

Falskt öryggi



Falskt öryggi

Framleiðendur iðnvéla segja að það þurfi ekki framkvæma veikleikaprófanir á kerfum því þau eru aldrei tengd við Internetið – **HALLÓ** → það er leitarvél á Internetinu sem leitar uppi svona tæki !

Árásarfletir (targets)

Því fleiri forrit því meiri líkur á að hægt sé að brjótast inn í kerfi!

Ef hugbúnaður er ókeypis þá hangir yfirleitt eitthvað vafasamt á spýttunni...

IT Security

Apple allows app developers to resume tracking with iOS 6

By Michael Kassner

October 24, 2012, 12:02 PM PDT

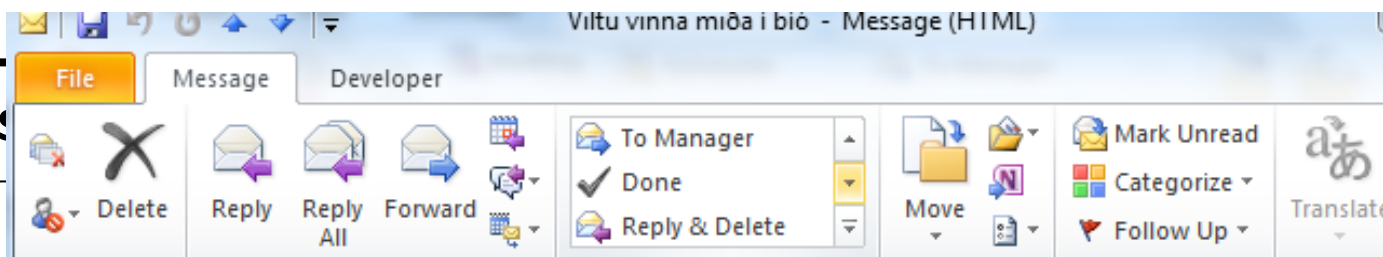
Takeaway: Apple was burnt once by allowing app developers to track users via the UDID. Will they get burnt again by allowing app developers to track using Apple's brand-new IDFA?

Online tracking of mobile devices for whatever reason is a touchy subject — just ask Apple. A while back, Apple was smack in the middle of the [tracking squabble](#). The panic started when the [Wall Street Journal](#) publicized how application developers were able to associate iPhone's Unique Device Identifier (UDID) — considered the phone's serial number — with other personal information (real names, addresses, and phone numbers) stored on the phone.

This [paper](#) written earlier by Eric Smith forecasted this inevitability:



