Digital Defense for Activists

(And the Rest of Us)

Who Am I?

- Michele Chubirka, aka "Mrs. Y.”
- Industry analyst, blogger, tech writer, podcaster and Security Jedi Knight.
- Researcher and pontificator on topics such as security architecture, privacy and best practices.
- Twitter: @MrsYisWhy
- www.postmodernsecurity.com
- Digs good nerd memes.

Topics

- Current Landscape
- Risk Management 101
- Digital Defense Techniques

What You Won’t Get From Me

- Digital *offensive* techniques and/or activities that violate state/federal laws.

- Legal Advice. I’m not an attorney or law enforcement official.

- I’m also not here to fix your computer, printer, or other digital device.

“Why does it say *paper jam* when there is no paper jam?”

"Never say anything in an electronic message that you wouldn't want appearing, and attributed to you, in tomorrow morning's front-page headline in the New York Times."

—Colonel David Russell, former head of DARPA's Information Processing Techniques Office

It’s Scary Out There

- In 2013, Edward Snowden, a Booz Allen employee contracted to the NSA , revealed massive domestic and global surveillance programs sponsored by the US, UK, and Australia .
- In May 2014, six officers of China’s People’s Liberation Army (PLA) were indicted for economic espionage against a number of U.S. based companies.
- In November 2014, a North Korean hacker group posted corporate data from Sony Pictures on Wikileaks. This included employee PII and email.
- In June 2015, Office of Personnel Management (OPM) announced it had been hacked. Records of 22.1M federal workers and contractors were compromised, including members of the intelligence community. Breach was attributed to China
- In April 2015, it was disclosed that Russian hackers had breached the White House’s network.
- In the 2015 Anthem Blue Cross breach, approximately 80M records were impacted. The breach was attributed to China.

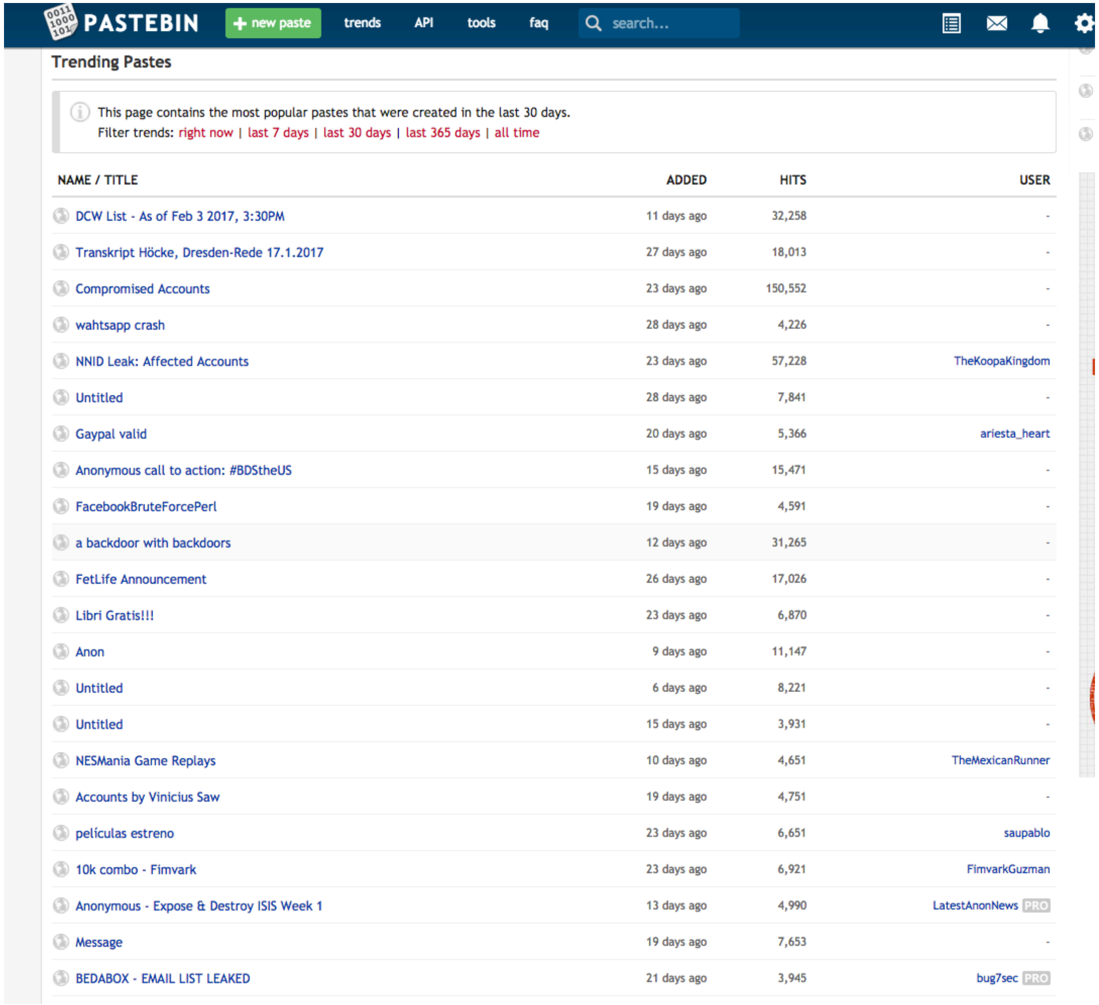
Not If, But When

- **Organizations hit over the last 12 months include:**
  - Arby’s, Wendy’s and other food chains.
  - InterContinental, Holiday Inn, Hyatt, Trump and Kimpton Hotels
  - LinkedIn, LANDESK, Scottrade, Experian, Oracle, Twitter, ADP, Pwnedlist, Spotify,Yahoo!

AND

  - ***Democratic National Committee and National Republican Senatorial Committee systems allegedly breached by Russia.***

How Criminals Get Your Data

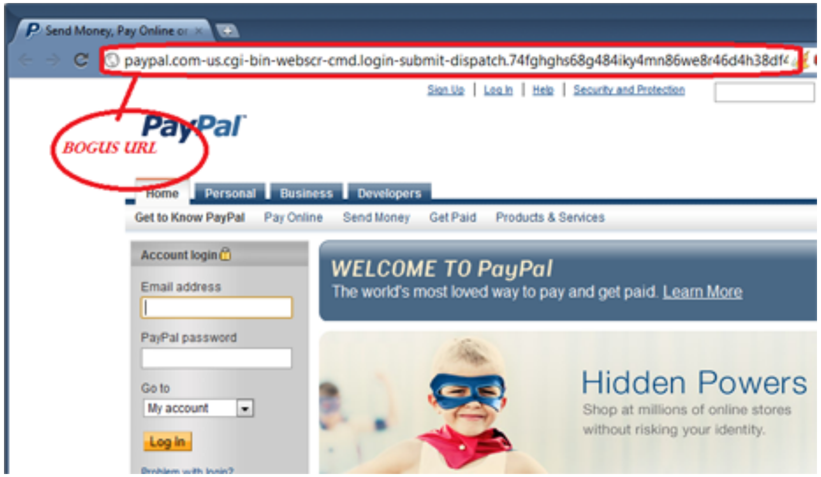


Trending Pastes

This page contains the most popular pastes that were created in the last 30 days.
Filter trends: right now | last 7 days | last 30 days | last 365 days | all time

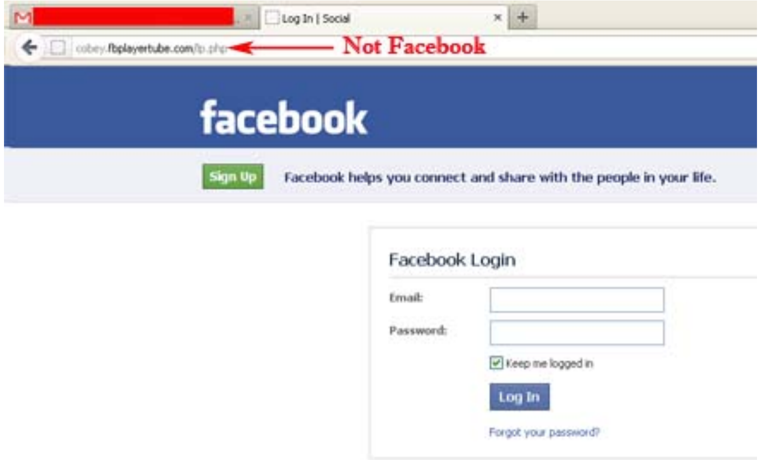
NAME / TITLE	ADDED	HITS	USER
DCW List - As of Feb 3 2017, 3:30PM	11 days ago	32,258	-
Transkript Höcke, Dresden-Rede 17.1.2017	27 days ago	18,013	-
Compromised Accounts	23 days ago	150,552	-
wahtsapp crash	28 days ago	4,226	-
NNID Leak: Affected Accounts	23 days ago	57,228	TheKoopaKingdom
Untitled	28 days ago	7,841	-
Gaypal valid	20 days ago	5,366	ariesta_heart
Anonymous call to action: #BDStheUS	15 days ago	15,471	-
FacebookBruteForcePerl	19 days ago	4,591	-
a backdoor with backdoors	12 days ago	31,265	-
FetLife Announcement	26 days ago	17,026	-
Libri Gratis!!!	23 days ago	6,870	-
Anon	9 days ago	11,147	-
Untitled	6 days ago	8,221	-
Untitled	15 days ago	3,931	-
NESMania Game Replays	10 days ago	4,651	TheMexicanRunner
Accounts by Vinicius Saw	19 days ago	4,751	-
películas estreno	23 days ago	6,651	saupablo
10k combo - Fimvark	23 days ago	6,921	FimvarkGuzman
Anonymous - Expose & Destroy ISIS Week 1	13 days ago	4,990	LatestAnonNews PRO
Message	19 days ago	7,653	-
BEDABOX - EMAIL LIST LEAKED	21 days ago	3,945	bug7sec PRO

Social Engineering, aka Phishing

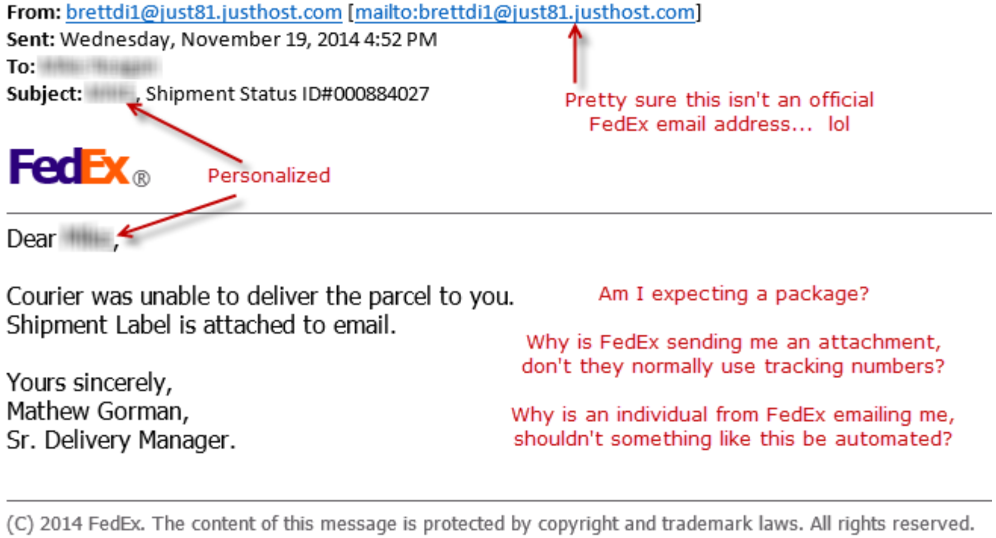


paypal.com-us.cgi-bin-webscr-cmd.login-submit-dispatch.74fghghs68g484iky4mn86we8r46d4h38df4

BOGUS URL



Not Facebook



From: brettdi1@just81.justhost.com [mailto:brettdi1@just81.justhost.com]
Sent: Wednesday, November 19, 2014 4:52 PM
To: [redacted]
Subject: [redacted], Shipment Status ID#000884027

FedEx®

Dear [redacted],

Courier was unable to deliver the parcel to you.
Shipment Label is attached to email.

Yours sincerely,
Mathew Gorman,
Sr. Delivery Manager.

(C) 2014 FedEx. The content of this message is protected by copyright and trademark laws. All rights reserved.

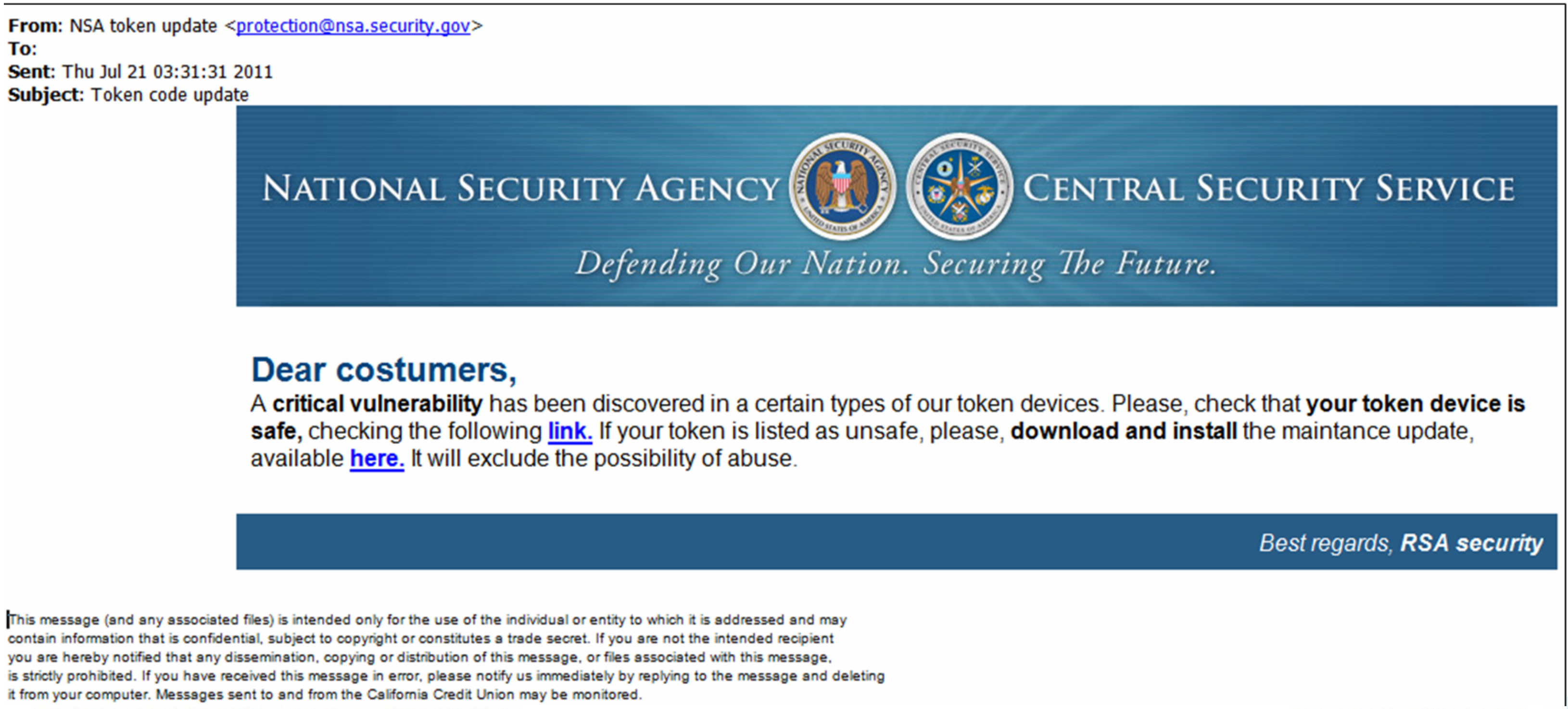
Pretty sure this isn't an official FedEx email address... lol

Personalized

Am I expecting a package?

Why is FedEx sending me an attachment, don't they normally use tracking numbers?

Why is an individual from FedEx emailing me, shouldn't something like this be automated?



