Informācijas drošības apzināšanās

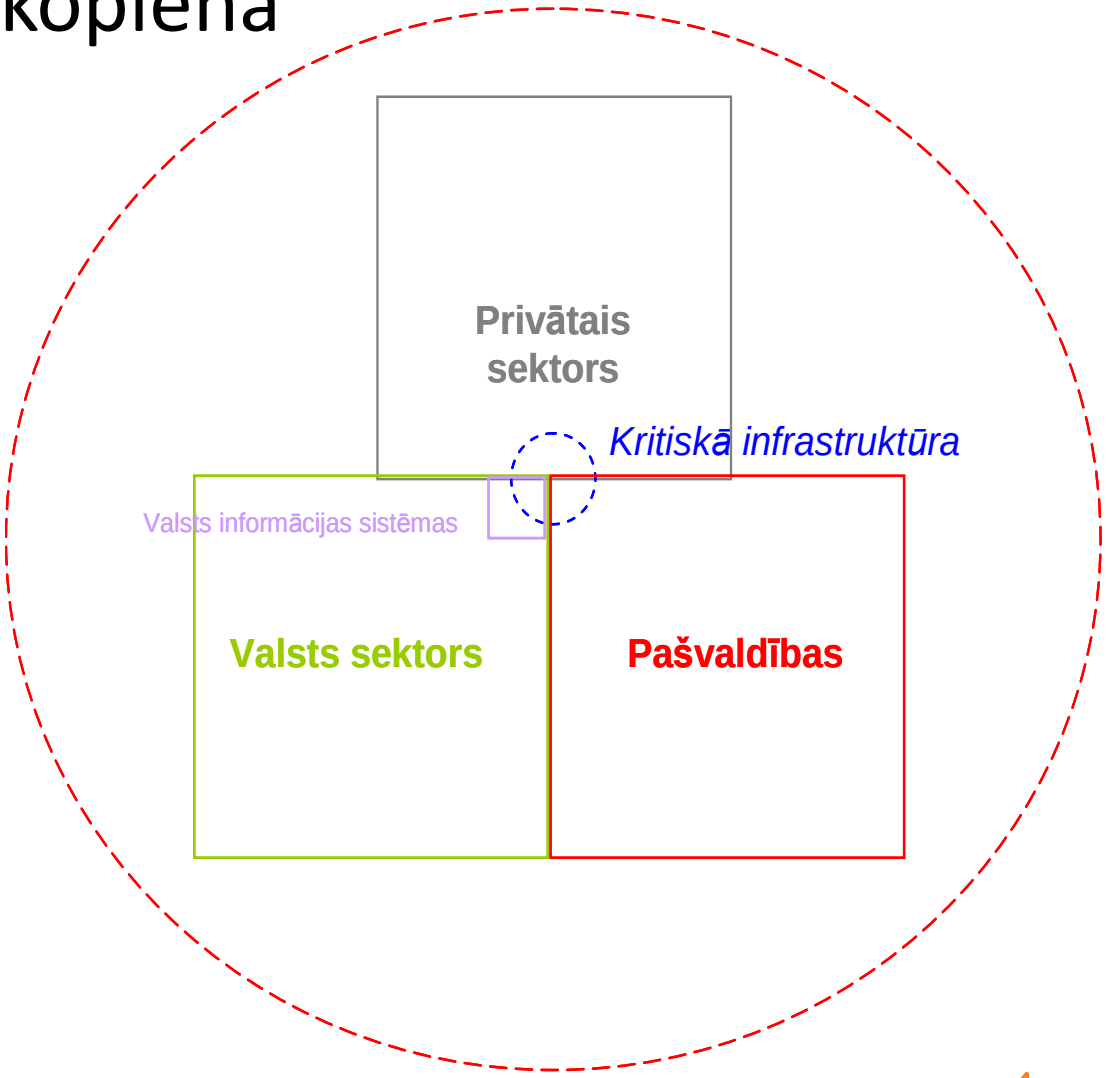
Ģirts Bitenieks
IT & drošības konsultants
girtsb@yahoo.com
Tālr.28348286

CERT.LV

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Misija: “Veicināt IT drošību Latvijā”

CERT.LV kopiena



CERT.LV sadarbojas

- Valsts un pašvaldību iestādes
- IT Kritiskā infrastruktūra
- Privātais sektors, piemēram:
  - Elektronisko sakaru komersanti
  - Finanšu sektors
- Nevalstiskās organizācijas
- NBS, Kiberaizsardzības vienība
- Starptautiskie partneri
  - NATO, ENISA, CCDCoE
  - Citu valstu līdzīgas institūcijas, CERT komandas

Ko CERT.LV nedara?

- Satura izvērtēšana
- Personas datu aizsardzība
- Valsts informācijas sistēmu jautājumi
- Noziegumu izmeklēšana
- Iestāžu, sistēmu auditi

Apdraudējumi

Mūsu ikdienas dzīvē nepārtraukti pieaug interneta un e-pasta nozīme, bet vienlaikus mums draud aizvien vairāk briesmu, kad lietojam šos tehnikas sasniegumus.

Lai varētu efektīvi apkarot šos draudus, mums par tiem jāzina pēc iespējas vairāk.