Bragðvísirás



Hva

Tak

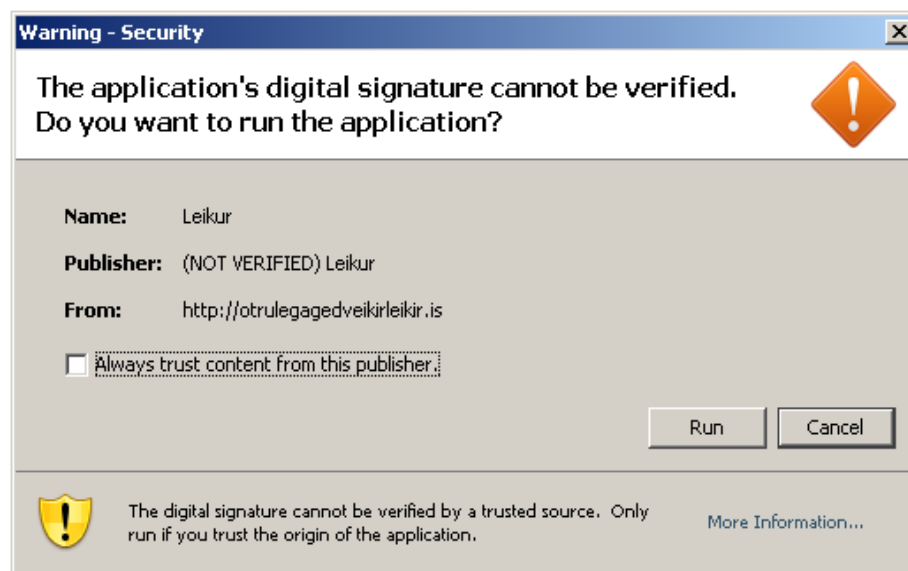
Hva

Hva

Ma

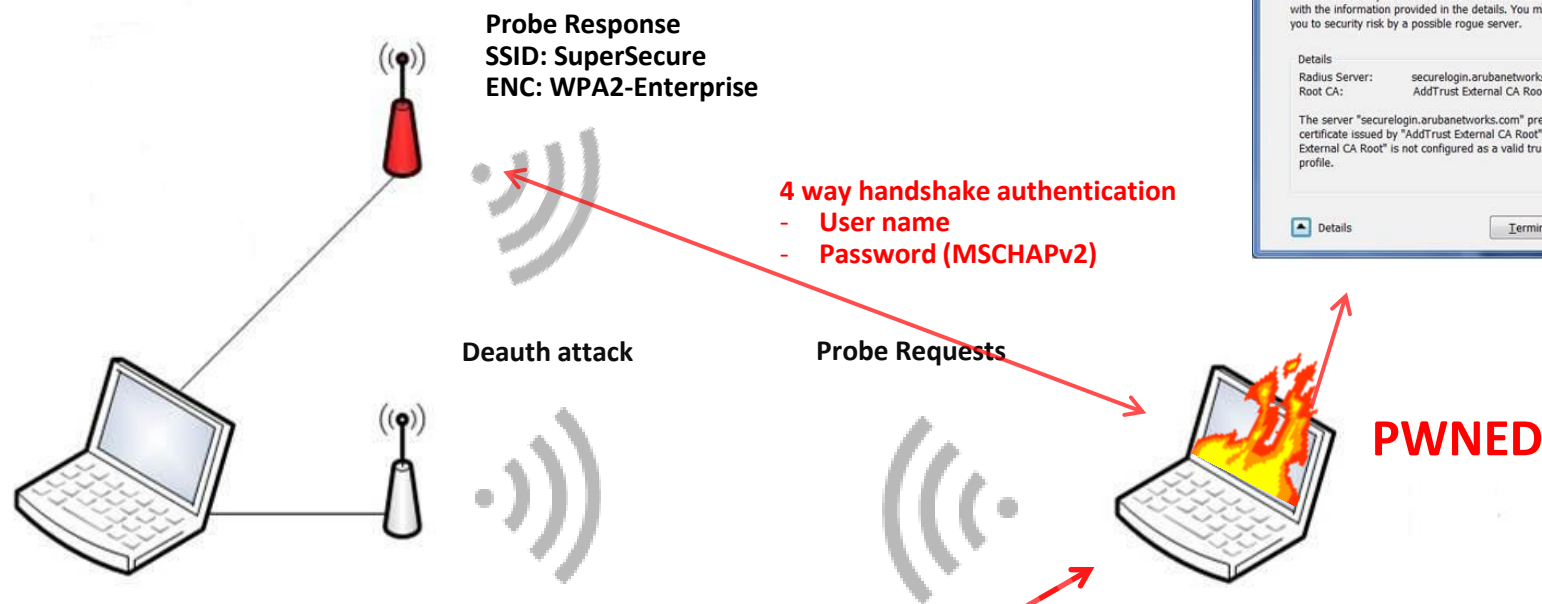


Keyri upp leikinn... Þú gætir þurft að Smella á "Run" til að byrja leikinn



[Smelltu hér til að eiga möguleika að vinna 4 miða á myndina](#)

Sýnidæmi – Öryggi þráðlausra neta



Þráðlaus sendir t.d. hjá fyrirtæki sem tölva (eða snjallsími) tengist sjálfkrafa með besta öryggi sem er í boði

