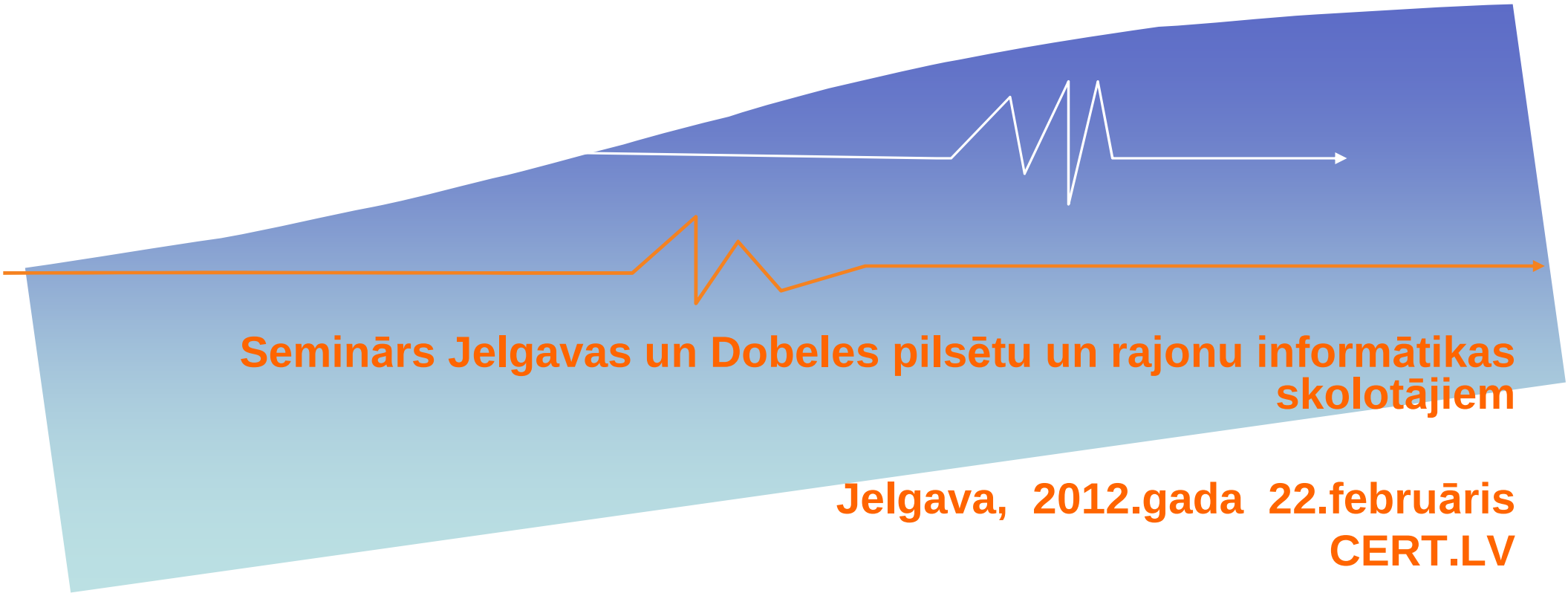
“Drošība virtuālajā vidē”



Seminārs Jelgavas un Dobeles pilsētu un rajonu informātikas skolotājiem

Jelgava, 2012.gada 22.februāris

CERT.LV

Saturs

- Ievads un CERT.LV
- Drošības jēdziens
- Autentifikācijas skaidrojums
- Pareiza paroles izvēle
- Uzbrucēji virtuālajā vidē
- Datoru tiesiska lietošana skolā
- Ārējie datu nesēji
- Viedtālruņi
- Droša Interneta lietošana
- Droša elektroniskā pasta lietošana
- Datorvīrusi un ļaunprātīga koda programmas
- Rīcība drošības incidenta un pārkāpumu gadījumos

Ievads un CERT.LV

- IT drošības likums
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV
- Visas Valsts un pašvaldību iestādes nozīmē atbildīgos par IT drošību – drošības pārzini
  - Pārziņu pienākumos ietilps 1x gadā organizēt darbinieku apmācību par IT drošības jautājumiem.
- CERT.LV atbalsts
  - IT incidentu gadījumā gadījumā 24x7 (tel. 67085858),e-pasts cert@cert.lv
  - Semināri
  - Apmācības
  - Prezentācijas
  - Dokumentu paraugi
  - Sabiedrības izglītošana – portāls “Esi drošs” - www.esidross.lv

Drošības jēdziens

- Ja drošībā ir informācija par
  - Ģimeni,
  - Personas datiem,
  - Finansēm,
  - Īpašumu,
  - Citām katram svarīgām lietām un personām.