No datorhuligānisma līdz krāpnieku programmatūrai

Vēl pirms dažiem gadiem datoru lietotājus galvenokārt apdraudēja tikai vīrusi un tārpi. Šīm programmām bija viens galvenais mērķis - pēc iespējas plašāk izplatīties, lai gan dažas no tām arī bojāja datus vai pašu datoru. Šādu kaitīgo programmu izplatīšanu sauc par datorhuligānismu.
Pēdējos gados stāvoklis ir stipri mainījies.

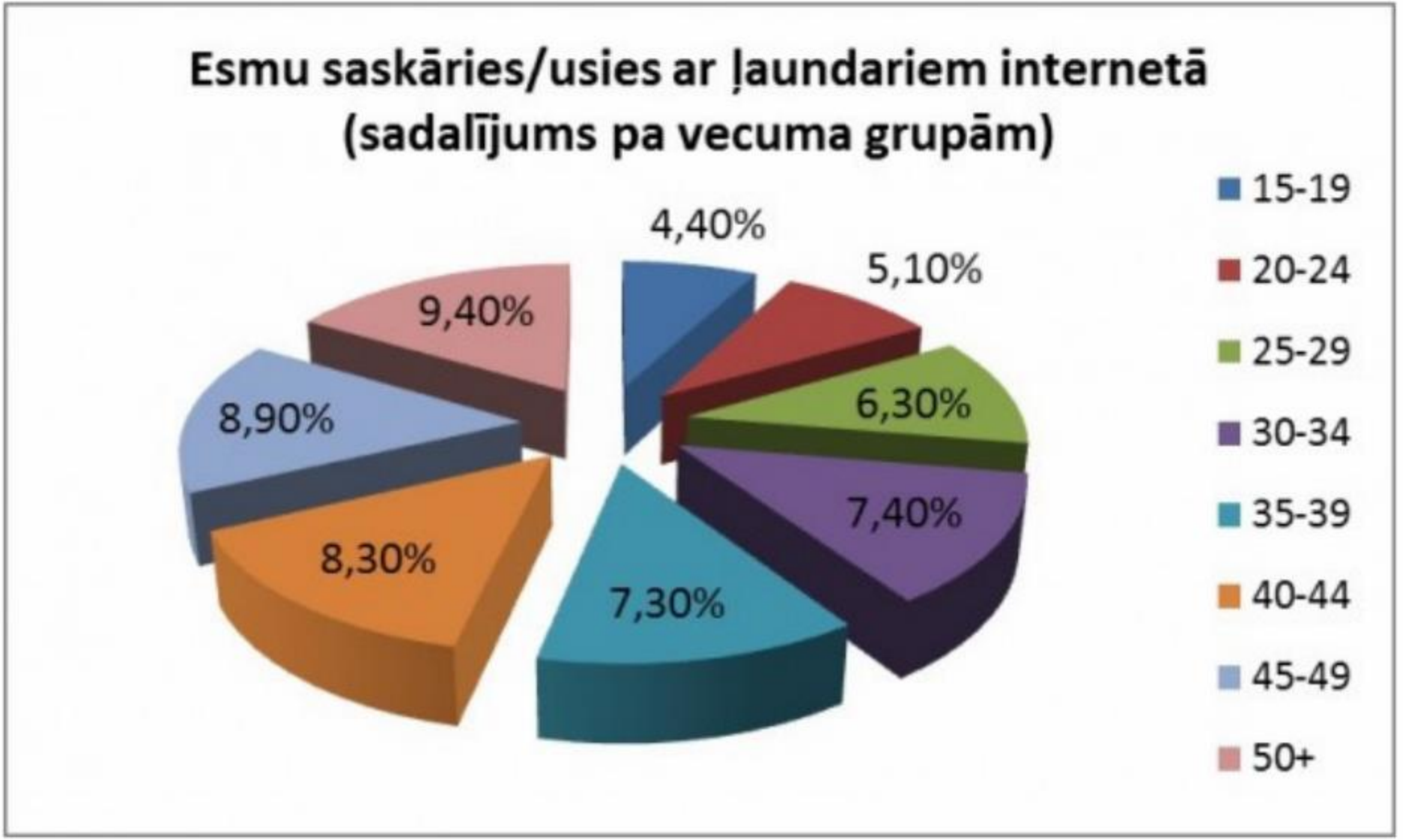
Šodien lielākais drauds ir krāpnieciskā programmatūra, ko noziedznieki izstrādā, lai gūtu nelikumīgus ienākumus. Vairums kaitīgo programmu, ko izmanto noziegumu pastrādāšanai, ir dažādi vīrusi, tārpi, Trojas zirgi u.c.

Lasiet par apdraudējumiem - zinošs lietotājs ir pakļauts daudz mazākam riskam!

Informācijas drošības, Iekšējās kārtības, resursu pieļaujamas izmantošanas un tīra galda politika (u.c.)

- Nepieciešams skaidri norādīt darbinieku pienākumus un atbildību, kā arī ierobežojumus (darba apraksts, departamenta/ nodaļas nolikums). Normatīvo aktu pieņemšanas apliecinājums.
- Darbinieki ir atbildīgi par visām darbībām, kas saistītas ar savu lietotāja ID.
- Kā daļa no darbā pieņemšanas procesa, darbiniekus ir jāiepazīstina ar informācijas drošības politiku (ieviest ikgadēju informācijas drošības informētības programmu).
- Informācijas klasifikācijas apzināšanās un pielietojums ikdienā.
- Informācijas drošības speciālists.