From: NSA token update <protection@nsa.security.gov>
To:
Sent: Thu Jul 21 03:31:31 2011
Subject: Token code update

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

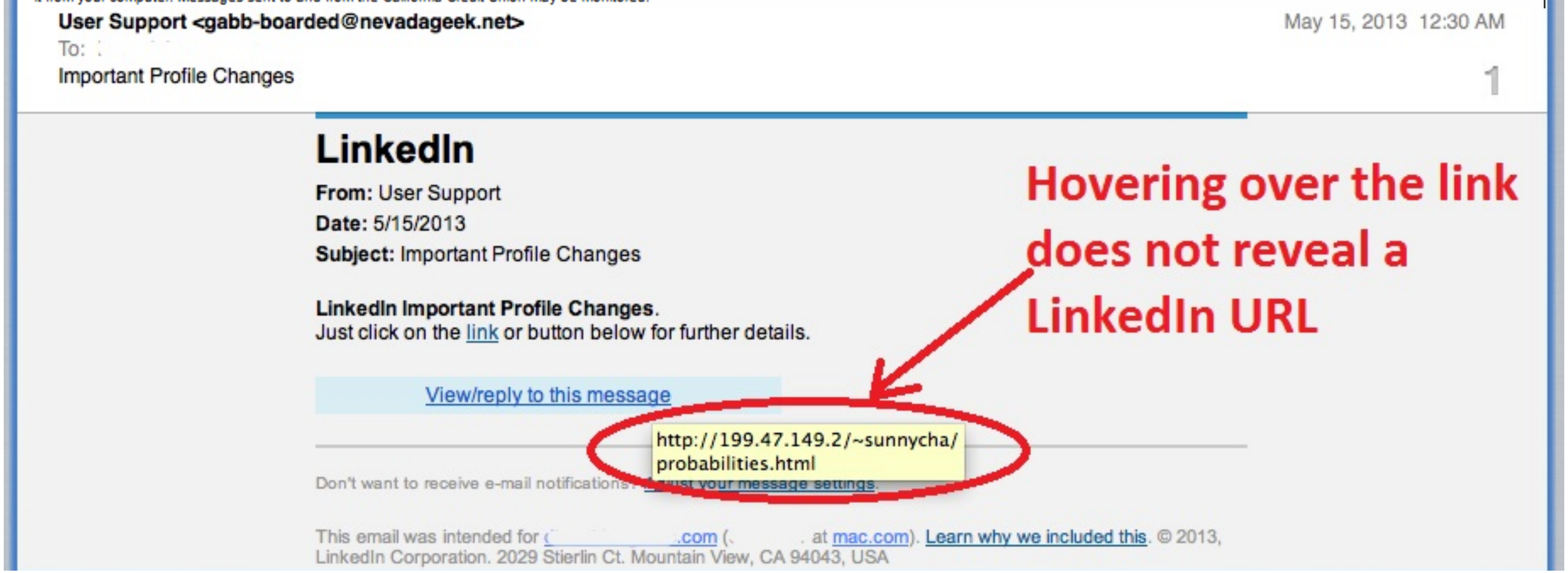
Defending Our Nation. Securing The Future.

Dear costumers,

A **critical vulnerability** has been discovered in a certain types of our token devices. Please, check that **your token device is safe,** checking the following **link.** If your token is listed as unsafe, please, **download and install** the maintance update, available **here.** It will exclude the possibility of abuse.

Best regards, ***RSA security***

This message (and any associated files) is intended only for the use of the individual or entity to which it is addressed and may contain information that is confidential, subject to copyright or constitutes a trade secret. If you are not the intended recipient you are hereby notified that any dissemination, copying or distribution of this message, or files associated with this message, is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer. Messages sent to and from the California Credit Union may be monitored.



User Support <gabb-boarded@nevadageek.net> May 15, 2013 12:30 AM
To:
Important Profile Changes

LinkedIn

From: User Support
Date: 5/15/2013
Subject: Important Profile Changes

LinkedIn Important Profile Changes.
Just click on the link or button below for further details.

View/reply to this message

http://199.47.149.2/~sunnycha/probabilities.html

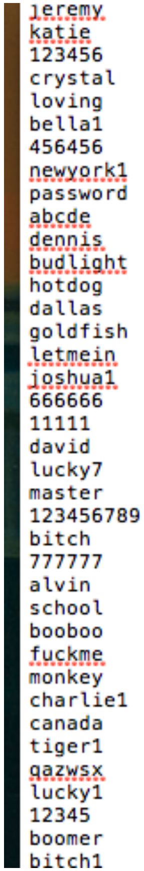
Don't want to receive e-mail notifications? Adjust your message settings.

This email was intended for .com (at mac.com). Learn why we included this. © 2013, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

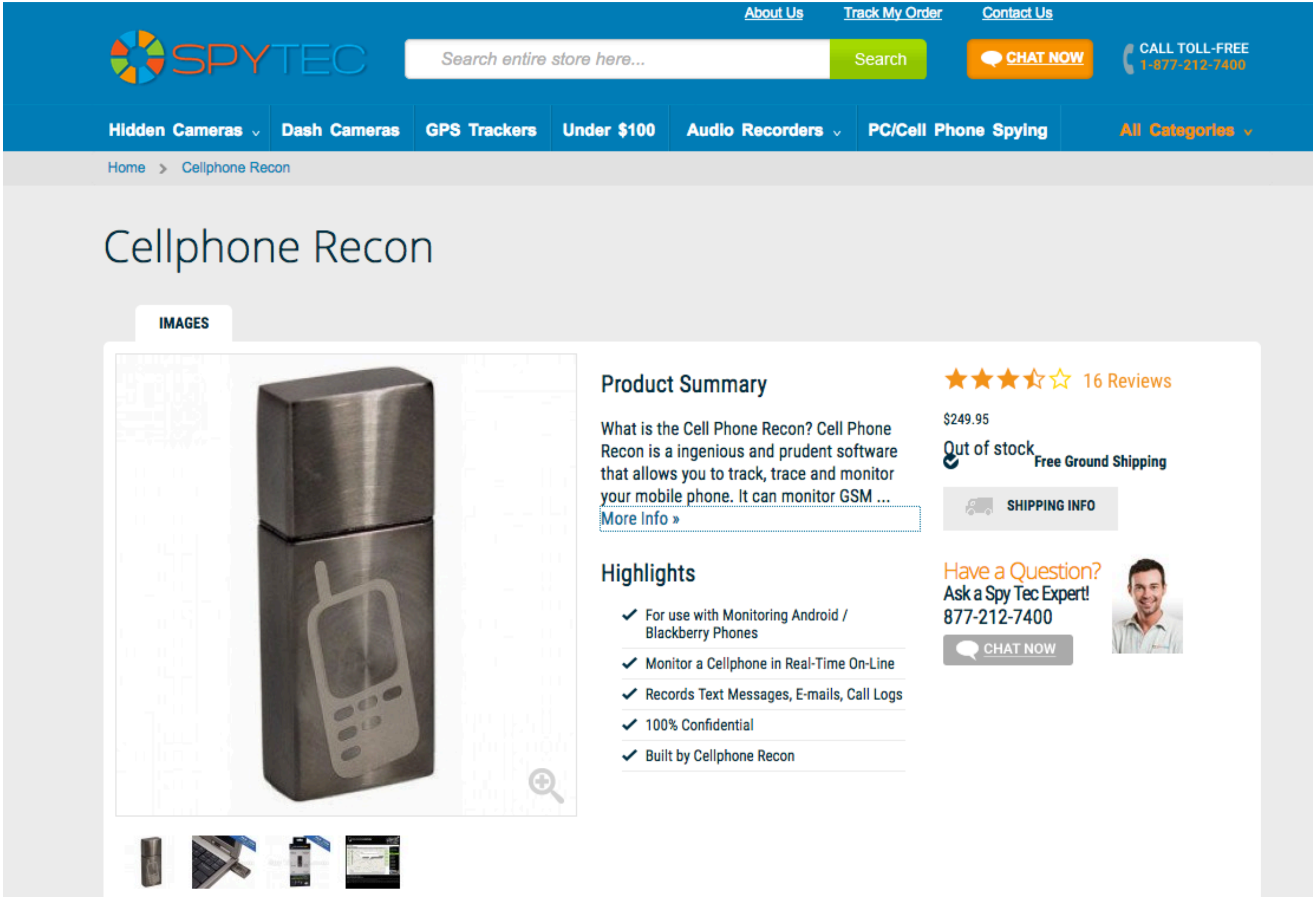
Hovering over the link does not reveal a LinkedIn URL

Passwords Really Suck

- Samples from the Ashley Madison breach
- Originally posted on Pastebin, a site for sharing text, but often used for distributing stolen data.



```
jeremy
katie
123456
crystal
loving
bella1
456456
newyork1
password
abcde
dennis
budlight
hotdog
dallas
goldfish
letmein
joshua1
666666
11111
david
lucky7
master
123456789
bitch
777777
alvin
school
booboo
fuckme
monkey
charlie1
canada
tiger1
qazwsx
lucky1
12345
boomer
bitch1
```



Cellphone Recon

Product Summary

What is the Cell Phone Recon? Cell Phone Recon is a ingenious and prudent software that allows you to track, trace and monitor your mobile phone. It can monitor GSM ...
More Info »

Highlights

- ✓ For use with Monitoring Android / Blackberry Phones
- ✓ Monitor a Cellphone in Real-Time On-Line
- ✓ Records Text Messages, E-mails, Call Logs
- ✓ 100% Confidential
- ✓ Built by Cellphone Recon

★★★½☆ 16 Reviews

$249.95

Out of stock

✓ Free Ground Shipping

Have a Question?
Ask a Spy Tec Expert!
877-212-7400

Brian Kreb's Immutable Truths About Data Breaches

- If you connect it to the Internet, someone will try to hack it.
- If what you put on the Internet has value, someone will invest time and effort to steal it.
- Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.
- The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.
- Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets.

https://krebsonsecurity.com/2017/01/krebss-immutable-truths-about-data-breaches/

"Only the paranoid survive."

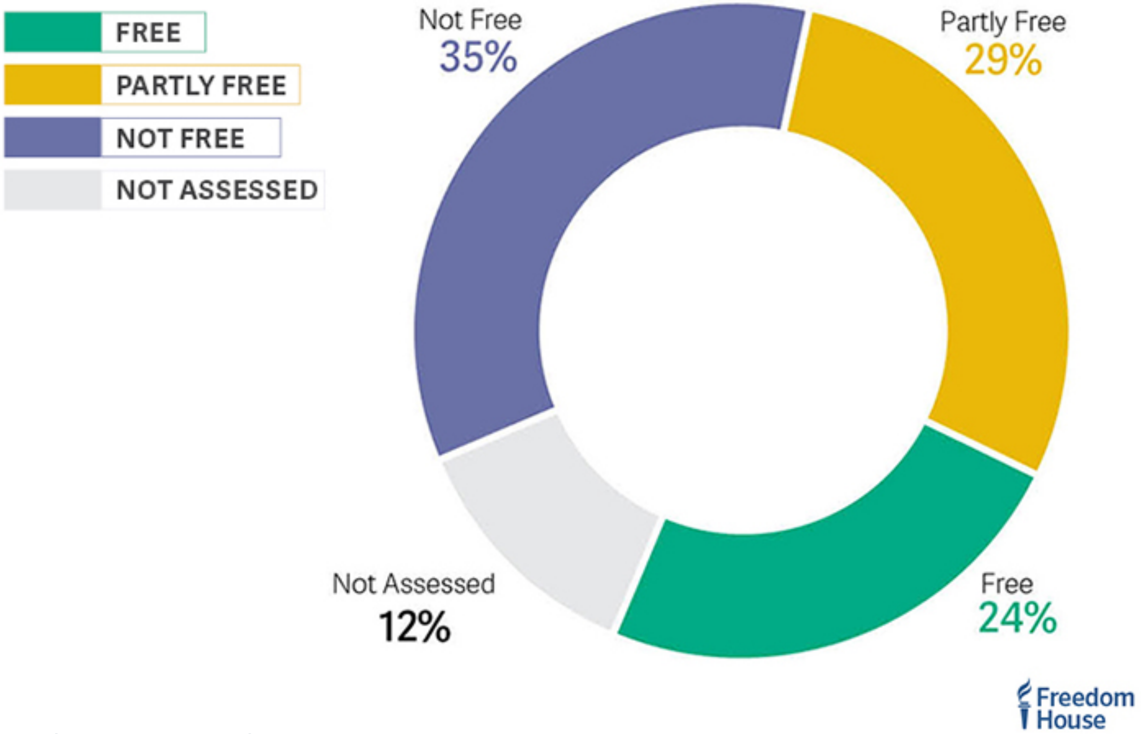
—Andy Grove, founder and former CEO of Intel

NOW AND THEN, I ANNOUNCE "I KNOW YOU'RE LISTENING" TO EMPTY ROOMS.
IF I'M WRONG, NO ONE KNOWS.
AND IF I'M RIGHT, MAYBE I JUST FREAKED THE HELL OUT OF SOME SECRET ORGANIZATION.

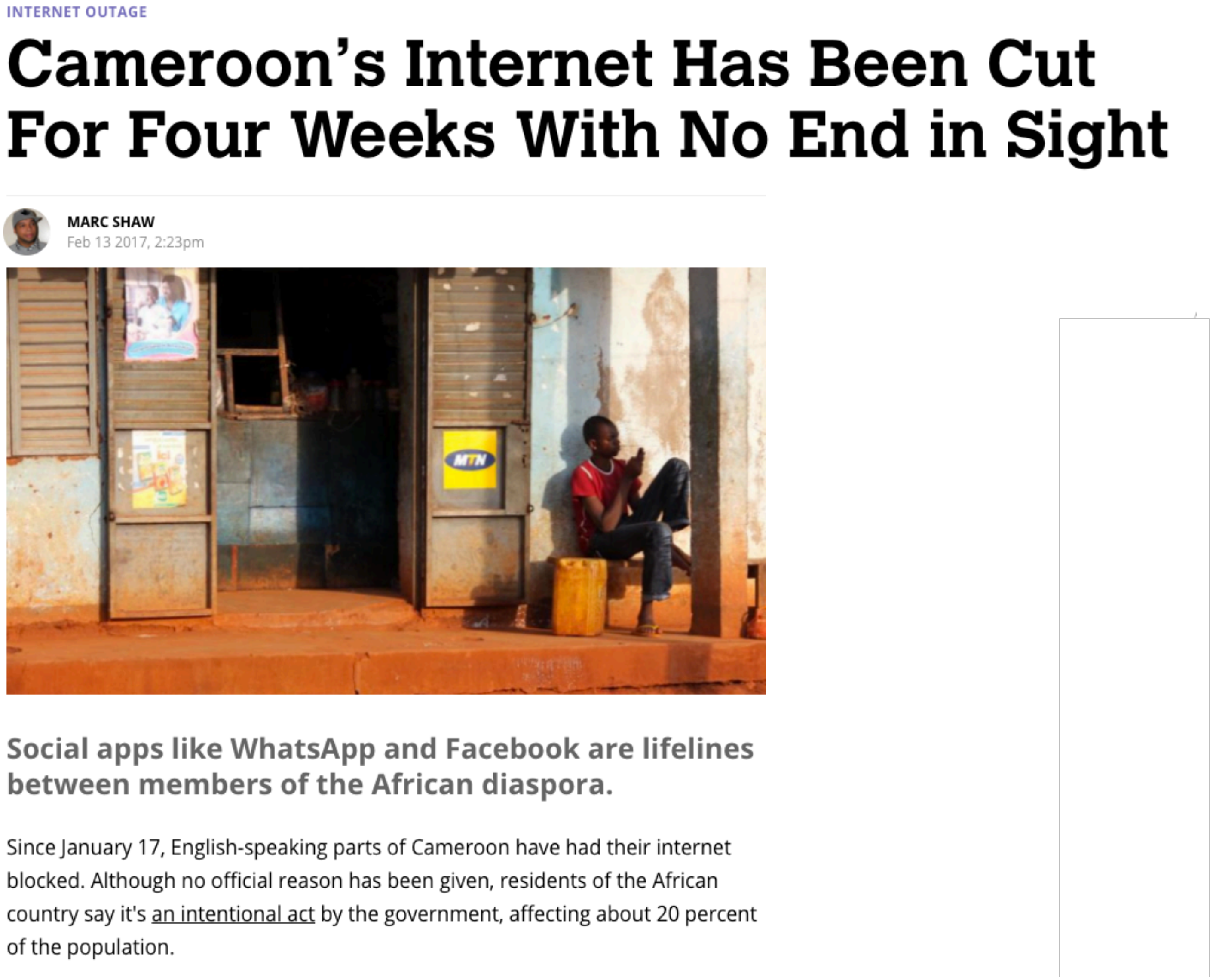
Freedom on the Net 2016

GLOBAL INTERNET POPULATION BY 2016 FOTN STATUS

FOTN assesses 88 percent of the world's internet user population.



An annual study of internet freedom around the world



INTERNET OUTAGE

Cameroon's Internet Has Been Cut For Four Weeks With No End in Sight

MARC SHAW
Feb 13 2017, 2:23pm

Social apps like WhatsApp and Facebook are lifelines between members of the African diaspora.

Since January 17, English-speaking parts of Cameroon have had their internet blocked. Although no official reason has been given, residents of the African country say it's an intentional act by the government, affecting about 20 percent of the population.