- Ja ir, kur rast padomu un atbalstu
  - CERT.LV,
  - Drossinternets.lv,
  - Esidross.lv,
  - Tiesibsargs.lv,
  - Valsts policija - sargi-sevi.lv,
  - Citi interneta resursi.

Autentifikācija - skaidrojums

- Autentifikācija ir process, kurā veic lietotāja identitātes pārbaudi datorsistēmā.
- Autentifikācijas veidus var iedalīt vairākās kategorijās:
  - Lietotājs kaut ko zina (piem., paroli vai personālo identifikācijas numuru - PIN);
  - Lietotājam kaut kas pieder (piem., magnētiskā karte, viedkarte u.c.);
  - Lietotājam kaut kas ir - pamatojoties uz lietotāja biometriskajām īpašībām (piem., balss, pirkstu nospiedumiem, paraksta atpazīšanas u.c.)
- Pēc autentifikācijas parasti notiek autorizācija - lietotāja piekļuves (sistēmas resursiem, informācijai) tiesību piešķiršana.

Pareiza paroles izvēle

- Labā prakse:
  - Lietotāja parole sastāv no lielo un mazo latīņu alfabēta burtu un ciparu kombinācijas, un tās garums nedrīkst būt īsāks par astoņiem simboliem. Kā paroli nedrīkst izmantot personu identificējošus datus (piemēram, lietotāja vārdu, uzvārdu, automašīnas numuru) un vārdus, kas saistīti ar organizāciju vai kas bieži tiek lietoti ikdienas darbā,
  - Mainīt paroli reizi X mēnešos,
  - Neizmantot iepriekšējās 2 paroles,
  - Dažādiem resursiem lietot atšķirīgas paroles
- Piemērs:
  - Sliktas paroles – Kaarlis2 Sanita09 CERT2011g
  - Ieteicamas paroles – 3Kotaz@s HL36b87m p3y6trEY

Uzbrucēji virtuālajā vidē

- Mērķi:
  - Identitātes zādzība,
  - Datoru resursu iegūšana,
  - Informācijas zagšana un viltošana.
- Uzbrucēju komunikāciju veidi:
  - Personīgi kontakti,
  - Telefons,
  - Elektroniskais pasts,
  - Ļaundabīgas programmas.
- Aizsardzības stratēģija:
  - Labākā aizsardzība – saprātīga rīcība,
  - Stingra paroļu izveidošanas un glabāšanas kārtība,
  - Zināšanas, kā un kam paziņot, ja noticis kas slikts.

Datoru tiesiska lietošana skolā

- IT drošības nodrošināšana skolā
- Labā prakse – lietotājam nav atļauts:
  - Veikt darbības, kas nevajadzīgi noslogo informācijas resursus, neņemot vērā citu lietotāju vajadzības,
  - Veikt internetā pieejamo datorprogrammu lejupielādi un instalāciju, nesaskaņojot ar informātikas skolotāju,
  - Veikt internetā pieejamu multimediju datņu (piemēram, mūzika, filmas, attēli, datorspēles) lejupielādi,
  - Patvaļīgi mainīt programmu uzstādījumus,
  - Pieslēgt skolas lokālajam datortīklam vai tā informācijas resursiem personīgo datortehniku.
- Svarīgi atcerēties:
  - Dators skolā ir mācību līdzeklis un paredzēts mācību procesa veikšanai.

Ārējie datu nesēji

- Labā prakse:
  - Datņu kopēšanu uz/no ārējiem informācijas nesējiem (piemēram, disketes, CD vai DVD diski, vai USB zibatmiņas) lietotājs drīkst veikt vienīgi konkrētu uzdevumu izpildei,
  - Pievienojot datoram ārējo datu nesēju to noskanēt ar antivīrusu programmu,
  - Ar īpašu piesardzību lietot ārējos datu nesējus, kurus iedevuši draugi un paziņas,
  - Neglabāt, bez vajadzības, svarīgu un aizsargājumu informāciju.

