



Mobilo iekārtu drošība

Gints Mālnietis, CERT.LV

Kas ir jāsargā?

- **Iekārtas, kurās ir kaut kas vērtīgs**
- **Iekārtas, ko var izmantot, lai piekļūtu jums vērtīgām lietām**
- **Iekārtas, kas satur informāciju, kas var radīt interesi jūsu konkurentiem**
- **Privātā informācija, ko nevēlamies atklāt**

Iekārtu apdraudējumi

- 1. Iekārtas fiziskā drošība**
- 2. Iekārtas operētājsistēma**
- 3. Ražotāja uzstādītās programmas**
- 4. Lietotāja uzstādītās programmas**
- 5. Bez lietotāja ziņas uzstādītās programmas**
- 6. Datu savienojuma pārtveršana**
- 7. Krāpšana, izmantojot sociālās inženierijas paņēmienus**

Fiziskā drošība

- 1. Neņemiet telefonu līdzi uz vietām, kur to nevarat aizsargāt**
- 2. Izmantojiet, ražotāja piedāvātos bloķēšanas risinājumus, biometriju utt.**
- 3. Šifrējiet tālrunī esošos datus**
- 4. Uzstādiet attālinātas dzēšanas, un iekārtas atrašanas programmas**

Iekārtas operētājsistēma

- 1. Nepērciet tālruņus, ar ļoti novecojušām OS versijām, kuras ražotājs vairs nesola atjaunot!**
- 2. Pārbaudiet, vai tālrunis ir sertificēts**
- 3. Sekojiet līdz OS jauninājumiem un uzstādiet tos**
- 4. Nelauziet OS (“root”, “jailrbreak”)**
- 5. Ja lauziet – nebrīnieties :)**

Ražotāja uzstādītās programmas

- 1. No nedrošiem avotiem iegādāts tālrunis var saturēt kaitīgas programmas jau iepakojumā!**
- 2. ADUPS, dažādas reklāmas programmas**
- 3. Šīs programmas nav iespējams atinstalēt**

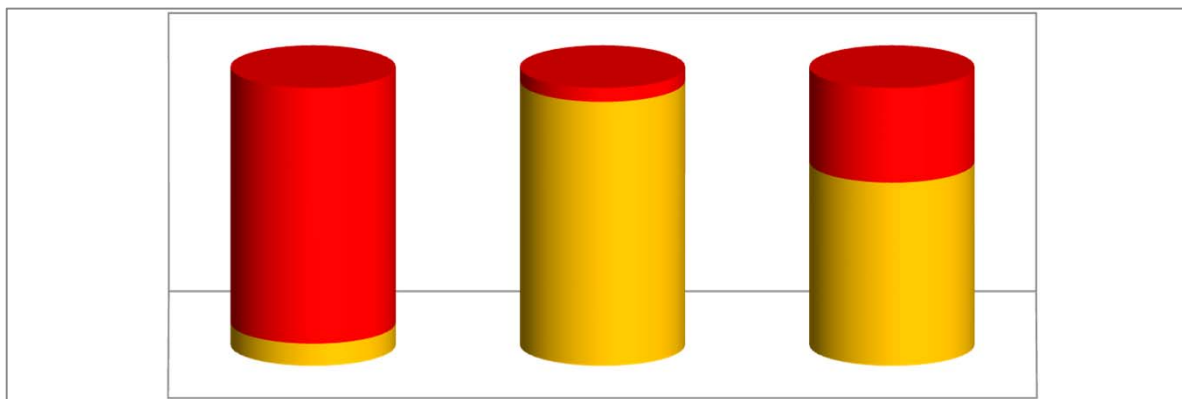
Lietotāja uzstādītās programmas

- 1. Apdraudēti, galvenokārt, ir “uzlauztu” programmu uzstādītāji, no neoficiālām vietnēm**
- 2. Palaikam, tiek kompromitēti pat legālu programmu izstrādātāji, un to ražotās lietotnes satur nevēlamu saturu**
- 3. Vēlams izmantot antivīrusu programmu**

Kas vērtīgs atrodams manā tālrunī?

