CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Mobilo iekārtu drošība

Gints Mālkalnietis, 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 līdzi 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**

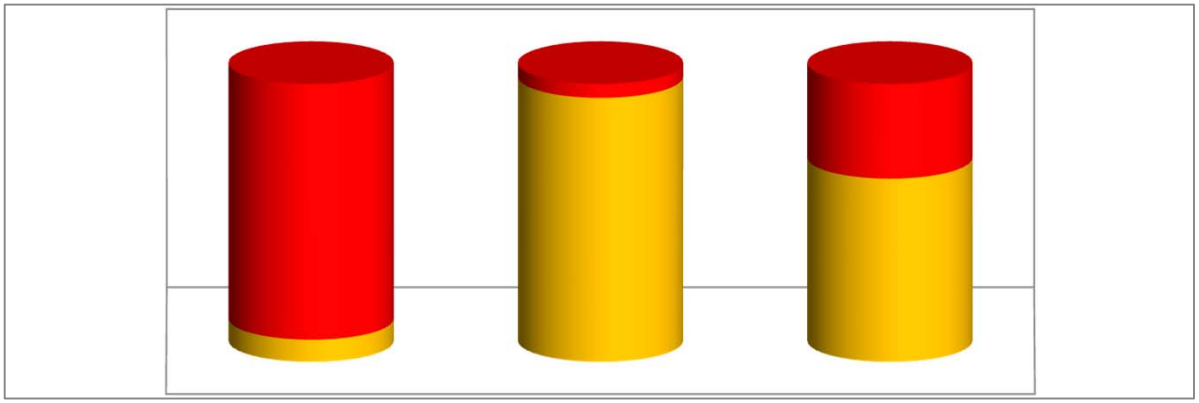
Lietotāja uzstādītās programmas

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**

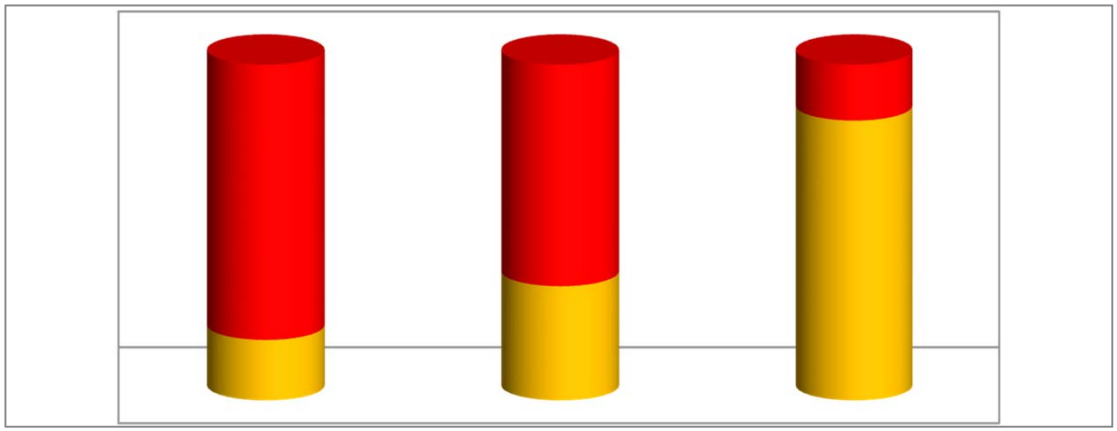
Vai jūs aizsargājat savu tālruni?



- **92% neizmanto tālruņa datu šifrēšanu**
- **5% «roototu» tālruņu**
- **34% neaizsargā tālruni ar jebkādu paroli**

(pēc Duo Labs datiem, 2015)