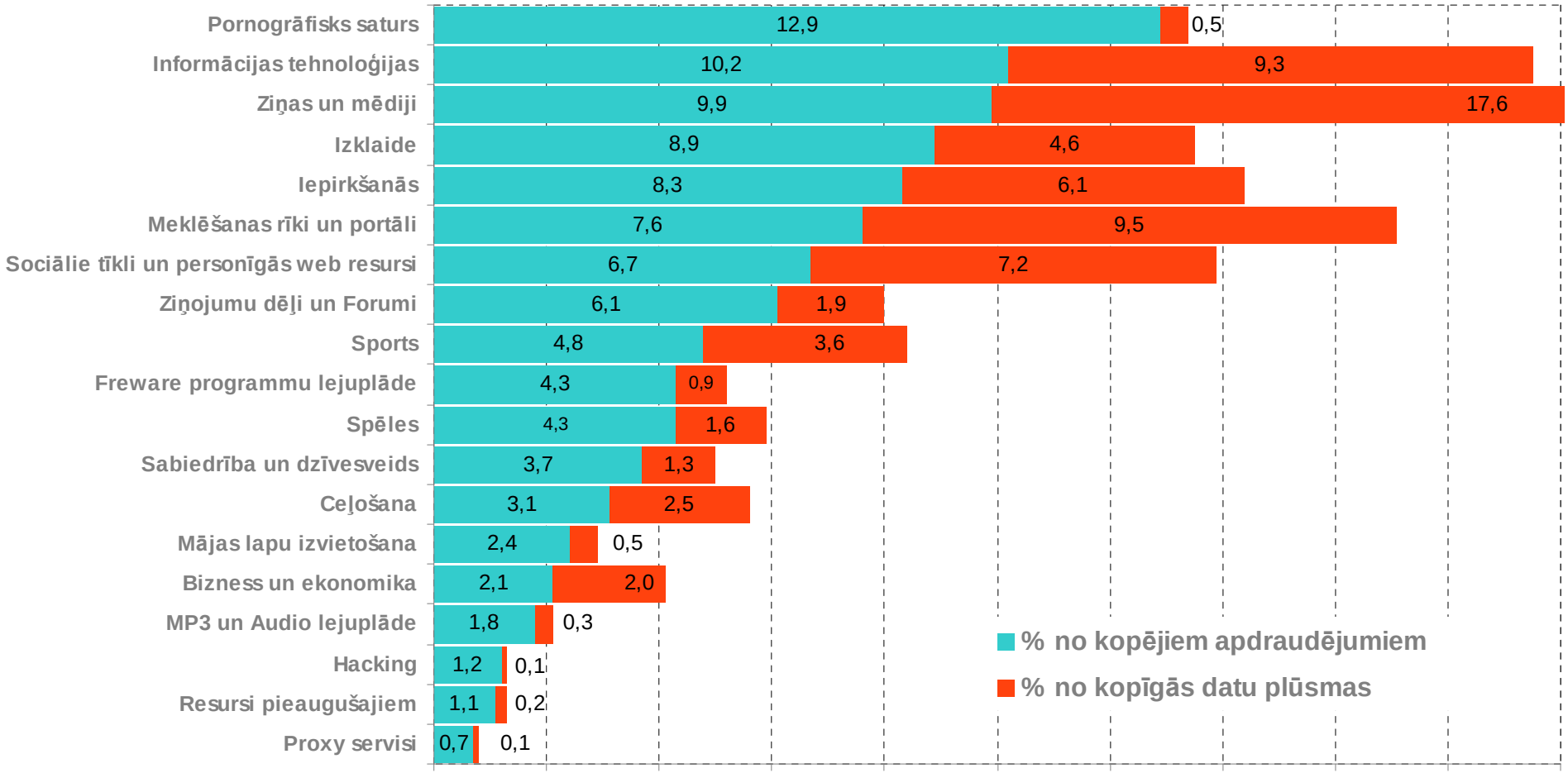
Viedtālruņi

- Viedtālrunis šodien ir miniatūrs dators, kurš spēj
  - pieslēgties bezvadu internetam
    - aplūkot tīmekļa vietnes, tajā skaitā sociālos tīklus,
    - apmainīties ar elektronisko pastu,
    - fotografēt un filmēt.
  - spēj noteikt atrašanās vietu
  - var kalpot kā datu nesējs
  - ... un visbeidzot pildīt arī telefona funkcijas.

