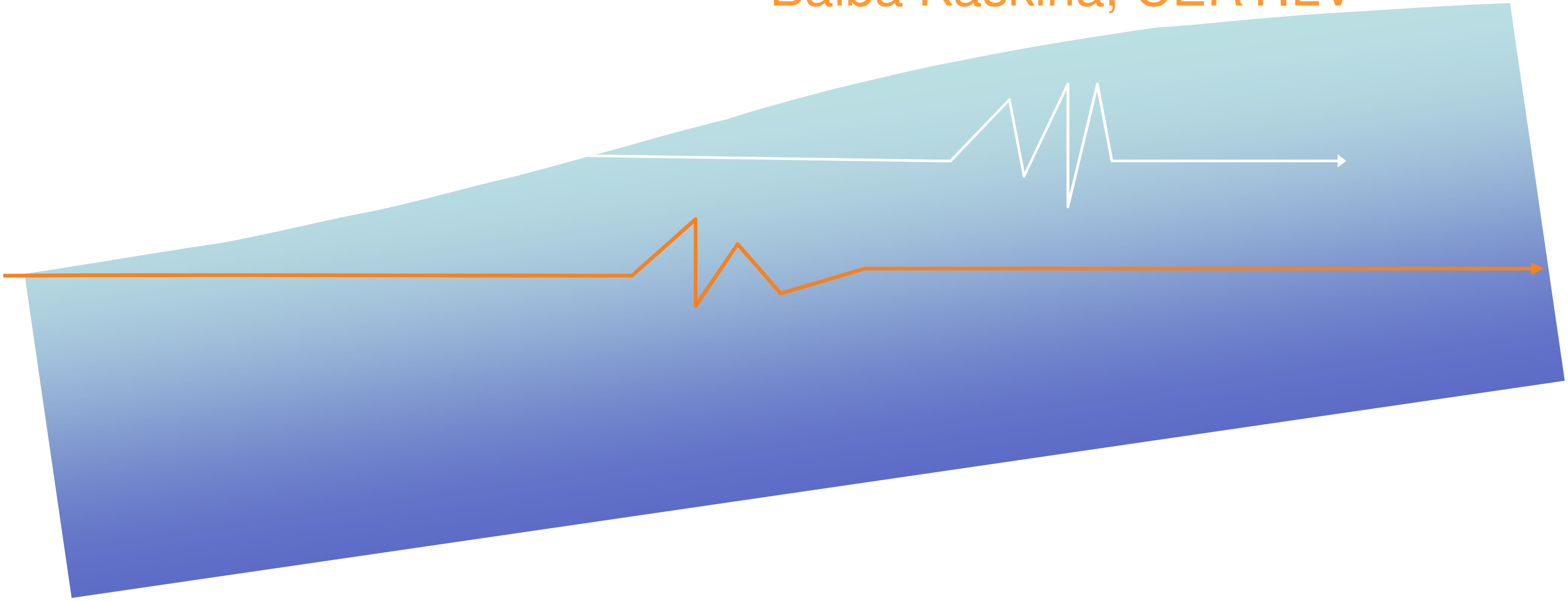
CERT.LV:

Overview and first 3 months

Baiba Kaškina, CERT.LV



Overview

CERT.LV

- Operational since 1 February 2011
- Operates on the basis of IT Security Law
- Tasks delegated to IMCS UL
- Merged CERT NIC.LV + DDIRV
- State funded
- Year 2011 - 10 people, 4-5 FTE

CERT.LV

- Experience in security incident handling since 2006
- Full member of FIRST since 2009
- Accredited by Trusted Introducer since 2007
- Facilitates LV-CSIRT initiative since 2007

LV-CSIRT initiative group

- Set up in March 2007
- Brings together IT Security professionals
- Experience and information exchange
- Awareness raising
- Cooperation in incident response and prevention

ABLV
Aizkraukles Banka Latvija
Swedbank
CSDD
VRAA
LATVIJAS BANKA
eiPro
IT feels good!
lattelecom
Citadele
sigma net
Latvenergo
POLICIJA
LMT
LATVIJAS MOBILAIS TELEFONS
RTU
SEB
elko
Grow to succeed. ELKO Group.
deac
IT ārpakalpojumi
CERT.LV
VZD
Telia Latvija
VALSTS KASE
.lv NIC

