



**Cloud**  
Study

# Kāpēc "lāpīt" lietotāju?

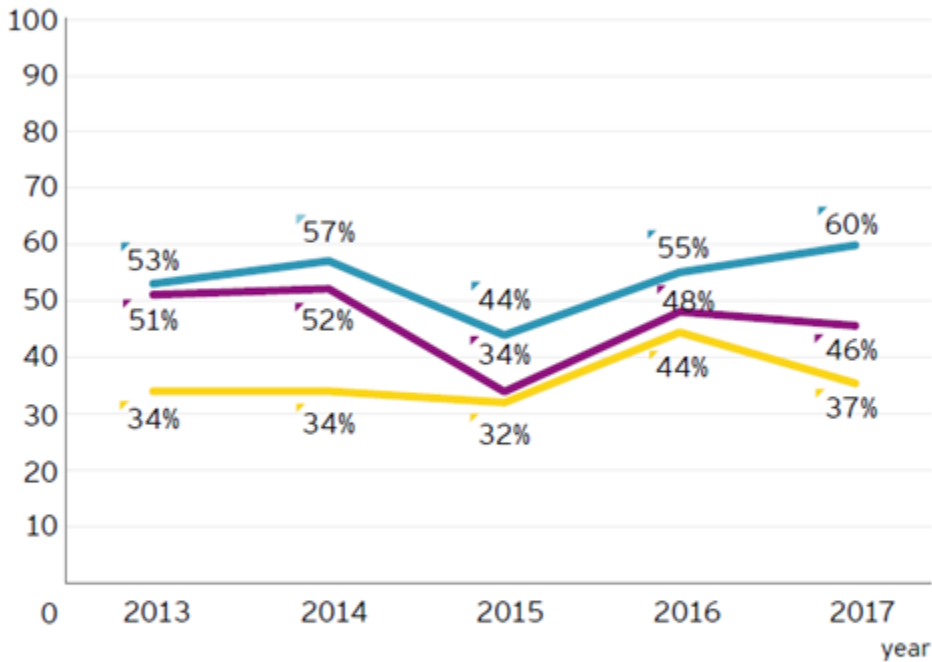
Juris Šmits | 12.Dec.2017



# Kāpēc tieši lietotāju? (2)

## Vulnerabilities

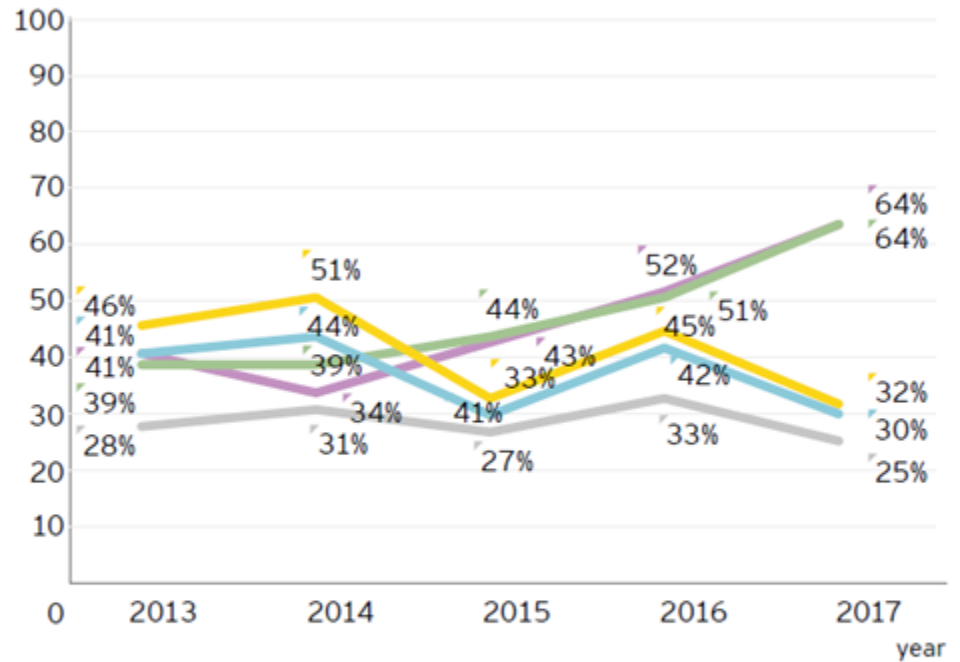
% of respondents stating as top two items to increase risk exposure



- Careless or unaware employees
- Outdated information security controls or architecture
- Unauthorized access

## Threats

% of respondents stating as top two items to increase risk exposure





- Malware
- Phishing
- Cyber attacks to steal financial information
- Cyber attacks to steal IP or data
- Internal attacks

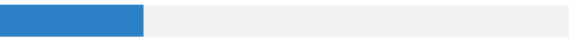
# Kas, kā un kāpēc mums uzbrūk?