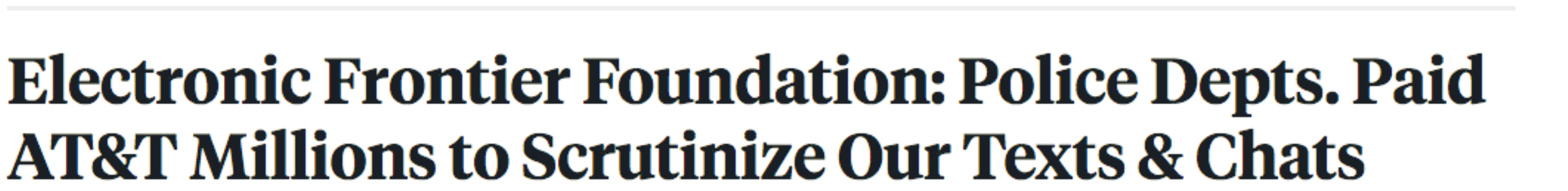
https://motherboard.vice.com/en_us/article/cameroon-internet-outage-diaspora-whatsapp

How the US Government Gets Your Data

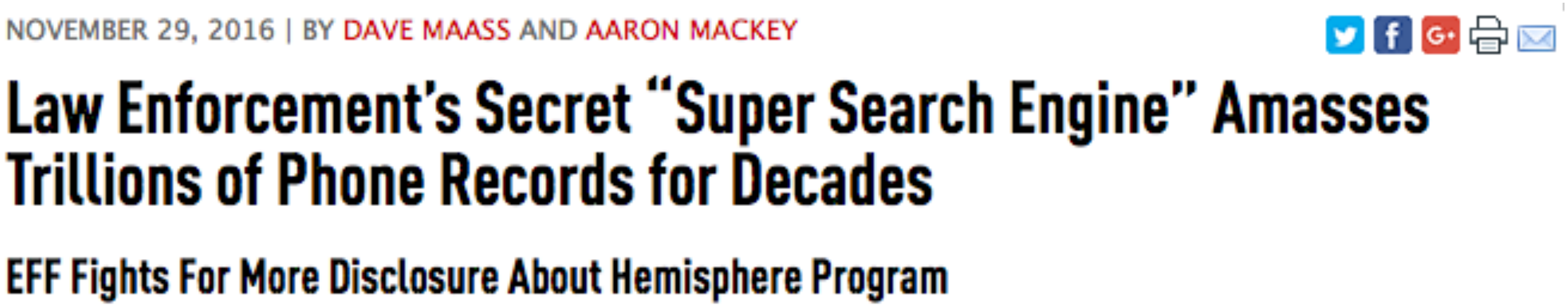
- Communications Assistance for Law Enforcement Act – CALEA is a wiretapping law requiring telecom providers and manufacturers to provide built-in surveillance capabilities for voice and Internet traffic.
- Digital Collection System Network - DCSNet is an FBI surveillance system used for instant wiretaps for telecommunications devices in the US.
- Computer Fraud and Abuse Act – federal law making it illegal to intentionally access a computer without authorization or in excess of authorization, but proposed amendments have been sought to justify increased data collection.
- USA FREEDOM Act – Update to Patriot Act that imposed some limits on bulk metadata collection but restored authorization for roving wiretaps and tracking lone wolf terrorists.

How Technology Companies and Service Providers May Violate Your Privacy

- Monitoring network traffic for RIAA (Recoding Industry of America) and MPAA (Motion Picture Association of America) violations.
- Information Sharing and Analysis Centers – ISACs are industry-focused associations that share threat data between members.
- Collection of telemetry data for security, performance analysis and troubleshooting.
- Collection of full packet data for security, performance analysis and troubleshooting.
- Providing data to law enforcement with and without warrants.



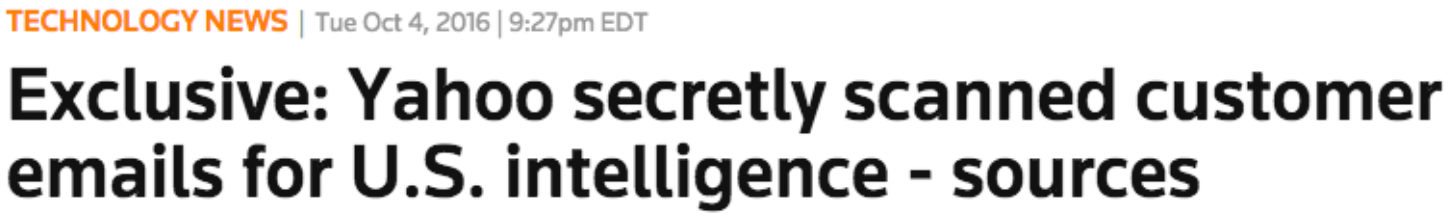
Electronic Frontier Foundation: Police Depts. Paid AT&T Millions to Scrutinize Our Texts & Chats



NOVEMBER 29, 2016 | BY DAVE MAASS AND AARON MACKEY

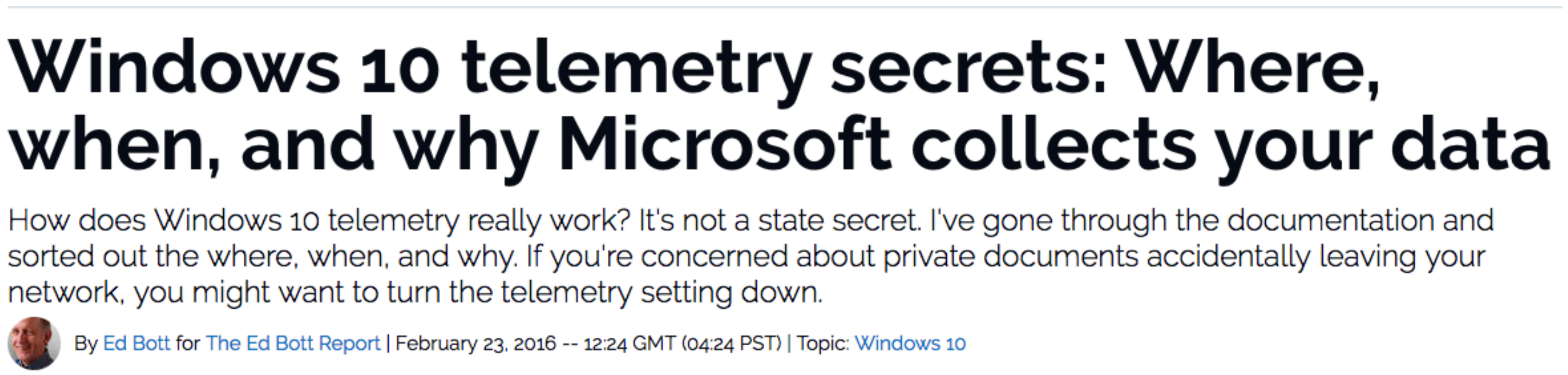
Law Enforcement's Secret "Super Search Engine" Amasses Trillions of Phone Records for Decades

EFF Fights For More Disclosure About Hemisphere Program



TECHNOLOGY NEWS | Tue Oct 4, 2016 | 9:27pm EDT

Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence - sources

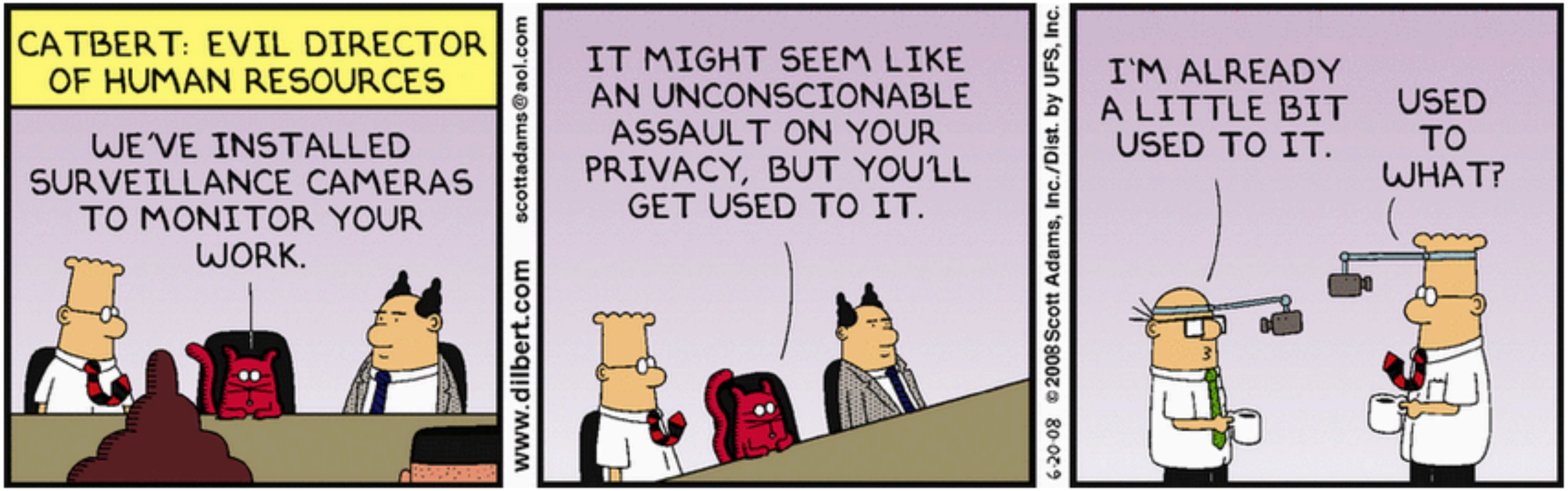


Windows 10 telemetry secrets: Where, when, and why Microsoft collects your data

How does Windows 10 telemetry really work? It's not a state secret. I've gone through the documentation and sorted out the where, when, and why. If you're concerned about private documents accidentally leaving your network, you might want to turn the telemetry setting down.

By Ed Bott for The Ed Bott Report | February 23, 2016 -- 12:24 GMT (04:24 PST) | Topic: Windows 10

Guess Who Else Is Watching?


CATBERT: EVIL DIRECTOR OF HUMAN RESOURCES
WE'VE INSTALLED SURVEILLANCE CAMERAS TO MONITOR YOUR WORK.
www.dilbert.com scottadams@aol.com
IT MIGHT SEEM LIKE AN UNCONSCIONABLE ASSAULT ON YOUR PRIVACY, BUT YOU'LL GET USED TO IT.
6-20-08 © 2008 Scott Adams, Inc./Dist. by UFS, Inc.
I'M ALREADY A LITTLE BIT USED TO IT.
USED TO WHAT?

How the Workplace Invades Your Privacy

- Acceptable Use Policy – AUPs are agreements that employees must sign to obtain network access from an organization. They set guidelines on how the network may be used and generally contain “consent to monitoring” clauses.

- Social Media Policies – this not only includes guidelines for how you may speak about your employer, it can also impact how you are allowed to access social media sites at work.

- Security and network technologies such as firewalls, proxy servers, SSL Intercept, IDS/IPS, DLP, network taps, endpoint agents, DNS filters and other metadata collection tools.

- Most workplaces implement controls on Internet traffic similar to repressive governments.

Risk Management 101

- Risk = threat x vulnerability x impact

  Asset – something of value

  Risk – exposure of asset to harm.

  Threat – a person or thing likely to cause damage or harm.

  Vulnerability – susceptibility to threat.

  Impact – effect of damage.

  Attack – action to cause harm.

"Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings."

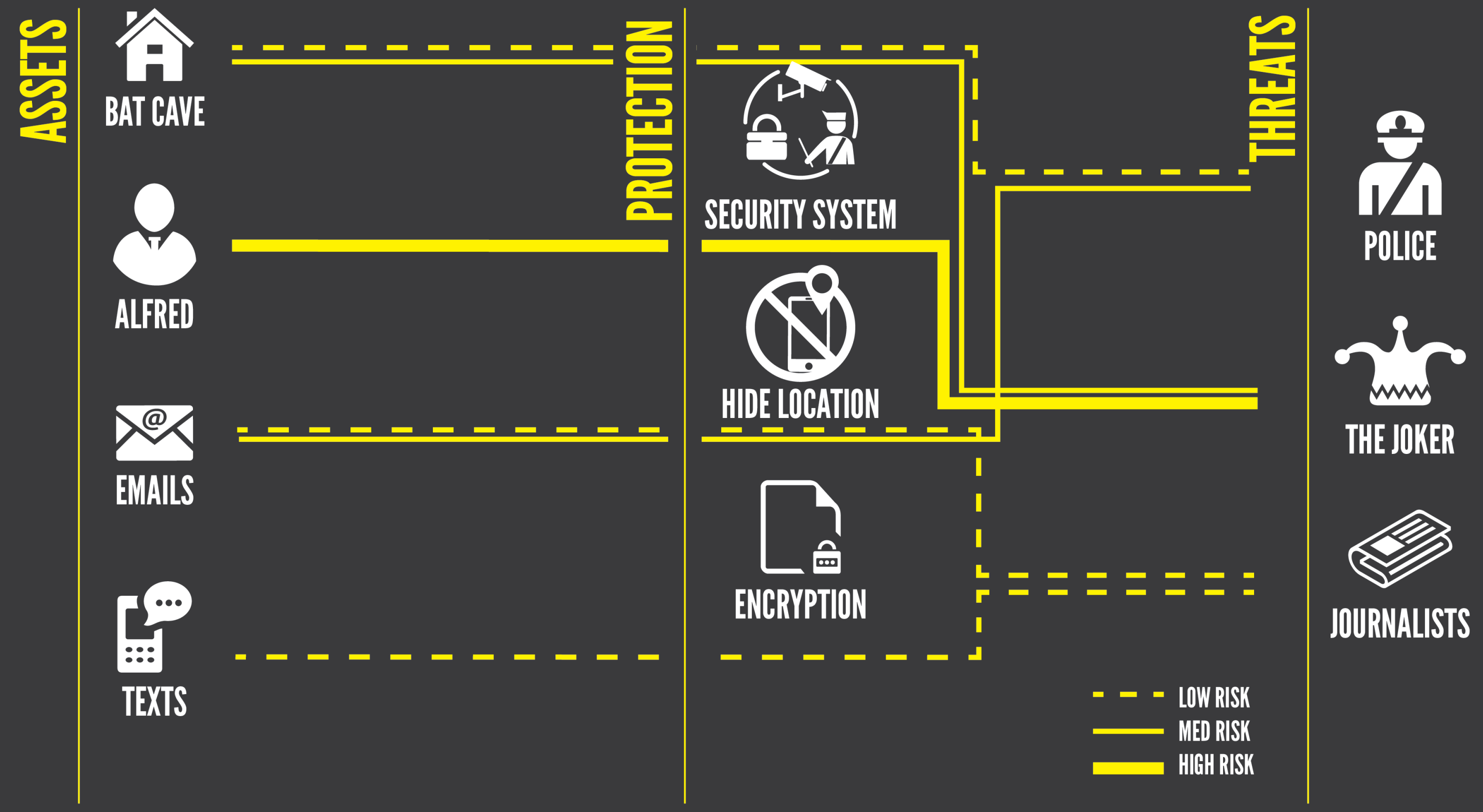
http://searchcompliance.techtarget.com/definition/risk-management

Threat Modeling 101

- A process in which potential threats are identified and analyzed for likelihood of damage to assets.
- Helps to identify your vulnerability to various attack types.
- Assessment questions:
  - What do you want to protect?
  - Who do you want to protect it from?
  - How likely is it that you will need to protect it?
  - How bad are the consequences if you fail?
  - How much trouble are you willing to go through in order to try to prevent those?