Achieved in 3 months

Monitoring of Latvian IT space and incident response

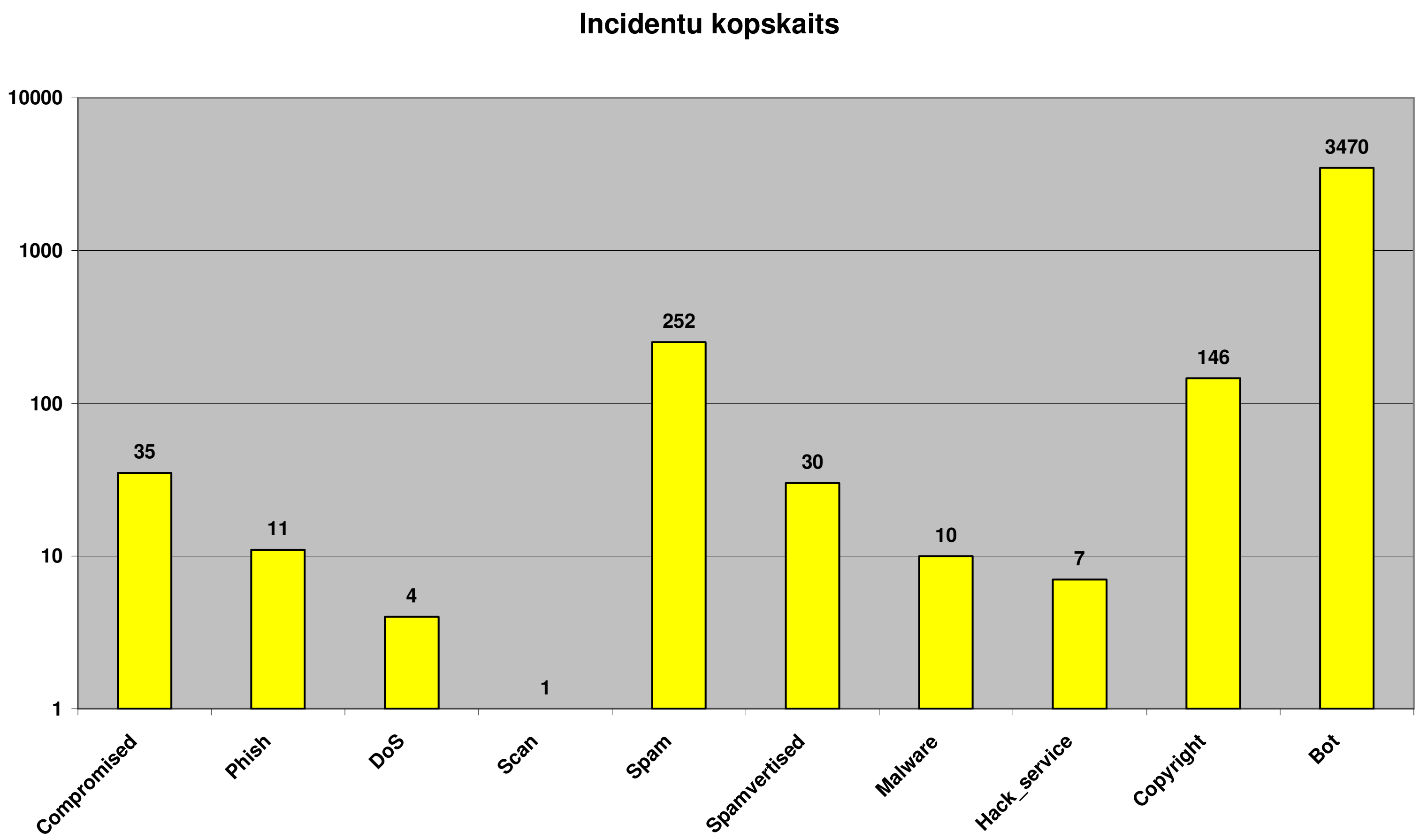
Situation in Latvia

- Overview of infected IPs in Latvia – on 30.04.2011. ~4500 infections
- Different information sources
- Only part of infections become incidents in tracking system
- Cooperation with ISPs

