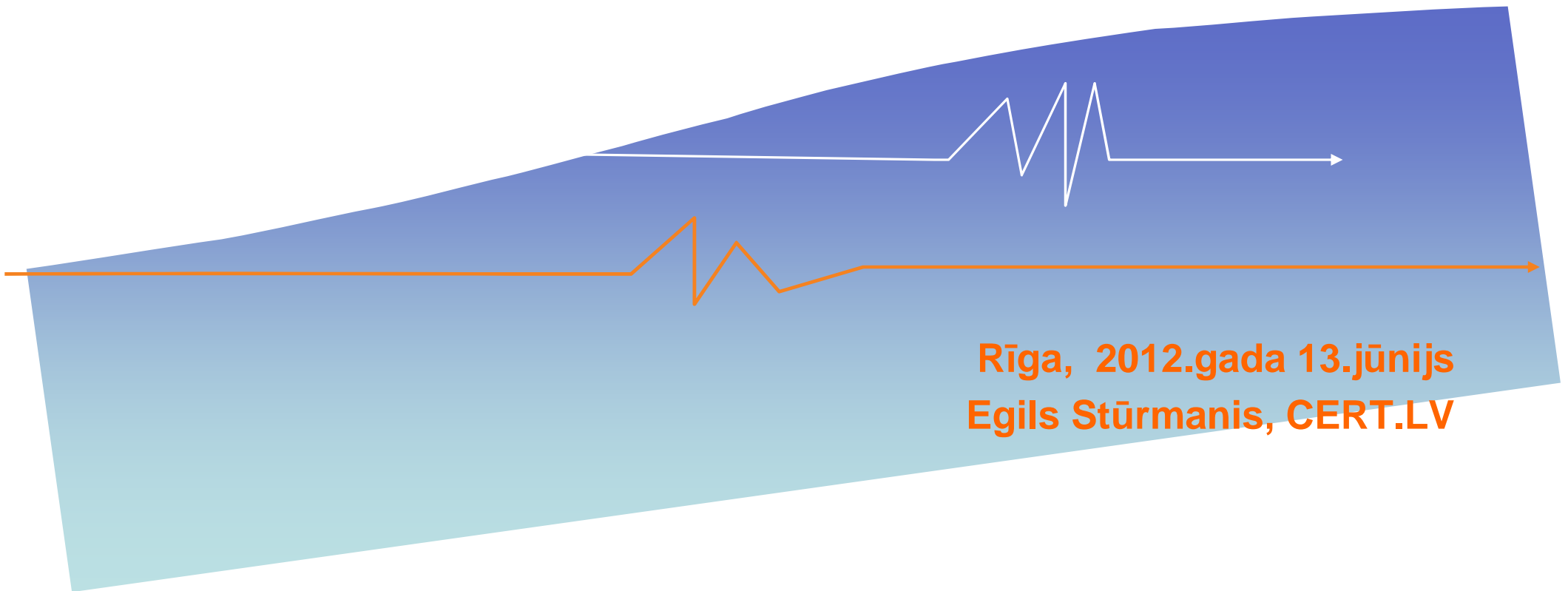




real-IT-āte ***virtuālajā vidē***

--- Kas jāzina skolniekiem par IT drošību ---

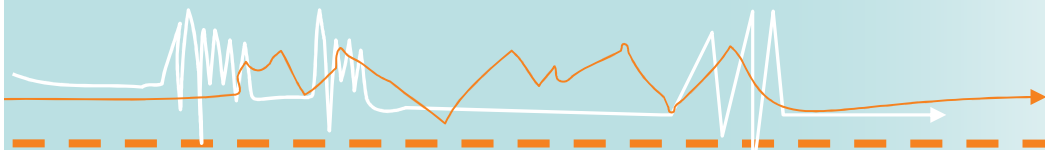




Saturs

- Ievads
- Drošības prasību neievērošana
- Sociālā inženierija
- Rīcība drošības incidenta un pārkāpumu gadījumos