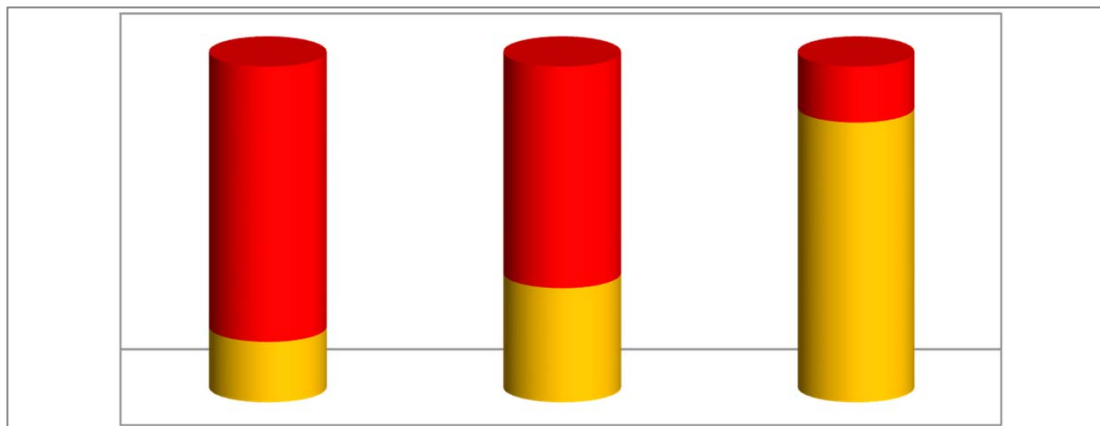
- **Piekļuve jūsu bankas kontam**
- **Aplikācijas, ar saglabātiem kredītkaršu datiem**
- **Bilde ar jūsu pasi**
- **Piekļuve jūsu e-pastam**
- **Darba dokumenti**
- **Personīgās fotogrāfijas un video**

Vai jūs aizsargājat savu tālruni?



- **92%** neizmanto tālruņa datu šifrēšanu
- **5%** «roototu» tālrunu
- **34%** neaizsargā tālruni ar jebkādu paroli
(pēc Duo Labs datiem, 2015)

Darbam paredzētajās iekārtās situācija ir labāka



- **18% izmanto bloķēšanas figūru**
- **34% izmanto PIN kodu**
- **1/6 neizmanto nekādu aizsardzību**
(pēc Samsung Living Business datiem, 2014)

Kāpēc uzbrukumi mobilajos ir vieglāki?

A screenshot of the Google account password change page. At the top left is the Google logo. Below it is a blue header with the word "Password" in white. The main content area has a light gray background. It contains a paragraph of instructions: "Choose a strong password and don't reuse it for other accounts. Learn more." followed by "Changing your password will sign you out of all your devices, including your phone. You will need to enter your new password on all your devices." Below this are three input fields: "Password", "New password", and "Confirm new password". The "New password" field has a small text block below it: "Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?". At the bottom left is a blue button with the text "CHANGE PASSWORD".

Google

Password

Choose a strong password and don't reuse it for other accounts. [Learn more.](#)

Changing your password will sign you out of all your devices, including your phone. You will need to enter your new password on all your devices.