IZZI aptauja draugiem.lv portālā



draugiem.lv/izzi/?p=8196107

Pieslēguma piemēri tīmeklim

- **Uzbrucēju komunikāciju veidi:**

- Personīgi kontakti

- Telefons

- Elektroniskais pasts

- Internets

Kas ir spiegu programmas?

Kā liecina šo programmu nosaukums, tās ir paredzētas informācijas vākšanai lietotāja datorā un tās nosūtīšanai kādai nepiederošai personai bez datora īpašnieka piekrišanas. Šīs programmas var reģistrēt klaviatūras taustiņu nospiešanu (klaviatūras nolasītāji), vākt jūsu konfidenciālo informāciju (paroles, kredītkaršu numurus, PIN kodus utt.), izspiegot e-pasta adreses pastkastītē un datora lietotāja darbību internetā.

Phishing jeb «Pikšķerēšana»

Pikšķerēšana ir gandrīz tas pats, kas makšķerēšana. Kibernoziedznieki, protams, nemakšķerē zivis, bet tik un tā velk lielus lomus, izmānot lietotāju konfidenciālo informāciju.

Tas ir īpašs interneta krāpniecības paveids. Personas datu izmānīšana.

Kibernoziedznieki izveido viltus vietni, kas mats matā līdzīga bankas vai kādas interneta maksājumu sistēmas vietnei. Pēc tam lietotājus aicina apmeklēt šo vietni un tur ievadīt savus konfidenciālos datus, piemēram, pieteikumvārdu, paroli vai PIN kodu. Vēlāk ļaundari šos datus izmanto, lai nozagtu piekrāpto lietotāju naudu.


From: Swedbank [mailto:info@swedbank.lv]
Sent: Wednesday, July 13, 2011 8:28 AM
Subject: Jums ir viens neizlasits zinojums
Importance: High
Swedbank
Dargais biedrs
Jums ir viens neizlasits zinojums
Ludzu ielogojieties sava profila
SSwedbank, tel. 67444444, info@swedbank.lv


From: Banka [info@banka.lv]
Sent: Wednesday, July 13, 2011 8:28 AM
Subject: Jums ir viens neizlasits zinojums
Importance: High
BANKA
Dargais biedrs
Jums ir viens neizlasits zinojums
Ludzu ielogojieties sava profila
Banka, 22222222 , info@banka.lv


Hansabanka <noreply@hanzanet.lv>
Pievienot adresi
Informacija no hanzanet.lv
Datums: Fri, 13 Jul 2007 06:17:06 -0400
Kam: redakcija@apollo.lv
Pielikums:
hanza.net
Sveiks, lietotaj.
Sakara ar kartejo sistemas uzlabosanu, mes jus ludzam atvert zemak noradito hipersaiti un aizpildit pieprasitos laukus.
https://www.hanzanet.lv/hanzaLV/1reg/
Atvainojamies par sagadatajam nertibam.
Hanzanet.lv

Banku vīruss

- inficē datoru
- pieprasa ievadīt kodu kartes numurus
- iespēja zaudēt naudu internetbankā

From: L****e <li***.la***@tesco.com>
Subject: Re:fails

Čau!
Lūdzu steidzami apskaties failu un izsaki savas domas! Gaidīšu atbildi!
http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Liene

vai

FROM: ja****.b****@dell.com
Subject: Re:dokuments

Čau,
Steidzami apskaties failu un dod ziņu! ...mums jārisina tā lieta steidzami!
http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Jānis