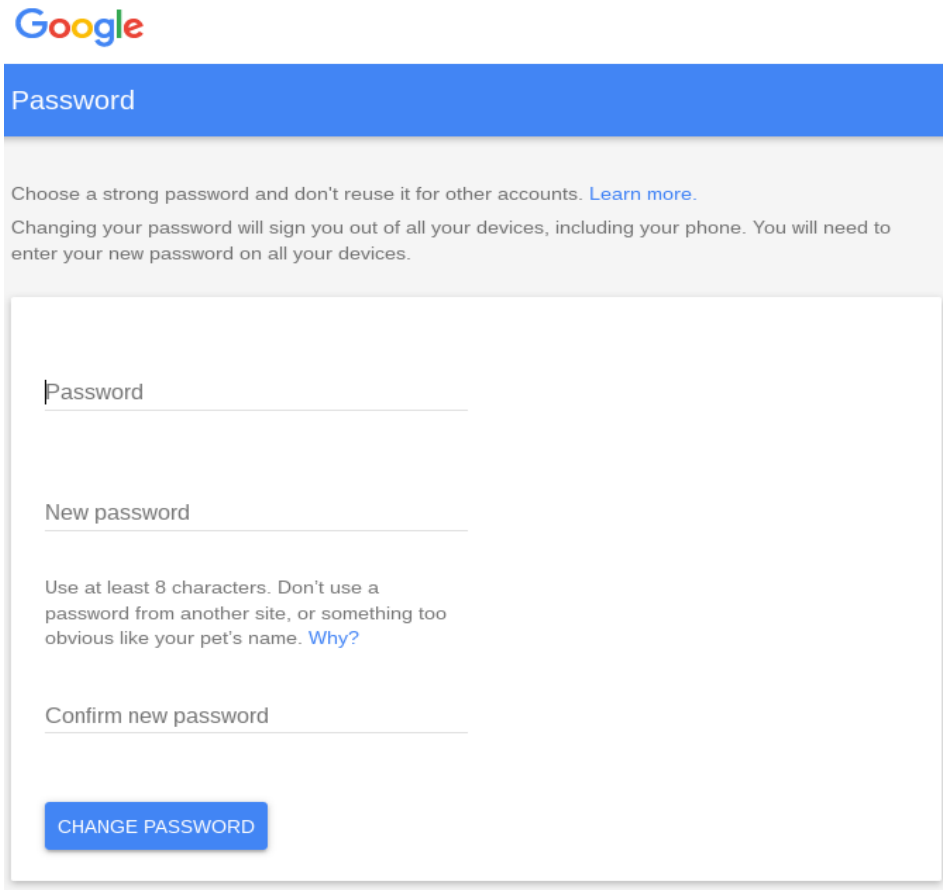
Darbam paredzētajās iekārtās situācija ir labāka