- Labā prakse:
  - izmantot tikai tās iespējas, kuras dotajā brīdī nepieciešamas
  - neinstalēt apšaubāmas izcelsmes programmas
  - neglabāt tālrunī banku karšu numurus un pin kodus, citu svarīgu un aizsargājamu informāciju.

Droša Interneta lietošana

Procentuālais mājas lapu apmeklējums ar saitēm uz kaitīgu kodu 2010.gadā

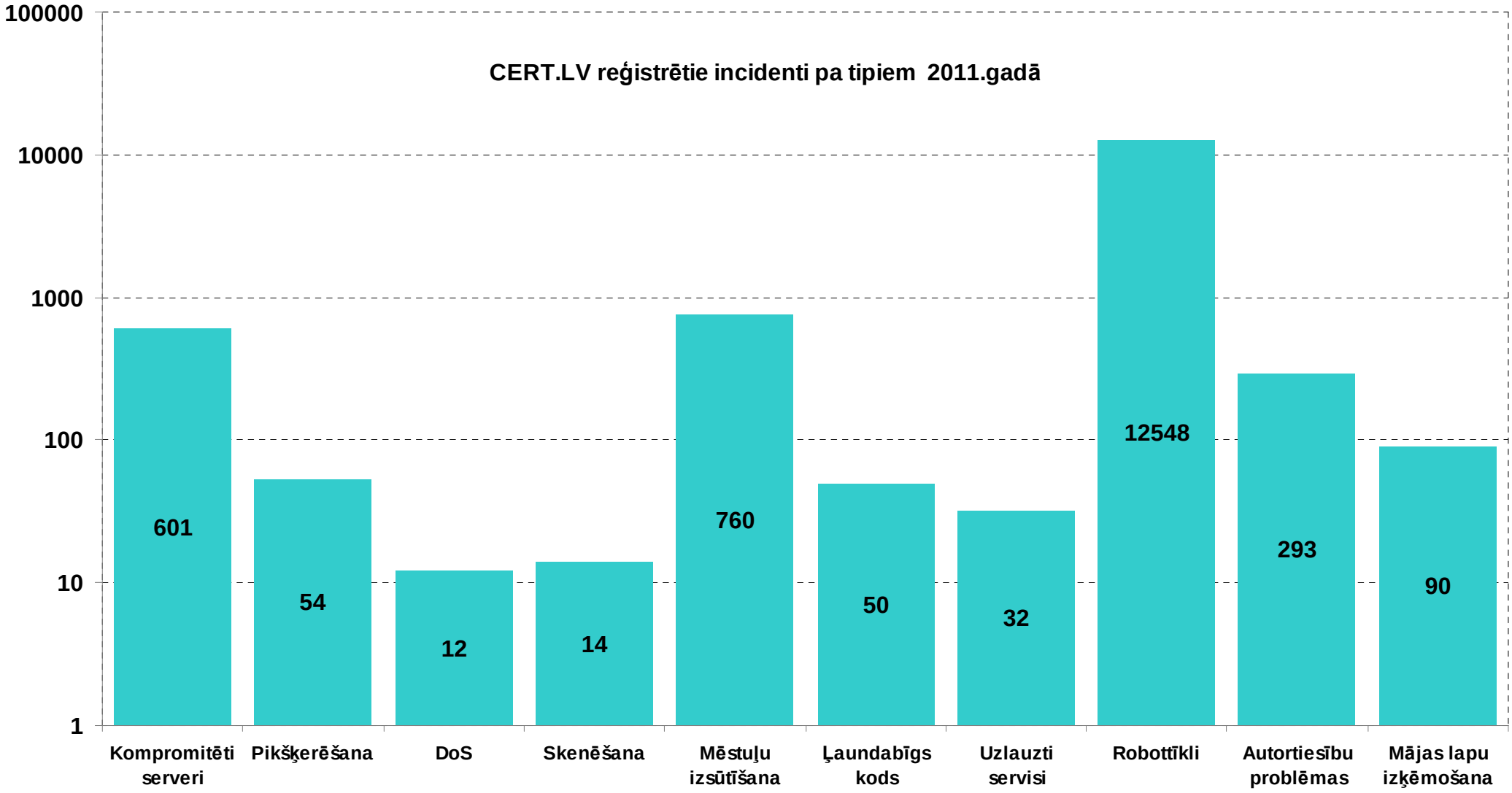


http://www.websense.com/content/threat-report-2010-malware.aspx

Droša elektroniskā pasta lietošana

- Kad jākļūst uzmanīgam?
  - Jūs saņemat sensacionāla rakstura paziņojums ar uzaicinājumu veikt zināmas darbības,
  - Interneta pārlūkprogramma rāda pieprasījumu nezināmas lietojumprogrammas palaišanai,
  - Saņemts uzaicinājums apmeklēt nezināmu tīmekļa vietni,
  - Jūs saņemat ziņojumu valodā, kuru ikdienas sarakstē nelietojat,
  - Jūs sākat saņemt dīvainas ziņas no draugiem un paziņām,
  - Draugi un paziņas sāk saņemt dīvainas ziņas no Jums.

Datorvīrusi un ļaunprātīga koda programmas



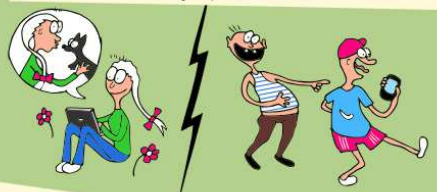
Vai esi Interneta profiņš?

Lieto drošas paroles!

Katram portālam izmanto savādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!

Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts" internetā, to vairs nevar iznīcināt vai padarīt par nebijušu.



Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satiec virtuālajā vidē, ir tie, par ko uzdodas. Bieži vien ļaundari slēpj savu patieso seju, lai vieglāk piekļūtu Tev, Taviem radiem un draugiem. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri reālajā dzīvē. Neatklāj, kā Tevi sauc, kur Tu dzīvo, kas ir Tavi vecāki vai kādas mantas Tev ir mājās.

Nesarunā tikšanās ar tīklā satiktajiem paziņām!

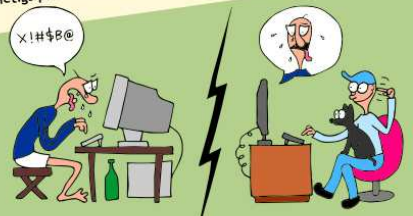
Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai neviens nevar nodarīt Tev pāri! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

Darbības internetā nav anonīmas!

Tavas darbības internetā nav anonīmas! Vajadzības gadījumā tām var izsekot gan skolotāji, gan vecāki, gan likumu sargājošas iestādes.

Neraksti aizskarošus komentārus!

Cilvēki, kas aizvaino citus, paši jūtas nelaimīgi. Taču, aizvainojot citus, neviens laimīgāks nekļūst. Nesāpini apkārtējos! Esi iecietīgs pret citu viedokli, dzīvesveidu, dzīves uzskatiem.



Mēstules nav vēstules!

Ignorē mēstules, ko saņem nepazīstamiem cilvēkiem. Neatsaucies to „vilinošajiem" piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt un par tām var sūdzēties.

Neiepērcies internetā bez vecāku ziņas!

Nesniedz internetā savas vai vecāku kredītkartes datus, iepriekš neapspriežoties ar vecākiem. Atceries - izmantojot kredītkartes datus, var nozagt visu naudu, kas pieejama ar šo karti.

Rūpējies par datora veselību!

Neinstalē nezināmas izcelsmes programmas uz datora, ko Tu lieto. Programma ļoti viegli var izlikties par spēli, bet patiesībā būt vīruss, kam Tu pats paver ceļu uz savu datoru.

