu pirātismu.

**Nelegālā datorprogrammu izmantošana ir, piemēram:**

- viena legāli iegādāta programmatūras kompaktdiska instalēšana uz vairākiem datoriem, ja licencē vai līgumā ir norādīts, ka to atļauts instalēt tikai uz viena datora;
- programmas kopēšana instalēšanai un izplatīšanai bez autora atļaujas;
- programmatūras instalēšana no nelegāli iegādāta diska;
- nelegālas datorprogrammu kopijas lejupielāde no interneta. Internetā lejupielādei bez maksas tiek piedāvāta gan programmatūra, gan cita veida datnes (teksti, attēli u.c.). Ne vienmēr to publicētājiem ir tiesības tos izplatīt lietošanai citiem. Tāpēc pirms lejupielādes nepieciešams pārliecināties, vai to kopēšana ir legāla.

## E-aizsardzība

**E-aizsardzība** aplūko iespējamos tehniskos draudus datoram.

Kaitīga programmatūra lielākoties ietekmē datora veiktspēju, bet dažreiz datoram ir novērojama neparasta uzvedība, kā, piemēram:

- programmas sāk strādāt lēnāk un vienkāršu darbību veikšanai tiek patērēts daudz vairāk laika nekā parasti;
- lietojumprogrammu darbībai sāk pietrūkt datora darba atmiņas;
- atverot interneta pārlūkprogrammu, parādās dažādi reklāmu logi;
- interneta pārlūkprogrammai pēc noklusējuma uzstādītā mājas lapa ir nomainījusies bez jūsu ziņas;
- sistēmas Windows pārlūkprogrammā vai arī citās parādās jaunas rīkjoslas, no kurām grūti atbrīvoties;
- programmas bez jūsu ziņas savienojas ar internetu un intensīvi, ilgu laiku lejupielādē datus.

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.

### Datorvīruss

**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. (Datu pārraides un apstrādes sistēmas. Skaidrojošā vārdnīca 1995).

**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.

Datora vīrusi darbojas līdzīgi bioloģiskajiem vīrusiem. Tie var ilgi uzturēties datorā, neliekot sevi manīt. Dažādi vīrusi aktivizējas dažādi, piemēram, ir vīruss, kurš aktivizējas, ja 13. datums iekrīt piektdienā. Arī to darbības izpausmes var būt dažādas. Jāņem vērā tas, ka vīrusi var būt arī samērā nekaitīgi, taču daži spēj iznīcināt visus datus.

**Pazīmes, kas vīrusu atšķir no parastas programmas:**

- tiek aktivizēti bez lietotāja ziņas un veic tās darbības, kuras tajā ielicis programmētājs, nevis pieprasījis lietotājs;
- tiem ir spēja "inficēt" vai izmainīt citas datnes, vai disku struktūru;
- pavairojot sevi, tie var izplatīties uz citām datnēm vai sistēmām.

Datorvīrusi tiek veidoti, izmantojot tās pašas programmēšanas valodas, kuras veidojot lietojumprogrammas (*Assembler, C, Visual Basic, Java*).

**Vīrusus klasificē pēc to uzvedības un iedarbības veida**, piemēram:

- **Sākumsektora inficētāji** inficē datora sāknēšanas programmas sistēmas diskā. Šie vīrusi uzsāk darbību pirms operētājsistēmas un tādējādi apiet pretvīrusu programmu. Pārsvarā izplatās ar disku palīdzību;
- **Datņu inficētāji** inficē datnes. Aktivizējot inficēto datni, vīruss sevi ievieto atmiņā un gaida iespēju inficēt citas datnes. Izplatās ar inficētiem diskiem, caur datortīkliem.