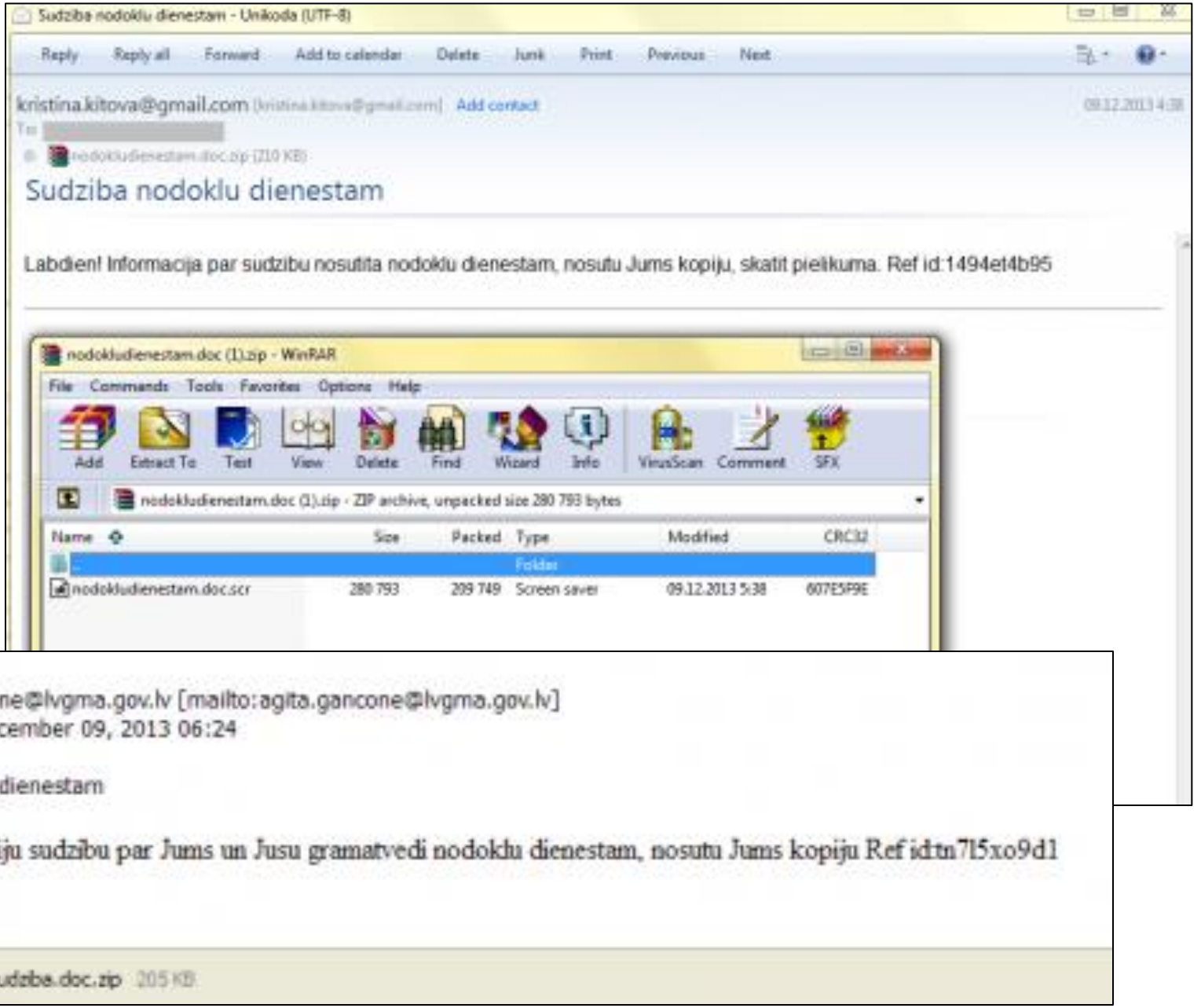
vai

FROM: *****e.vik****@github.com
Subject: Re:x

Čau,
Sūtu Tev failu ko runājām. Ja fails nonāks presē būs ļoti lielas problēmas un skandāls. Mums steidzami ir jārisina tā problēma!
http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Signe

VID Vīrus



From: agita.gancone@lvgma.gov.lv [mailto:agita.gancone@lvgma.gov.lv]
Sent: Monday, December 09, 2013 06:24
To:
Subject: nodoklu dienestam

Labdien! Uzrakstiju sudzību par Jums un Jusu gramatvedi nodoklu dienestam, nosutu Jums kopiju Ref id:tn7l5xo9d1

1 attachment: sudziba.doc.zip 205 KB

https://www.esidross.lv/2013/12/10/vid-viruss-ka-to-atpazit-un-iztirit/

Atlikušais laiks: 47:57:29

paysafecard

IP: [redacted]

Valsts: **LV Latvia**
Rajons: **Riga**
Pilsēta: **Riga**
ISP: [redacted]
OperētājSistēma: **Windows 7 (64-bit)**
Lietotāja Vārds: [redacted]

UZMANĪBU! Jūsu dators ir bloķēts zemāk norādīto drošības apsvērumu dēļ.

Jūs esat apsūdzēts par aizliegtu pornogrāfisku datu (bērnu pornogrāfija/zoofilija/izvarošana utt.) skatīšanos/uzglabāšanu un/vai izplatīšanu. Jūs esat pārkāpis Vispasaules deklarāciju par bērnu pornogrāfijas neizplatīšanu. Jūs esat apsūdzēts noziegumā, kas paredzēts Latvijas Republikas Krimināllikuma 161. pantā.

Latvijas Republikas Krimināllikuma 161. pants paredz brīvības atņemšanu uz laiku no **5** līdz **11** gadiem.

Tāpat jūs tiekat turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiekat turēts aizdomās par Latvijas Republikas Krimināllikuma 148. panta pārkāpšanu.

Latvijas Republikas Krimināllikuma 148. pants paredz brīvības atņemšanu uz laiku no 3 līdz **7** gadiem vai naudas sodu no **150** līdz **550** minimālo algu apmērā.

No jūsu datora ar nelikumīgas piekļuves starpniecību iegūta pieeja valsts nozīmes informācijai un publiskai pieejai slēgtiem datiem.

PIN Kods

Summa 50

1 2 3 4 5 6 7 8 9 0

Apmaksāt PaySafeCard

Kur es varu saņemt naudas sertifikātu PaySafeCard?

Pārskats par tirgotājiem: Latvijā PaySafeCard tu vari iegādāties visos **Plus Punkts** veikalos un **Narvesen** un **Qiwi** mašīna. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (**R-Kiosk**).

QIWI Baltic

VALSTS POLICIJA

Jūsu informācija ir šifrēta. Nemēģiniet atbloķēt jūsu datoru.

Uzmanību!