Password

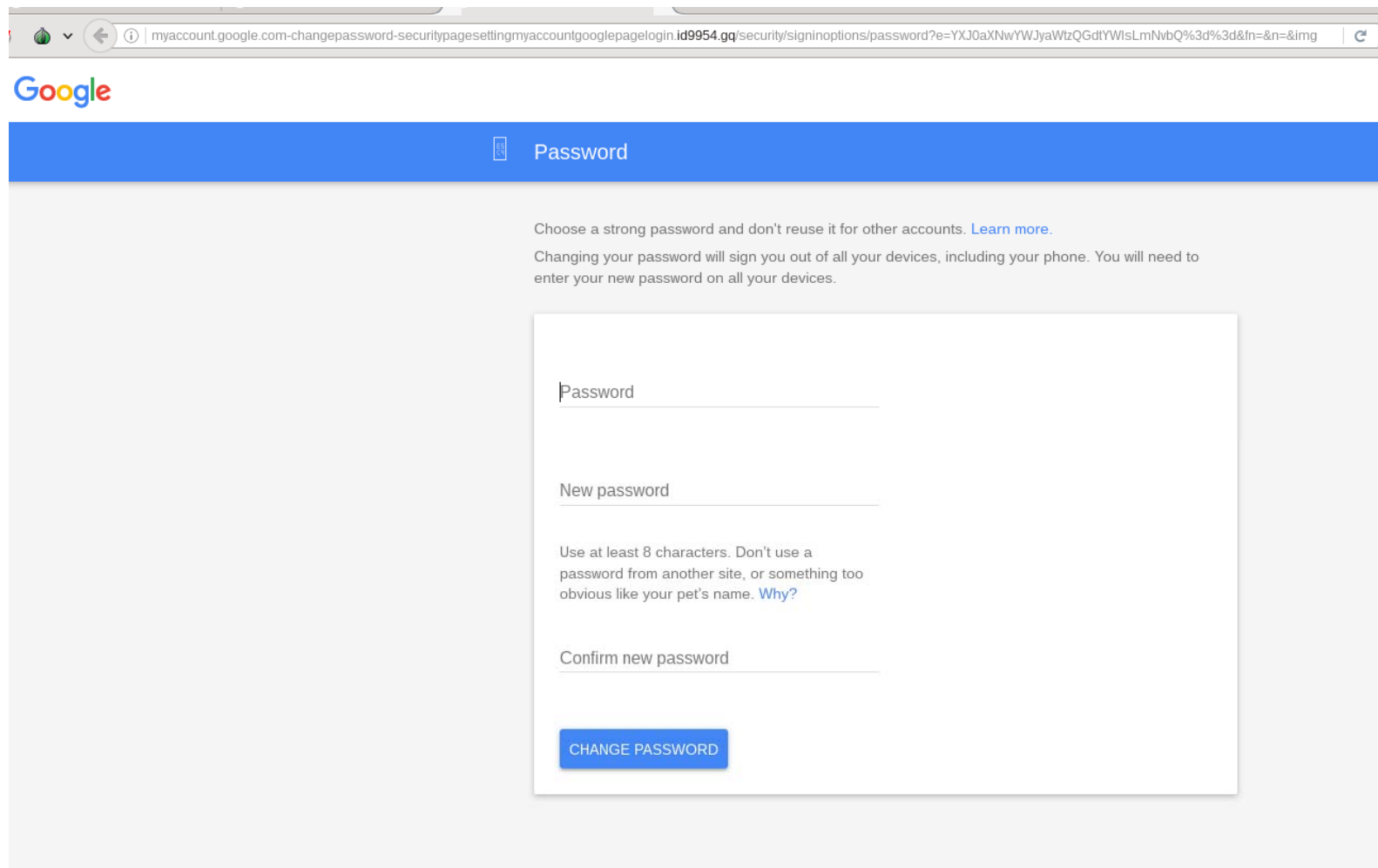
New password

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Confirm new password

CHANGE PASSWORD

Tā pati lapa, parastā pārlūkā



The image shows a browser window displaying the Google account password change page. The address bar shows the URL: `myaccount.google.com-changepassword-securitypagesettingmyaccountgooglepagelogin id9954.gq/security/signinoptions/password?e=YXJ0aXNwYWJyaWtzQGdtYWIsLmNvbQ%3d%3d&fn=&n=&img`. The Google logo is visible in the top left corner. The page title is "Password".