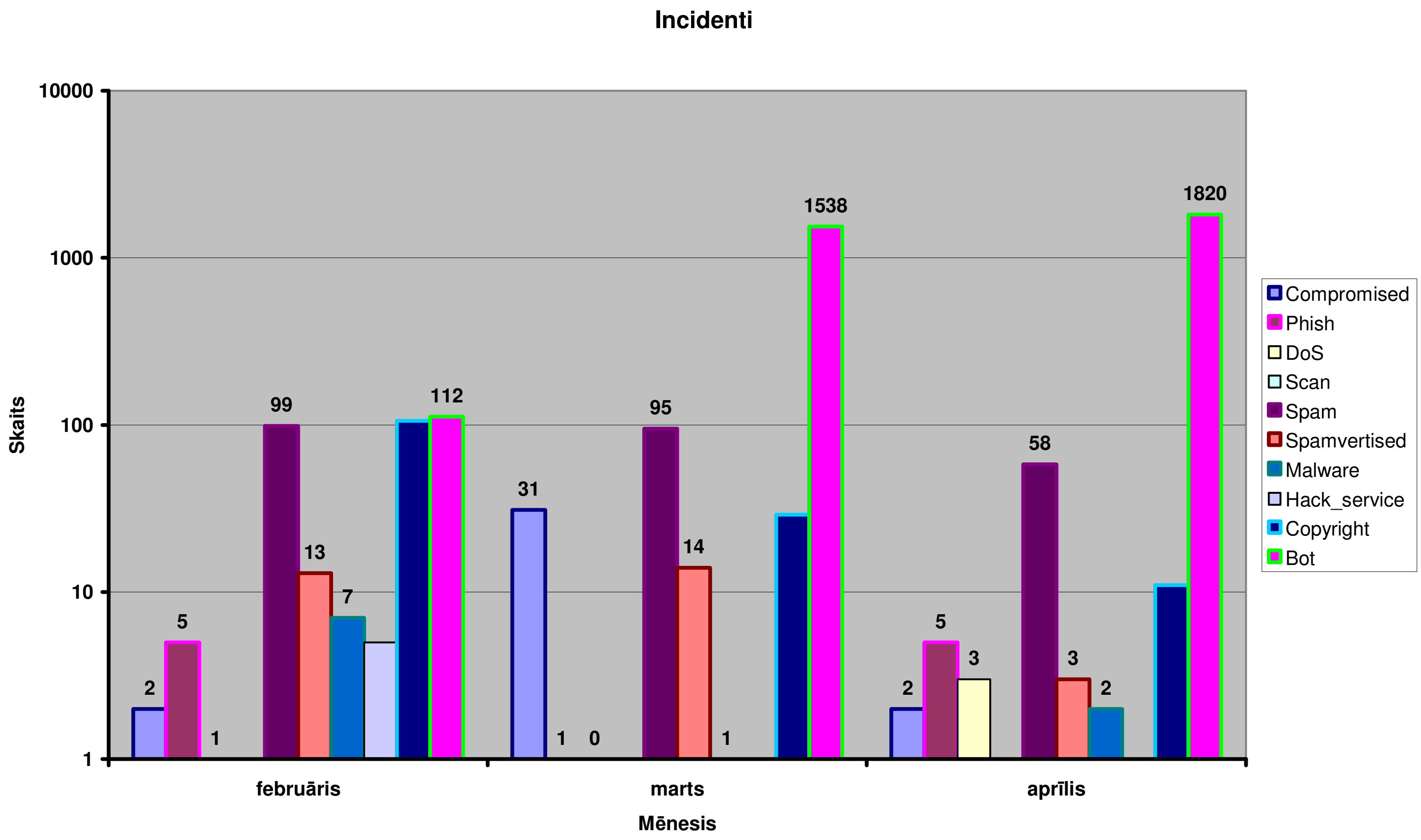
Incident response

- Dealt with 3966 incidents
- Numbers increase – new cooperation agreements with ISPs