Jūs pārkapāt citu personu autortiesības vai saistītas tiesības (videomateriāli, mūzika, programmatūra) un nelegāli izmantojat aizsargātus materiālus, pārkapājot 1. panta, 8. daļas, 8. noteikumu, zināmu arī, kā Latvijas republikas krimināllikums.
1. panta, 8. daļas, 8. noteikums paredz sodu no diviem līdz pieciem simtiem minimālu algu apmērā, vai brīvības atņemšanu no diviem līdz astoņiem gadiem.
Jūs esat skatījis/jusi vai izplatījis/jusi aizliegtus pornogrāfiskus materiālus (pornogrāfija ar bērniem vai citi materiāli tika atrasti jūsu datorā). Jūs pārkapāt Latvijas krimināllikuma 202. Pantu, kas paredz brīvības atņemšanu no četriem līdz divpadsmit gadiem.
Nelegāla piekļuve datiem tika iniciēta no jūsu datora bez jūsu zināšanas, kas varētu but datora piesārņojuma dēļ ar vīrusiem, toties jūs pārkapāt likumu par nolaidīgu datora izmantošanu. Latvijas krimināllikuma 210. Pants paredz sodu līdz 100,000 Eur un brīvības atņemšanu no četriem līdz deviņiem gadiem. Ievērojot krimināllikuma grozījumus (ja pārkāpums tika konstatēts pirmo reizi), jūs netiksiet sodīts, ja samaksāsiet sodu.
Lai atbloķētu jūsu datoru un izvairīties no legālam sekām, jums ir obligāti jāsamaksā atbrīvošanas maksa 100 Eur apmērā caur PAYSAFECARD (jums ir jāiegādājas PAYSAFECARD, jāpapildina konts par 100 Eur un jāievadā kods). Jūs varat nopirkt kodu jebkura veikalā vai DUS. PAYSAFECARD ir pieejama visos nacionālajos veikalos.

Kā es varu samaksāt sodu un atbloķēt savu datoru?
1. Atrādiet PAYSAFECARD tirgošanas vietu jums blakus:

QIWI · plus punkts svarīgi sīkumi · NARVESEN · R kiosk

2. Saņemiet PAYSAFECARD ar priekšapmaksas opciju un papildiniet balansu par 100 Eur skaidrā naudā pie kases.
3. Ievadiet jusu PAYSAFECARD kodu un nospiediet submit un "Atbloķējiet jūsu datoru tagad"

Jūsu IP adrese: [redacted]
Atrašanas vieta: Riga, Riga, Latvia

paysafecard pay cash. pay safe — *Drošas transakcijas forma*

Ievadiet PAYSAFECARD kodu

Lūdzu ievadiet PAYSAFECARD kodu izmantojot PIN tastatūru apakšā

1	2	3	4	5	6	7	8	9	0	Izdzēst

Atbloķējiet jūsu datoru tagad!

Uzmanību: Soda naudai jābūt samaksātai **12.** stundu laikā. Pēc 12. stundām nebūs iespējas samaksāt sodu.
Visi jūsu dati tiks aizturēti un pret jums tiks uzsākts kriminālprocess, ja sods nebūs samaksāts.

From Mr. Samson Adekunle <offiice23432@gmail.com>

Subject **Best Regards**

Reply to fund_offiice@zbavitu.net

To undisclosed-recipients:;

UNITED NATIONS / WORLD BANK ORGANIZATION*
United Nations House, 617/618
Diplomatic Zone,
Central Area District,
Federal Capital Territory
Abuja, Nigeria

Our Ref: YBNGWB/UN/2014

Attention: Dear Beneficiary

RE: APPROVED COMPENSATION PAYMENT AWARD OF US$2.3M

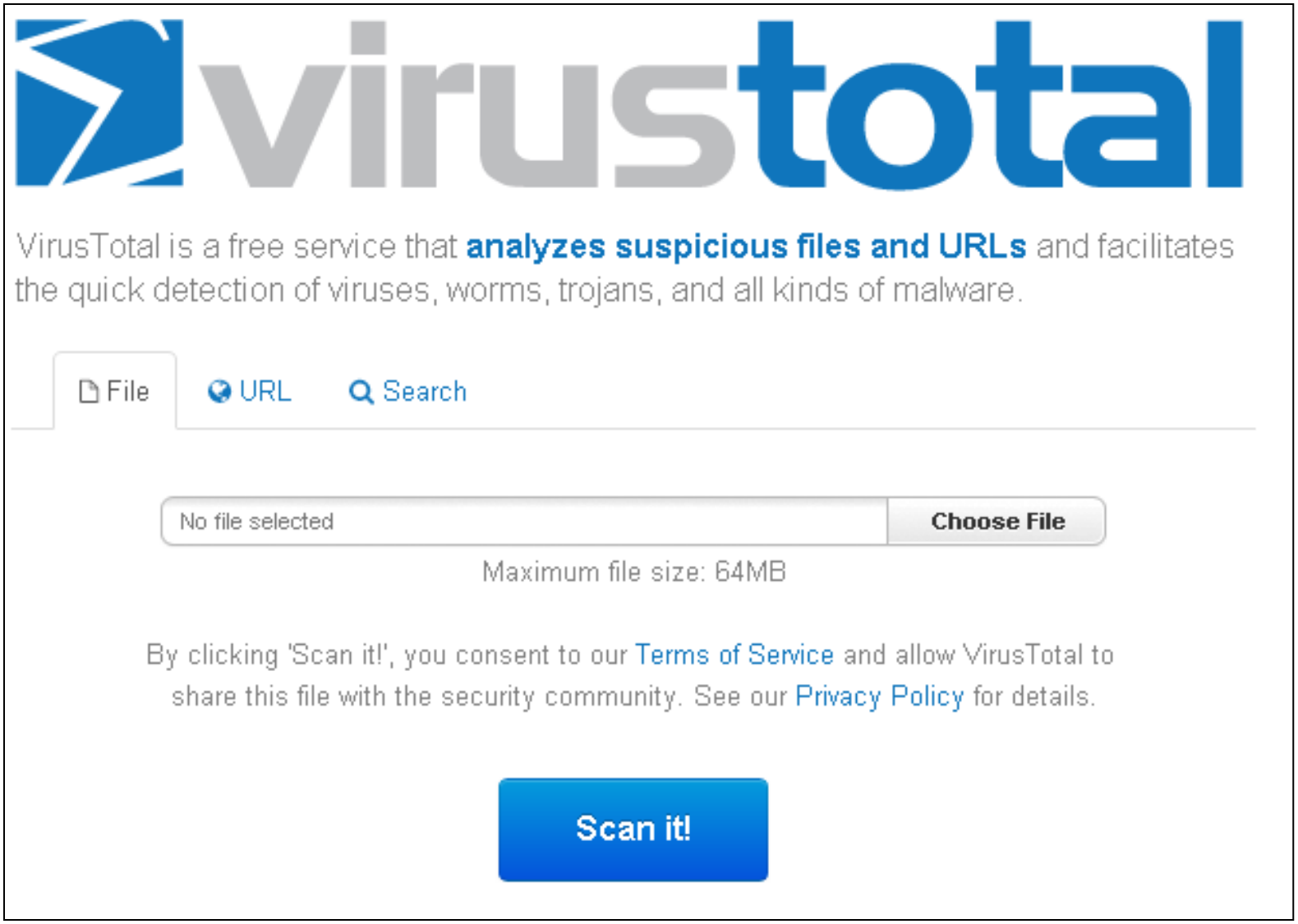
This is to inform you that a Debit Cash Card Number 7876310003001422 Valued at $2.3 Million United States Dollars has been accredited in your favor