Choose a strong password and don't reuse it for other accounts. [Learn more.](#)

Changing your password will sign you out of all your devices, including your phone. You will need to enter your new password on all your devices.

Password

New password

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Confirm new password

[CHANGE PASSWORD](#)

Ko nesaskata lietotājs?

← → ↻ data:text/html;https://apple.verifications.com/verificationsid=54652101;base64,PCFET0NUWVBFiGh0bWwgUFVCTEIDICtLy9XM0MvL0RURCBIVE1MIDQuMDEgVHJhbnNpdGlvbmFsLy9FTiI+DQo8aHRtdD4N



Apple Store

1-800-MY-APPLE | Account | Cart

Please Sign In

Secure

Enter your Apple ID and password

[Forgot your Apple ID or Password?](#)

Sign In

You can use your Apple ID for other Apple services such as

- iTunes Store
- iPhoto Print Products
- iCloud

[Create Apple ID now](#)

Cancel

Questions? Just ask 1-800-MY-APPLE

My Apple ID

Shop the [Apple Online Store](#), call 0800 048 0408, visit an [Apple Retail Store](#) or find a [retailer](#).

[Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#)

Copyright © 2016 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#) | [Use of Cookies](#)

Ko nesaskata lietotājs?



A screenshot of a browser address bar. The address bar contains the text: data:text/html,https://apple.verification.com/verificationsid=54652101;base64,F. A red vertical line is drawn at the end of the data URI, and a red horizontal line is drawn under the entire address bar content.

Interneta pārlūka adreses laukā esošos datus ir jāmāk pareizi uztvert!

Mobilajos telefonos ekrāna vietas taupīšanas nolūkā adreses laukus bieži nerāda vispār!

My Apple ID

Sign In to iTunes Connect

Please Sign In to you Apple ID to resolve the problem.

Apple ID

Password

Sign In

[Forgot your Apple ID or password?](#)



Give the gift of iTunes.

Music, movies, apps, and more.



(RED)

(PRODUCT)RED

Red is a good color for you.
And millions of others.

Apple source code

```
!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<?php
/*


PRIVATE Apple SCAM



BY Mister Spy Tn


http://www.facebook.com/tazspy
*/
?>

<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<title>iTunes Connect</title>
<link rel="icon" href="http://im53.gulfup.com/Qhffdz.ico">

<style>
.btn {
background: #3baee7;
background-image: -webkit-linear-gradient(top, #3baee7, #08c);
background-image: -moz-linear-gradient(top, #3baee7, #08c);
background-image: -ms-linear-gradient(top, #3baee7, #08c);
background-image: -o-linear-gradient(top, #3baee7, #08c);
background-image: linear-gradient(to bottom, #3baee7, #08c);
-webkit-border-radius: 7;
-moz-border-radius: 7;
border-radius: 7px;
```


Viltus loterijas – maksāt 3 EUR nedēļā par neko

security.mobile82.com/?c=LV&tsc=M

Android Security Center

UZMANĪBU! Tālrunī var būt inficēts!

Android Security Center

Skenēšanas vīrusiem ...

53%

Progress Scan: 2droid.lib.flash378

2 iespējams vīruss

NOŅEMT VISUS VĪRUSUS

Maksa (€3,66) tiks pievienota telefona rēķinam vai atrēķināta no priekšapmaksas kartes. Atbalsts: +34722663819 | support@medianetpay.com Piedāvā fortumo.com

letaupot mājas lapu

security.mobile82.com/?c=LV&tsc=M

Android Security Center

UZMANĪBU! Tālrunī var būt inficēts!