Bez klasiskajiem vīrusiem pastāv arī **vīrusiem līdzīgas programmas** (parasti arī tās mēdz dēvēt par datorvīrusiem), piemēram:

- „tārpi" ir līdzīgi vīrusiem, taču nebojā datnes, bet tikai izplata sevi citās sistēmās, izmantojot tīklu. Tie ir kļuvuši par izplatītāko vīrusu formu;
- „Trojas zirgi", maskējas par citām datnēm, piemēram, ar nosaukumu READ.ME. „Trojas zirgi" parasti pēc aktivizēšanas instalē vīrusus vai arī sagatavo urķiem slēptu piekļuvi sistēmai. Parasti izplatās e-pastā ar piesaistītajām datnēm;
- „pipetes" ir „Trojas zirgu" vīrusu paveids, kas radīts, lai datoros instalētu vai nogādātu vīrusus vai „Trojas zirgus";
- „bumbas" ir programmas, ko izmanto, lai aktivizētu vīrusus noteiktā laikā vai konkrētos apstākļos.

Ir vairāki iespējamie iemesli, kāpēc tiek radīti vīrusi: ļaunprātība (tāpat kā, piemēram, huligāni, kas izdemolē parkus, apkrāso māju sienas vai ļaunprātīgi dedzinātāji), saviļņojums, ko izraisa noskatīšanās, kā kaut kas tiek izpostīts, lielība, ka kaut ko tādu var izveidot, ļauni joki.

## Datoru inficēšana

Atverot jaunas tīmekļa lappuses vai e-pasta piesaistnes, tiek realizēta datņu lejupielāde, kuras procesā pastāv risks inficēties ar datoru vīrusiem. Datoru vīrusi (virus) ir programmas, kas patvaļīgi pievienojas citām datora programmām un to darba laikā veic dažādas nevēlamas darbības: bojā vai dzēš datnes, piesārņo

atmiņu vai arī kā citādi traucē datora darbību. Atsevišķos gadījumos vīrusi ir inficējuši miljoniem datoru visā pasaulē.

**To, ka datorā ir iekļuvis vīruss, var konstatēt divējādi**:

- par to ziņo pretvīrusu programma;
- tiek novēroti netipiski programmu ziņojumi vai kļūmes datora darbībā. Šajos gadījumos iemesli var būt ne tikai vīrusu darbība, bet arī citi, piemēram, disku bojājumi vai lietotāja, vai programmu kļūdas.

Aizsardzībai pret datorvīrusiem izmanto **pretvīrusu programmas**.

**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** (informācija par vīrusiem un to saturu).

**Lai savu datoru aizsargātu no vīrusiem:**

- lietojiet labas pretvīrusu programmas. Izmantojiet tās, lai pirms lietošanas pārbaudītu jebkuru datni, programmu vai disku;
- regulāri skenējiet datoru ar pretvīrusu programmu. Lielāko daļu vīrusu var likvidēt, pirms tie sākuši nodarīt kaitējumus;
- parasti vīrusu veidotāji meklē un izmanto operētājsistēmas un citu programmu drošības “caurumus”, caur kuriem tos izplata. Tāpēc regulāri jāatjaunina programmatūra;
- nedodiet koplietošanai visu cieto disku. Aizsargājiet to ar paroli un ierobežojiet piekļūšanas tiesības (tikai lasīšanai).

**Strādājot internetā, lai izvairītos no datorvīrusiem, ieteicams:**

- datnes lejupielādēt tikai no uzticamiem publiskiem interneta avotiem un pēc saņemšanas tūlīt pārbaudīt ar pretvīrusu programmu;
- lejupielādētās datnes vēlams saglabāt nevis cietajā diskā, bet citā datu nesējā, ko pēc tam pārbaudīt;
- neatvērt e-pasta vēstuļu pielikumus pat tad, ja tie ir saņemti no uzticamiem adresātiem (ir vīrusi, kuri, izmantojot adrešu grāmatās esošās adreses, paši sevi izplata). Vispirms jāveic atsūtīto datņu pārbaude;
- ja neesat droši par saņemtā pielikuma uzticamību, izdzēsiet to tūlīt. Vēstule ir jāizmet arī no dzēsto (deleted) vēstuļu mapes.