SSID: SuperSecure



Helstu áhættur

Netþjónar eru oftast hakkaðir

Figure 26. Categories of compromised assets by percent of breaches and percent of records

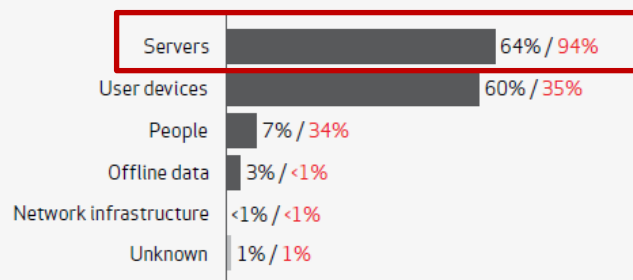
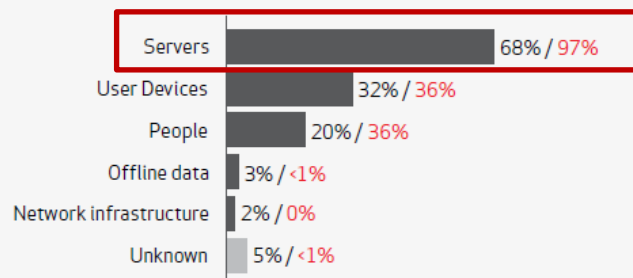


Figure 27. Categories of compromised assets by percent of breaches and percent of records - LARGER ORGS



2010

6.051 hættulegar vefsíður

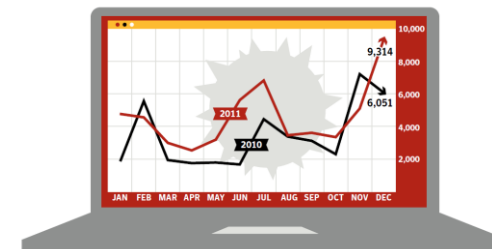
2011

9.314 hættulegar vefsíður

*Rannsókn á vegum
Verizon Risk Team með
stuðning frá CIA, FBI ofl.*

*Web Security Threat Report
- Update to Internet
Security Threat Report –
Maí 2012*

Average Number Of Malicious Web Sites Identified Per Day, 2011



Most Dangerous Web Site Categories, 2011

Rank	Top-10 Most Frequently Exploited Categories Of Web Sites	% Of Total Number Of Infected Web Sites
1	Blogs/Web Communications	19.8%
2	Hosting/Personal hosted sites	15.6%
3	Business/Economy	10.0%
4	Shopping	7.7%
5	Education/Reference	6.9%
6	Technology Computer & Internet	6.9%
7	Entertainment & Music	3.8%
8	Automotive	3.8%
9	Health & Medicine	2.7%
10	Pornography	2.4%

Hverjir eru þessir „snillingar“?



MONDAY, AUGUST 1, 2011



LulzSec hacker Topiary arrested, looks exactly how you thought he would.

Security Predictions for 2012 **from Websense® Security Labs™**

Your social media identity may prove more valuable to cybercriminals than your credit cards. Bad guys will actively buy and sell social media credentials in online forums.