Android Security Center

6 iespējams vīruss

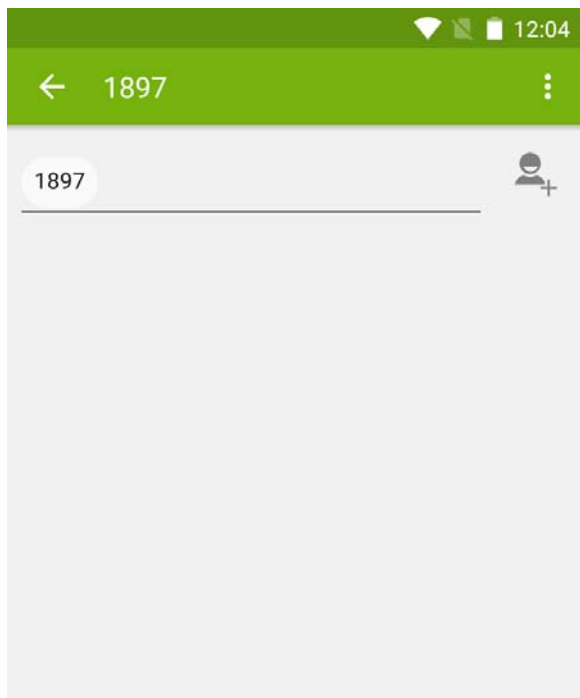
Novērs vīrusu un draudiem, kas lēni pareizu tālruni.

Whatsapp (3) Facebook (1) Mail (2)

NOŅEMT VISUS VĪRUSUS

Maksa (€3,66) tiks pievienota telefona rēķinam vai atrēķināta no priekšapmaksas kartes. Atbalsts: +34722663819 | support@medianetpay.com Piedāvā fortumo.com

Viltus loterijas – maksāt 3 EUR nedēļā par neko



FOR ANTIVIRUS
-2:1486460679mb18873715824:
1-

Apstiprinātu, ka vēlies izdzēst
vīrusu.

22/2



[Noklikšķiniet uz iesniegt.](#)



Viltus loterijas

```
713 <script type="text/javascript">
714     function spinnerAction() {
715         //alert("Welcome to Lucky Wheel!\n\nSpin the Wheel and you may win exclusive prizes!\n\nClick OK to Start the Game!")
716     }
717
718     function startSpin() {
719         var e = document.getElementById("spin"),
720             n = document.getElementById("win"),
721             t = document.getElementById("winP"),
722             o = document.getElementById("win2");
723         e.className = e.className + " spinAround", n.style.display = "none", t.style.display = "block", setTimeout(function() {
724             t.style.display = "none", o.style.display = "block"
725         }, 150), setTimeout(function() {
726             alert(" Apsveicam!\n\n Jūs uzgriezāt Papildus griezienu.\n\n Jums ir iespēja griez laimes ratu velreiz."), spin2enabled = !0
727         }, 6500)
728     }
729
730     function spin2() {
731         if (spin2enabled) {
732             var e = document.getElementById("spin"),
733                 n = document.getElementById("win"),
734                 t = document.getElementById("winP"),
735                 o = document.getElementById("win2");
736             e.className = e.className + " spinAround2", n.style.display = "none", t.style.display = "block", setTimeout(function() {
737                 t.style.display = "none", o.style.display = "block"
738             }, 150), setTimeout(function() {
739                 var e = alert("Apsveicam!\n\n Jūs Uzgriezāt Apple iPhone 7 (Black, 32GB). \n\n ");
740                 e === !0 || $(".hide-all").hide(), $(".show-all").show();
741                 var n = 299,
742                     t = setInterval(function() {
743                         $("#countdown").text(n--), -1 == n && clearInterval(t)
744                     }, 1e3);
745                 javascript_countdown.init(300)
746             }, 6800)
747         }
748     }
749 }
```

Viltus loterijas

← → ↻ faceb00ks.com/laimesrats/ ☆

Latvijas Lielākā Veiksmes Spēle.
Ziemmasvētku balvas!

Apsveicam Tevi!