## Antivīrusu programmas

**Antivīrusu mērķis ir** atklāt un neitralizēt kaitīgo programmatūru. Modernas antivīrusu programmas spēj likvidēt ne tikai īstos vīrusus, bet arī “Trojas zirgu” un “tārpus”. Dažas no tām pat novērš datu pikšķerēšanu (phishing).

Ir dažādas antivīrusu programmas, kuras atšķiras pēc iespējām, efektivitātes un cenas.

Kaut arī jums ir ļoti laba antivīrusu programma, tā būs efektīga tikai tad, ja jūs to **regulāri atjaunosiet**, jo katru dienu tiek radīti jauni datorvīrusi. Vairums šo programmu automātiski pieslēdzas internetam katru dienu (uzstādījumos var atjaunošanas biežumu mainīt) un atjauno informāciju par jaunākajiem vīrusiem.

Iegādājoties antivīrusu programmu, pievērsiet uzmanību perioda ilgumam, kad ir iespējams **atjaunot programmu**. Vairums datoru tirgotāju piedāvā antivīrusu programmas jau instalētas datorā un iespēju tās par brīvu atjaunot pusgadu vai gadu. Ja jūs to nedarāt, tad tās kļūst neefektīvas. Turklāt dažas no tām nevar vienkārši atinstalēt un uzinstalēt citu, bet darboties vienlaicīgi var tikai viena programma. Tāpēc jums uzreiz vajadzētu izlemt, vai lietosiet komerciālās programmas ar regulāru maksu par atjaunošanu, vai arī bezmaksas antivīrusu programmu.

**Bezmaksas antivīrusu programmas**:

| | |
|---|---|
|  | **Avast**<br><br>https://www.avast.com/index |
|  | **AviraAntiVirPersonalEditionClassic**<br><br>http://www.avira.com |
|  | **AVG Anti-VirusFree**<br><br>http://www.grisoft.com |
|  | **ClamWin**<br><br>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.

Vīrusu ķeršanai var izmantot arī nelielu bezmaksas programmu **McAfee AvertStinger**, kuru var lejupielādēt .

Šo programmu nav nepieciešams instalēt un saglabāt datorā. Labāk ir katru reizi tās jaunāko versiju iegūt no interneta.

## Bezmaksas antivīrusa programma MS Windows lietotājiem

**MS Windows** lietotāji, lejupielādējot atjauninājumus, regulāri saņem programmatūras līdzekļus, kas pārbauda viņu datorus un likvidē bīstamus vīrusus.

Piemēram, standarta komplektācijā **Windows 8 operētājsistēmai** datora lietotājam ir pieejams Microsoft Security Essentials ir rīks. Šo programmu gan nav atļauts izmantot valsts un mācību iestādēm.

## Aizsardzība pret spiegprogrammatūru

**Spiegprogrammatūra** ir ļoti līdzīga "Trojas zirgam". Ar tās palīdzību tiek novērotas lietotāja darbības un, izmantojot internetu, nosūtīti dati.

Tas notiek bez lietotāja ziņas un piekrišanas. Šāda programma var tikt iekļauta arī legālā licencētā programmā. Spiegprogrammatūra, iespējams, atrodas arī jūsu datorā.

Pētījumi rāda, ka tāda ir 4 datoros no 5.

Neskatoties uz to, ka likums nosaka katrai personai tiesības uz privātumu un personīgas informācijas aizsardzību, spiegprogrammatūra šīs tiesības rupjā veidā pārkāpj.

Šīs programmatūras galvenais mērķis ir ievākt un nosūtīt informāciju par interneta lietotāju paradumiem - kādas mājas lapas tiek apmeklētas, cik ilgi viņi tur uzturas utt. Bieži tiek ievākta informācija par pašu datoru - operētājsistēmu, procesoru, atmiņu, utt. Dažreiz tiek arī izsekots, vai lietotās datorprogrammas ir legālas vai ne.