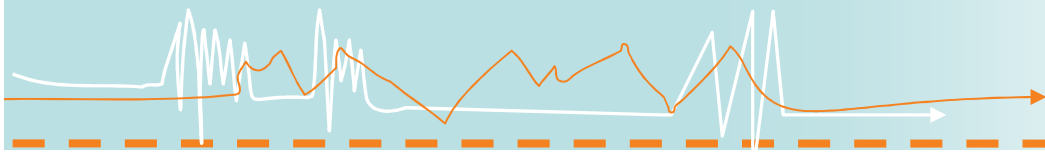
CERT.LV

levads



Drošības prasību neievērošana



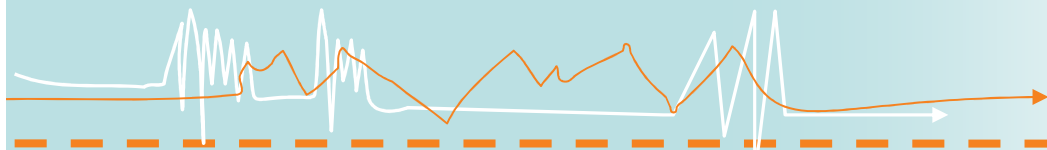


Drošības prasību neievērošana



Ekrānšāviņš no Krievijas televīzijas kanāla NTV, kurā redzamas ātrās palīdzības automašīnas pie Maskavas Domodedovas lidostas, 24.janvāris, Foto: AFP/LETA





Dezinformācija - integritātes izjaukšana



Informācijas noplūde - konfidencialitātes izjaukšana

Noplūdušie dokumenti un Latvija



Izstrādāti plāni
Baltijas aizsardzībai
pret Krieviju (25)



'WikiLeaks': 'Arctic
Sea' nolaupīšanā bija
iesaistīti Krievijas
politīķi (66)



ASV atsauks
'nogrēkojušos'
vēstniekus (18)



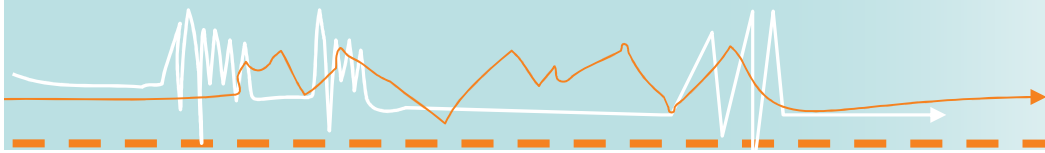
'WikiLeaks' publicē
ASV drošībai vitāli
svarīgu objektu
sarakstu (168)