## Who's behind the breaches?


**75%**   
perpetrated by outsiders.


**51%**   
involved organized criminal groups.


**25%**   
involved internal actors.



## What tactics do they use?


**62%**   
of breaches featured hacking.


**51%**   
over half of breaches included malware.

**81%**   
of hacking-related breaches leveraged either stolen and/or weak passwords.



## What else is common?

**66%**   
of malware was installed via malicious email attachments.

**73%**   
of breaches were financially motivated.

# Ko dara valsts iestādes Latvijā?



- Neko
- Instruktaža darbiniekam stājoties darbā
- CERT.LV u.c. organizētās apmācības
- Klātienes apmācības
- E-apmācības

# Apmācību saturs

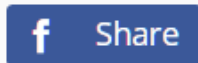
- **Paroļu drošība**
- **E-pasta drošība**
- **Darbstaciju drošība**
- Sociālie tīkli
- Mobilās iekārtas
- Sociālā inženierija
- Wi-Fi lietošana
- Fiziskā drošība
- Fizisko personu datu drošība
- Datu aizsardzība un iznīcināšana




# Par parolēm...

## Skolnieks uzgājis skolotājas parolu datus un «e-klasē» mainījis savas un klasesbiedru atzīmes

Ieteikt:



29. septembris, 2016, 20:25 | [Latvijā](#) | 

[3 komentāri](#) 

**Kāds vidusskolas skolnieks labojis savas un klasesbiedru atzīmes portālā "e-klase", izmantojot internetā atrastus skolotājas paroles datus, teikts informācijas tehnoloģiju drošības incidentu novēršanas institūcijas "Cert.lv" pārskatā par nedēļas drošības incidentiem.**

Parole tikusi iegūta no "LinkedIn" kompromitēto parolu datiem, kas ir brīvi pieejami internetā.

# Kādai tai jābūt? (1)

- **Minimums 8 simboli**
- **Lielie un mazie burti**
- **Cipari**
- **Speciālie simboli**
- **Nesatur lietvārdus, dzimšanas datus u.c. viegli paredzamus skaitļus**
- **Unikālai katrā vietnē**

Jaunā parole: 8^RLa:4YL+DM





# Kādai tai jābūt? (2)

Jaunā parole: 8^RLa:4YL+DM

## BitFBRud\_5Dra

**Bit**īt, tavu darbu meitu  
**Rud**ajām actiņām;  
**Dra**veniek's kaitināja,  
Ozolē sēdēdams.

BitFBRud\_5Dra

BitTWRud\_5Dra

FB un TW – servisa (vietnes identifikators)

5 – mēneša numurs, kad mainīta parole

# Secinājumi

- **Iemācam lietotājam sistēmu**
- Paroļu glabātavas
- **Neuzstājam** uz paroles maiņu reizi mēnesī!
- Paroļu hešsummu pārbaude

# Par e-pasta un datora drošību... (1)

## Petya ransomware: Cyberattack costs could hit \$300m for shipping giant Maersk

June's cyberattack will cost the international shipping firm hundreds of millions of dollars in lost revenue.

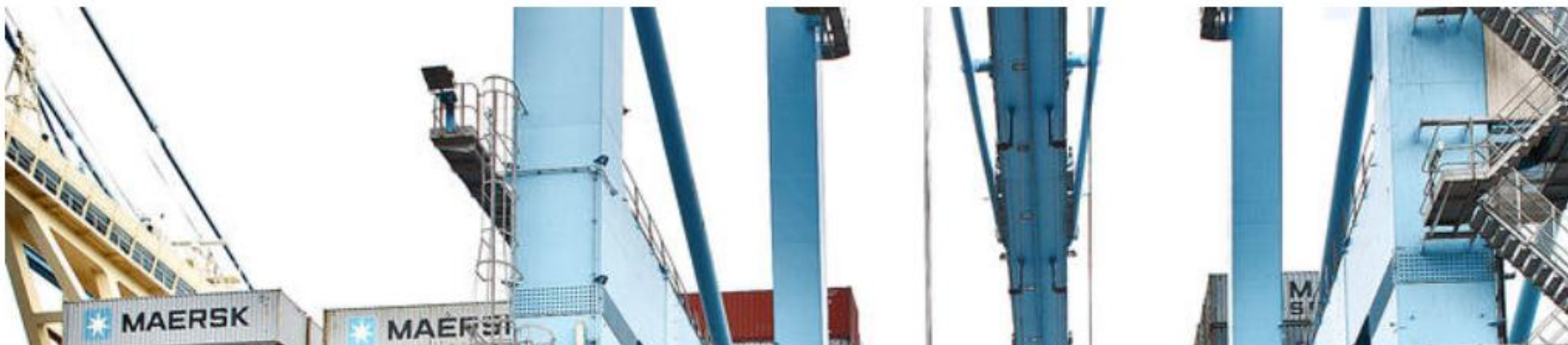


By [Danny Palmer](#) | August 16, 2017 -- 11:28 GMT (12:28 BST) | Topic: [Security](#)