Savāktā informācija var tikt lietota komerciāliem mērķiem vai statistikai, bet lietotājs nezina, kāda informācija tiek vākta un kas ar to tiek darīts vēlāk.

**Dažas no pazīmēm, kas liecina, ka dators, iespējams, ir inficēts ar spiegprogrammatūru:**

- parādās jaunas rīkjoslas, saites, kuras datora lietotājs pats tīmekļa pārlūkprogrammai nav pievienojis;
- parādās negaidītas izmaiņas sākumlapā, meklēšanas programmā, mainās peles rādītājs;
- ievadot kādas noteiktas vietnes adresi, atveras pavisam cita vietne;
- redzama uznirstoša informācija pat tad, ja dators nav savienots ar internetu;
- datora darbība pēkšņi kļūst lēnāka.

Viens no novērošanas sistēmu piemēriem ir meklēšanas sistēma *Google* un e-pasta sistēma *Gmail*. *Google* ir pilnīgi nekaitīga, kad tiek lietota atsevišķi. Tomēr savienojumā ar *Gmail* vienlaicīgu lietošanu *Google* ievāc informāciju par meklēto informāciju un apmeklētajām mājas lapām, un lietotājam uz e-pastu var tikt nosūtītas reklāmas vēstules/spams.

Daži darba devēji lieto spiegprogrammatūru, lai novērotu savus darbiniekus. Pastāv plaši izplatīts uzskats, ka katram darba devējam ir tiesības kontrolēt savu darbinieku korespondenci un interneta lietojumu, tomēr Latvijas Republikas likumi aizliedz novērot darbiniekus, noklausīties viņu sarunas vai ievākt citu personīgo informāciju.

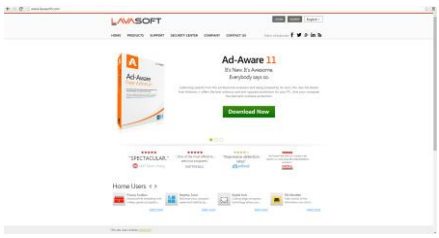
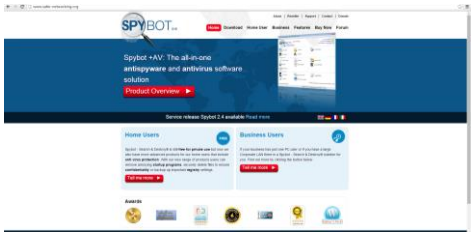
**Kā interneta spiegotāji nokļūst pie jūsu datora?**

Datora un interneta lietotāji paši lejupielādē un instalēt daudz **spiegprogrammatūras**, mēģinot lietot dažādās piedāvātās iespējas. Kā piemēru var minēt agrāk populāro programmu *Gator*, kas tika izmantota dažādu mājas lapu paroļu saglabāšanai un reģistrācijas lauku aizpildīšanas atvieglošanai. Šādi daudzas interneta pārlūkprogrammas un e-pasta programmu papildprogrammas, kas tās it kā "izdekorē", veicina jūsu datu iegūšanu. Tādēļ neuzticieties šķietami noderīgām programmām, ko iesaka dažādas mājas lapas un lejupielādējiet tās tikai no drošiem avotiem. Internetā viegli var atrast vairāk informācijas par instalējamo programmatūru un tās novērtējumu no drošības speciālistu puses.

Tika jau minēts *Google* un *Gmail*. Lielākā daļa mājas lapu atstāj nelielus ierakstus jūsu datorā, t.s. - **sīkdatnes** (*cookies)*, kas ļauj atpazīt mājas lapas apmeklētājus un atcerēties viņu darbības. Piemēram, interneta banku mājas lapas pārbauda *sīkdatnes* (*cookies)* pēc katras lietotāja veiktās darbības un neprasa paroles ievadīt atkārtoti. Līdzko sesija ir pabeigta, attiecīgās sīkdatnes (*cookies)* tiek dzēstas. Savukārt citu mājas lapu atstātās sīkdatnes saglabājas gadiem ilgi, un tās var izmantot citas mājas lapas.

