

Datu drošība un cilvēciskais faktors, izmantojot mobilās iekārtas bezvadu tīklos

Didzis Balodis, CISSP, GPEN
DPA IT drošības virziena vadītājs

2013.gada 23.oktobris



Saturs

- Fakti un skaitļi
- Prakse
- Risinājumi

Didzis Balodis

DPA IT drošības virziena vadītājs

- Vairāk kā 10 gadi IT industrijā (sākot no 1999.g)
- Administrēšana, izstrāde, drošība
- Pēdējie 5 gadi – IT konsultācijas, audits un drošības audits, ielaušanās testi (veikti vairāk kā 50 auditi)
- Hobijs - bezvadu tīklu drošība

Sertifikāti:

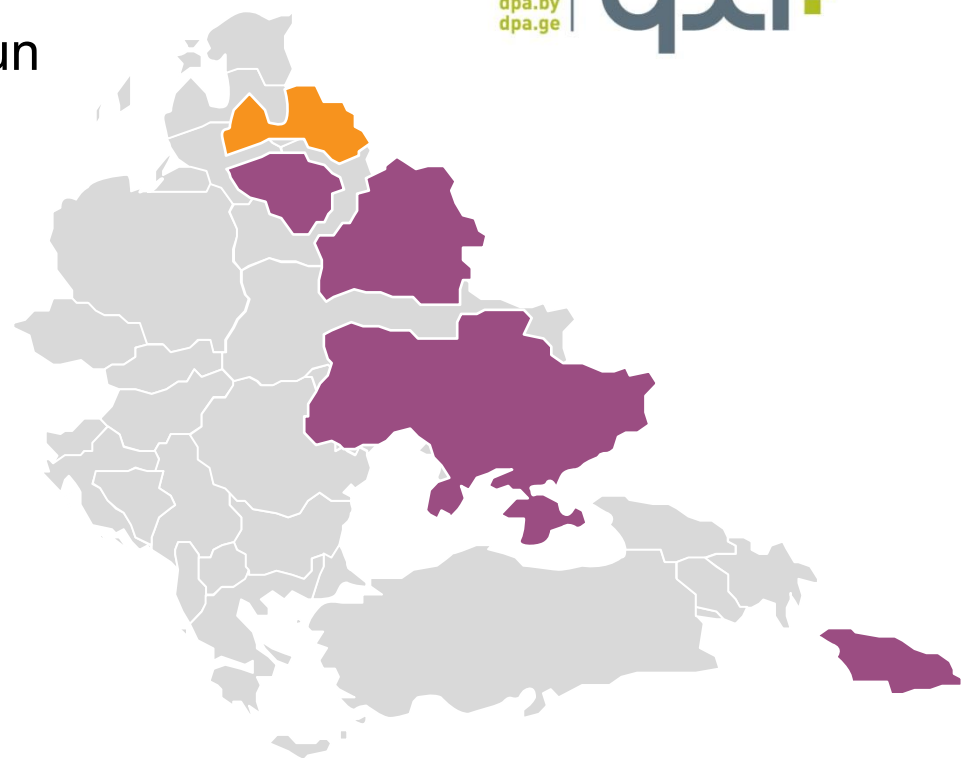
- CISSP- Certified Information System Security Professional
- GPEN – GIAC Certified Penetration Tester

DPA drošības pakalpojumi

IT auditi un ielaušanās testēšana:

- Atbilstības auditi LR normatīviem un labākās prakses standartiem
- Tīkla ielaušanās testi
- Bezvadu tīklu auditi
- Web aplikāciju drošības testēšana
- Sociālās inženierijas testēšana
- Darbinieku IT drošības apmācība

dpa.lv
dpa.lt
dpa.ua
dpa.by
dpa.ge



Sertifikāti



96%

viegli

uzbrukumi

79%

gadījuma
raksturs

85%

netika laicīgi
atklāti

Lietotājs – vājākais ķēdes posms IT drošībā

Phishing

Malware



Avots: www.stockvault.net

Soc.
engineering

Mobile threats

Riski bezvadu tīklos

Lietotājiem:

Datu pārķeršana/
noklausīšanās

Viltus piekļuves
punkts
(Rogue AP)

Uzbrukumi ierīcēm

Īpašniekiem:

Vāja vai noklusētā
parole/ paroles nav

WEP šifrēšana

Uzbrukumi ierīcēm,
pēc tam, kad iegūta
pieeja tīklam

DPA pētījums (1)

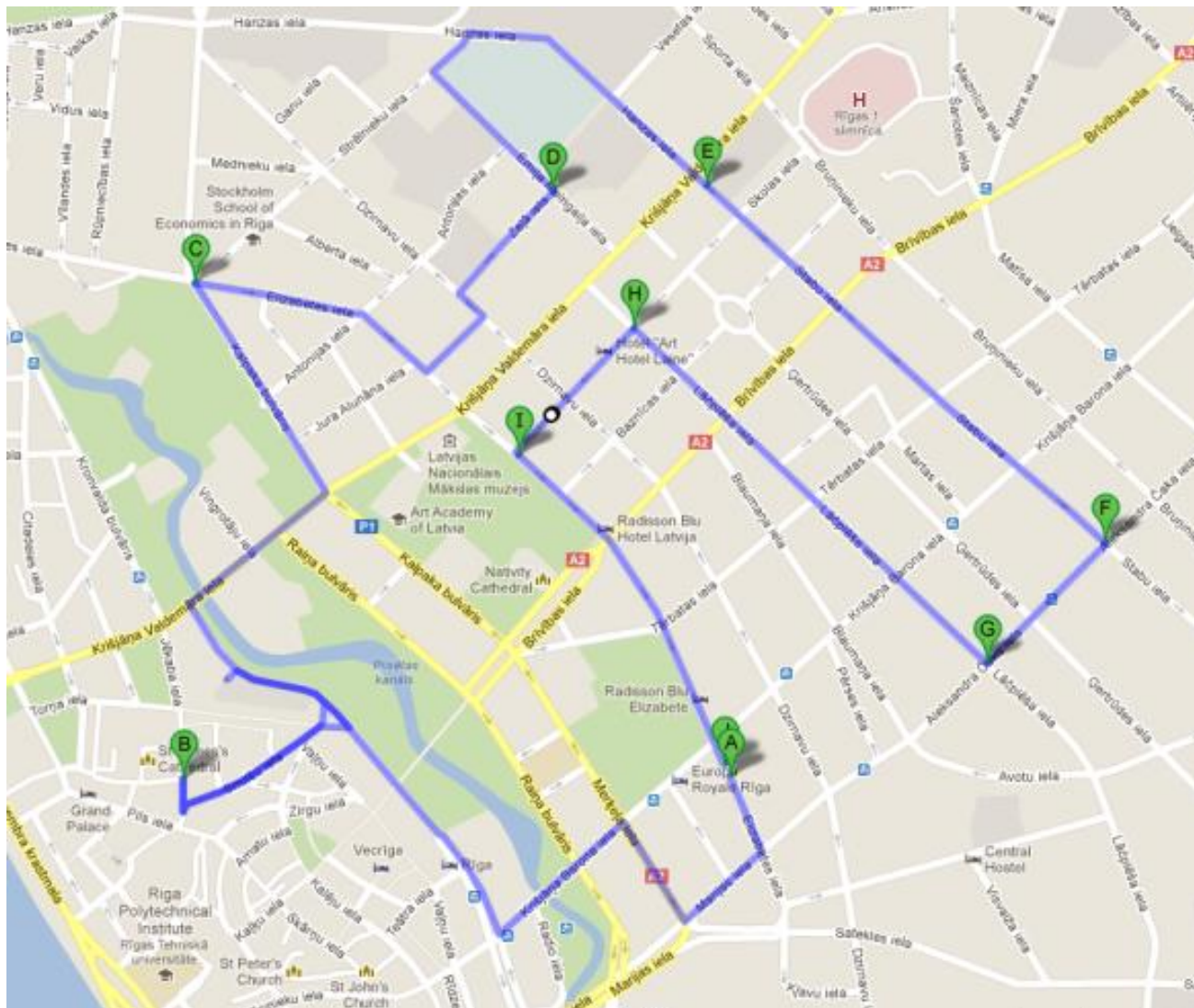
Uzdevums:

Apzināt wi-fi tīklu specifiku Rīgas centrā un mikrorajonā:

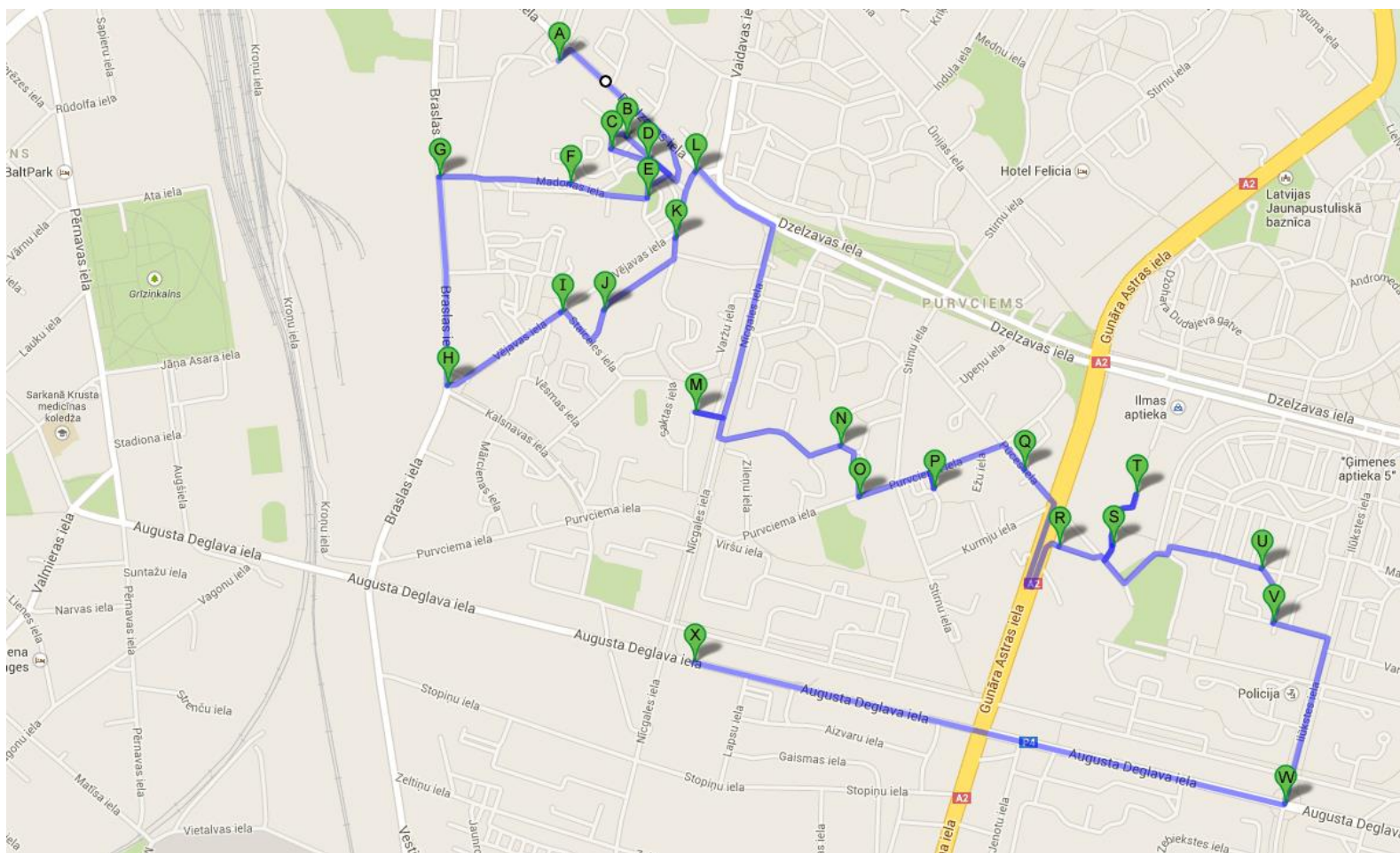
- Šifrēšanas veids
- Atvērtie tīkli
- Nosaukumi (SSID)