Informācijas noplūde - konfidencialitātes izjaukšana

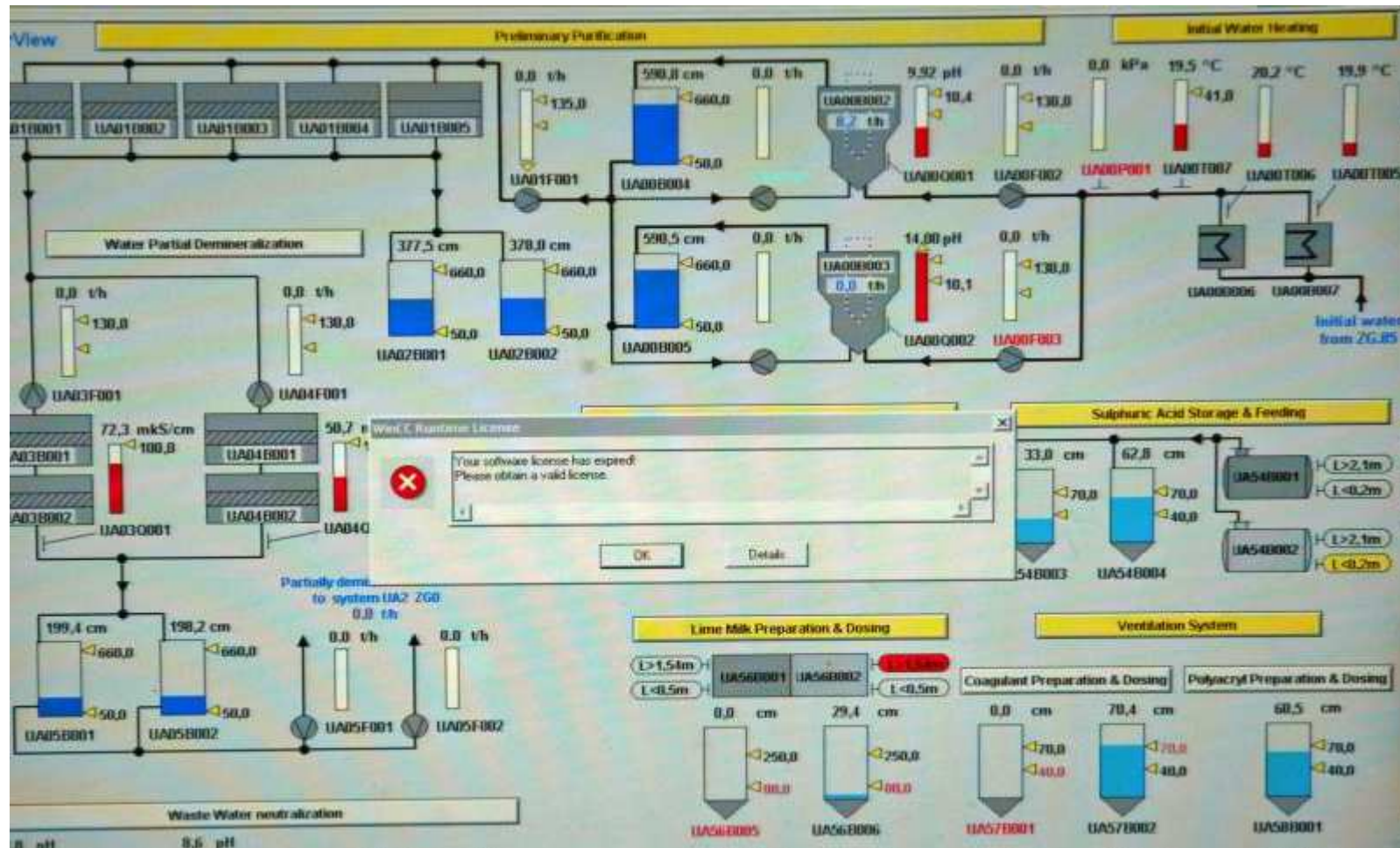
Okupantu autoparks

Piedāvājam sarakstu ar Latvijai acimredzami neobjāiem auto īpašniekiem (okupantiem), kuri savus auto numuriem, kuri norādīti **treknrakstā**, iespējams uzklāksināt, lai redzētu atbilstošā auto foto.