Vairums antivīrusu programmu neaizsargā datoru pret spiegprogrammatūru. Ir nepieciešamas īpašas programmas, kas seko datora atmiņai un failiem un meklē pazīstamus informācijas vākšanas līdzekļus, un atrašanas gadījumā ierosina tos likvidēt. Līdzīgi kā ar vīrusiem, arī šai programmatūrai tiek radītas jaunas un jaunas versijas, tādēļ bieži jāatjauno attiecīgās programmas, kas domātas cīņai pret spiegprogrammatūru.

**Dažas no populārākajām bezmaksas programmām pret spiegprogrammatūru ir:**

| | |
|---|---|
|  | **LavasoftAd-AwareFree**<br><br>http://www.lavasoft.com/ |
|  | **Spybot - Search&Destroy**<br><br>http://www.safer-networking.org |

Kompānija *Microsoft* piedāvā legāliem *Windows* operētājsistēmas (Windows 7) lietotājiem programmu Windows Defender, ko var lejupielādēt *Microsoft* mājas lapā. Tur ir arī pieejama lietošanas instalēšanas pamācība.

## Tiešsaistes skeneri

Gadījumā, ja antivīrusu programma parāda, ka datorā ir atrasts vīruss, tad neveiciet nekādas darbības, jo antivīrusu programma to jau ir atpazinusi un neitralizējusi. Citādi ir, ja lietotājs pats ir ievērojis izmaiņas datora procesos, bet antivīrusu programma neko neuzrāda. Tādā gadījumā ir ieteicams noskenēt visas sistēmas datnes, izmantojot **dziļās analīzes tiešsaistes skeneri**, jo tam ir ievērojami lielāka parakstu datu bāze un daudzreiz efektīvākas pro-aktīvās tehnoloģijas.

Papildus informācija - http://www.pandasecurity.com/activescan/index/.

Ikvienam lietotājam ieteicams regulāri, vismaz vienu reizi mēnesī, padziļināti noskenēt savu datoru ar kādu no **tiešsaistes skeneriem**. Sevišķi aktuāli tas ir šobrīd, kad jaunie ļaunie kodi kļūst lietotājam arvien nepamanāmāki.

## Programmatūras atjaunošana

Pat vislabākajai programmatūrai ir vairāk vai mazāk drošības problēmu. Tās radītāji cenšas šīs nepilnības labot, piedāvājot **jaunākas un drošākas programmas versijas - atjauninājumus**.

Tikko kā uzlabotā programmatūra ir izdota, ieteicams to uzreiz lejupielādēt un instalēt. Ja tas netiek darīts, tad ilgu laiku un lielam cilvēku skaitam ir zināms par minētajiem drošības trūkumiem, kas nopietni var apdraudēt gan datoru, gan tajā esošos datus.

Visas operētājsistēmas un vairums lietojumprogrammu spēj lejupielādēt un ieinstalēt **atjauninājumus** pašas. MS Windows ir iespēja uzstādīt manuālu vai automātisku atjaunināšanu. Individuāliem lietotājiem ieteicams izmantot automātisku atjaunināšanu. Ja nepieciešams, var pieslēgties Microsoft produktu atjaunināšanas centram un lejupielādēt piedāvātos produktus.

Jāatzīmē, ka tikai legāli iegādātas programmas tiek atjaunotas korekti. Tādēļ nav vērts lietot nelegālas programmu kopijas. Ja nevēlaties maksāt par programmām, tad labāk izvēlēties analoģiskas bezmaksas programmas.

Viena no visievainojamākajām datorprogrammām ir interneta pārlūkprogramma. Tādēļ, pirmkārt, ir jāpievērš uzmanība tās drošībai. Izmantojiet tikai modernas un drošas pārlūkprogrammas, piemēram, *Google Crome*, *Mozilla Firefox, Internet Explorer, Opera*. Modernas pārlūkprogrammas ir viegli papildināt ar dažādiem papildus produktiem, kas ļauj internetu lietot vēl drošāk.