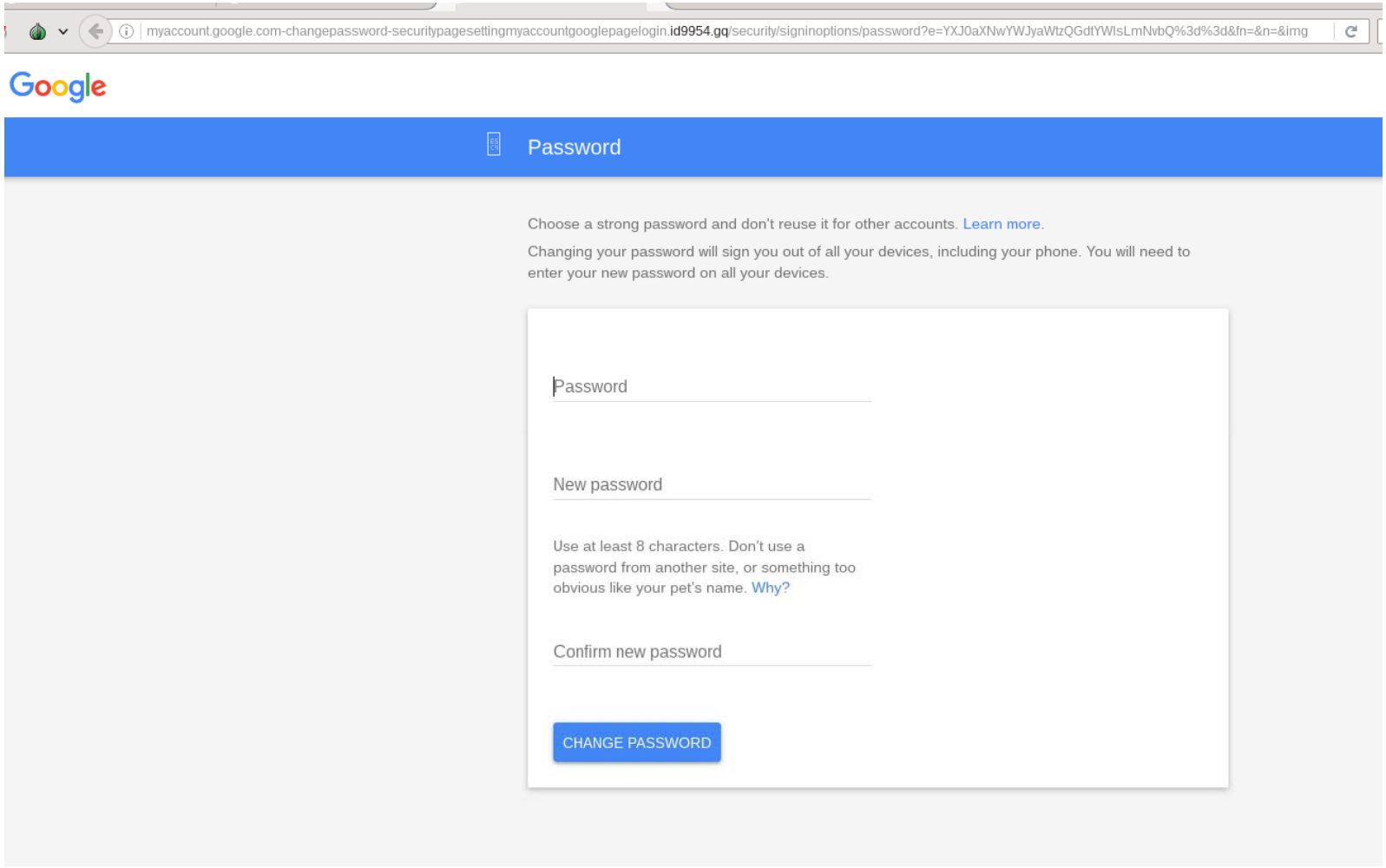
- **18% izmanto bloķēšanas figūru**
- **34% izmanto PIN kodu**
- **1/6 neizmanto nekādu aizsardzību**

(pēc Samsung Living Business datiem, 2014)