0

f 57

in 437



# Par e-pasta un datora drošību ... (2)

Oops, your important files are encrypted.

---

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbbWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

74f296-2Nx1GM-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.

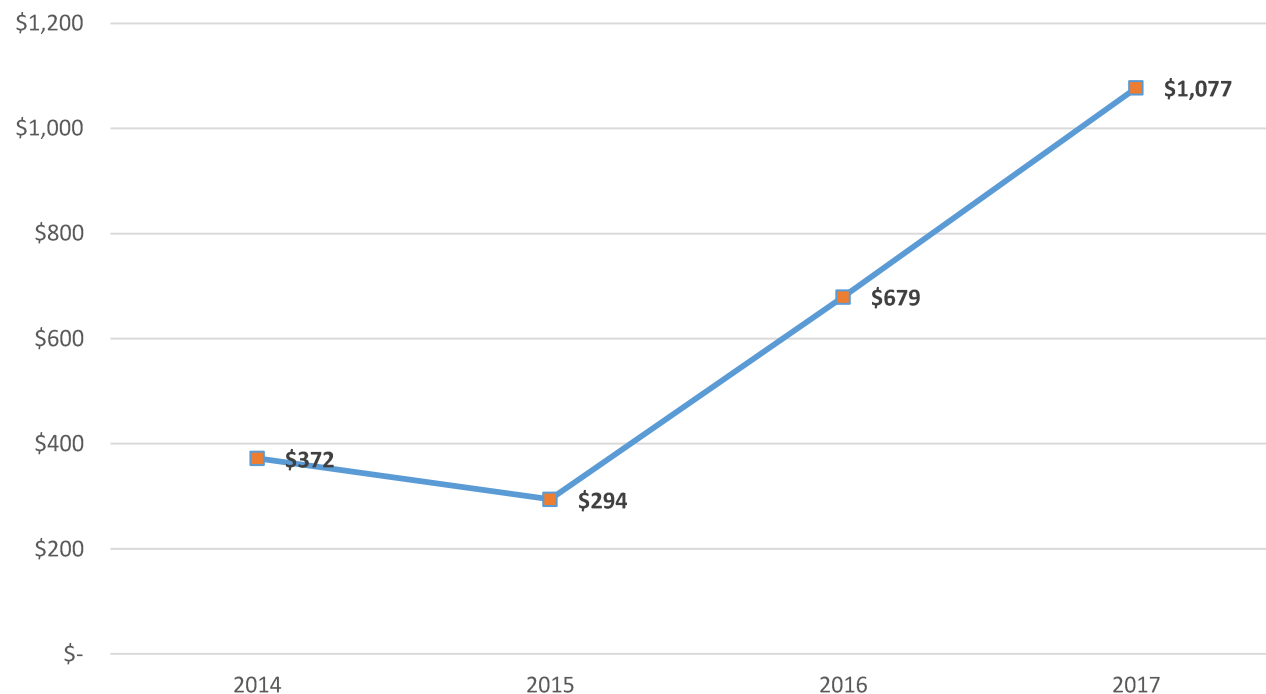
Key: \_

# Par e-pasta un datora drošību ... (3)

- **Ransomware** – ļaunatūra, kas sašifrē Jūsu informāciju un pieprasa izpirkuma maksu.