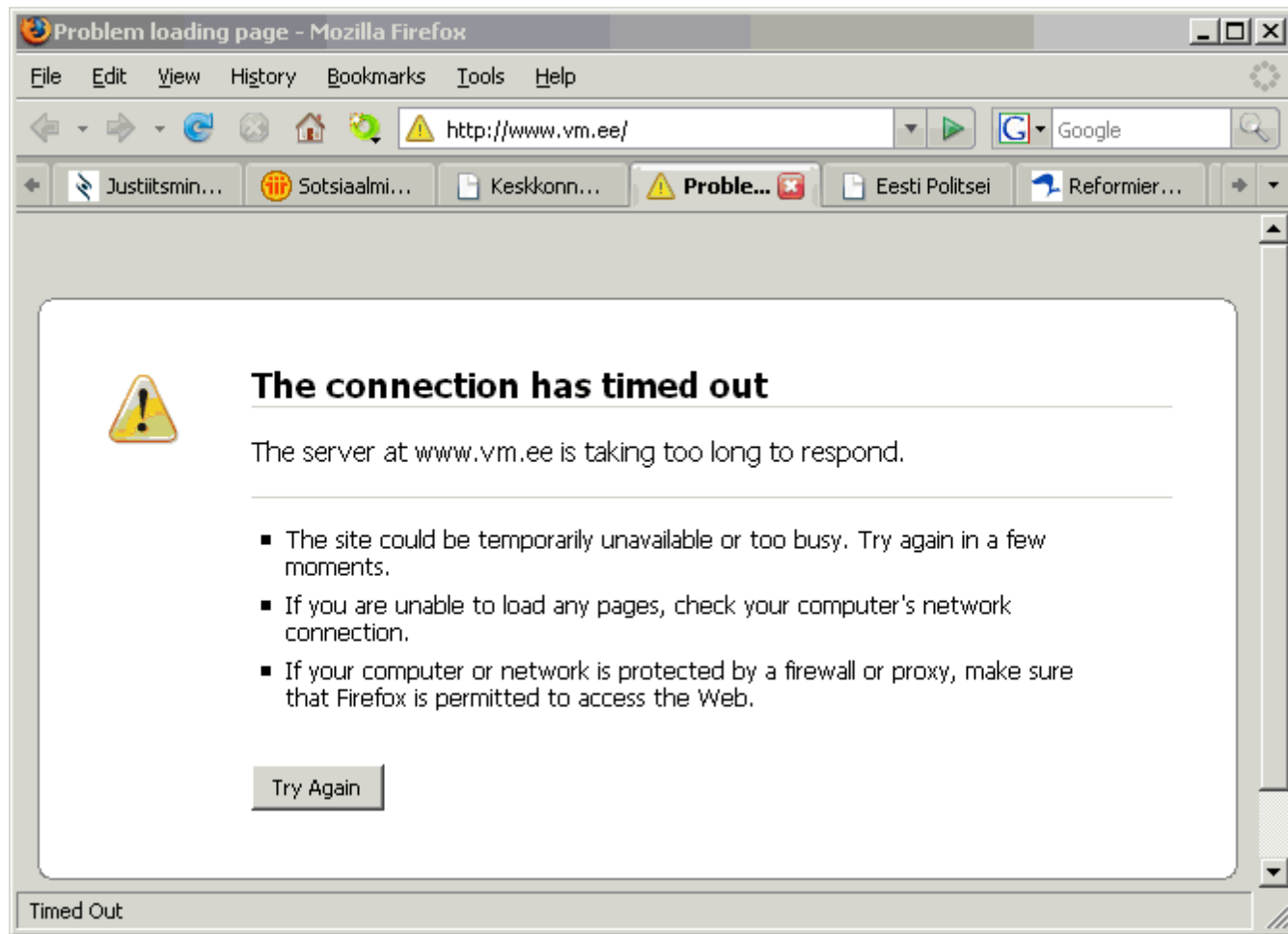
Valsts nr.	Auto marka	Īpašnieks/turētājs	Reģ. nr.
001-12345	BMW M3	Jevgēnijs Sopkins	001-12345
002-67890	Opel Frontera	Dmitrijs Gridņovs	002-67890
003-11111	Opel Astra Caravan	Eduards Krupko	003-11111
004-22222	audi 100	Ija Sedhs	004-22222
005-33333	Toyota Corolla Verso	Aleksejs Poplavskis	005-33333
006-44444	BMW 318	Eduards Stahovskis	006-44444
007-55555	BMW 523	Inna Šalajeva	007-55555
008-66666	Ford Mondeo	Nikolajs Solodovičs	008-66666
009-77777	VW Golf	Vladimirs Husnutdinovs	009-77777
010-88888	Mitsubishi Eclipse	Stajislavs Žuravjovs	010-88888
011-99999	Citroen C2	SIA "Ausek"	011-99999
012-00000	citroen berlingo	Dmitrijs Vasiljevs	012-00000
013-11111	Nissan Sunny	Aleksejs Žuvaks	013-11111



Informācijas tehnoloģiju uzbrukumu ieroči - pieejamības izjaukšana



Informācijas tehnoloģiju uzbrukumu ieroči - pieejamības izjaukšana: Igaunijas gadījums