Tikai pareizi konfigurēta moderna pārlūkprogramma aizsargās jūs no kaitīgām *Java, JavaScript* un *ActiveX* programmām mājas lapās.

## Reklāmu bloķēšana

Lielākā daļa reklāmu tiek pieskaitītas pie kaitīga un nevēlama interneta satura. Pašas uzmācīgākās reklāmas tiek rādītas izlecošajos pārlūkprogrammu logos, tie var parādīties tik ātri, ka datora lietotājam pat nav laika tos aizvērt. Noteiktas mājas lapas ar nolūku rada reklāmas, kuras aizverot, atkārtoti atveras jaunas reklāmas.

Reklāmas novērš uzmanību, izmanto papildus datora resursus un to saturs paredzēts pieaugušajiem.

Mūsdienīgākās pārlūkprogrammas var pasargāt no daudzām izlecošo logu reklāmām. Piemēram, pārlūkprogrammā Mozilla Firefox nevēlamo saturu var bloķēt ***Tools*** *(Rīki)/****Add-ons*** *(Pievienojumprogrammas)/meklēšanas laukā ierakstot* ***block*** *(bloķēt)* un izvēloties vajadzīgo rīku. Piemēram, **AdBlock Plus** nodrošinās to, ka mājas lapās reklāmu vietā parādās tukši lauki, **FlashBlock** bloķē Flash tipa animācijas.

## Pārlūkprogrammu saturu filtri

Viena no populārākajām **bezmaksas interneta filtra programmatūrām** ir K9 WEB Protection. Tā darbojas kā papildinājums datora pretvīrusu programmai, jo spēj ātri un efektīvi fiksēt lapas, kurās iespējamas kaitīgās lietojumprogrammas.

## Vecākvadības programmatūra

Izmantojot jaunākās operētājsistēmās, ir iespējas noteikt laika limitus datora lietošanai, piemēram, kontrolēt bērnu, mazbērnu piekļuvi dažādām spēlēm un citām programmām, kā arī neļaut tiem strādāt ar viņu vecumam nepiemērotām programmām.

Vairāk par vecākvadības programmatūru var izlasīt, piemēram, interneta vietnē Esi drošs.

## Windows ugunsmūris

**Ugunsmūris ir** programmatūra vai aparatūra, kura pārbauda informāciju, kas ienāk no interneta vai tīkla, un atkarībā no ugunsmūra iestatījumiem to bloķē vai arī ļauj ienākt datorā.

Ugunsmūris var palīdzēt novērst urķu vai ļaunprātīgu programmatūru (piemēram, "tārpu") piekļuvi datoram, izmantojot tīklu vai internetu. Ugunsmūris var arī liegt datoram sūtīt ļaunprātīgu programmatūru citiem datoriem.

Interneta ugunsmūris ir jau iestrādāts operētājsistēmā Windows. To var ieslēgt/izslēgt sadaļā ***Control Panel*** (*Vadības Panelis)*/***Windows Firewall*** (*Windows Ugunsmūris).*

Ja jūs izmantojat dažādus tīkla pieslēgumus, pārliecinieties, ka ikvienam no tiem ir ugunsmūris. Lai iegūtu vairāk informācijas un palīdzību, apmeklējiet Microsoft mājas lapu.

## Pārlūkošanas pēdu dzēšana

Interneta pārlūkošanas programmās ir viegli izdzēst jebkādas pārlūkošanas pēdas. Piemēram, Internet Explorer 7-11 versijā šim nolūkam izmanto sadaļu ***Tools*** (*Rīki)*, komandu ***Safety*** (Drošība)/***Delete browsing history***/(*Izdzēst pārlūkošanas vēsturi)*. Atvērsies uzstādījumu dialoglogs, kurā atzīmē nepieciešamās izvēlnes par vēstures dzēšanu un nospiež pogu ***Delete*** (*Dzēst)*. Pārlūkošanas pēdas citās pārlūkprogrammās var dzēst līdzīgi - izvēlnes joslā atrodot sadaļu ***Tools*** (*Rīki)*.