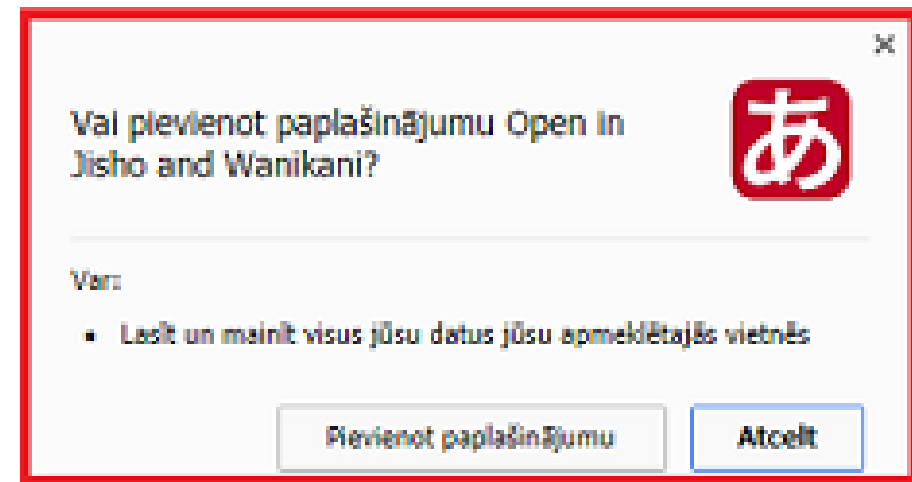
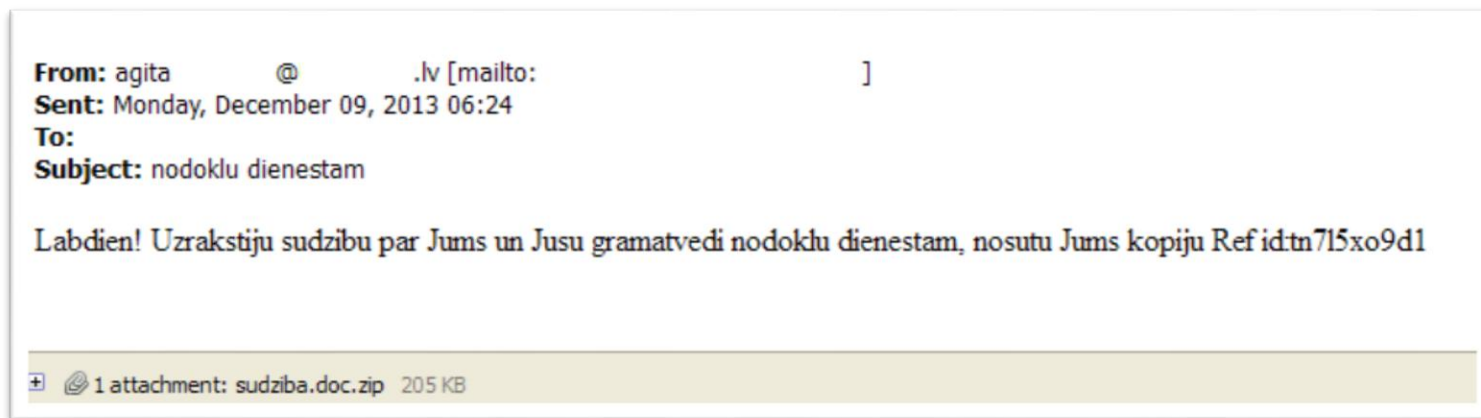


Atlīdzības izmērs (USD) pa gadiem



# Par e-pasta un datora drošību ... (4)

- **Phishing** – mēģinājums izgūt informāciju vai panākt konkrētu darbību izliekoties par uzticamu vietni/resursu





# Ko varam darīt?

---

- Rezerves kopijas
- Kritiskā domāšana
- Lasām -> saprotam -> darām
- Antivīruss
- OS un lietojumu atjauninājumi
- CERT.LV, EsiDross.lv

# Galvenie izaicinājumi

- **Regularitāte** (1x gadā ir parāk reti)
- Kompetence
- Laiks
- Cilvēku organizēšana
- Zināšanu pārbaude?





# CloudStudy IT drošības apmācības

**Cloud Study**

Lietotājvārds Parole **AUTENTIFICĒTIES** LV RU EN

Aizmirstu paroli

## Cloud Study

Interaktīva platforma e-apmācībām tiešsaistē

**PIETEIKTIES**

**Par Cloud Study**  
Informācija par Cloud Study apmācību platformu

**UZZINĀT VAIRĀK**

**Palīdzība**  
Lietošanas instrukcija, kontaktinformācija saziņai

Kā lietot?  
info@cloudstudy.eu  
+371 67847762

Izstrādāts Corporate Consulting

# Kontakti



**Cloud**  
Study

**[www.cloudstudy.eu](http://www.cloudstudy.eu)**

**Juris Šmits**

IT drošības un veiktspējas grupas vadītājs  
Corporate Solutions grupa

Tel.: +371 67 847 762

[juris.smits@csolutions.lv](mailto:juris.smits@csolutions.lv)

[info@cloudstudy.eu](mailto:info@cloudstudy.eu)

*Tehnoloģiju un biznesa konsultācijas*