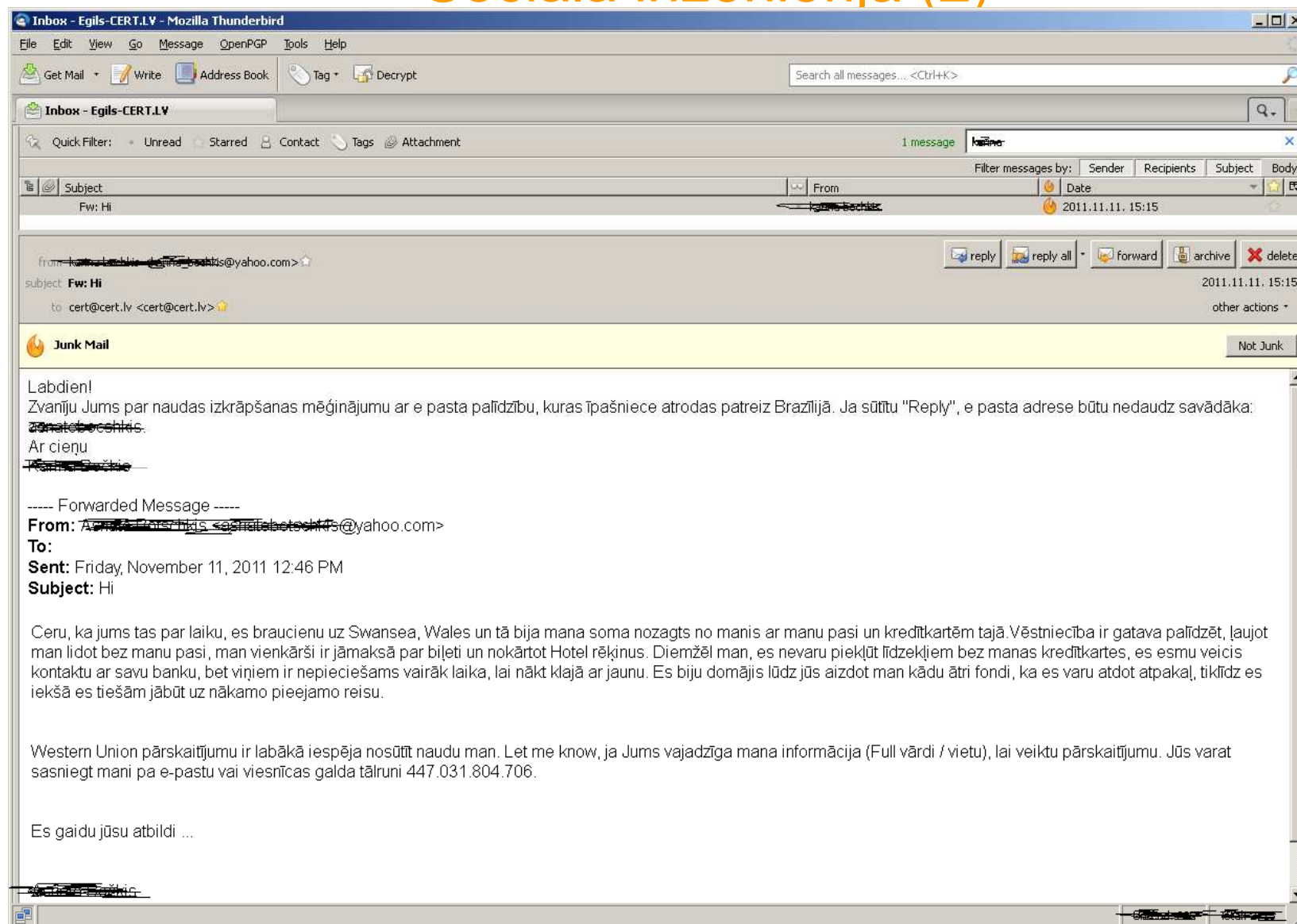
Sociālā inženierija



Sociālā inženierija (1)

- **Sociālā inženierija** – manipulēšana ar cilvēku, lai tas veiktu zināmas darbības vai izpaustu konfidenciālu informāciju, tehniski nepieklūstot informācijas sistēmai.
- Sociālās inženierijas paņēmieni tiek īstenoti, pamatojoties uz īpašiem atribūtiem cilvēka lēmumu pieņemšanas mehānismos.
- **Svarīgi atcerēties:**
 - Šķietami visnenozīmīgākā komunikācija ar nepazīstamu cilvēku nedrīkst sevī informāciju par darbu, dzīves vietu, radniekiem utt.

Sociālā inženierija (2)



The screenshot shows the Mozilla Thunderbird email interface. The window title is "Inbox - Egils-CERT.LV - Mozilla Thunderbird". The menu bar includes File, Edit, View, Go, Message, OpenPGP, Tools, and Help. The toolbar contains icons for Get Mail, Write, Address Book, Tag, and Decrypt, along with a search bar "Search all messages... <Ctrl+K>".