https://ssd.eff.org/en/module/introduction-threat-modeling

BRUCE WAYNE/BATMAN'S THREAT MODEL



http://web.mit.edu/tweilu/www/eff-ssd-mockup/threatmodel.html

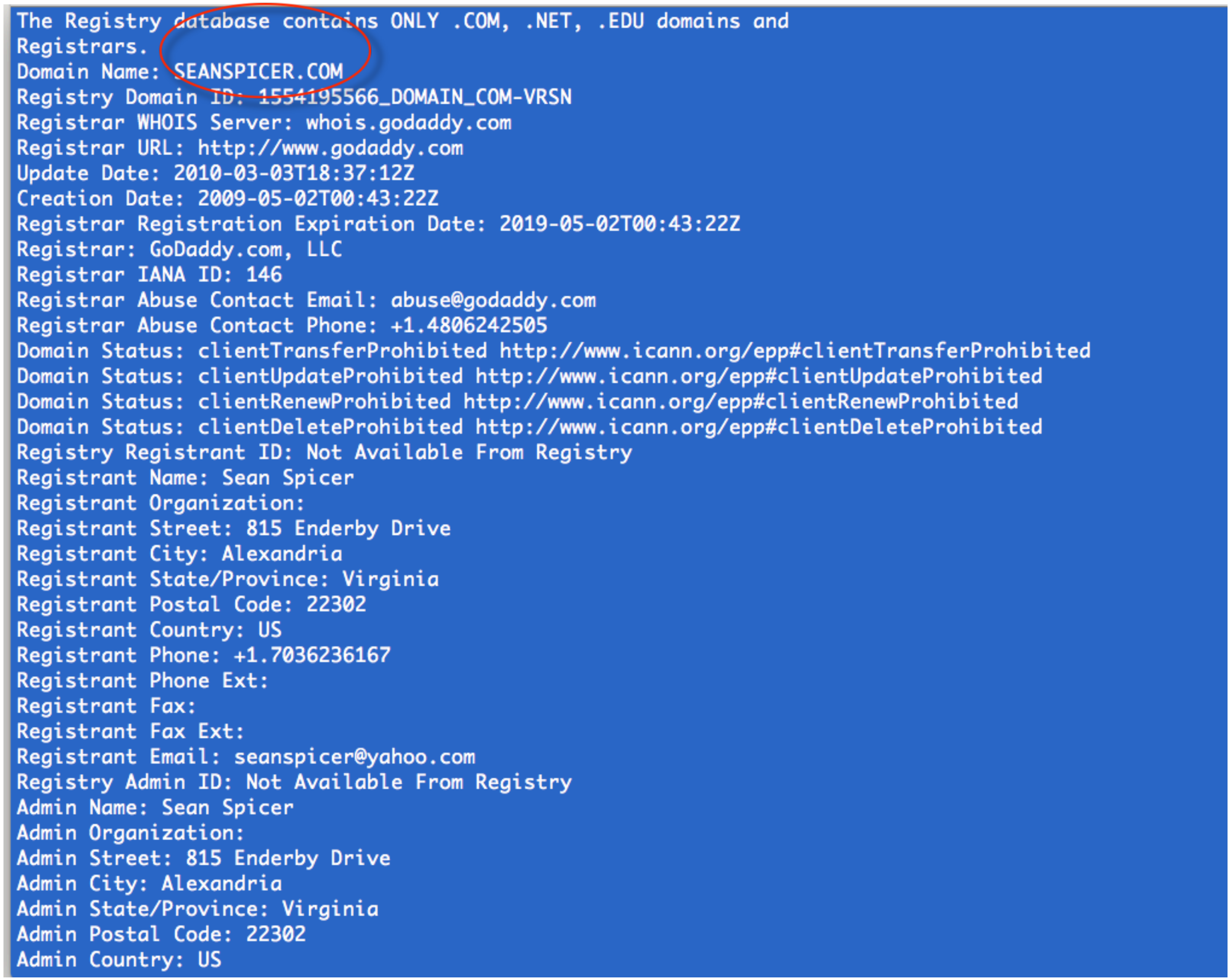
Common Threats

- Stingrays aka “IMSI catchers”, Wireless “evil twins”
- Social engineering campaigns using phishing/spearphishing
- Malware, backdoors and surveillance software
- OSINT (open source intelligence aka “passive recon”) – gathered from social media, blogs, whois, EXIF data,Spokeo, PeekYou, Google Hacking, etc…
- Denial of Service (DoS/DDoS) attacks
- Compromised privacy software and technologies (open source encryption, hiding or purchasing vulnerabilities, setting up bogus Tor nodes)

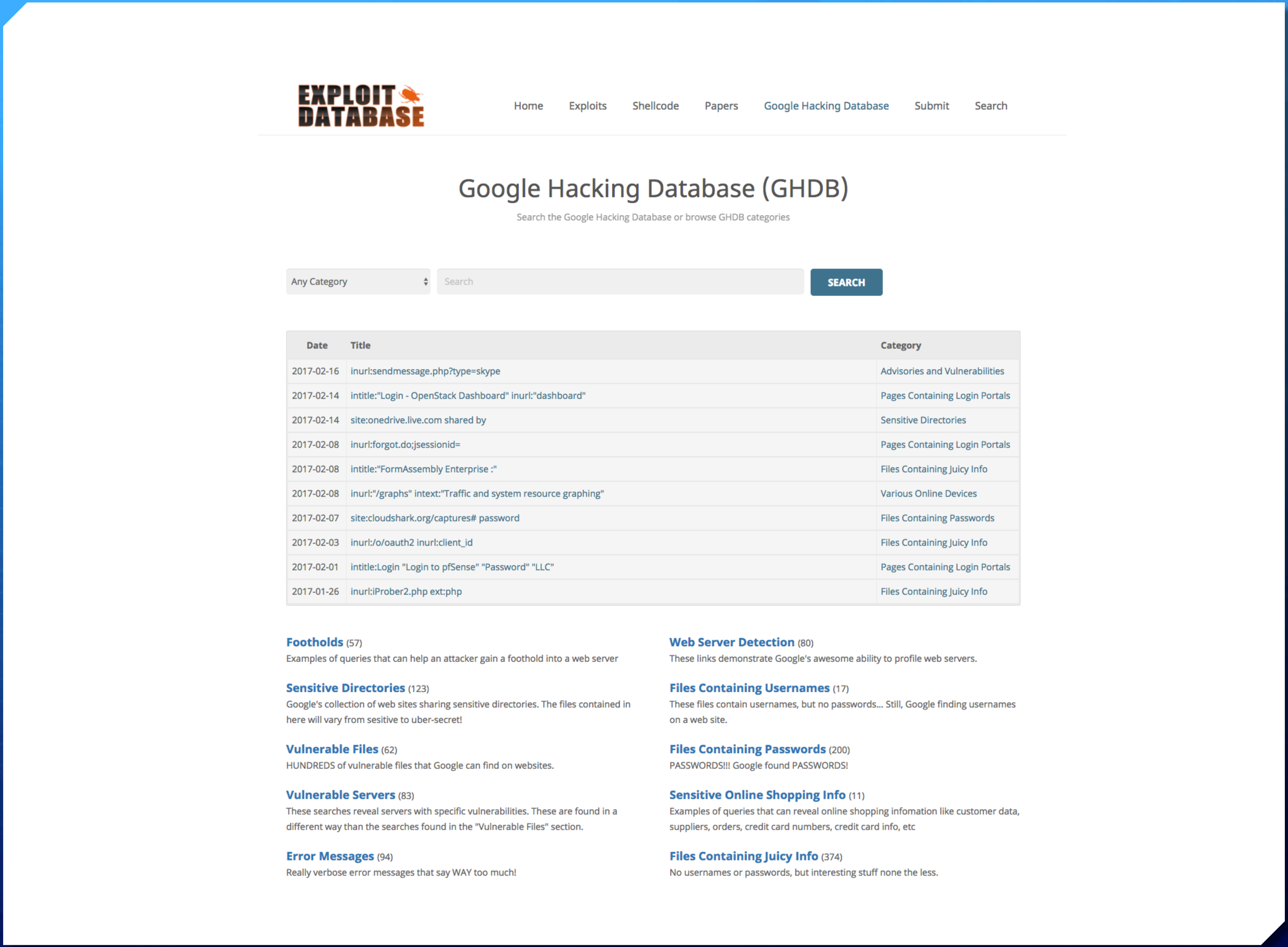
Governments use the SAME TECHNIQUES AS HACKERS to track you and violate your privacy.

WARNING!

Passive Reconnaissance Using Whois



```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: SEANSPICER.COM
Registry Domain ID: 1554195566_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2010-03-03T18:37:12Z
Creation Date: 2009-05-02T00:43:22Z
Registrar Registration Expiration Date: 2019-05-02T00:43:22Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Sean Spicer
Registrant Organization:
Registrant Street: 815 Enderby Drive
Registrant City: Alexandria
Registrant State/Province: Virginia
Registrant Postal Code: 22302
Registrant Country: US
Registrant Phone: +1.7036236167
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: seanspicer@yahoo.com
Registry Admin ID: Not Available From Registry
Admin Name: Sean Spicer
Admin Organization:
Admin Street: 815 Enderby Drive
Admin City: Alexandria
Admin State/Province: Virginia
Admin Postal Code: 22302
Admin Country: US
```



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Date	Title	Category
2017-02-16	inurl:sendmessage.php?type=skype	Advisories and Vulnerabilities
2017-02-14	intitle:"Login - OpenStack Dashboard" inurl:"dashboard"	Pages Containing Login Portals
2017-02-14	site:onedrive.live.com shared by	Sensitive Directories
2017-02-08	inurl:forgot.do;jsessionid=	Pages Containing Login Portals
2017-02-08	intitle:"FormAssembly Enterprise :"	Files Containing Juicy Info
2017-02-08	inurl:"/graphs" intext:"Traffic and system resource graphing"	Various Online Devices
2017-02-07	site:cloudshark.org/captures# password	Files Containing Passwords
2017-02-03	inurl:/o/oauth2 inurl:client_id	Files Containing Juicy Info
2017-02-01	intitle:Login "Login to pfSense" "Password" "LLC"	Pages Containing Login Portals
2017-01-26	inurl:iProber2.php ext:php	Files Containing Juicy Info

Footholds (57)
Examples of queries that can help an attacker gain a foothold into a web server

Sensitive Directories (123)
Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sesitive to uber-secret!

Vulnerable Files (62)
HUNDREDS of vulnerable files that Google can find on websites.

Vulnerable Servers (83)
These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Error Messages (94)
Really verbose error messages that say WAY too much!

Web Server Detection (80)
These links demonstrate Google's awesome ability to profile web servers.

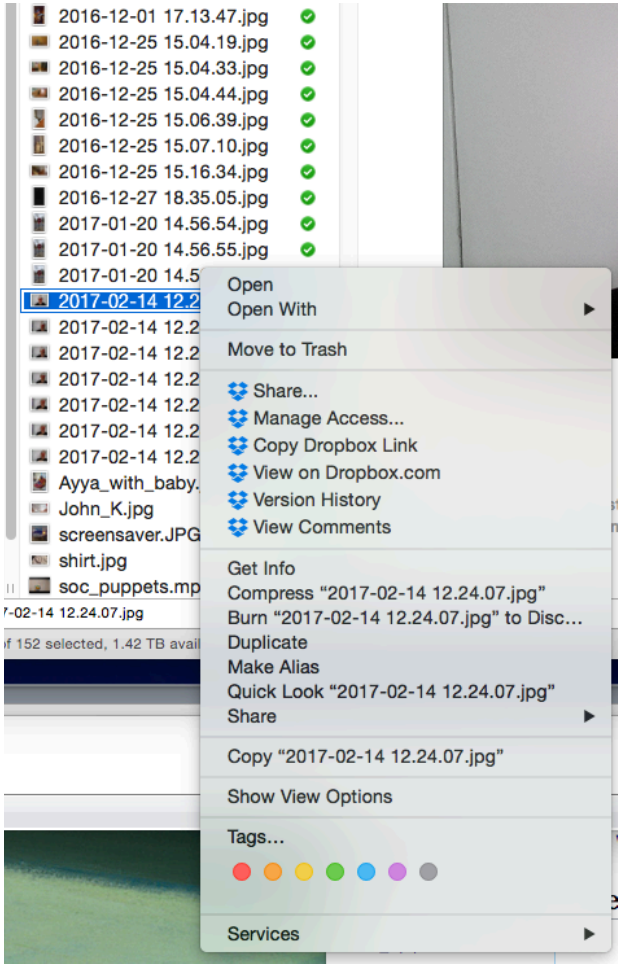
Files Containing Usernames (17)
These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

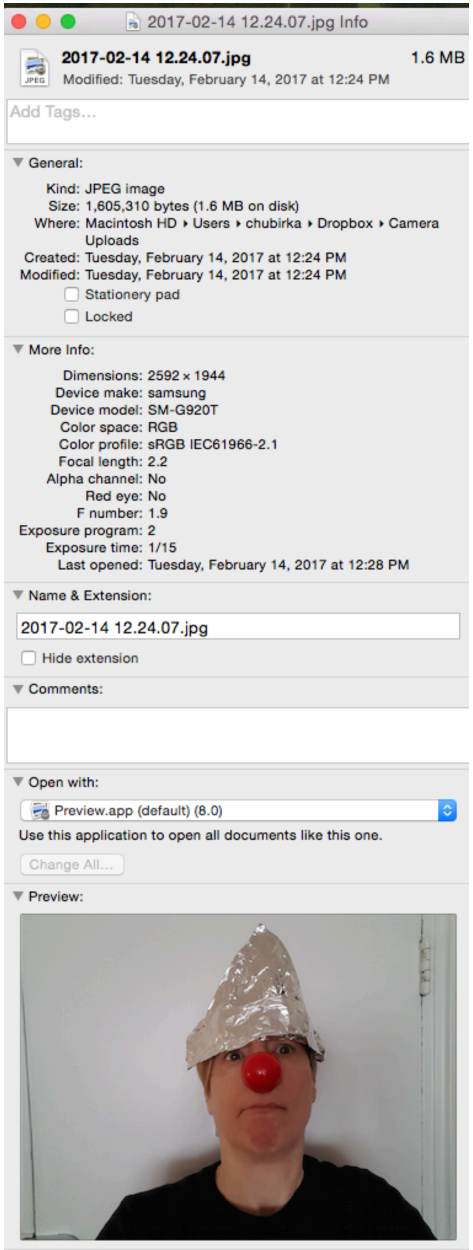
Files Containing Passwords (200)
PASSWORDS!!! Google found PASSWORDS!

Sensitive Online Shopping Info (11)
Examples of queries that can reveal online shopping infomation like customer data, suppliers, orders, credit card numbers, credit card info, etc

Files Containing Juicy Info (374)
No usernames or passwords, but interesting stuff none the less.

EXIF Photo Data




2017-02-14 12.24.07.jpg Info

2017-02-14 12.24.07.jpg 1.6 MB
Modified: Tuesday, February 14, 2017 at 12:24 PM

Add Tags...

General:

Kind: JPEG image
Size: 1,605,310 bytes (1.6 MB on disk)
Where: Macintosh HD ▸ Users ▸ chubirka ▸ Dropbox ▸ Camera Uploads
Created: Tuesday, February 14, 2017 at 12:24 PM
Modified: Tuesday, February 14, 2017 at 12:24 PM
□ Stationery pad
□ Locked

More Info:

Dimensions: 2592 × 1944
Device make: samsung
Device model: SM-G920T
Color space: RGB
Color profile: sRGB IEC61966-2.1
Focal length: 2.2
Alpha channel: No
Red eye: No
F number: 1.9
Exposure program: 2
Exposure time: 1/15
Last opened: Tuesday, February 14, 2017 at 12:28 PM

Name & Extension:

2017-02-14 12.24.07.jpg
□ Hide extension

Comments:

Open with:

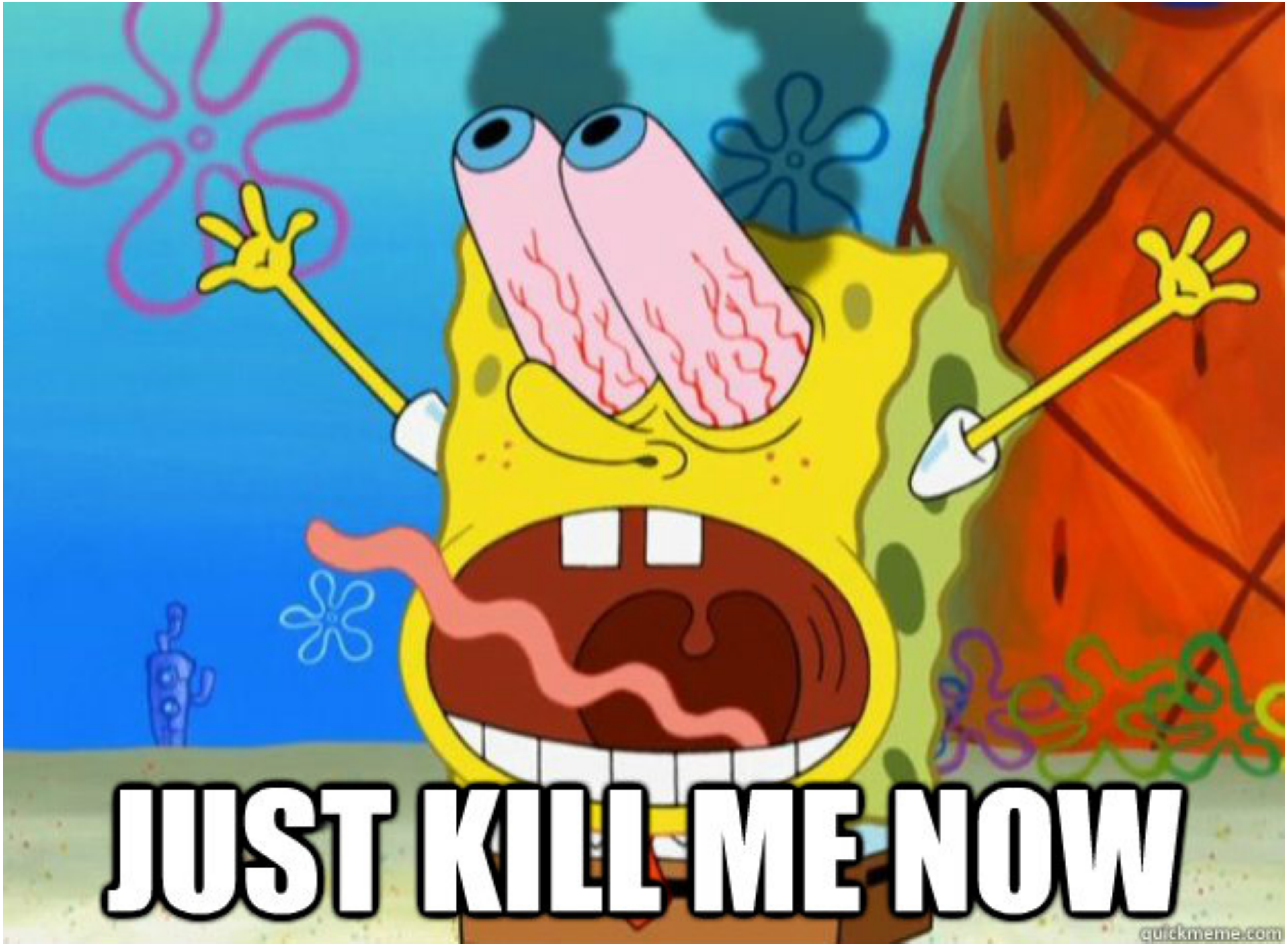
Preview.app (default) (8.0)
Use this application to open all documents like this one.
Change All...