CERT.LV incident statistics – 3 months



CERT.LV incident statistics - monthly



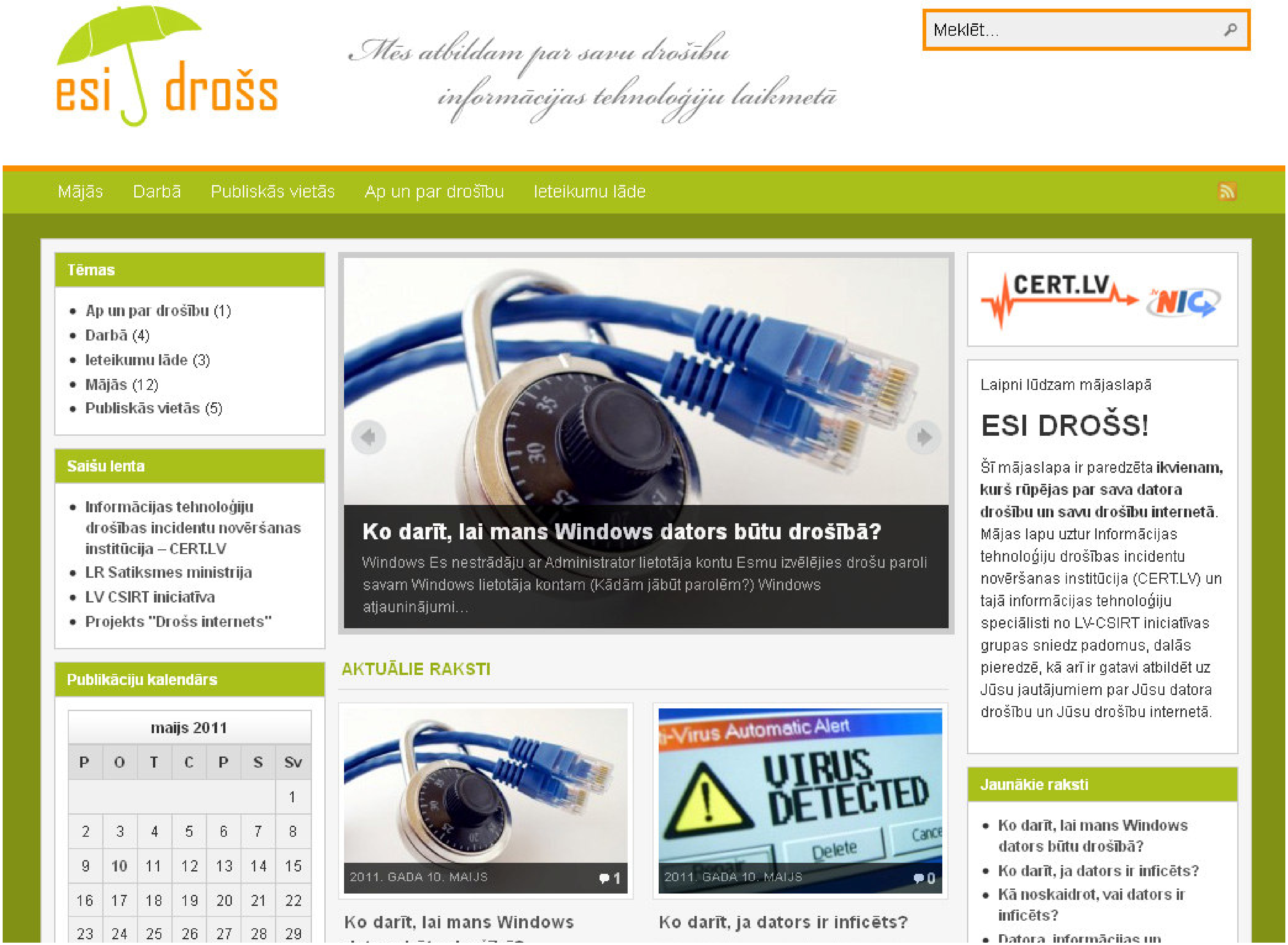
Some incidents

- News agency server hacking
- IMCS UL servers under severe hacking
- Energy company's case
- Analysis of targeted viruses
- Virus removals at several State authorities
- Identity theft
- DDoS municipality web servers
- Botnet activities targeting .LV primary name servers

Awareness raising, education, exercise organization, recommendations

Information, recommendations

- Information on newest viruses and threats
- Articles, suggestions
- Examples for IT security principles and rules
- Portal www.esidross.lv (“be safe”)



Tēmas

- Ap un par drošību (1)
- Darbā (4)
- Ieteikumu lāde (3)
- Mājās (12)
- Publiskās vietās (5)

Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija
- LV CSIRT iniciatīva
- Projekts "Drošs internets"

Publikāciju kalendārs

maijs 2011

P	O	T	C	P	S	Sv
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Ko darīt, lai mans Windows dators būtu drošībā?

Windows Es nestrādāju ar Administrator lietotāja kontu Esmu izvēlējies drošu paroli savam Windows lietotāja kontam (Kādām jābūt parolēm?) Windows atjauninājumi...