facebook

LinkedIn

You Tube

Google™

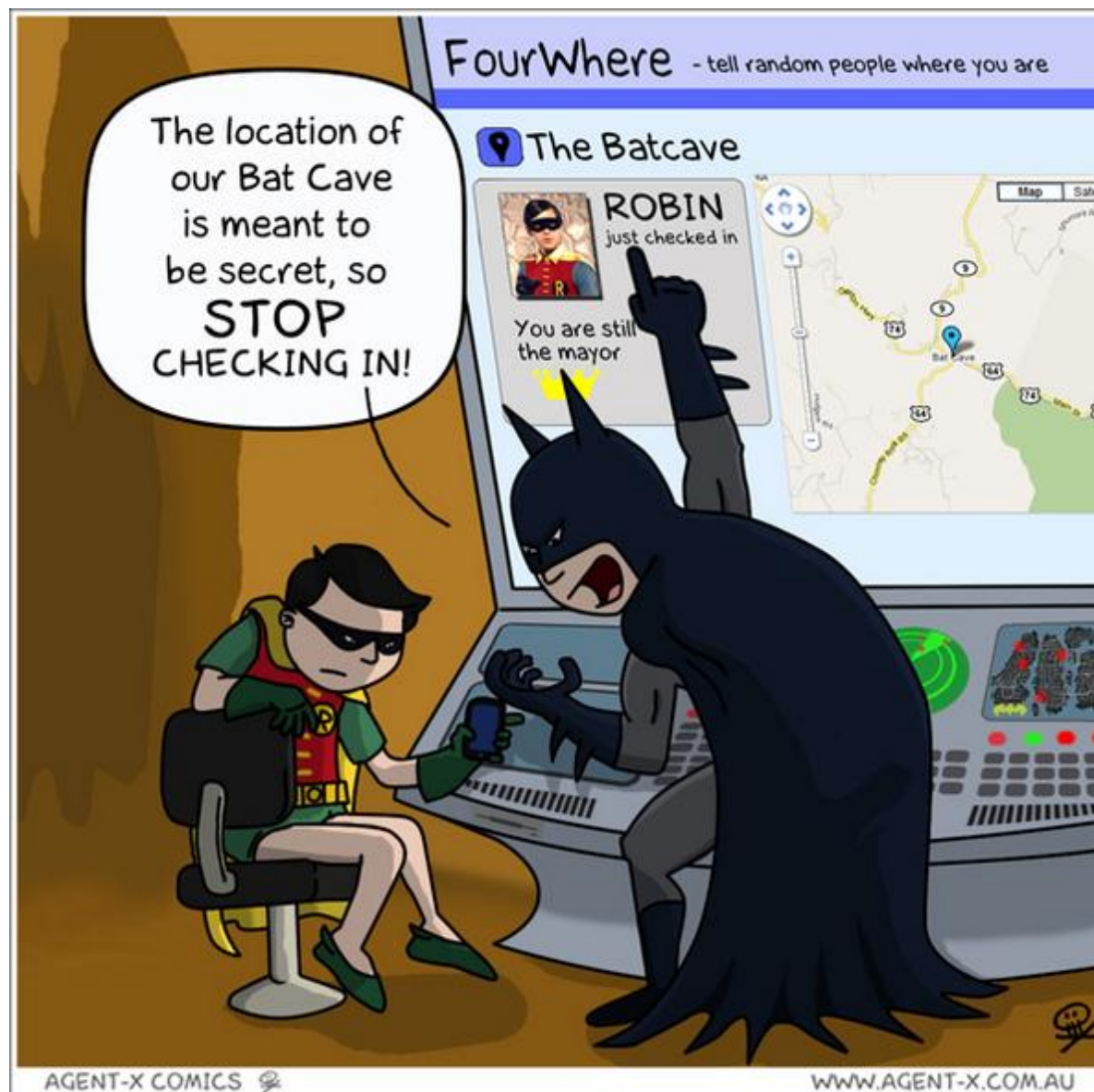
Windows Live™
Messenger

skype™



foursquare

Upplýsingaleynd er mikilvæg



Android Malware Infections Increase^{AA} By 700%

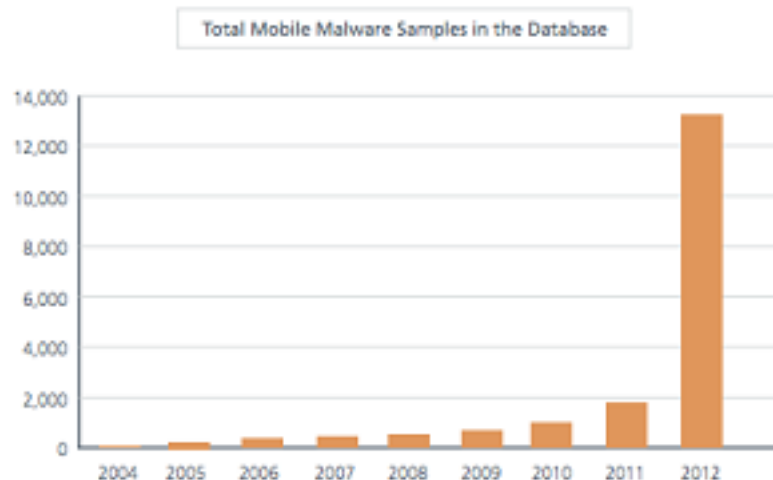
MARSHALL LEMON | 4 SEPTEMBER 2012 10:44 PM

21

Approximately 85% of all mobile malware attacks since 2011 occurred on Android smartphones.

When it comes to the world of internet security and malware, being the biggest fish in the sea also makes you the biggest target. Such was the case when Windows operating systems dominated the PC landscape in the 90s, and such is the case today in the mobile sphere with Android phones. The platform is [fast becoming the mobile operating system of choice](#), but its

rampant growth combined with its open source nature is an ideal breeding ground for virus and malware distribution. Tracking reports by security firm McAfee have revealed that in the last year, malware breaches have grown by an astronomical 700%, putting the Android at approximately 85% of reported malware instances.



Símasvindlarar herja á Ísland

Fyrst birt: 01.11.2012 14:13, Síðast uppfært: 01.11.2012 14:20



Tölvuprjótar eru enn að hringja í fólk og biðja það að gefa alls kyns upplýsingar til að tölvan bili ekki. Mynd: Shutterstock