DPA pētījums (2)

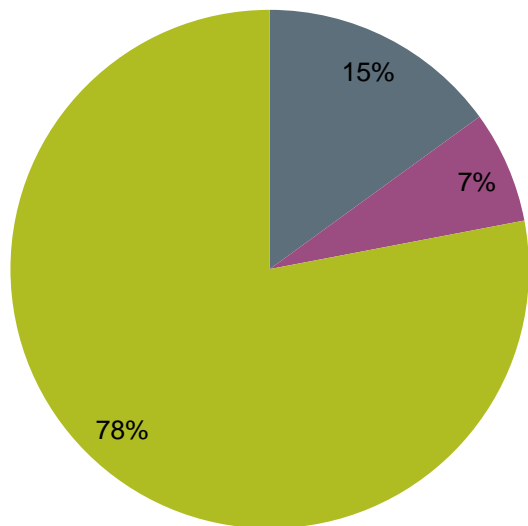


DPA pētījums (3)

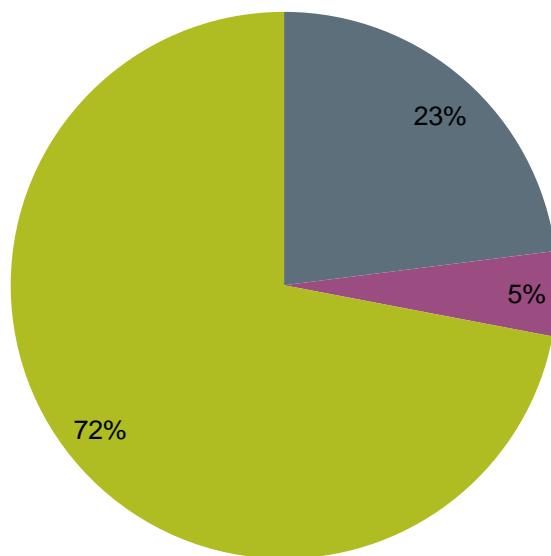


DPA pētījums (4)

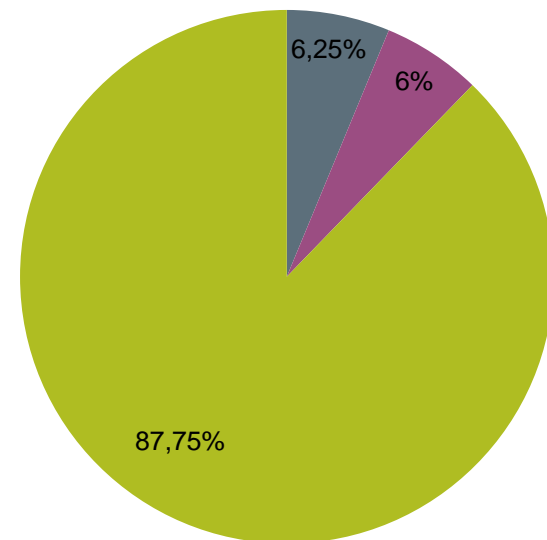
2012 centrs



2013 centrs



2013 Purvciems



■ Nešifrēti ■ WEP ■ WPA

Atvērtie tīkli (1)



Atvērtie tīkli (2)



Atvērtie tīkli (3)



Atvērtie tīkli (4)