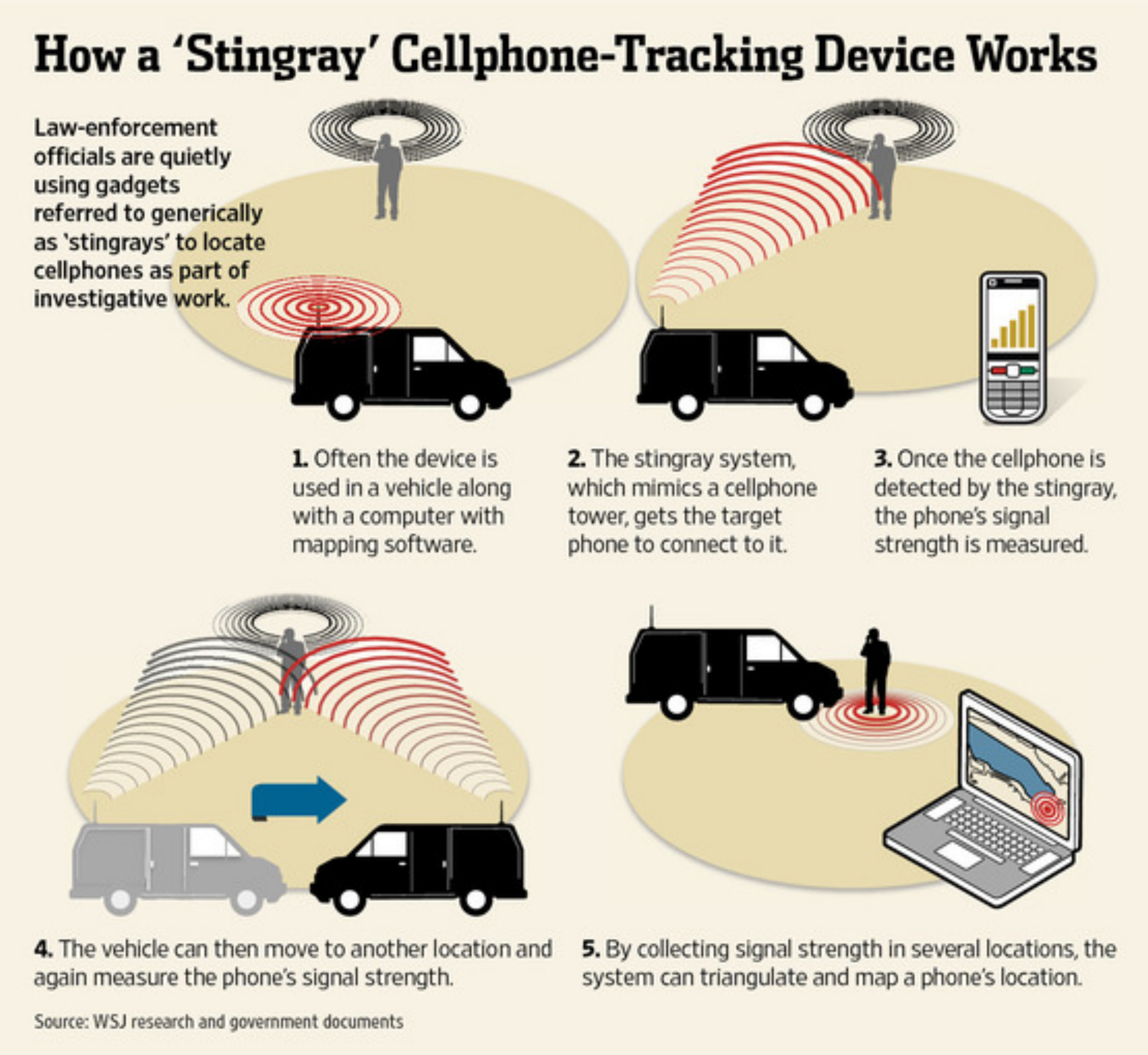
Preview:

Your Cell Phone Is a Tracking Device

Even when the GPS is disabled, your phone may leak location information.

- When a device isn't associated to a Wi-Fi network, it sends "beacons" attempting to reconnect to a previously used network. On some devices, "airplane mode" doesn't disable the wireless functionality. This leaks information about the device and can also make it vulnerable to "man in the middle" attacks, hijacking any Internet traffic.
- Cellular networks can use cell tower position and distance to calculate your location.
- Mobile devices and laptops have unique hardware addresses such as the MAC, IMSI, IMEI and MEID. These can be used for tracking.
- Internet traffic uses a logical address, an IP number, for sending and receiving traffic. This data is easily captured and viewed over an open wireless network.
- Bluetooth – a short range wireless device for connecting to speakers or keyboards. It has a physical address and signal that can be intercepted or tracked.
- IMSI "catchers" aka Stingrays can track the hardware address of your phone and intercept cellular connections allowing data and voice traffic to be monitored.


JUST KILL ME NOW
quickmeme.com



How a 'Stingray' Cellphone-Tracking Device Works

Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.

1. Often the device is used in a vehicle along with a computer with mapping software.

2. The stingray system, which mimics a cellphone tower, gets the target phone to connect to it.

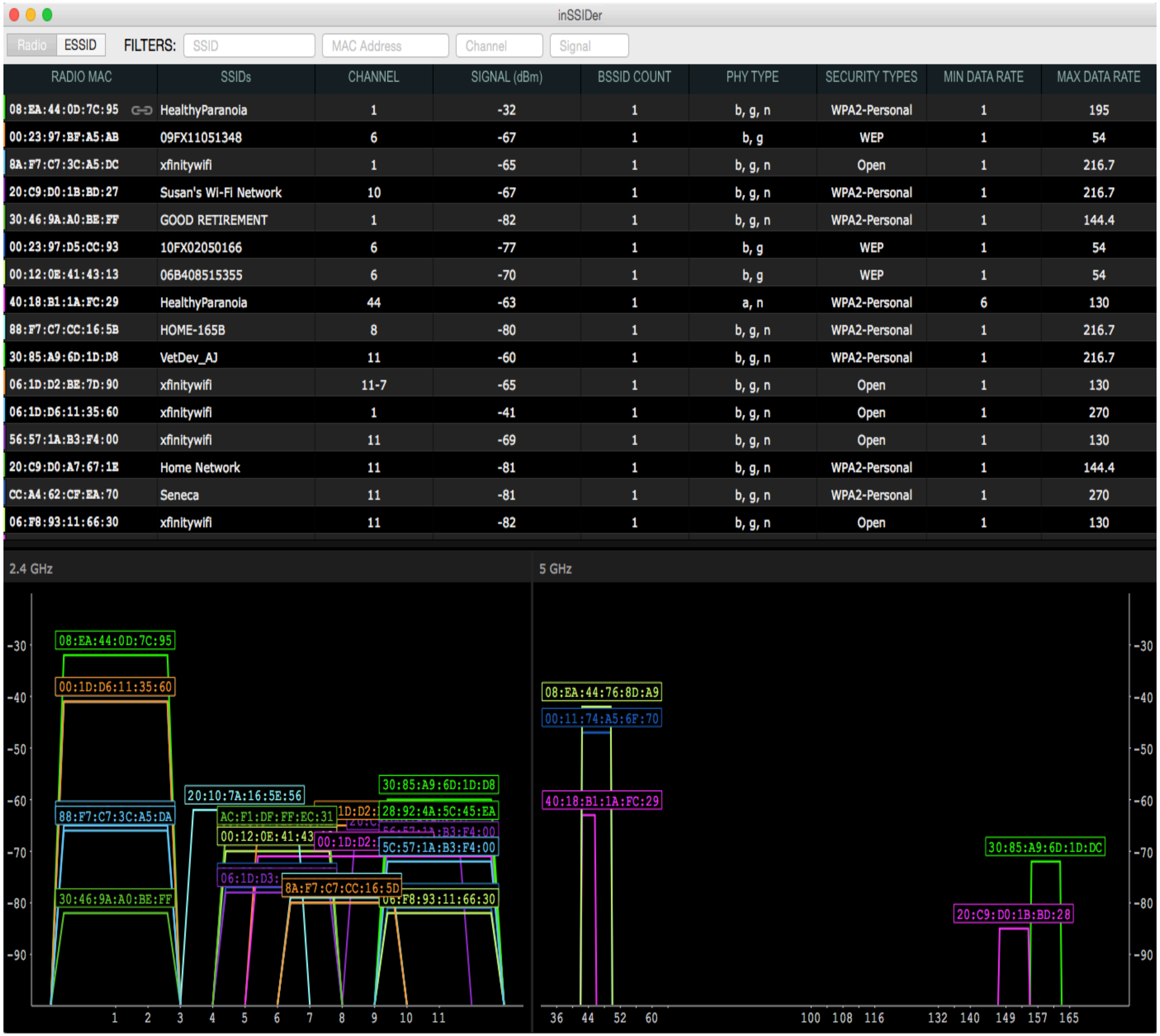
3. Once the cellphone is detected by the stingray, the phone's signal strength is measured.

4. The vehicle can then move to another location and again measure the phone's signal strength.

5. By collecting signal strength in several locations, the system can triangulate and map a phone's location.

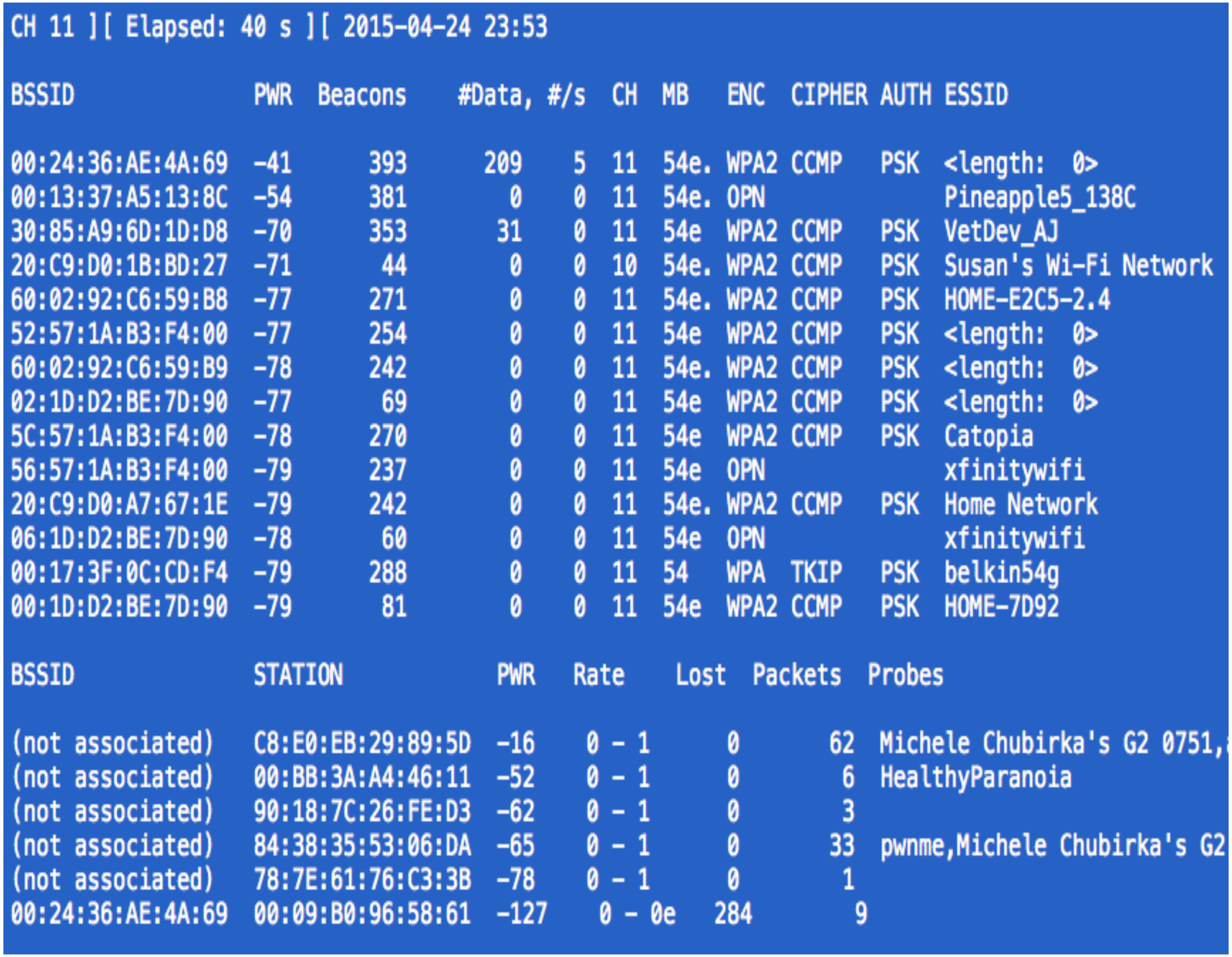
Source: WSJ research and government documents

Monitoring Wireless Networks



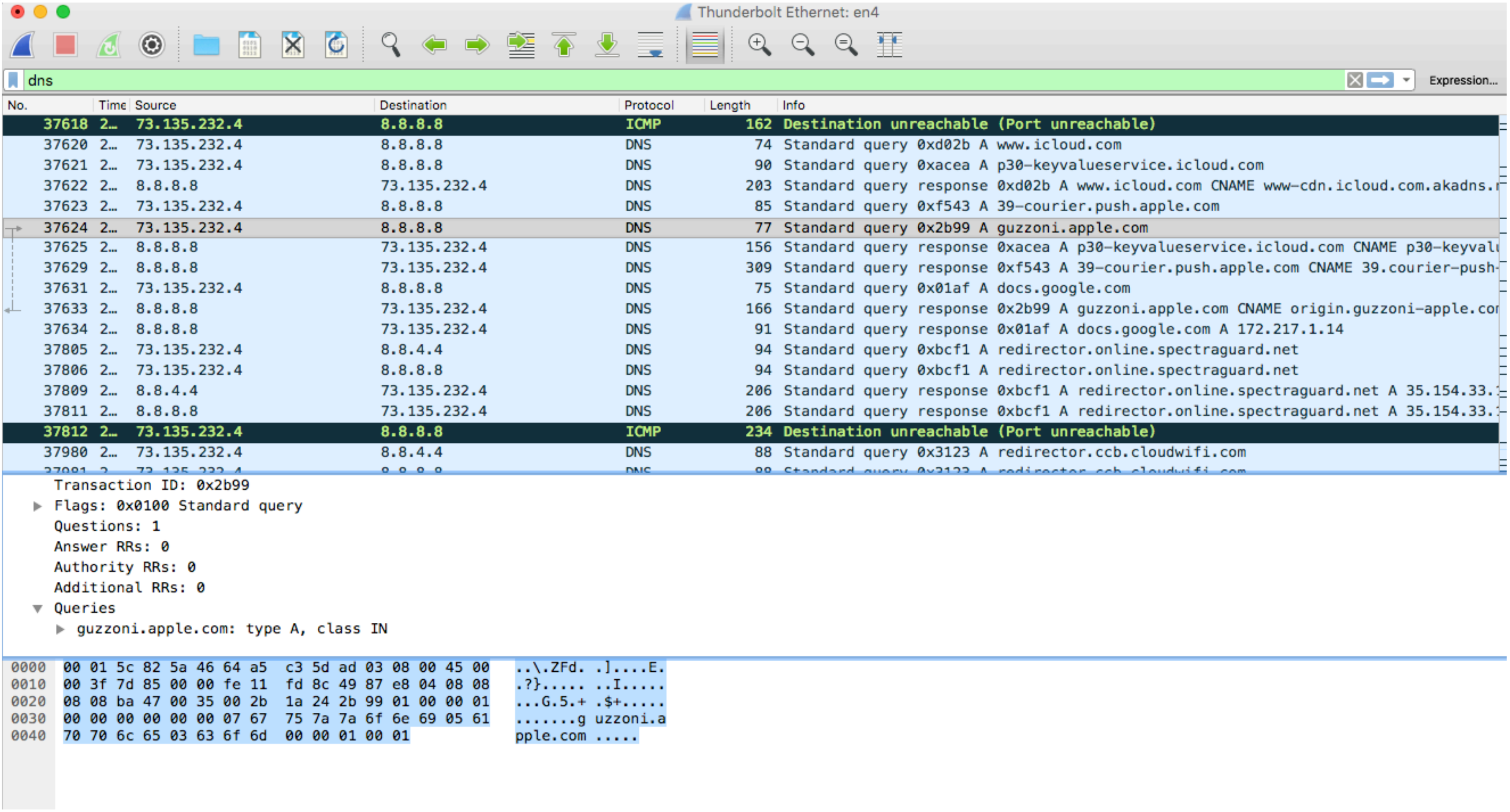
RADIO MAC	SSIDs	CHANNEL	SIGNAL (dBm)	BSSID COUNT	PHY TYPE	SECURITY TYPES	MIN DATA RATE	MAX DATA RATE
08:EA:44:0D:7C:95	HealthyParanoia	1	-32	1	b, g, n	WPA2-Personal	1	195
00:23:97:BF:A5:AB	09FX11051348	6	-67	1	b, g	WEP	1	54
8A:F7:C7:3C:A5:DC	xfinitywifi	1	-65	1	b, g, n	Open	1	216.7
20:C9:D0:1B:BD:27	Susan's Wi-Fi Network	10	-67	1	b, g, n	WPA2-Personal	1	216.7
30:46:9A:A0:BE:FF	GOOD RETIREMENT	1	-82	1	b, g, n	WPA2-Personal	1	144.4
00:23:97:D5:CC:93	10FX02050166	6	-77	1	b, g	WEP	1	54
00:12:0E:41:43:13	06B408515355	6	-70	1	b, g	WEP	1	54
40:18:B1:1A:FC:29	HealthyParanoia	44	-63	1	a, n	WPA2-Personal	6	130
88:F7:C7:CC:16:5B	HOME-165B	8	-80	1	b, g, n	WPA2-Personal	1	216.7
30:85:A9:6D:1D:D8	VetDev_AJ	11	-60	1	b, g, n	WPA2-Personal	1	216.7
06:1D:D2:BE:7D:90	xfinitywifi	11-7	-65	1	b, g, n	Open	1	130
06:1D:D6:11:35:60	xfinitywifi	1	-41	1	b, g, n	Open	1	270
56:57:1A:B3:F4:00	xfinitywifi	11	-69	1	b, g, n	Open	1	130
20:C9:D0:A7:67:1E	Home Network	11	-81	1	b, g, n	WPA2-Personal	1	144.4
CC:A4:62:CF:EA:70	Seneca	11	-81	1	b, g, n	WPA2-Personal	1	270
06:F8:93:11:66:30	xfinitywifi	11	-82	1	b, g, n	Open	1	130