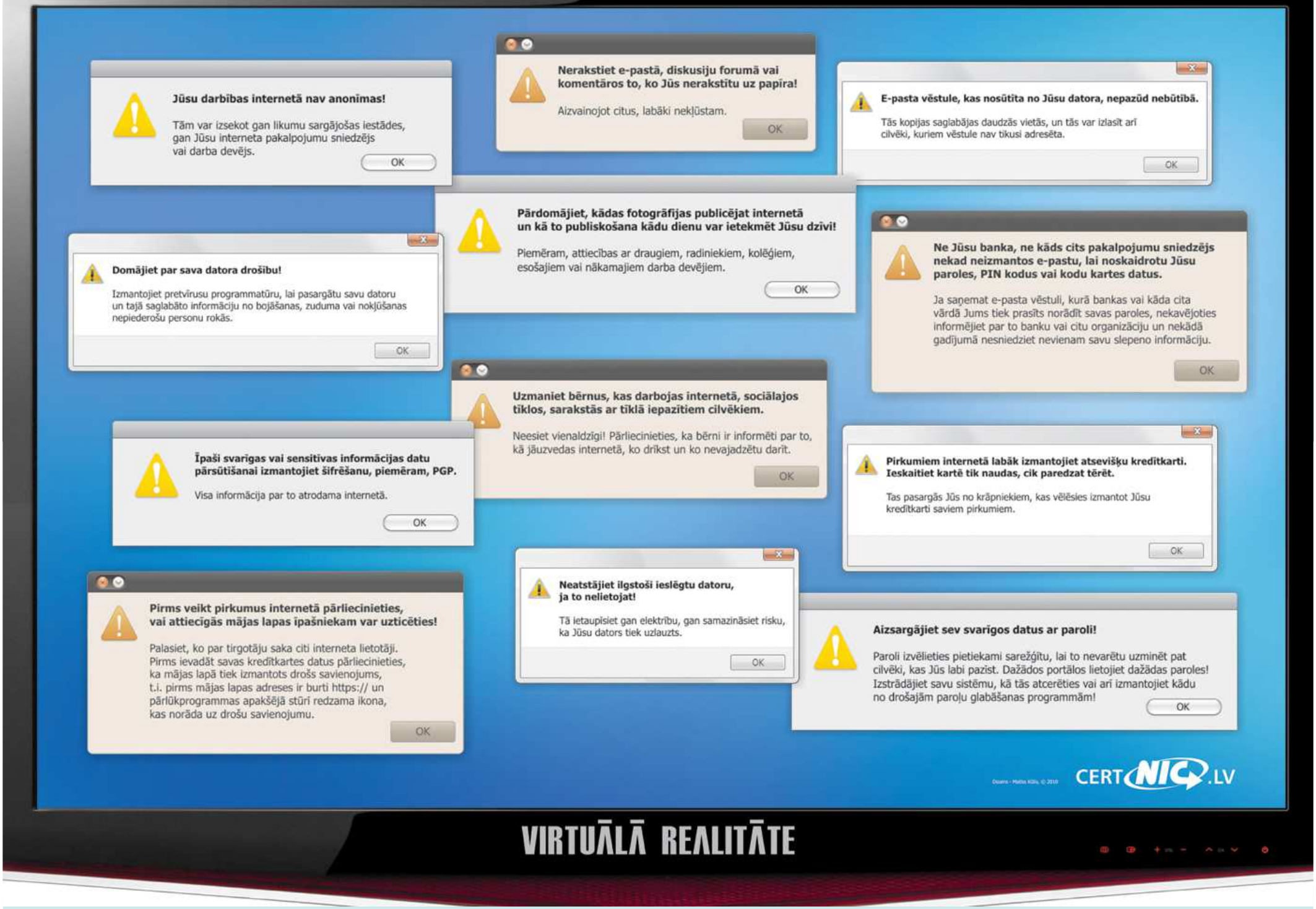
Ja Tu:

- saņem nepatīkamas, aizvainojošas vēstules internetā,
- esi saskāries ar nepatīkamiem materiāliem internetā,
- esi pamanījis aizdomīgas darbības internetā,
- esi satraukts par savu drošību internetā,

pastāsti par to saviem vecākiem vai kādam citam no pieaugušajiem, kam uzticies! Vari zvanīt Bērnu un jauniešu bezmaksas uzticības tālrunim 116111 vai rakstīt uz: zinojumi@drossinternets.lv vai abuse@nic.lv