## Pārlūkprogrammas rīki pret pikšķerēšanu

**Pikšķerēšana** tiešsaistē ir veids, kā ar krāpniecisku e-pasta ziņojumu vai vietnes palīdzību izvilināt no datorlietotājiem personisku vai finanšu informāciju.

Ikviena moderna interneta pārlūkprogramma var apstiprināt aplūkotās mājas lapas drošību. Informācija par rīka pret pikšķerēšanu uzstādīšanu programmā Internet Explorer 11 versijā.

Kā atpazīt pikšķerēšanu, vairāk iespējams uzzināt mājas lapā Esi drošs.

## Datoru aizsardzība Latvijā

Tā kā internetā nepastāv fiziskas robežas, kā starp valstīm, tad ar vien biežāk, lai apkarotu kibernoziegumus valstīm ir jāsadarbojas savā starpā. No 2011. gada Latvijā darbojas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija **CERT.LV**, kas nodarbojas ar incidentu novēršanu, iedzīvotāju izglītošanu datoru drošības jautājumos, tehnoloģisko risku novēršanu un valsts un pašvaldību institūciju uzraudzību. Taču ir gandrīz neiespējami paredzēt pārkāpumu un aizturēt vainīgo pirms noziegums ir izdarīts.

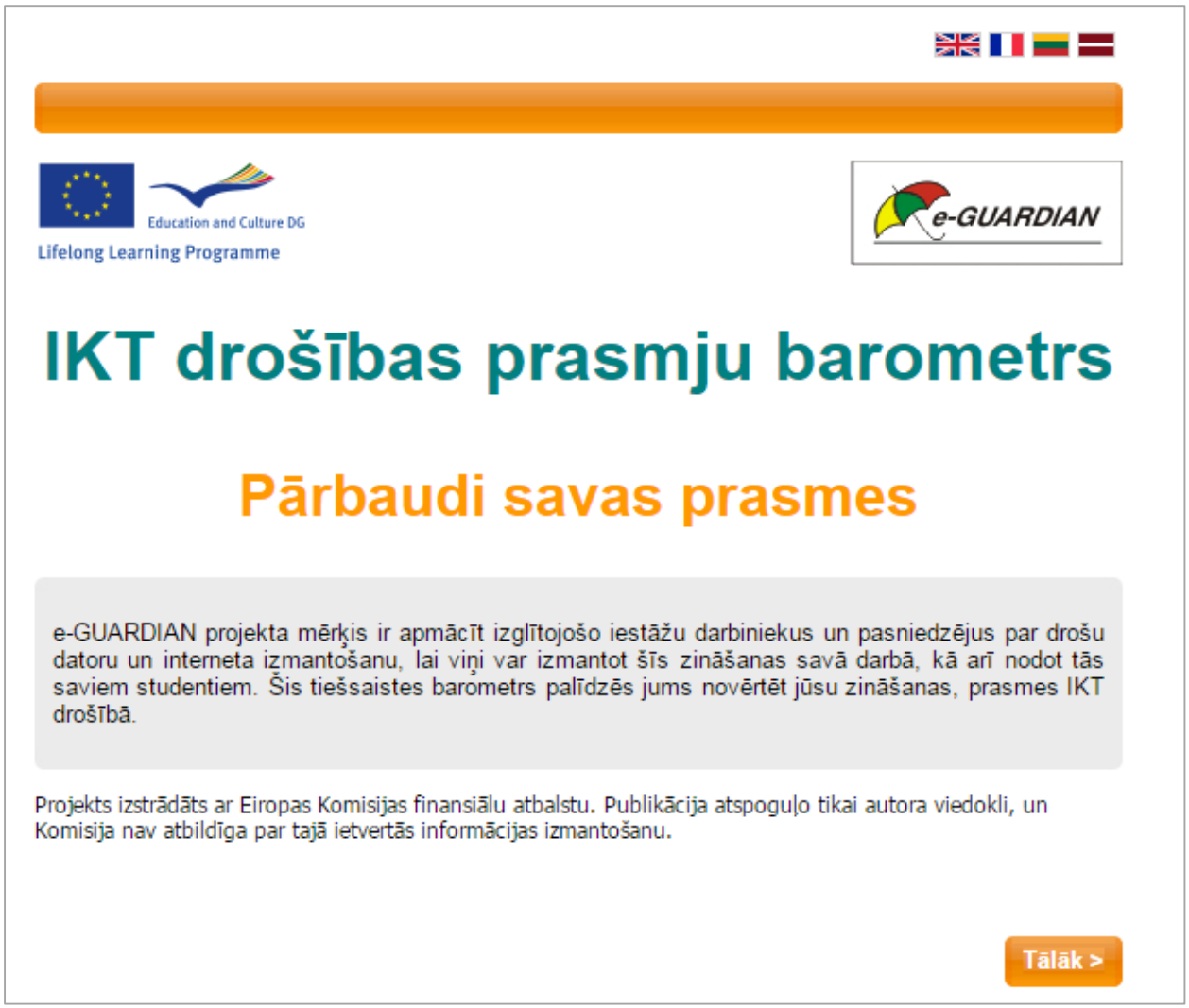
CERT.LV strādā arī ar iedzīvotāju un uzņēmumu iesniegtajiem incidentiem datu drošības jautājumos.