Identifying Wireless User Devices



```
CH 11 ][ Elapsed: 40 s ][ 2015-04-24 23:53

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:24:36:AE:4A:69  -41      393      209    5  11  54e. WPA2 CCMP   PSK  <length:  0>
00:13:37:A5:13:8C  -54      381        0    0  11  54e. OPN              Pineapple5_138C
30:85:A9:6D:1D:D8  -70      353       31    0  11  54e  WPA2 CCMP   PSK  VetDev_AJ
20:C9:D0:1B:BD:27  -71       44        0    0  10  54e. WPA2 CCMP   PSK  Susan's Wi-Fi Network
60:02:92:C6:59:B8  -77      271        0    0  11  54e. WPA2 CCMP   PSK  HOME-E2C5-2.4
52:57:1A:B3:F4:00  -77      254        0    0  11  54e  WPA2 CCMP   PSK  <length:  0>
60:02:92:C6:59:B9  -78      242        0    0  11  54e. WPA2 CCMP   PSK  <length:  0>
02:1D:D2:BE:7D:90  -77       69        0    0  11  54e  WPA2 CCMP   PSK  <length:  0>
5C:57:1A:B3:F4:00  -78      270        0    0  11  54e  WPA2 CCMP   PSK  Catopia
56:57:1A:B3:F4:00  -79      237        0    0  11  54e  OPN              xfinitywifi
20:C9:D0:A7:67:1E  -79      242        0    0  11  54e. WPA2 CCMP   PSK  Home Network
06:1D:D2:BE:7D:90  -78       60        0    0  11  54e  OPN              xfinitywifi
00:17:3F:0C:CD:F4  -79      288        0    0  11  54   WPA  TKIP   PSK  belkin54g
00:1D:D2:BE:7D:90  -79       81        0    0  11  54e  WPA2 CCMP   PSK  HOME-7D92

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:E0:EB:29:89:5D  -16    0 - 1      0       62  Michele Chubirka's G2 0751,
(not associated)   00:BB:3A:A4:46:11  -52    0 - 1      0        6  HealthyParanoia
(not associated)   90:18:7C:26:FE:D3  -62    0 - 1      0        3
(not associated)   84:38:35:53:06:DA  -65    0 - 1      0       33  pwnme,Michele Chubirka's G2
(not associated)   78:7E:61:76:C3:3B  -78    0 - 1      0        1
00:24:36:AE:4A:69  00:09:B0:96:58:61  -127    0 - 0e   284        9
```

Network Protocol Analyzer



dns

```
No.    Time Source          Destination     Protocol Length Info
37618  2…   73.135.232.4    8.8.8.8         ICMP        162 Destination unreachable (Port unreachable)
37620  2…   73.135.232.4    8.8.8.8         DNS          74 Standard query 0xd02b A www.icloud.com
37621  2…   73.135.232.4    8.8.8.8         DNS          90 Standard query 0xacea A p30-keyvalueservice.icloud.com
37622  2…   8.8.8.8         73.135.232.4    DNS         203 Standard query response 0xd02b A www.icloud.com CNAME www-cdn.icloud.com.akadns.r
37623  2…   73.135.232.4    8.8.8.8         DNS          85 Standard query 0xf543 A 39-courier.push.apple.com
37624  2…   73.135.232.4    8.8.8.8         DNS          77 Standard query 0x2b99 A guzzoni.apple.com
37625  2…   8.8.8.8         73.135.232.4    DNS         156 Standard query response 0xacea A p30-keyvalueservice.icloud.com CNAME p30-keyvalu
37629  2…   8.8.8.8         73.135.232.4    DNS         309 Standard query response 0xf543 A 39-courier.push.apple.com CNAME 39.courier-push-
37631  2…   73.135.232.4    8.8.8.8         DNS          75 Standard query 0x01af A docs.google.com
37633  2…   8.8.8.8         73.135.232.4    DNS         166 Standard query response 0x2b99 A guzzoni.apple.com CNAME origin.guzzoni-apple.cor
37634  2…   8.8.8.8         73.135.232.4    DNS          91 Standard query response 0x01af A docs.google.com A 172.217.1.14
37805  2…   73.135.232.4    8.8.4.4         DNS          94 Standard query 0xbcf1 A redirector.online.spectraguard.net
37806  2…   73.135.232.4    8.8.8.8         DNS          94 Standard query 0xbcf1 A redirector.online.spectraguard.net
37809  2…   8.8.4.4         73.135.232.4    DNS         206 Standard query response 0xbcf1 A redirector.online.spectraguard.net A 35.154.33.1
37811  2…   8.8.8.8         73.135.232.4    DNS         206 Standard query response 0xbcf1 A redirector.online.spectraguard.net A 35.154.33.1
37812  2…   73.135.232.4    8.8.8.8         ICMP        234 Destination unreachable (Port unreachable)
37980  2…   73.135.232.4    8.8.4.4         DNS          88 Standard query 0x3123 A redirector.ccb.cloudwifi.com
37981  2…   73.135.232.4    8.8.8.8         DNS          88 Standard query 0x3123 A redirector.ccb.cloudwifi.com
```

```
    Transaction ID: 0x2b99
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ guzzoni.apple.com: type A, class IN
```

```
0000  00 01 5c 82 5a 46 64 a5  c3 5d ad 03 08 00 45 00   ..\.ZFd. .]....E.
0010  00 3f 7d 85 00 00 fe 11  fd 8c 49 87 e8 04 08 08   .?}..... ..I.....
0020  08 08 ba 47 00 35 00 2b  1a 24 2b 99 01 00 00 01   ...G.5.+ .$+.....
0030  00 00 00 00 00 00 07 67  75 7a 7a 6f 6e 69 05 61   .......g uzzoni.a
0040  70 70 6c 65 03 63 6f 6d  00 00 01 00 01            pple.com .....
```

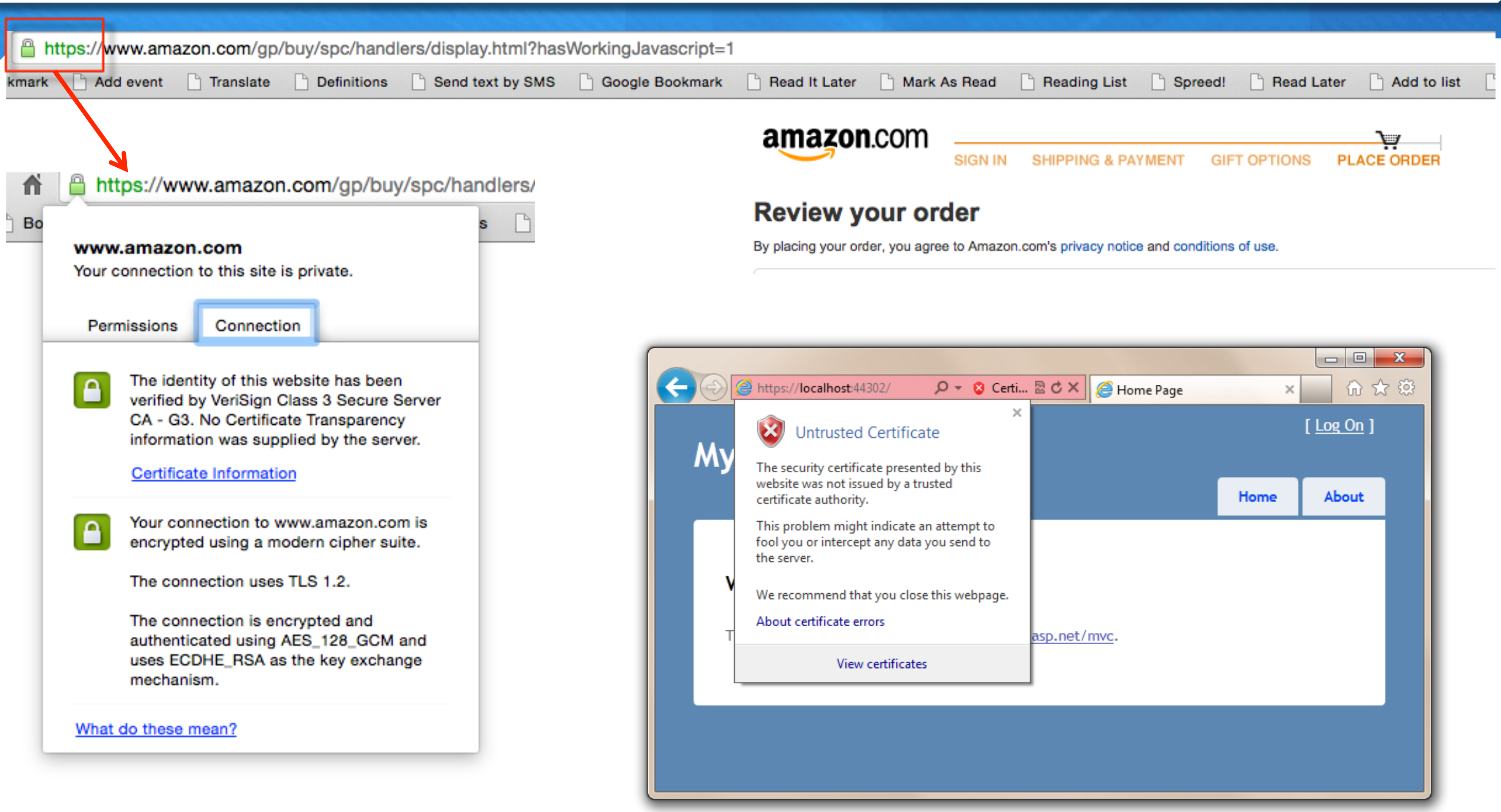
Online Security Basics

- Email Links are dangerous. Use caution.
- Don't open attachments you aren't expecting. Scan with an AV program prior to opening.
- Be careful when sharing information on social media.
- Use secure, encrypted connections when transmitting personal information.
- Never send passwords in email.
- Avoid using public computers in libraries or hotels.
- Don't use Wi-Fi in airports, coffee shops or hotels. If you must, use a VPN.
- Never leave passwords, credit card numbers or your SSN unencrypted in email, in the cloud or on your computer.
- Shred anything with your data before throwing away.

Data Privacy Principles

- Identify and categorize your personal data in terms of risk. The most sensitive information deserves the greatest care.
- Minimize the creation of sensitive data.
- Delete any sensitive data whenever possible.
- Encrypt any of this data that can’t be deleted.

How to Verify a Secure Browser Connection



https://www.amazon.com/gp/buy/spc/handlers/display.html?hasWorkingJavascript=1

https://www.amazon.com/gp/buy/spc/handlers/

www.amazon.com

Your connection to this site is private.

The identity of this website has been verified by VeriSign Class 3 Secure Server CA - G3. No Certificate Transparency information was supplied by the server.

Certificate Information

Your connection to www.amazon.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

What do these mean?

Review your order

By placing your order, you agree to Amazon.com's privacy notice and conditions of use.

Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

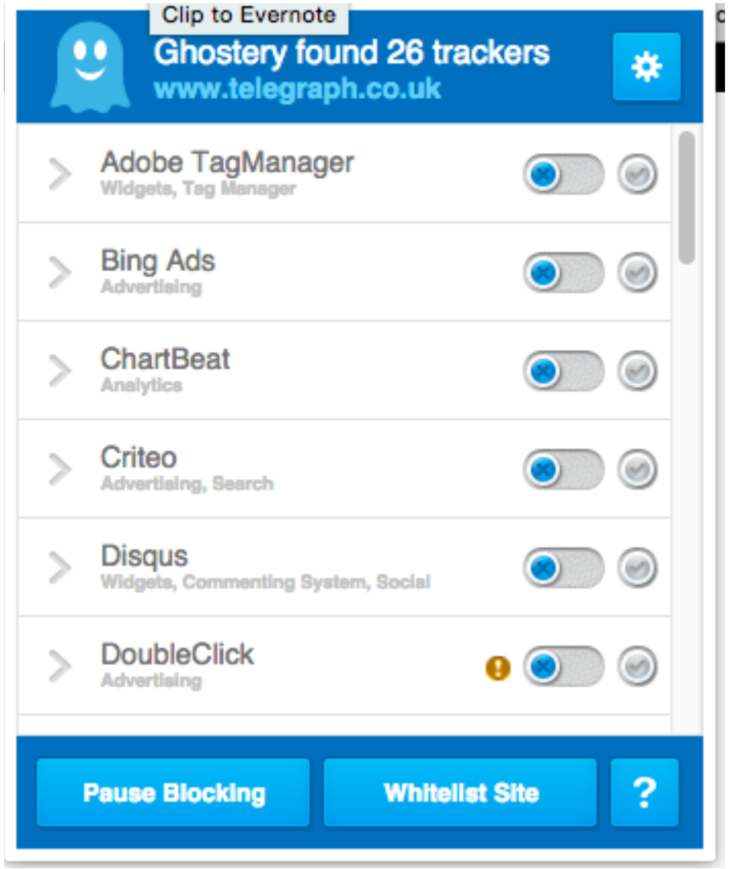
View certificates

Securing Your Browser (and Your Privacy)

- Web browsers can be dangerous. Information they collect and store can be used by malicious actors for surveillance. A web browser can also be used to deliver malware or backdoors.

- Helpful tools:
  - Tor browser (there are mobile versions for Android and iOS)
  - Privacy Badger
  - Ghostery privacy extension
  - Incognito mode in Chrome or private browsing in Firefox.
  - Search engines without personalization or tracking
    - DuckDuckGo https://duckduckgo.com/
    - searX https://searx.me/
    - Startpage https://www.startpage.com/
    - Trackmenot https://addons.mozilla.org/en-us/firefox/addon/trackmenot/
  - Avoid Flash and other helper apps, they leak information. Disable by default.
  - Periodically delete cache, cookies and other stored data.