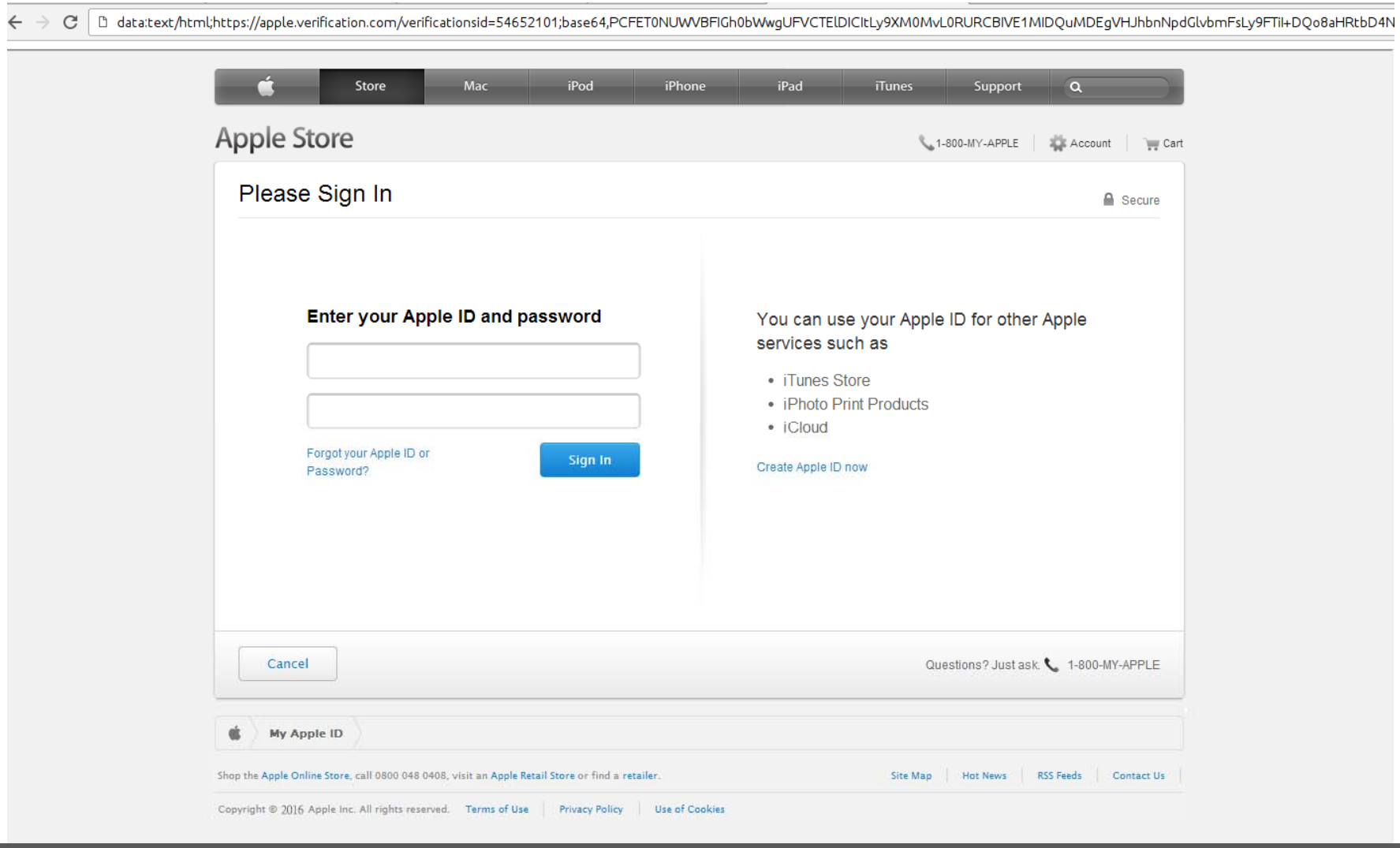
Kāpēc uzbrukumi mobilajos ir vieglāki?



Tā pati lapa, parastā pārlūkā



Ko nesaskata lietotājs?