Enn eru tölvuprjótar að hringja heim til fólks og biðja það að fara í tölvuna sína og gefa upp alls kyns upplýsingar til að koma í veg fyrir að tölvan bili. Lögreglan á höfuðborgarsvæðinu hefur fengið tilkynningar um slík símtöl sem oftast eru á ensku.

Jafnan segist sá sem hringir vera á vegum Microsoft eða annarra þekktra tölvufyrirtækja, og sá sem hringt er í er hvattur til setjast við tölvuna, veita upplýsingar og jafnvel fara inn á tilteknar vefsíður.

Óhætt er að fullyrða að sá sem hringir, er ekki í forvarnahugleiðingum, heldur er ætlunin að komast inn í tölvur fólks, til að stela fjármunum þess.

Svindl af þessum toga er þekkt víða um heim og er fólk hvatt til að vera á varðbergi gagnvart svona símtölum.

Flokkar

Innlent

Líkar þetta 31

Tweet 0

+1 0

Deila á Facebook

Senda frétt

Prenta

Fleiri fréttir

[Verða að greiða gengislán](#)

[Tónleikum fyrir bændur frestað](#)

[Þrjú fíkniefnamál í Hafnarfirði](#)

[Of lítill peningur í skólamat](#)

[Rafmagnslínur komnar í lag](#)

[Ernir með óskerta áætlun](#)

[Nýr yfirlögregluþjónn á Vestfjörðum](#)

[Óveður og ófærð víða](#)

Hver er besta vörnin?



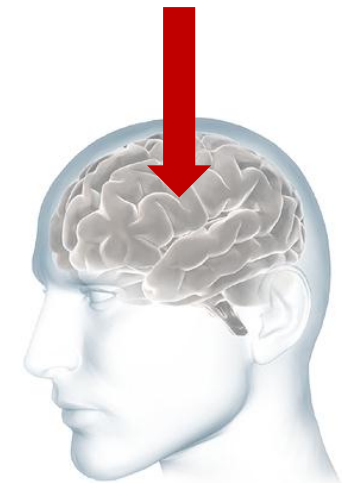
Staðlar



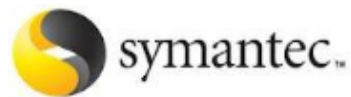
ITIL®



Er það ekki bara þessi?