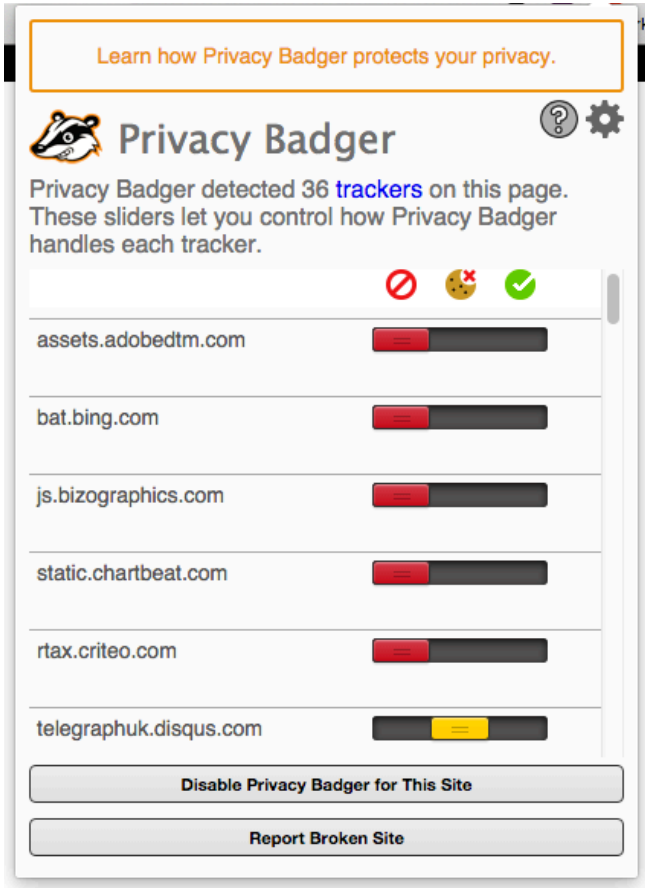
Ghostery and Privacy Badger



Clip to Evernote

Ghostery found 26 trackers
www.telegraph.co.uk

- Adobe TagManager
  Widgets, Tag Manager
- Bing Ads
  Advertising
- ChartBeat
  Analytics
- Criteo
  Advertising, Search
- Disqus
  Widgets, Commenting System, Social
- DoubleClick
  Advertising



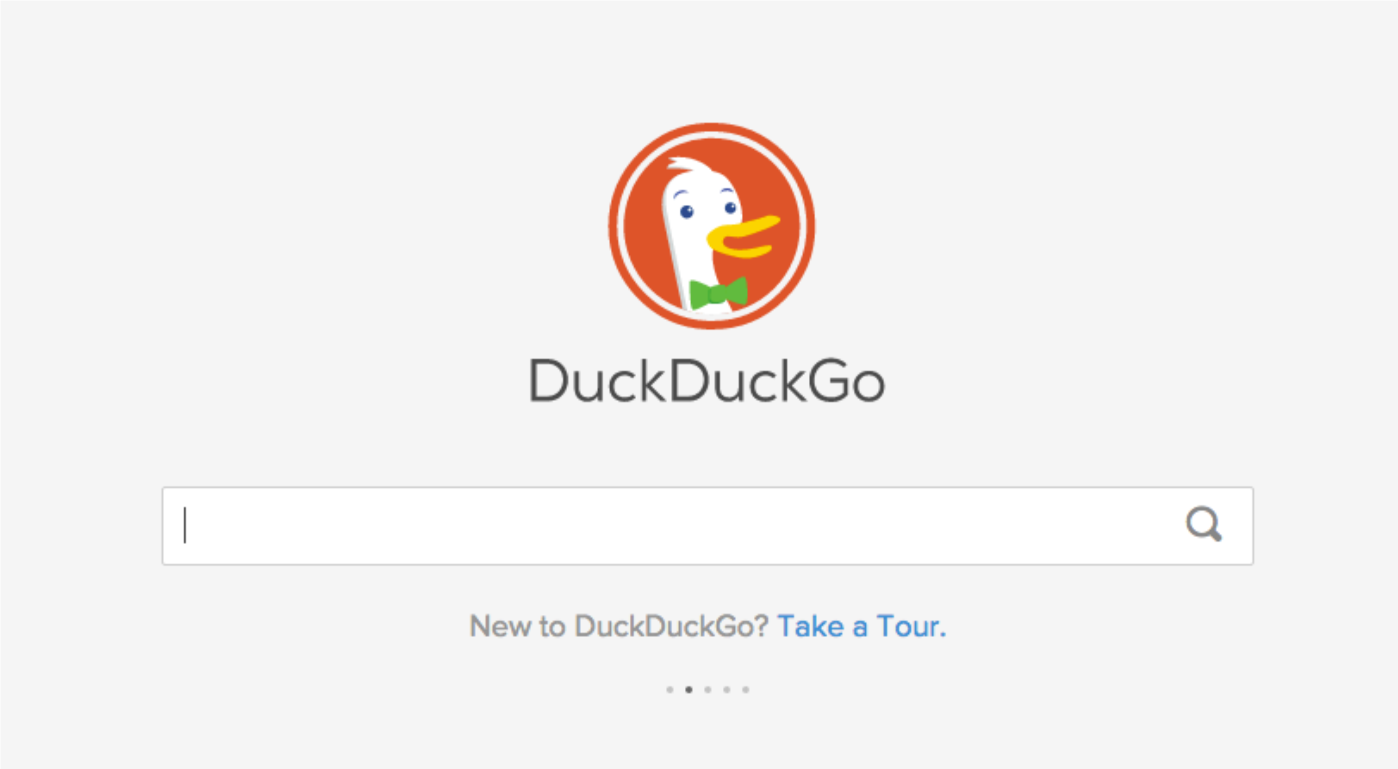
Learn how Privacy Badger protects your privacy.

Privacy Badger

Privacy Badger detected 36 trackers on this page. These sliders let you control how Privacy Badger handles each tracker.

- assets.adobedtm.com
- bat.bing.com
- js.bizographics.com
- static.chartbeat.com
- rtax.criteo.com
- telegraphuk.disqus.com

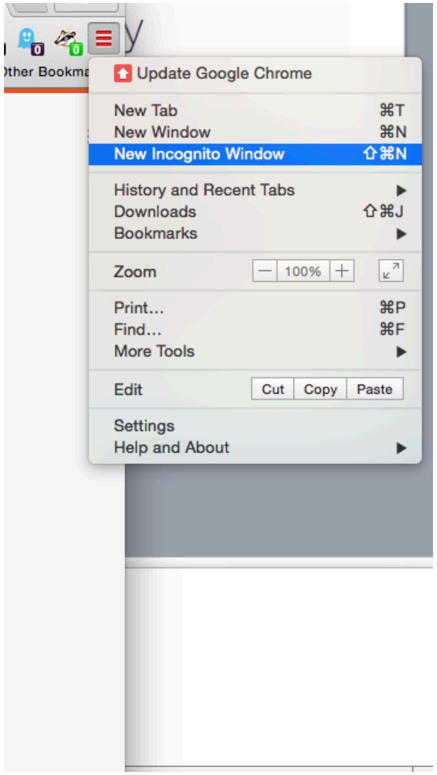
Secure Searching

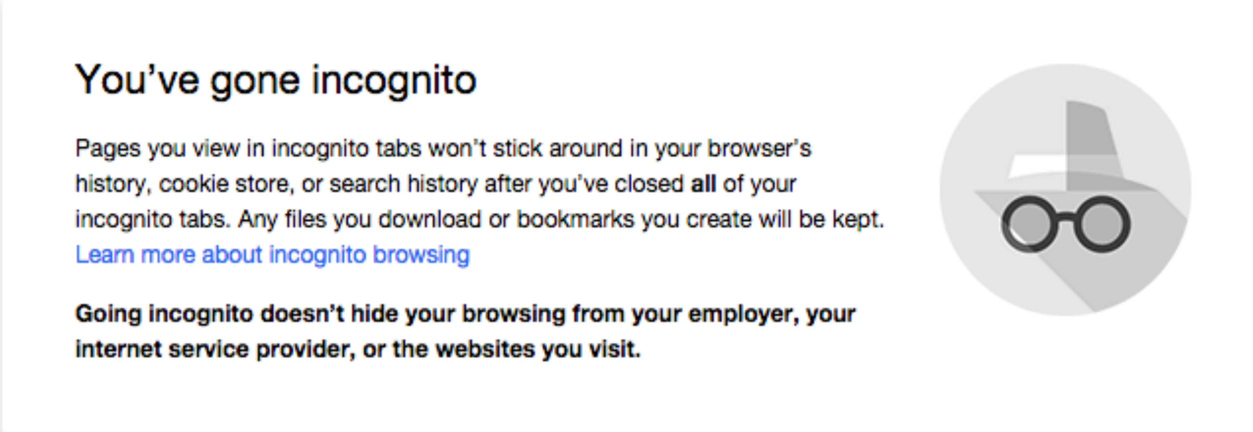


New to DuckDuckGo? Take a Tour.

DuckDuckGo is a non-tracking search engine
https://duckduckgo.com/

Chrome and Firefox Private Browsing

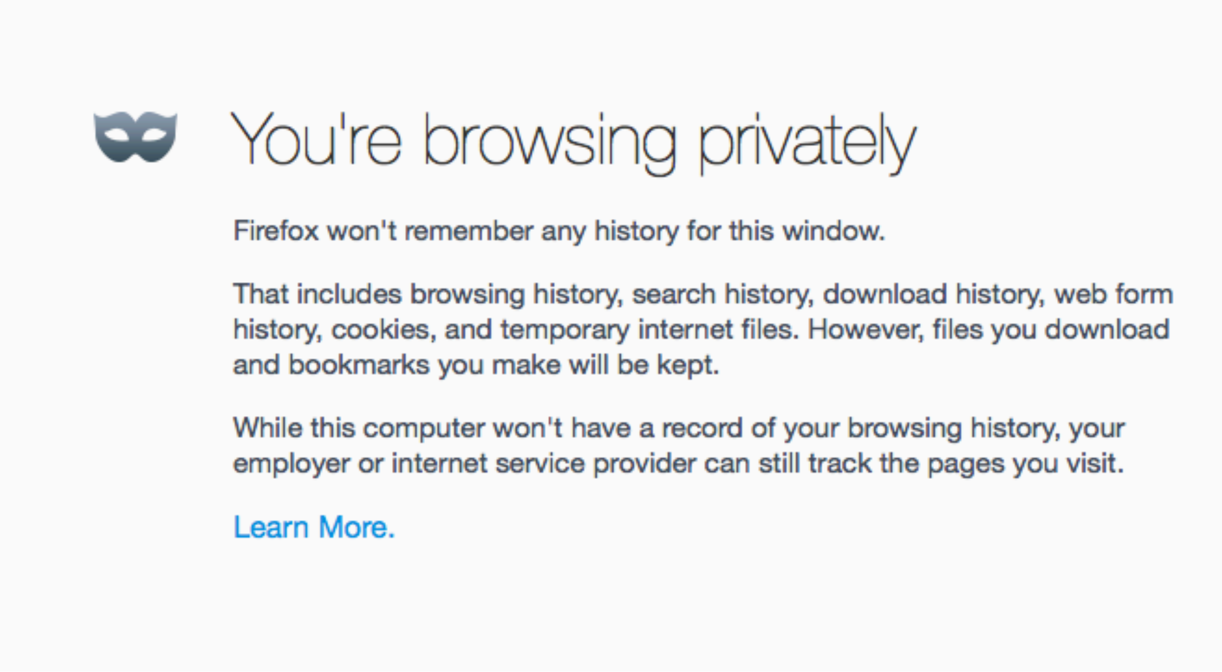




You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed **all** of your incognito tabs. Any files you download or bookmarks you create will be kept. Learn more about incognito browsing

Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.



You're browsing privately

Firefox won't remember any history for this window.

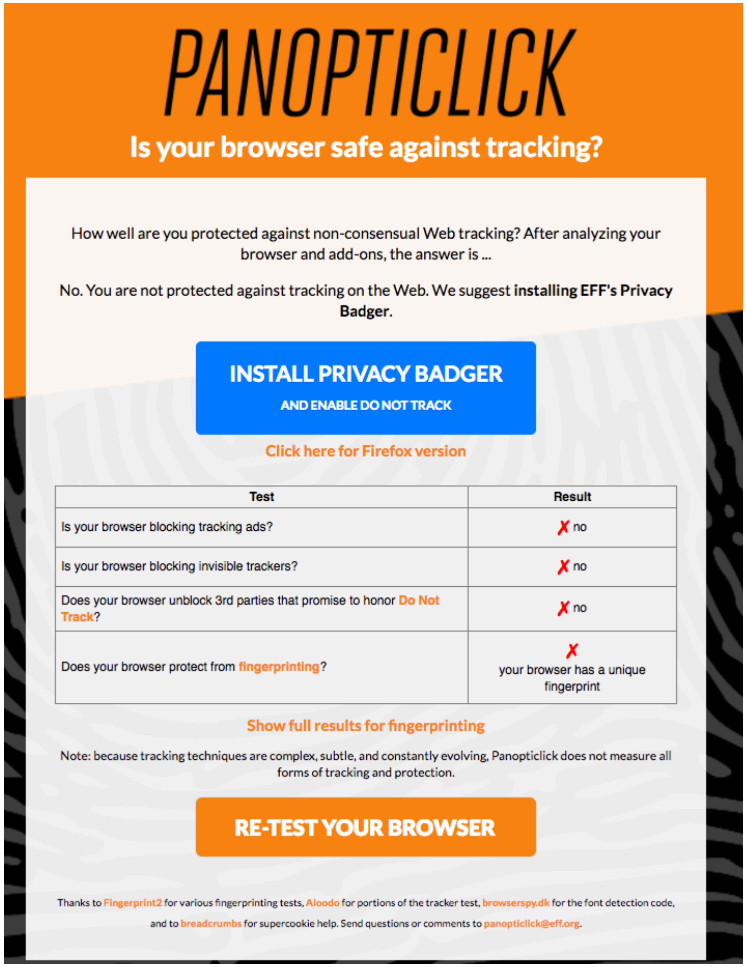
That includes browsing history, search history, download history, web form history, cookies, and temporary internet files. However, files you download and bookmarks you make will be kept.

While this computer won't have a record of your browsing history, your employer or internet service provider can still track the pages you visit.

Learn More.

Panopticlick

https://panopticlick.eff.org/



PANOPTICLICK

Is your browser safe against tracking?

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

No. You are not protected against tracking on the Web. We suggest **installing EFF's Privacy Badger**.

INSTALL PRIVACY BADGER
AND ENABLE DO NOT TRACK

Click here for Firefox version

Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

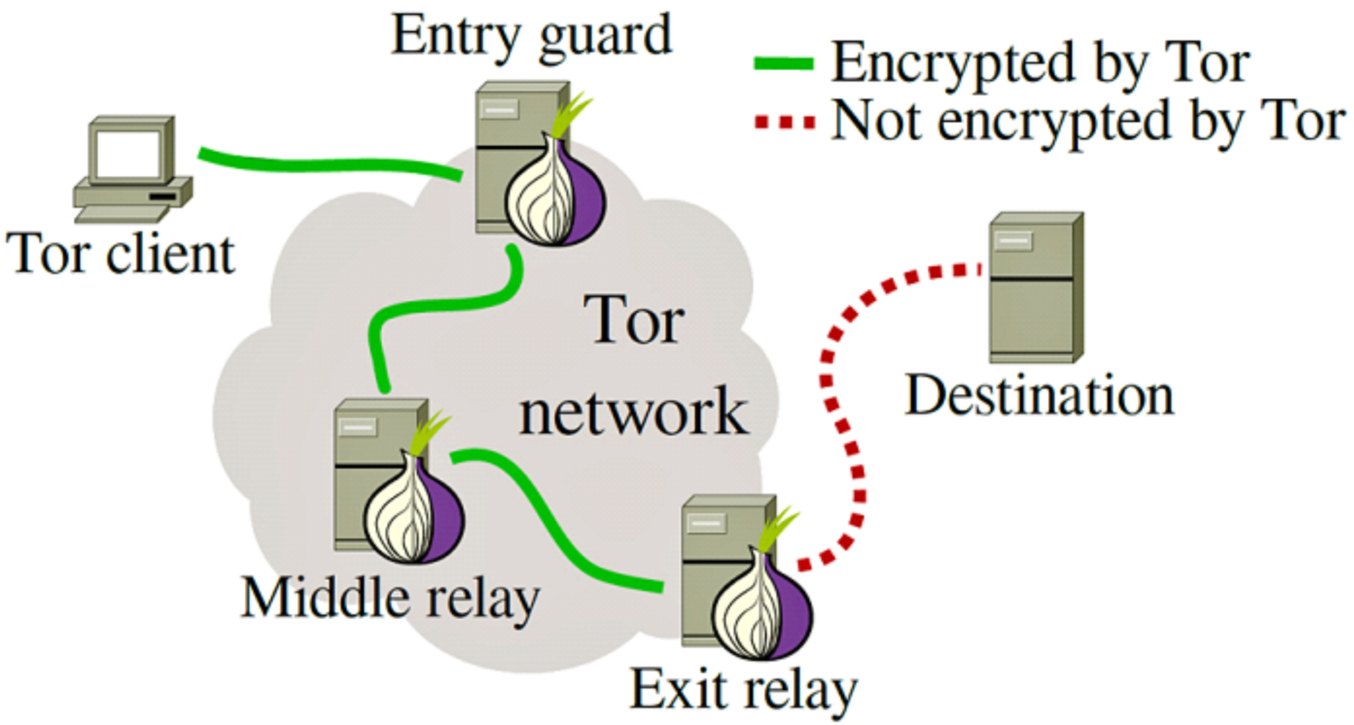
Show full results for fingerprinting

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

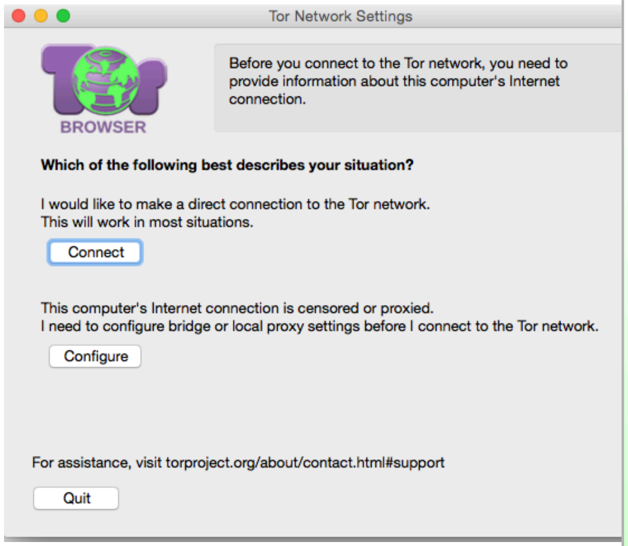
RE-TEST YOUR BROWSER

Thanks to Fingerprint2 for various fingerprinting tests, Aloodo for portions of the tracker test, browserspy.dk for the font detection code, and to breadcrumbs for supercookie help. Send questions or comments to panopticlick@eff.org.