Apple Iphone 7 (Black, 32GB)

Par pateicību mums, pastāsti par savu veiksmi 10 saviem labākajiem draugiem izmantojot whatsapp

1. Uzspied 10x 'IETEIKT' pogu.
2. Spied 'TURPINĀT'

IETEIKT

TURPINĀT

Rezervācijas ilgums **0** sekundes

Viltus loterijas



← → ↻ ⓘ www.skill2win.net/lv-lv/m-avg/?tc=0&media=QY&cid=SPO9-10211 ☆

 **AVG Antivīrusu aizsardzība**
AVG mobilais

Ievadiet savu mobilā telefona numuru, lai instalētu

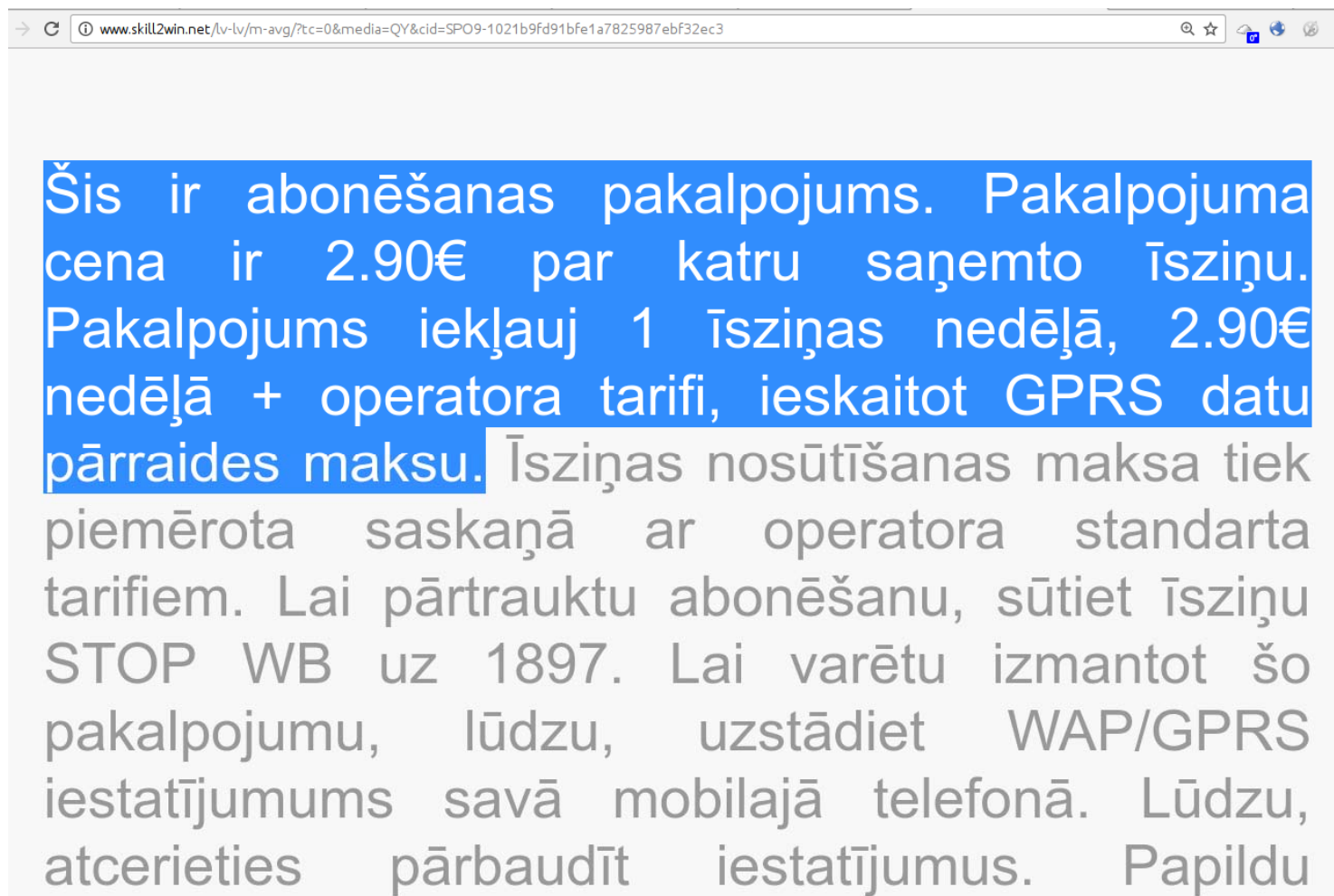
INSTALĒT

Pasaulē labākais antivīruss!