Öryggislausnir



Eftirlit er mikilvægt og vanmetinn þáttur

Virkt eftirlit

[Unsubscribe and turn off activity reporting](#) | [Ask for help](#) | [See frequently asked questions](#) | [Learn more](#)

Fá hæfan á



Microsoft®
Family Safety

Reglubundun

Weekly Activity Report for
Eva Júlía Ólafsdóttir

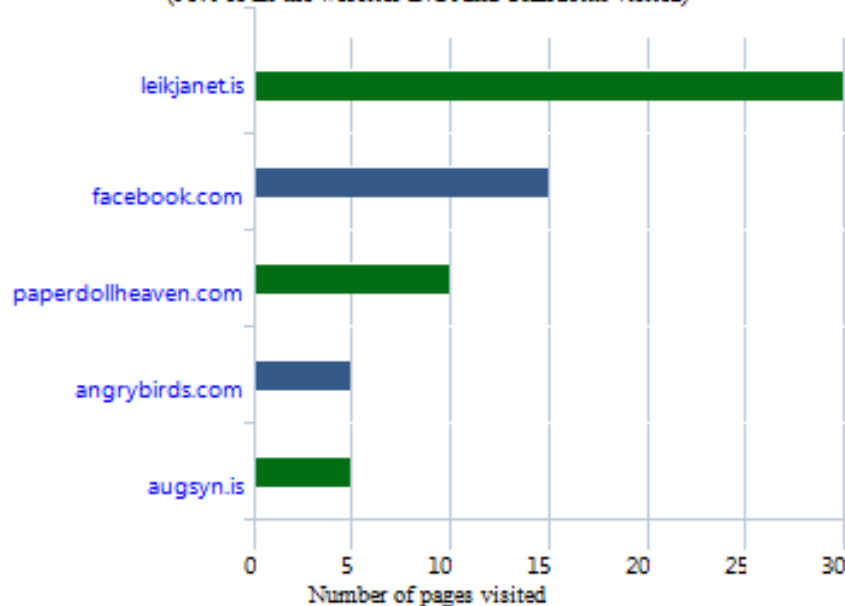
Óhæði er í



áhættu

Most popular websites ([View all](#))

(98% of all the websites Eva Júlía Ólafsdóttir visited)



Latest blocked pages ([View all](#))

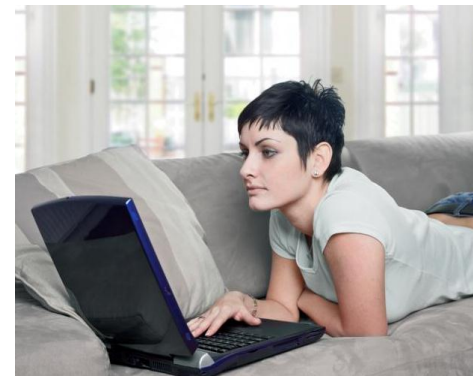
[Paperdoll Heaven](#)

Latest searches ([View all](#))

No results this week

Nokkur atriði sem stuðla að hærri öryggisstigi og -vitund

1. Ábyrg notkun
2. Staðlað umhverfi og uppfært
3. Efla öryggisvitund með reglubundinni fræðslu
4. Halda kerfisstjóraréttindum í lágmarki
5. Ekki treysta alfarið á hugbúnað eða kerfi
6. Framkvæma reglulega öryggisprófanir, bæði handvirkar og með tólum
7. Útbúa helstu stefnur, innleiða og fara eftir þeim!



Þú vilt ekki vera veikasti hlekkurinn í öryggiskeðjunni



*Til að vera ekki auðvelt
skotmark, er mikilvægt að hafa
góðan skilning á þeim hættum
sem steðja að okkur og hvað
hægt er að gera til að lágmarka
hættuna á að verða fyrir barðinu
á tölvuglæpamönnum.*

olafur.rafnsson@capacent.is



@OlafurRobert