Ziņot par drošības incidentiem vai sazināties ar CERT.LV komandu var pa e-pastu cert@cert.lv vai telefonu +371 67085858.

# PĀRBAUDIET SAVAS ZINĀŠANAS - IKT DROŠĪBAS PRASMJU BAROMETRS

**IKT drošības prasmju barometrs** palīdzēs novērtēt jūsu zināšanas, prasmes IKT drošībā. Tas pieejams.

Vairāk infomācijas par barometra aizpildīšanu un rezultātu saņemšanu skatīt.



# PALĪGMATERIĀLI UN AVOTI

- Bezmaksas drošības risinājumi - https://www.esidross.lv/category/bezmaksas-risinajumi/
- Bērna izglītošana datora izmantošanā: https://www.esidross.lv/2013/07/16/berna-izglitosana-datora-lietosana/;
- Bērni un internets: http://kaspersky.antivirus.lv/lat/threats/childprotect/;
- Datora drošība izmantojot internetu: http://windows.microsoft.com/lv-lv/windows-8/shared-help-protect-yourself-ie-10;
- Informācija par bērnu aizsardzību Microsoft: http://www.microsoft.com/protect/parents/childsafety/age.aspx;
- Kas būtu jāzina par e-drošību; http://www.la.lv/klientu-skola-2/
- Kā veikt uzstādījumus bērnu aizsardzībai Windows 7 vidē: http://windows.microsoft.com/lt-Lt/windows7/set-up-parental-controls;
- Labākās bezmaksas antivīrusu programmas uzņēmuma un mājām http://devini.com/antiviruss-bezmaksas-programma/;
- Rokasgrāmata skolotājiem "Drošība internetā"; www.drossinternets.lv;
- Mājas datora aizsardzība http://www.drossinternets.lv/upload/materiali/majas_datoru_aizsardziba.pdf ;
- Microsoft Datora aizsardzība Windows 8: http://windows.microsoft.com/lv-lv/windows-8/protect-pc;
- Vīrusi un ļaunprogrammatūra: http://windows.microsoft.com/lv-lv/windows-8/windows-defender;
- Windows Live aizsardzība ģimenes locekļiem: http://windows.microsoft.com/lt-Lt/windows-vista/protecting-your-kids-with-family-safety.
- Ziņojums par bērnu aizsardzību digitālā pasaulē: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0353+0+DOC+XML+V0//LV;

- Projekta Trans-eFacilitator ietvaros izstrādātie materiāli.