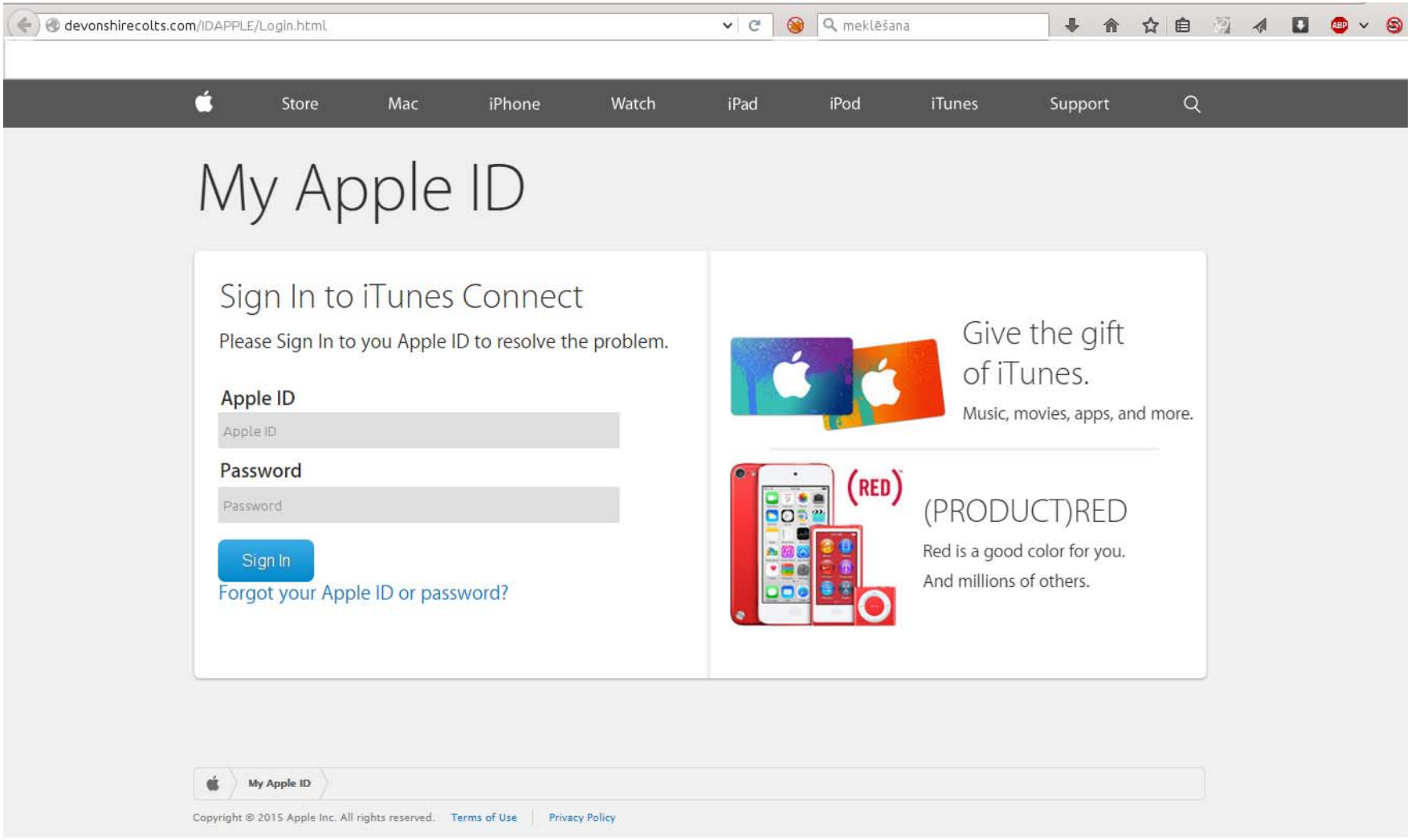


Ko nesaskata lietotājs?

Interneta pārlūka adreses laukā esošos datus ir jāmāk pareizi uztvert!