Vērtējums: **4.2** ★ ★ ★ ★ ★ 1 226 750 skatījumi

- Skenē lietotnes, korekcijas, multimedijus reāllaikā
- Ļauj interneta atrast/izsekot nozaudēto/nozagto tālruni ar Google Maps
- Nobloķē/nodzēs savu ierīci, lai aizsargātu savu privātumu
- Izdzēs lietotnes vai uzdevumus, kas palēnina ierīces darbību
- Droši pārlūko internet
- Kontrolē savu akumulatoru, glabāšanas un datu paketi
- Instalē tūlīt, palielini sava mobilā tālruņa drošību un pārsteidz sevi
- AVG AntiVirus - mobilā tālruņa programmatūras aizsardzība Android sistēmai. Ātra un vienkārša aizsardzība tavam tālrunim

Viltus loterijas



Šis ir abonēšanas pakalpojums. Pakalpojuma cena ir 2.90€ par katru saņemto īsziņu. Pakalpojums iekļauj 1 īsziņas nedēļā, 2.90€ nedēļā + operatora tarifi, ieskaitot GPRS datu pārraides maksu. Īsziņas nosūtīšanas maksa tiek piemērota saskaņā ar operatora standarta tarifiem. Lai pārtrauktu abonēšanu, sūtiet īsziņu STOP WB uz 1897. Lai varētu izmantot šo pakalpojumu, lūdzu, uzstādiet WAP/GPRS iestatījumus savā mobilajā telefonā. Lūdzu, atcerieties pārbaudīt iestatījumus. Papildu

Kā drošāk lietot mobilās iekārtas

- **Aizsargāt tālruni ar paroli**
- **Nerakstīt savu paroli viltus lapās**
- **Nesalauzt iekārtu aizsardzību!**
- **Atjaunināt tālruņu operētājsistēmu**
- **Neuzstādīt programmas no nepārbaudītiem aplikāciju veikaliem**
- **Publiskos datu pārraides tīklos ieteicams izmantot tikai ar SSL aizsargātus datu pārraides veidus. Vēl labāk – VPN.**
- **Laicīgi ieslēgt tālruņa attālinātas bloķēšanas iespēju**

Piebilde par viltotiem rēķiniem

- Krāpšanā ar viltus rēķiniem jauns rekords – **1 000 000 EUR no uzņēmuma!**
- Brīdiniet savus kolēģus/paziņas no privātajiem uzņēmumiem
- Finanšu darījumos iesakām izmantot e-doc!
- Jāseko līdz e-pasta serveru konfigurācijai, jāpārbauda tajos uzstādītie filtri un pāradresācijas
- Svarīgākais – aizsargāt lietotāju paroles!
- Datoros regulāri jāveic pilna pārbaude ar AV programmām

Piebilde par viltotiem rēķiniem

- **Iemāciet kolēģiem – ir tāds lauks “Reply To” !!**
- **Ja vēlaties pārbaudīt e-pasta ticamību:**
 - Vai sarakste vēl arvien notiek ar īsto e-pasta adresi (pārbaudām domēnu, lietotāju, reply-to laukus, filtrus serverī)
 - Vai e-pasti tiek nosūtīti, uz tiem MX serveriem, kas norādīti DNS ierakstos
 - Vai datorā izmanto pareizo DNS serveri?
- **Pārbaudām iepriekš veikto saraksti, vai visi rekvizīti sakrīt**
- **Nemainām, maksājuma detaļas, pēc pirmā pieprasījuma!**



Paldies!

cert@cert.lv

<https://www.cert.lv>

 **certlv**

 **certlv**