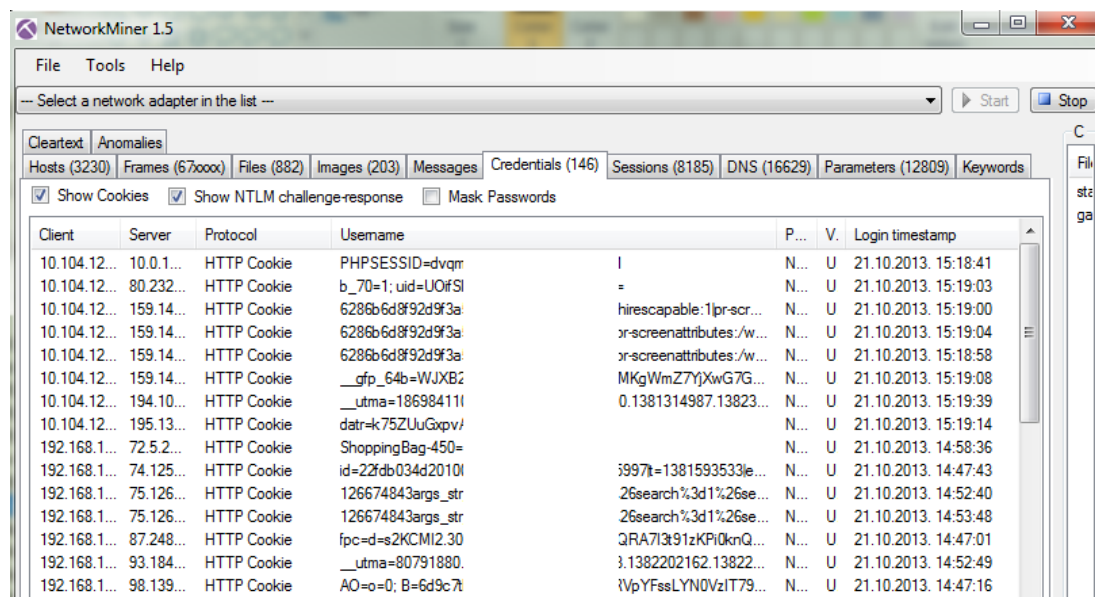


Atvērtie tīkli (5)



1. Scenārijs. Stunda atvērtajā tīklā

- 100 MB trafika
- 203 attēli
- Vairāk kā 3000 IP adreses
- Vairāk kā 100 session ID



The screenshot shows the NetworkMiner 1.5 application window. The interface includes a menu bar (File, Tools, Help), a network adapter selection dropdown, and a toolbar with 'Start' and 'Stop' buttons. Below the toolbar, there are tabs for different data types: Cleartext, Anomalies, Hosts (3230), Frames (67000), Files (882), Images (203), Messages, Credentials (146), Sessions (8185), DNS (16629), Parameters (12809), and Keywords. The 'Credentials' tab is active, displaying a table of network traffic data. The table has columns for Client, Server, Protocol, Username, P..., V., and Login timestamp. The data rows show various HTTP Cookie entries from different clients to servers, including session IDs and other identifiers.

Client	Server	Protocol	Username	P...	V.	Login timestamp
10.104.12...	10.0.1...	HTTP Cookie	PHPSESSID=dvqnr	I	N...	U 21.10.2013. 15:18:41
10.104.12...	80.232...	HTTP Cookie	b_70=1; uid=UOfSI	=	N...	U 21.10.2013. 15:19:03
10.104.12...	159.14...	HTTP Cookie	6286b6d8f92d9f3a	hirescapable:1jpr-scr...	N...	U 21.10.2013. 15:19:00
10.104.12...	159.14...	HTTP Cookie	6286b6d8f92d9f3a	r-screenattributes:/w...	N...	U 21.10.2013. 15:19:04
10.104.12...	159.14...	HTTP Cookie	6286b6d8f92d9f3a	r-screenattributes:/w...	N...	U 21.10.2013. 15:18:58
10.104.12...	159.14...	HTTP Cookie	__gfp_64b=WJXB2	MKgWmZ7YjXwG7G...	N...	U 21.10.2013. 15:19:08
10.104.12...	194.10...	HTTP Cookie	__utma=186984111	0.1381314987.13823...	N...	U 21.10.2013. 15:19:39
10.104.12...	195.13...	HTTP Cookie	datr=k75ZUuGxpv/		N...	U 21.10.2013. 15:19:14
192.168.1...	72.5.2...	HTTP Cookie	ShoppingBag-450=		N...	U 21.10.2013. 14:58:36
192.168.1...	74.125...	HTTP Cookie	id=22fdb034d2010f	;997t=1381593533le...	N...	U 21.10.2013. 14:47:43
192.168.1...	75.126...	HTTP Cookie	126674843args_str	26search%3d1%26se...	N...	U 21.10.2013. 14:52:40
192.168.1...	75.126...	HTTP Cookie	126674843args_str	26search%3d1%26se...	N...	U 21.10.2013. 14:53:48
192.168.1...	87.248...	HTTP Cookie	fpc=d=s2KCM12.30	QRA7l3t91zKPI0knQ...	N...	U 21.10.2013. 14:47:01
192.168.1...	93.184...	HTTP Cookie	__utma=80791880.	.1382202162.13822...	N...	U 21.10.2013. 14:52:49
192.168.1...	98.139...	HTTP Cookie	AO=o=0; B=6d9c7t	YFssLYNOVzIT79...	N...	U 21.10.2013. 14:47:16