CERT.LV

CERT NIC .LV


Jūsu darbības internetā nav anonīmas!
Tām var izsekot gan likumu sargājošas iestādes, gan Jūsu interneta pakalpojumu sniedzējs vai darba devējs.
OK
Nerakstiet e-pastā, diskusiju forumā vai komentāros to, ko Jūs nerakstītu uz papīra!
Aizvainojot citus, labāki nekļūstam.
OK
E-pasta vēstule, kas nosūtīta no Jūsu datora, nepazūd nebūtībā.
Tās kopijas saglabājas daudzās vietās, un tās var izlasīt arī cilvēki, kuriem vēstule nav tikusi adresēta.
OK
Pārdomājiet, kādas fotogrāfijas publicējat internetā un kā to publiskošana kādu dienu var ietekmēt Jūsu dzīvi!
Piemēram, attiecības ar draugiem, radiniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem.
OK
Domājiet par sava datora drošību!
Izmantojiet pretvīrusu programmatūru, lai pasargātu savu datoru un tajā saglabāto informāciju no bojāšanas, zuduma vai nokļūšanas nepiederošu personu rokās.
OK
Ne Jūsu banka, ne kāds cits pakalpojumu sniedzējs nekad neizmantos e-pastu, lai noskaidrotu Jūsu paroles, PIN kodus vai kodu kartes datus.
Ja saņemat e-pasta vēstuli, kurā bankas vai kāda cita vārdā Jums tiek prasīts norādīt savas paroles, nekavējoties informējiet par to banku vai citu organizāciju un nekādā gadījumā nesniedziet nevienam savu slepeno informāciju.
OK
Uzmaniet bērnus, kas darbojas internetā, sociālajos tīklos, sarakstās ar tīklā iepazītiem cilvēkiem.
Neesiet vienaldzīgi! Pārliecinieties, ka bērni ir informēti par to, kā jāuzvedas internetā, ko drīkst un ko nevajadzētu darīt.
OK
Īpaši svarīgas vai sensitīvas informācijas datu pārsūtīšanai izmantojiet šifrēšanu, piemēram, PGP.
Visa informācija par to atrodama internetā.
OK
Pirkumiem internetā labāk izmantojiet atsevišķu kredītkarti. Ieskaitiet kartē tik naudas, cik paredzat tērēt.
Tas pasargās Jūs no krāpniekiem, kas vēlēsies izmantot Jūsu kredītkarti saviem pirkumiem.
OK
Pirms veikt pirkumus internetā pārliecinieties, vai attiecīgās mājas lapas īpašniekam var uzticēties!
Palasiet, ko par tirgotāju saka citi interneta lietotāji. Pirms ievadāt savas kredītkartes datus pārliecinieties, ka mājas lapā tiek izmantots drošs savienojums, t.i. pirms mājas lapas adreses ir burti https:// un pārlūkprogrammas apakšējā stūrī redzama ikona, kas norāda uz drošu savienojumu.
OK
Neatstājiet ilgstoši ieslēgtu datoru, ja to nelietojat!
Tā ietaupīsiet gan elektrību, gan samazināsiet risku, ka Jūsu dators tiek uzlauzts.
OK
Aizsargājiet sev svarīgos datus ar paroli!
Paroli izvēlieties pietiekami sarežģītu, lai to nevarētu uzminēt pat cilvēki, kas Jūs labi pazīst. Dažādos portālos lietojiet dažādas paroles! Izstrādājiet savu sistēmu, kā tās atcerēties vai arī izmantojiet kādu no drošajām paroļu glabāšanas programmām!
OK
CERT NIC .LV
VIRTUĀLĀ REALITĀTE

Portāls www.esidross.lv

Rīcība drošības incidenta un pārkāpumu gadījumos

- Neslēpt problēmu – tādēļ tā pati no sevis nepazudīs,
- Sazināties ar zināmu un uzticamu speciālistu,
- Ja nepieciešama tehniska palīdzība un padoms kā rīkoties – sazināties ar CERT.LV,
- Ja aizskartas Jūsu tiesības vai nodarīti zaudējumi – ziņot Valsts policijai.

Paldies par uzmanību!

E-pasts: egils.sturmanis@cert.lv
Tīmekļa vietne: http://www.cert.lv
Portāla Esi drošs tīmekļa vietne: http://www.esidross.lv
CERT.LV Twitter vietne: http://twitter.com/certlv