Please contact Mr. Lancelot Ego, Email: <fund_offiice@zbavitu.net> with the following information to facilitate your claims:.

FULL NAME:
AGE:
GENDER:
ADDRESS:
COUNTRY:
OCCUPATION:
MOBILE NUMBER:

Aizdomīgu failu un mājas lapu pārbaude

https://www.virustotal.com

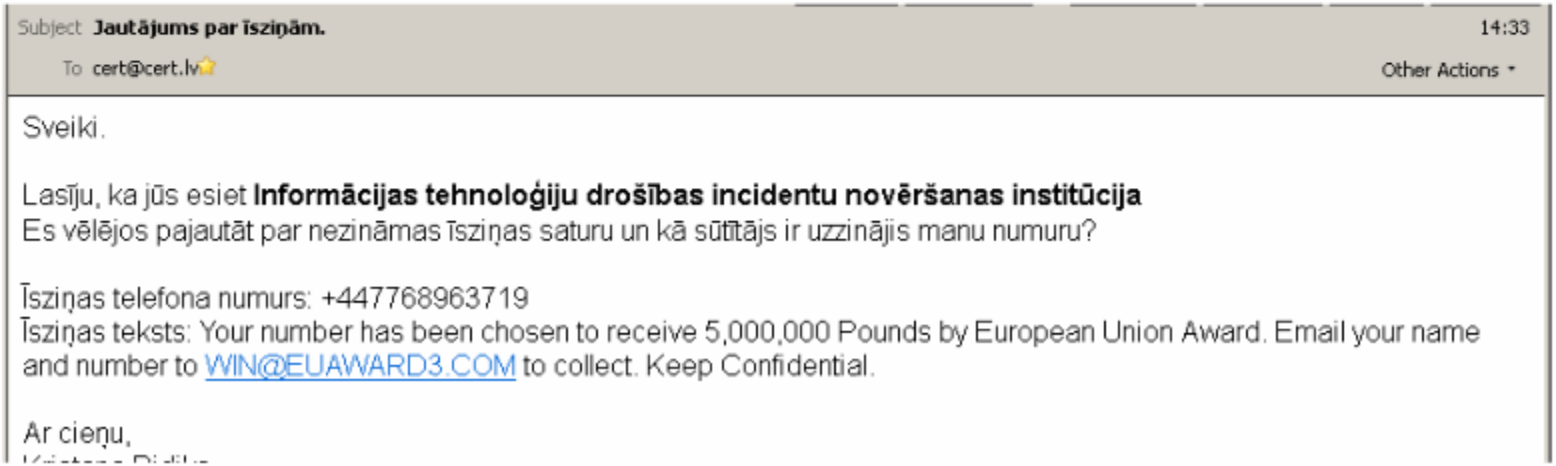


Viedtālruņu ievainojamības

- piemērs:

Android.Skullkey vīruss spēj:

- Attālināti kontrolēt ierīci
- Pārsūtīt informāciju no telefona
- Izsūtīt paaugstinātas maksas SMS



Subject **Jautājums par īsziņām.** 14:33

To cert@cert.lv Other Actions

Sveiki.