2 .Scenārijs. Viltus AP (1)

Mobilā ierīce ar wi-fi ->

Viltus AP (airbase-ng + dnsspoof)->

Datu pārtveršana



2 .Scenārijs. Viltus AP (2)

```
root@kali: ~  
File Edit View Search Terminal Help  
s00f00 nFE0`u000d00^X00$0#  
00(0'00000000&0%0*0)00000000  
=</04  
gk3900000000  
;00000000  
smtp.0 c.lv  
000000  
0000  
[*] SMTP: 192.168.10.101:60307 Command: 0000000000[0000v000GQ0[ tDr00z000N000bZ0  
00(0'00000000&0%0*0)00000000  
=</04  
gk3900000000  
;00000000  
smtp.< c.lv  
000000  
0000  
[*] IMAP LOGIN 192.168.10.123:62575 m00000000 / D00000000  
[*] POP3 LOGIN 192.168.10.123:62586 /  
[*] POP3 LOGIN 192.168.10.167:53556 00000000 inbox.lv / 00000000  
msf auxiliary(smtp) >  
[*] POP3 LOGIN 192.168.10.84:49087 c000000000 / k.lv / u000d00^X00$0#  
[*] IMAP LOGIN 192.168.10.144:37141 / @gmail.com / u000d00^X00$0#  
[*] POP3 LOGIN 192.168.10.252:33273 e- / / u000d00^X00$0#  
[*] POP3 LOGIN 192.168.10.252:58389 e- / / u000d00^X00$0#  
[*] POP3 LOGIN 192.168.10.252:57550 e- / / u000d00^X00$0#  
[*] POP3 LOGIN 192.168.10.252:33045 e- / / u000d00^X00$0#  
[*] POP3 LOGIN 192.168.10.252:57930 e- / /  
[*] IMAP LOGIN 192.168.10.45:50512 user / pass  
msf auxiliary(smtp) >
```

3. Scenārijs

Live probe requests



Kopsavilkums

➤ **Ar Wi- Fi izmantošanu saistītie riski bieži vien līdz galam nav apzināti:**

- Publisko tīklu izmantošana
- Privāto tīklu ierīkošana
- Droša izmantošana uzņēmumos un iestādēs

Būtiska loma ir gala lietotāju izglītošanai kā arī pareizai tehnoloģiju pielietošanai.

Sociālā inženierija

+

Apmācība

+

Sociālā inženierija

Lietotāju mācību programma

- Ikviens ir mērķis
- Sociālā inženierija
- Droša e-pasta lietošana
- Interneta pārlūkošana
- Sociālo tīklu izmantošana
- Mobilo ierīču drošība
- Paroles
- Datu un informācijas aizsardzība
- Bezvadu tīklu droša lietošana
- Darbs no mājām vai ceļā
- Iekšējie draudi
- Fiziskās drošības aspekti
- Datora drošība mājās
- Drošības incidents



Avots: www.stockvault.net

Jautājumi?