AKTUĀLIE RAKSTI

2011. GADA 10. MAIJS 1

Ko darīt, lai mans Windows

2011. GADA 10. MAIJS 0

Ko darīt, ja dators ir inficēts?

Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta **ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā**. Mājas lapu uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tajā informācijas tehnoloģiju speciālisti no LV-CSIRT iniciatīvas grupas sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Ko darīt, lai mans Windows dators būtu drošībā?
- Ko darīt, ja dators ir inficēts?
- Kā noskaidrot, vai dators ir inficēts?
- Datora informācijas un

Events, presentations

- “Be safe -1” in Riga and Kuldiga
- Presentation of CERT.LV at the 69th conference of the University of Latvia
- Participation in World Wide Safer Internet day

Other activities

- Educational posters
- Participation in TV and radio programs
- Interviews with journalists
- Articles for portals, news releases
- Academic activities

P4c78Tm
X620m59
D3Øafg4
VISA
x!#$B@
REVCON
TORRENT
CRACK
MasterCard
VISA
SPAM

Vai esi Interneta profiņš?

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.

Lieto drošas paroles!

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

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 neklūst. 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:

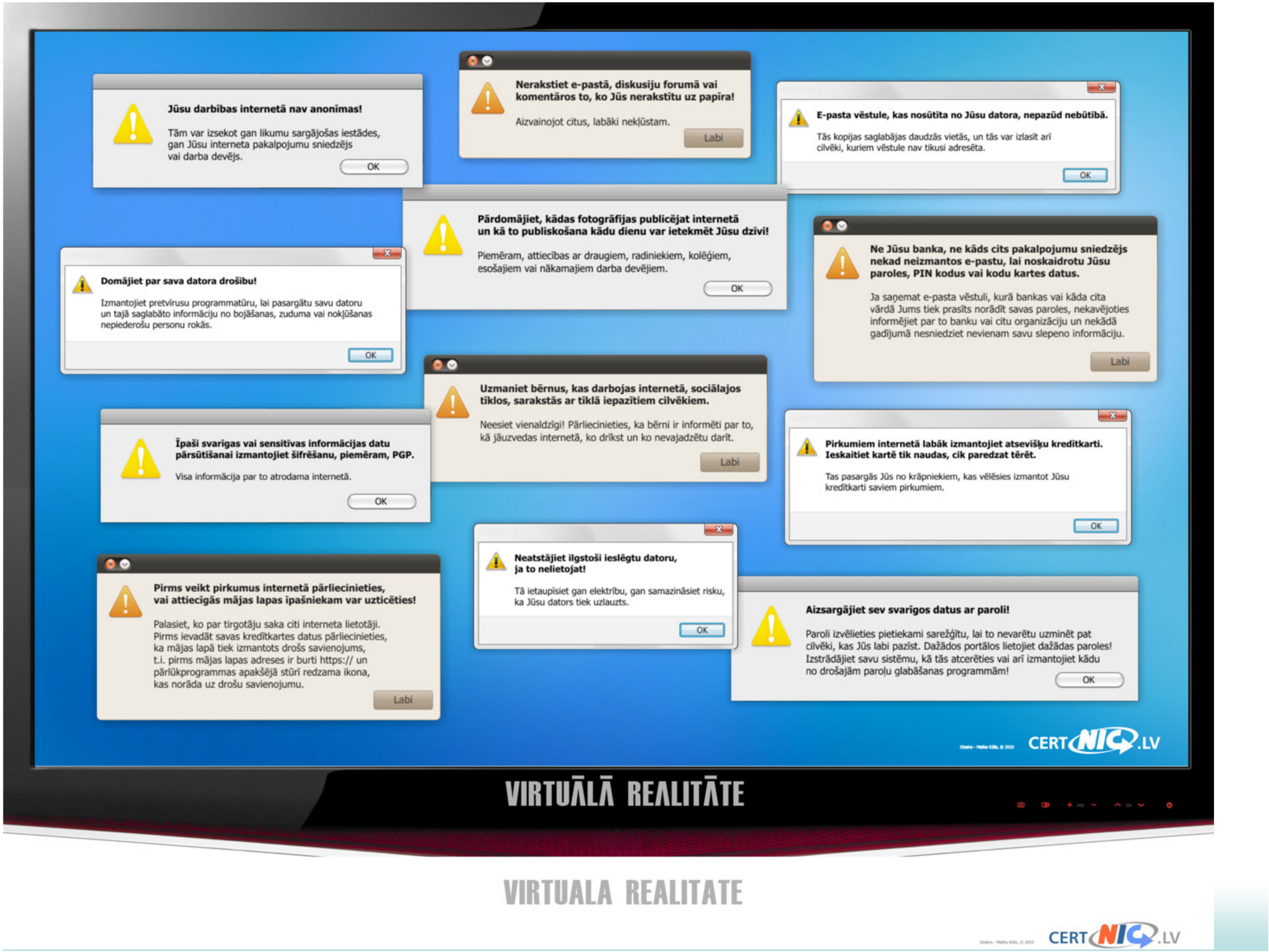
- saņem nepatīkamas, aizvainojošas vēstules internetā,
- esi saskāries ar nepatīkamiem materiāliem internetā,
- esi pamanījis aizdomīgas darbības internetā,
- esi satraukts par savu drošību internetā,