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

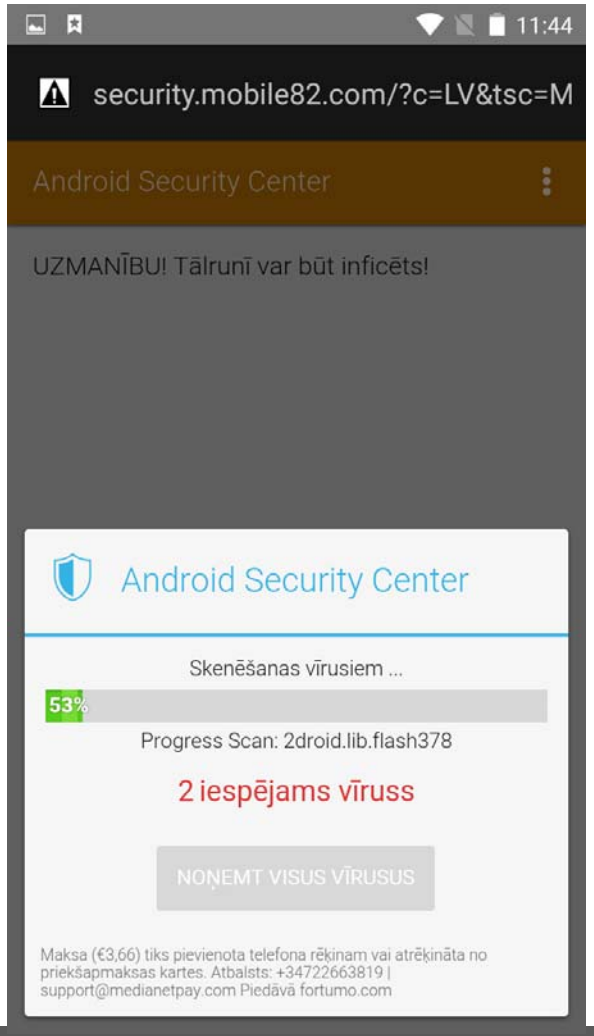
Apple

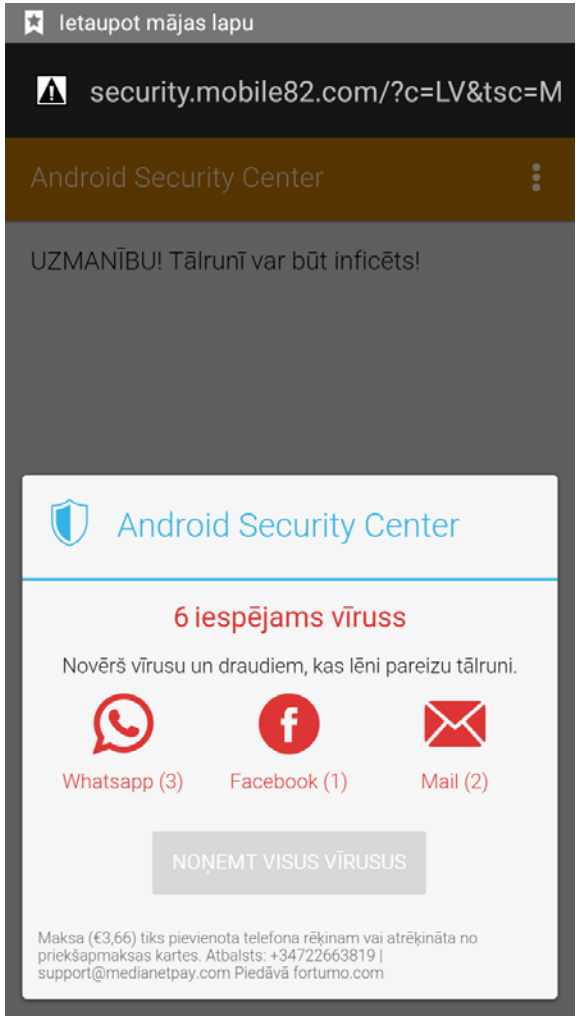

devonshirecolts.com/IDAPPLE/Login.html
meklēšana
Store
Mac
iPhone
Watch
iPad
iPod
iTunes
Support
My Apple ID
Sign In to iTunes Connect
Please Sign In to you Apple ID to resolve the problem.
Apple ID
Apple ID
Password
Password
Sign In
Forgot your Apple ID or password?
Give the gift of iTunes.
Music, movies, apps, and more.
(RED)
(PRODUCT)RED
Red is a good color for you.
And millions of others.
My Apple ID
Copyright © 2015 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