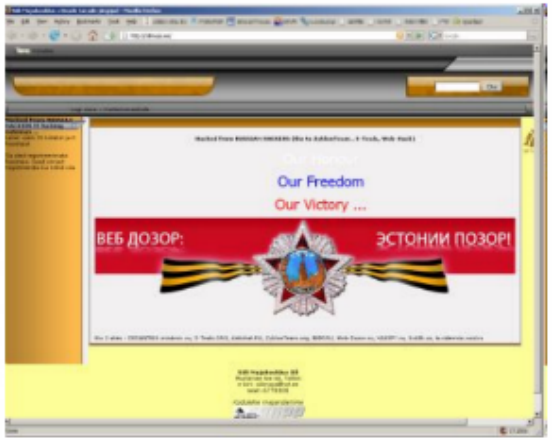
Lasīju, ka jūs esiet **Informācijas tehnoloģiju drošības incidentu novēršanas institūcija**
Es vēlējos pajautāt par nezināmas īsziņas saturu un kā sūtītājs ir uzzinājis manu numuru?

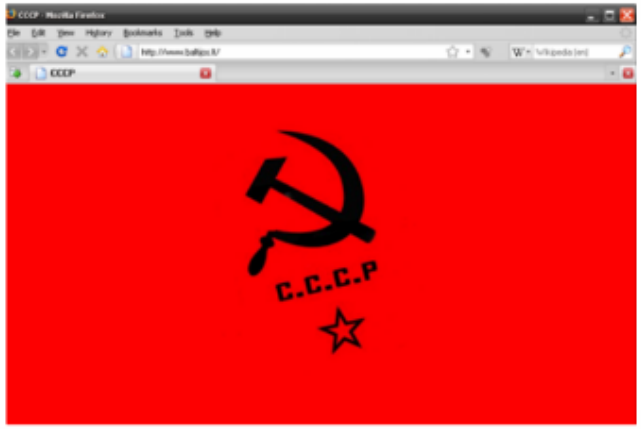
Īsziņas telefona numurs: +447768963719
Īsziņas teksts: Your number has been chosen to receive 5,000,000 Pounds by European Union Award. Email your name and number to WIN@EUAWARD3.COM to collect. Keep Confidential.

Ar cieņu,

Web lapu izķēmošnas piemēri

- Lietuva - servera ievainojamība
- Igaunija - 2007.gada kiberuzbrukums
- Latvija
  - 'caura' aplikācija
  - neapmierināts darbinieks



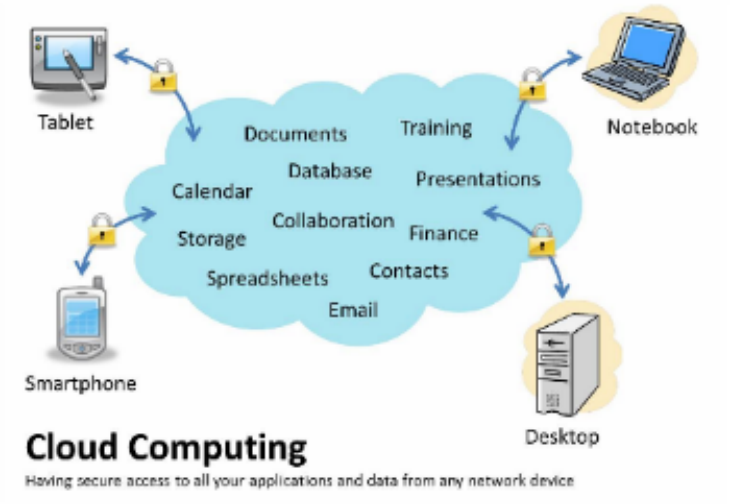


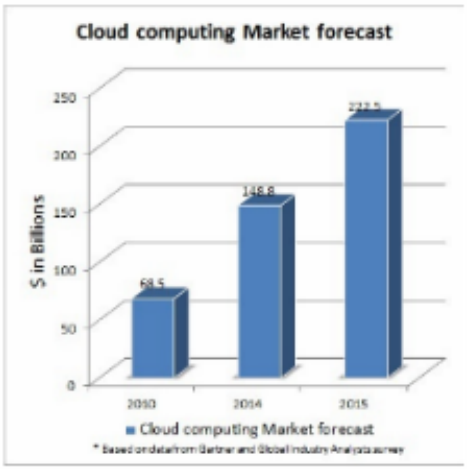
Informācijas aprite

- failu apmaiņas vietnes
- interešu portāli
- sociālie tīkli
- komunikācijas rīki
    - Skype
    - Twitter

Mākoņskaitļošana

- pakalpojums pēc pieprasījuma
- nav atkarīgs no atrašanās vietas
- samaksa par izmantotajiem resursiem
- nepazīstami riski
- ērts priekš 'BYOD'