The main pane shows a list of messages. The selected message has the subject "Fw: Hi" and is dated "2011.11.11. 15:15". The sender is "Egils-CERT.LV".

The message content is as follows:

Labdien!
Zvanīju Jums par naudas izkrāpšanas mēģinājumu ar e-pasta palīdzību, kuras īpašniece atrodas patreiz Brazīlijā. Ja sūtītu "Reply", e-pasta adrese būtu nedaudz savādāka:
~~znanate@cschds~~
Ar cieņu
~~Kristina Svecie~~

----- Forwarded Message -----
From: ~~Anna Svecie~~ <~~anna.svecie@yahoo.com~~>
To:
Sent: Friday, November 11, 2011 12:46 PM
Subject: Hi

Ceru, ka jums tas par laiku, es braucīenu uz Swansea, Wales un tā bija mana soma nozagts no manis ar manu pasi un kredītkartēm tajā. Vēstniecība ir gatava palīdzēt, ļaujot man līdot bez manu pasi, man vienkārši ir jāmaksā par biļeti un nokārtot Hotel rēķinus. Diemžēl man, es nevaru piekļūt līdzekļiem bez manas kredītkartes, es esmu veicis kontaktu ar savu banku, bet viņiem ir nepieciešams vairāk laika, lai nākt klajā ar jaunu. Es biju domājis lūdz jūs aizdot man kādu ātri fondi, ka es varu atdot atpakaļ, tiklīdz es iekšā es tiešām jābūt uz nākamo pieejamo reisu.

Western Union pārskaitījumu ir labākā iespēja nosūtīt naudu man. Let me know, ja Jums vajadzīga mana informācija (Full vārdi / vietu), lai veiktu pārskaitījumu. Jūs varat sasniegt mani pa e-pastu vai viesnīcas galda tālruni 447.031.804.706.

Es gaidu jūsu atbildi ...

~~Kristina Svecie~~

Sociālā inženierija (3)

- Mērķa sasniegšanai sociālais inženieris var manipulēt ar darbinieku motivāciju:
 - bailes pazaudēt darbu;
 - vēlme tikt novērtētam;
 - nogurums vai pārstrādāšanās;
 - mobings darba vietā.
- Mērķa sasniegšanai tiek izmantota arī cilvēku sociālo vērtības akceptēšanas paradumi:
 - cilvēki pieņem uzvedību, kura viņuprāt piemīt lielākajai daļai citu cilvēku;
 - cilvēki ir tendēti sadarboties ar cilvēkiem kuri izraisa viņos simpātijas.

Sociālā inženierija (5)

- **Uzbrucēju komunikāciju veidi:**
 - personīgi kontakti;
 - Telefons;
 - elektroniskais pasts;
 - ļaundabīga programma.
- **Aizsardzības stratēģija skolā:**
 - darbojošies IT drošības noteikumi;
 - stingra piekļuves procedūra IT resursiem ar lietotājevārdu un paroli;
 - stingra parolu izveidošanas procedūra;
 - lojālas un draudzīgas darba vides izveidošana;
 - procedūra, kā un kam paziņot par incidentu.

Rīcība drošības incidenta un pārkāpumu gadījumos

Rīcība drošības incidenta un pārkāpumu gadījumos

- **Labā prakse skolā:**

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

- **Mājās:**

- Pats atbildīgs par sava datora drošību,
- Jānovērtē kaitējums, un ja nepieciešams jāraksta iesniegums Valsts policijai,
- Portālā www.esidross.lv var meklēt padomus, kā risināt problēmas un kā aizsargāt savu informāciju nākotnē.

Paldies par uzmanību!

<http://www.cert.lv>

cert@cert.lv

egils.sturmanis@cert.lv

Prezentācijā daļēji izmantoti Centrālās Statistikas pārvaldes materiāli.

Prezentācijas saturs sagatavots Latvijā, izmantot Wikipedia publicētās definīcijas, publikācijas interneta medijos un ņemot vērā autoru personīgo izpratni informācijas drošības un datu aizsardzības jautājumos.