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

Dizains - Matīss Kūlis, © 2010

CERT NIC .LV

CERT.LV



Jūsu darbības internetā nav anonīmas!

Tām var izsekot gan likumu sargājošas iestādes, gan Jūsu interneta pakalpojumu sniedzējs vai darba devējs.

Nerakstiet e-pastā, diskusiju forumā vai komentāros to, ko Jūs nerakstītu uz papīra!

Aizvainojot citus, labāki neklūstam.

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.

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.

Domājiet par sava datora drošību!

Izmantojiet pretvīrusu programmatūru, lai pasargātu savu datoru un tajā saglabāto informāciju no bojāšanas, zuduma vai nokļūšanas nepiederošu personu rokās.

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.

Uzmaniet bērnus, kas darbojas internetā, sociālajos tīklos, sarakstās ar tiklā iepazītiem cilvēkiem.

Neesiet vienaldzīgi! Pārliecinieties, ka bērni ir informēti par to, kā jāuzvedas internetā, ko drīkst un ko nevajadzētu darīt.

Īpaši svarīgas vai sensitīvas informācijas datu pārsūtīšanai izmantojiet šifrēšanu, piemēram, PGP.

Visa informācija par to atrodama internetā.

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.

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.

Neatstājiet ilgstoši ieslēgtu datoru, ja to nelietojat!

Tā ietaupīsiet gan elektrību, gan samazināsiet risku, ka Jūsu dators tiek uzlauzts.

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!

Dizains - Matīss Kūls, © 2010

VIRTUĀLĀ REALITĀTE

Cooperation with state and local authorities institutions, CSIRT units from different countries

Support for state institutions

- Incident response, help with malware
- Cooperation with Security agencies
- Participation in working groups to design regulations of the Cabinet of Ministers
- Expertise and opinion on request

International cooperation

- Cooperation with other CSIRTs
  - CERT-EE, CERT-SE, CERT.GOV.PL, CERT-LT, SURFNet CERT, GovCERT.NL, CERT.BE, ...
- CERT.LV presented in Barcelona at TF-CSIRT & FIRST symposium

Other activities

- Cooperation with Microsoft Cyber Crime Unit
- Participation in “ECO Workshop on Botnet Detection, Measurement, Disinfection & Defense”
- Cooperation with NATO

Other activities

Other activities

- Set up of local framework at IMCS UL
- Adjustment of internal systems
- Design of a contact database
- Style, logo, home page, business cards, etc.
- Twitter account

More – other activities

- Permission from Carnegie-Melon university to use CERT.LV
- RFC document update
- Update of information in FIRST and Trusted Introducer registries

Future plans

CERT.LV future plans - 1

- Strengthening CERT.LV’s position as a competent IT security research and response institution
- Strengthen cooperation with governmental and municipality institutions
- Improve communication with ISPs
- Fine-tuning of incident monitoring tools and processing technique, knowledge base gathering

CERT.LV future plans - 2

- IS security research, honeypots, botnet infiltration, etc.
- Organizing regular seminars and training
- Disaster recovery planning and exercises
- NATO, CCDCoE - training and knowledge transfer
- Maintaining educational portal - www.esidross.lv ("*be safe*")
- Information exchange with news and media

Thank you!!!

http://ww.cert.lv/

cert@cert.lv

baiba.kaskina@cert.lv