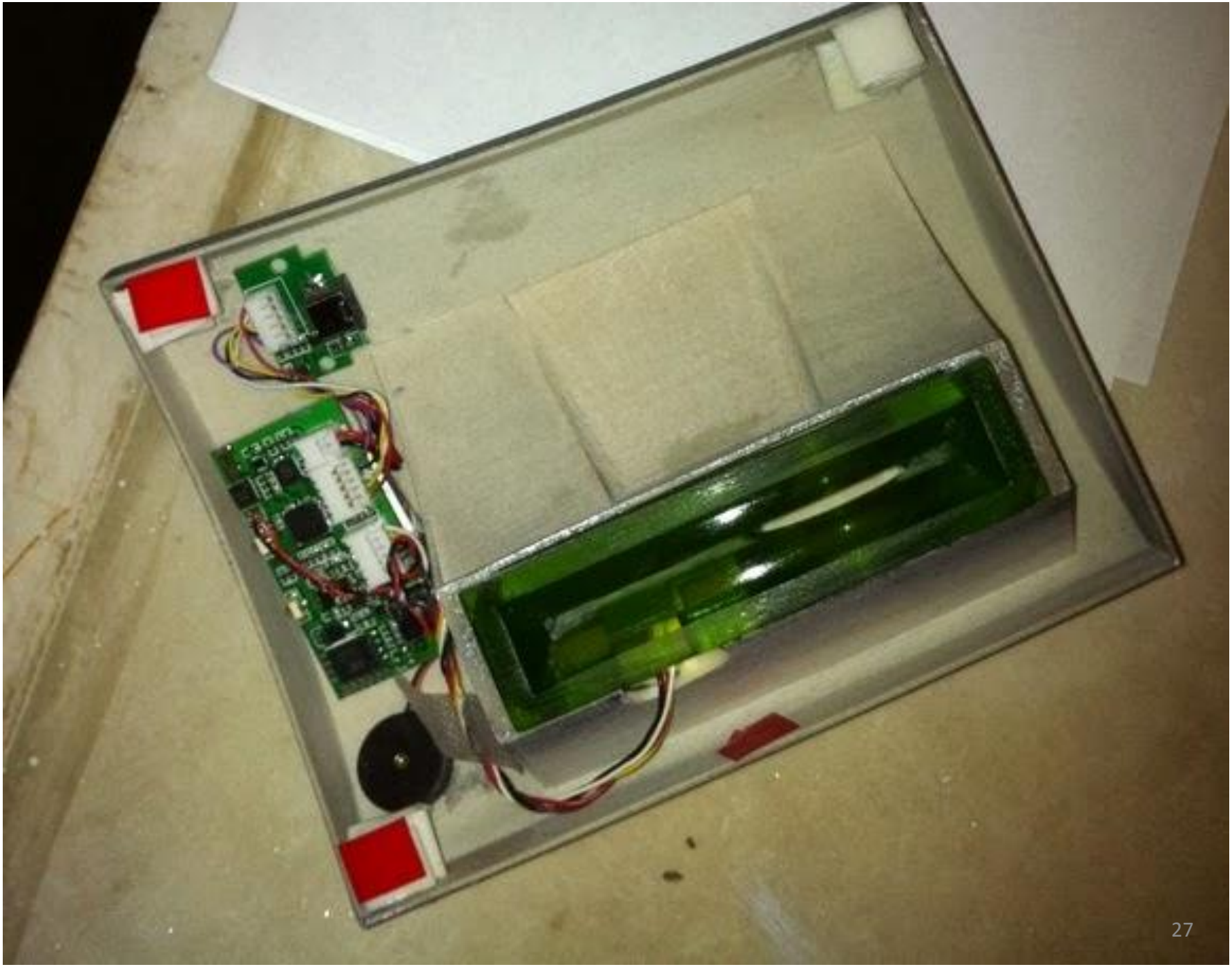




Bankomātu skimmeri


BDN


QZ 1
ABC 2
DEF 3
ENTER
GHI 4
JKL 5
MNO 6
CLEAR
PRS 7
TUV 8
WXY 9
CANCEL
0




guidance
ENTER
CLEAR
CANCEL
AMERICA
NOW


MAIN MY PAGE MEMBERS PHOTOS FORUM BLOGS
BLOG POSTS
PAYMENT AND SHIPPING
Shipping And Payment Information
We Ship Via TNT, UPS, DHL or EMS (given tracking)
We ship worldwide using your choice of preferred currier.All items that are currently in stock will be shipped out on the first available day after you have made a order,and custom made items will be shipped no longer than 5 working days from when payment has... Continue
Posted by Skim ltd on March 17, 2010 at 6:06am
SPECIFICATIONS AND SKIMMING TYPE
... Continue
Posted by Skim ltd on March 17, 2010 at 6:01am
WORK WITH US
SKIM WITH OUR EQUIPMENT FOR 50%
PHOTOS
skimnetwork@hushmail.com
skimnetwork@hushmail.com
7/9
+ Add Photos
View All
Welcome to atmbrakers
Sign Up
or Sign In
ABOUT
Skim ltd created this Ning Network.
Create a Ning Network! »
BADGE
I'm a member of:
atmbrakers
For custom made skimmers built to fit all atm models do get in contact with our...
Get Badge

Kā ziņot par drošības incidentu?

Ja jums ir radušās aizdomas par ielaušanos savā datorā, nedzēsiet ārā nekādu informāciju, atvienojiet datoru no tīkla un sazinieties ar CERT.LV! CERT.LV speciālisti palīdzēs jums saglabāt vajadzīgos pierādījumus un atrast drošības nepilnības, kuru dēļ ielaušanās vai datu zādzība varēja notikt.

Lai sazinātos ar CERT.LV, jūs varat izmantot: e-pastu cert@cert.lv

abuse@cert.lv, abuse@cert.gov.lv - lai ziņotu par mēstuļu (*spam*) gadījumiem

telefonu: +371 67085858 (ziņojumu pieņemšana - 24x7, CERT.LV darba laiks - darba dienās no 9:00 līdz 18:00)
faksu: +371 67225072
pastu: CERT.LV, Raiņa bulvāris 29, Rīga, LV-1459, Latvija

Valsts un pašvaldību institūcijām

Informāciju par atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā , lūdzam sūtīt uz e-pastu: kontakti@cert.lv vai pa pastu:

Baiba Kaškina
CERT.LV
Raiņa bulvāris 29
Rīga, LV-1459
Latvija