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





Viltus loterijas – maksāt 3 EUR nedēļā par neko

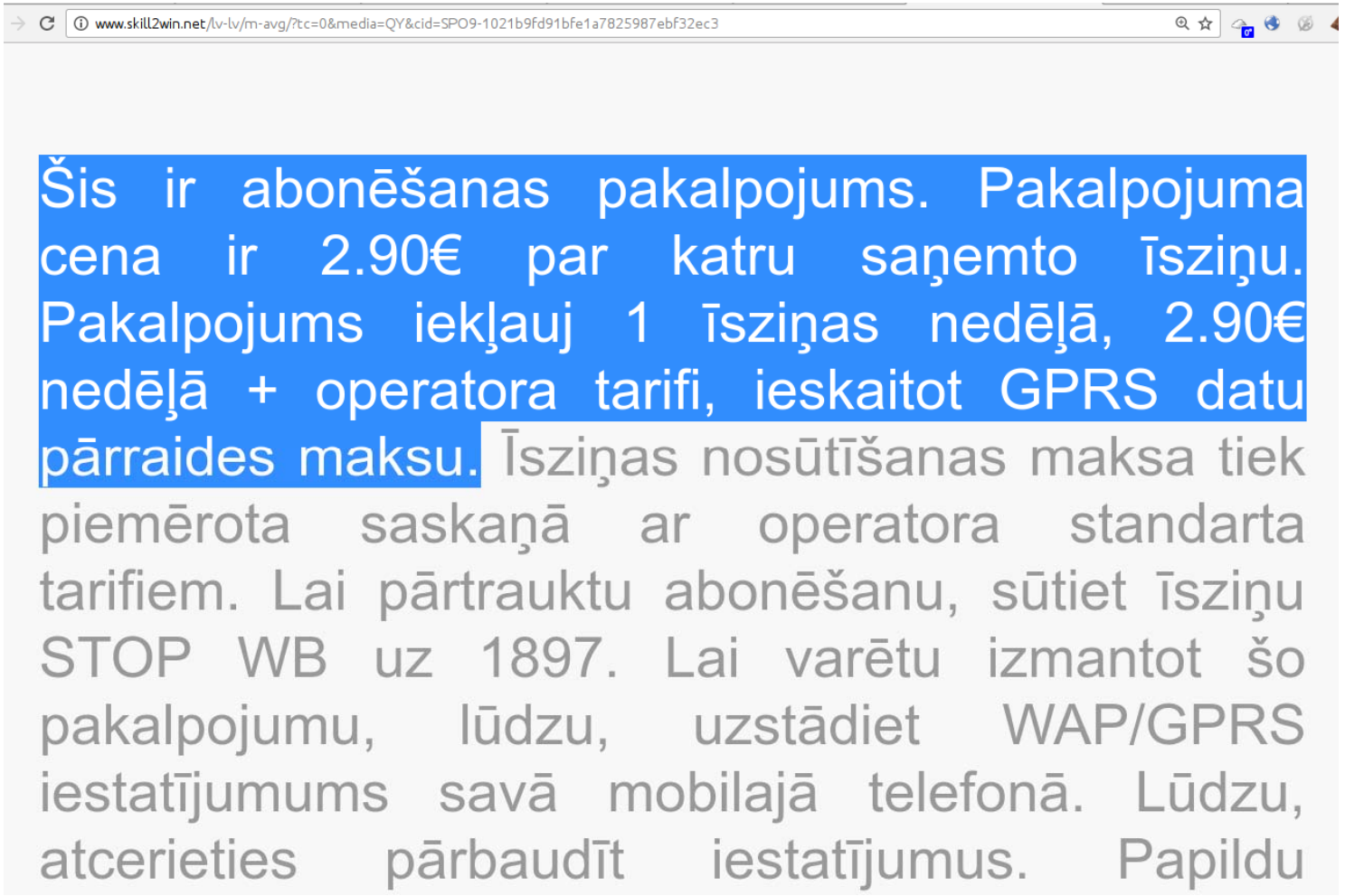
Viltus loterijas

```
<script type="text/javascript">
    function spinnerAction() {
        //alert("Welcome to Lucky Wheel!\n\nSpin the Wheel and you may win exclusive prizes!\n\nClick OK to Start the Game!")
    }

    function startSpin() {
        var e = document.getElementById("spin"),
            n = document.getElementById("win"),
            t = document.getElementById("winP"),
            o = document.getElementById("win2");
        e.className = e.className + "spinAround", n.style.display = "none", t.style.display = "block", setTimeout(function() {
            t.style.display = "none", o.style.display = "block"
        }, 150), setTimeout(function() {
            alert(" Apsveicam!\n\n Jūs uzgriezāt Papildus griezienu.\n\n Jums ir iespēja griez laimes ratu velreiz."), spin2enabled = !0
        }, 6500)
    }

    function spin2() {
        if (spin2enabled) {
            var e = document.getElementById("spin"),
                n = document.getElementById("win"),
                t = document.getElementById("winP"),
                o = document.getElementById("win2");
            e.className = e.className + " spinAround2", n.style.display = "none", t.style.display = "block", setTimeout(function() {
                t.style.display = "none", o.style.display = "block"
            }, 150), setTimeout(function() {
                var e = alert("Apsveicam!\n\n Jūs Uzgriezāt Apple IPhone 7 (Black, 32GB). \n\n ");
                e === !0 || $(".hide-all").hide(), $(".show-all").show();
                var n = 299,
                    t = setInterval(function() {
                        $("#countdown").text(n--), -1 == n && clearInterval(t)
                    }, 1e3);
                javascript_countdown.init(300)
            }, 6800)
        }
    }
```

Viltus loterijas

Viltus loterijas

Viltus loterijas



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 līdzi 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**