Tor – the onion router



Tor Browser - https://www.torproject.org/



Tor Network Settings

Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

I would like to make a direct connection to the Tor network.
This will work in most situations.

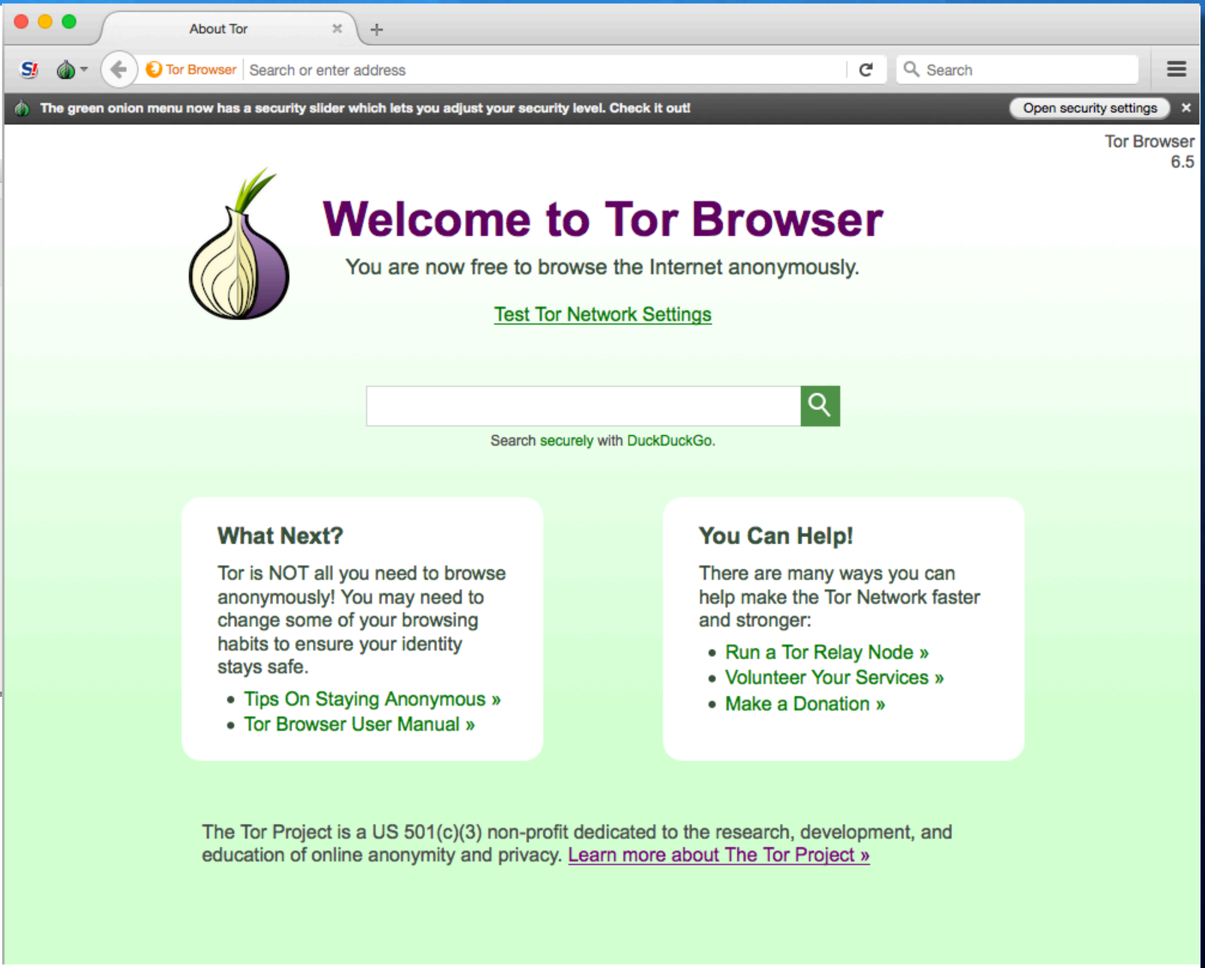
Connect

This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings before I connect to the Tor network.

Configure

For assistance, visit torproject.org/about/contact.html#support

Quit



The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Open security settings

Tor Browser
6.5

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- Tips On Staying Anonymous »
- Tor Browser User Manual »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Tor Tips

- Tor only protects applications that are configured to send Internet traffic through Tor. To avoid problems, use the pre-configured Tor Browser or Tails OS.
- The Tor Browser blocks browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address.
- Use HTTPS versions of websites. Tor will only encrypt your traffic to and within the Tor network
- Don't open documents downloaded through Tor while online, this could leak data through helper apps.
- If you must work with DOC and/or PDF files, use a disconnected computer, a virtual machine image with networking disabled, or Tails.
- Tor prevents the disclosure of websites you connect to, but it does not prevent someone learning that you're using Tor.

Personal VPNs

- Similar to Tor, Virtual Private Networks (VPNs) can provide an additional layer of protection from surveillance.
- It creates an encrypted tunnel for your traffic and can route it through another network, sometimes through another country.
- A VPN hides your original IP address and all your traffic inside the tunnel.
- Can also help to evade monitoring and censorship of Internet content.

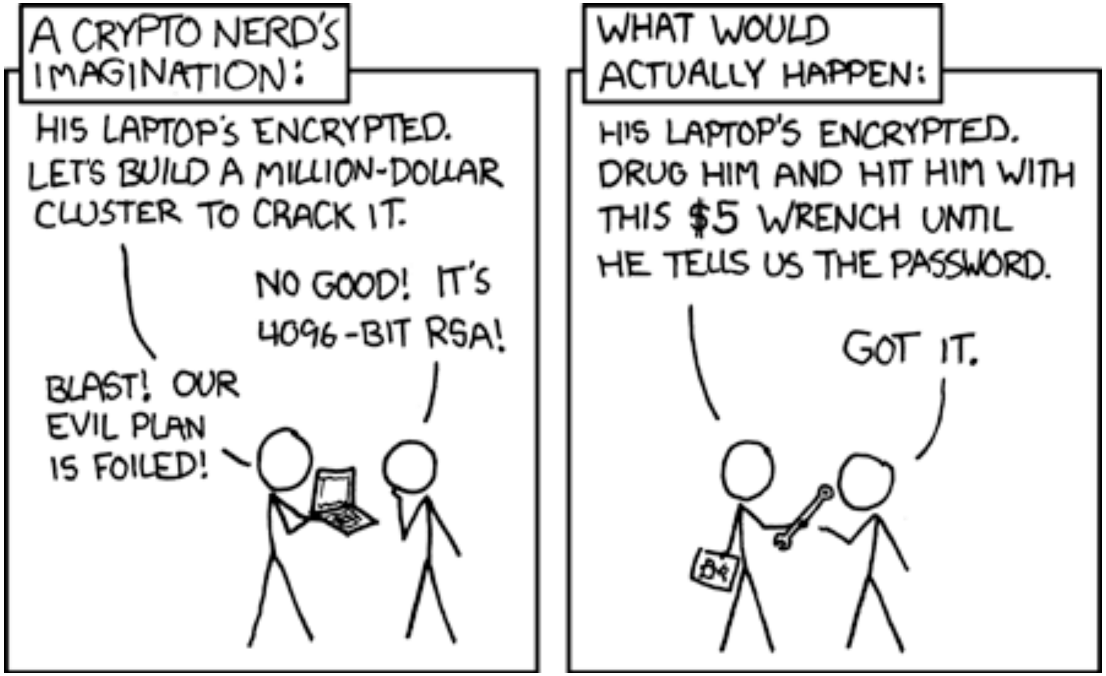
VPN Tips

- Look for a VPN provider with locations outside the US. Some have stricter privacy laws and won’t readily provide traffic logs or user data to US law enforcement.
- Focus on providers that don’t store traffic logs at all, so the history of your online activity is less likely to be tracked.

http://www.techradar.com/news/the-best-vpn-services-and-vpn-deals-of-2017

http://www.pcmag.com/article2/0,2817,2403388,00.asp

Encryption


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Cryptography Basics

- Encryption is the technique of obfuscating data to prevent unauthorized access.
- Cryptographic tools can provide the following:
  - Confidentiality – keeping information private through encryption
  - Integrity – making sure data hasn't been altered
  - Authentication- ensuring identity
  - Non-repudiation – preventing refutation

Always ask yourself, "*Who has the keys*?" If it isn't you, that organization can be forced to provide them to law enforcement.

Encryption Use-Cases

- Encryption-at-rest means data on a device is stored encrypted (a computer disk or mobile device).
- Encryption-in-transit means data is encrypted while in motion over a network (HTTPS).
- Full disk or device encryption is used to prevent unauthorized *physical* access to information on a device.
- Email encryption can be used to ensure confidentiality, integrity and non-repudiation of email communication.
- Encrypted chat and text messaging is used to ensure confidentiality of communication in transit. Sometimes integrity and non-repudiation as well.

Encryption Tools

- FileVault on OSX or Bitlocker on Windows
- Android and iOS have native encryption
- For email: Thunderbird with the Enigmail plugin, Protonmail, Virtru, Voltage, Hushmail
- With chat: ChatSecure, Zom Mobile Messenger, Pidgin or Adium and OTR (off the record)
- Text messaging: Signal, WhatsApp

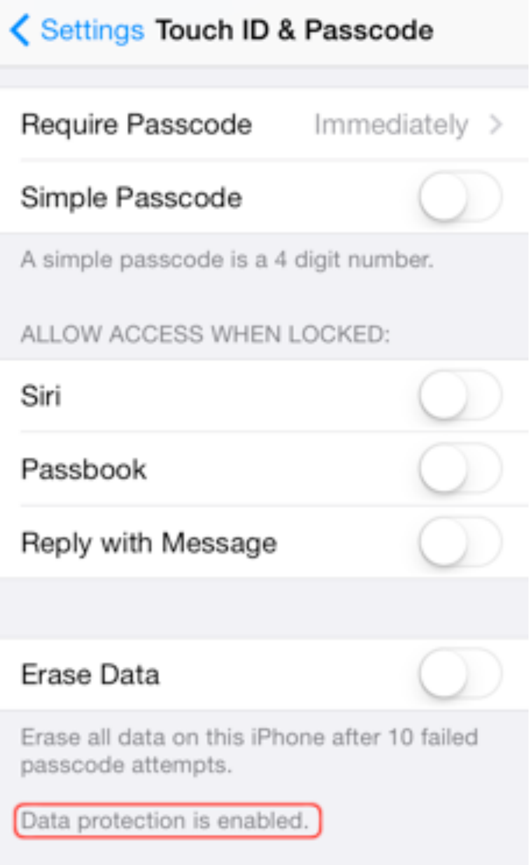
Why Encryption Fails

- Poor password (i.e. key)
- Unsecured password/key
- Physical access to a running device (Cold Boot Attack, Evil Maid Attack)
- Email is sent encrypted, but stored unencrypted.
- Unencrypted chat logs are stored on a device.
- Failure to delete data securely.
- Encryption implementation has a backdoor, uses a weak cipher or implemented improperly.

Gert and Bernie on Email Security

https://postmodernsecurity.com/category/security-soc-puppets/

Turning On Encryption: iOS and Android



Settings Touch ID & Passcode

Require Passcode Immediately

Simple Passcode ○

A simple passcode is a 4 digit number.

ALLOW ACCESS WHEN LOCKED:

Siri ○

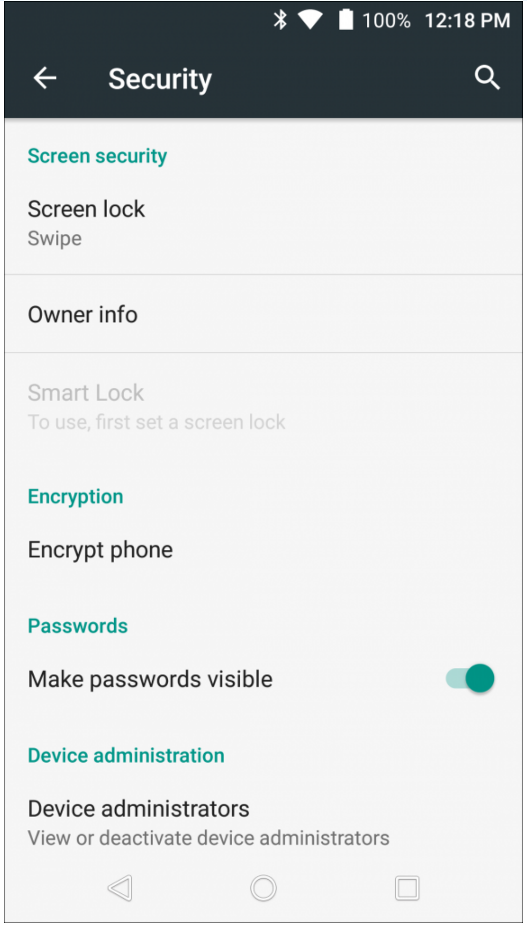
Passbook ○

Reply with Message ○

Erase Data ○

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.



100% 12:18 PM

Security

Screen security

Screen lock
Swipe

Owner info

Smart Lock
To use, first set a screen lock

Encryption

Encrypt phone

Passwords

Make passwords visible ●

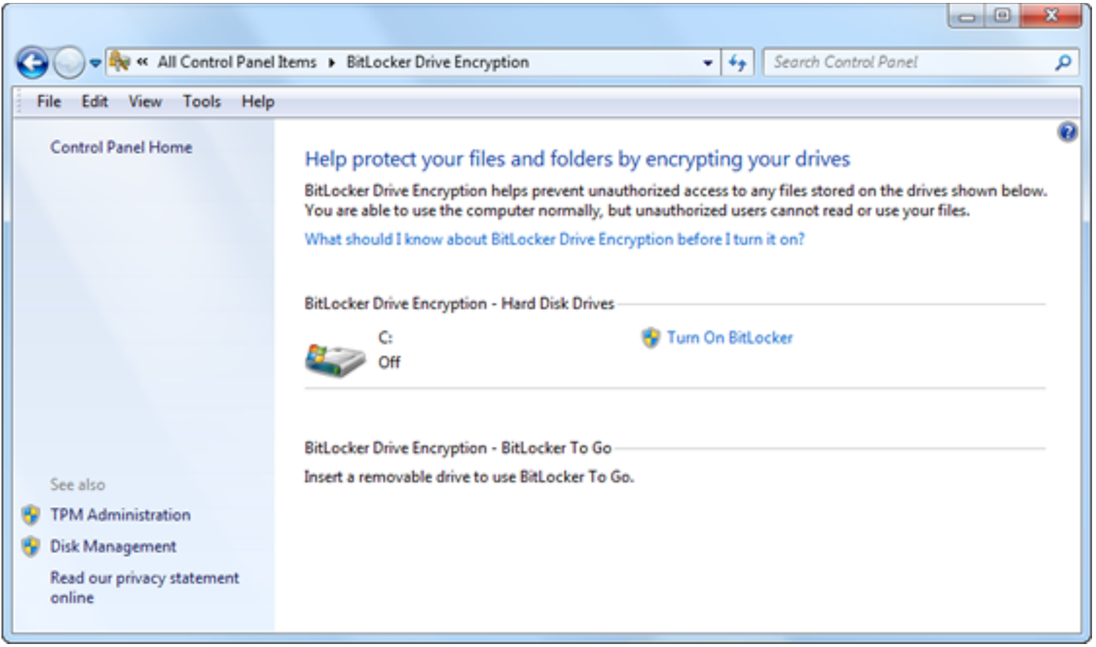
Device administration

Device administrators
View or deactivate device administrators

How to encrypt an iPhone http://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/

How to encrypt Android https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/

Enable Encryption: Windows and OSX



« All Control Panel Items ▸ BitLocker Drive Encryption
Search Control Panel
File Edit View Tools Help
Control Panel Home
See also
TPM Administration
Disk Management
Read our privacy statement online

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

What should I know about BitLocker Drive Encryption before I turn it on?

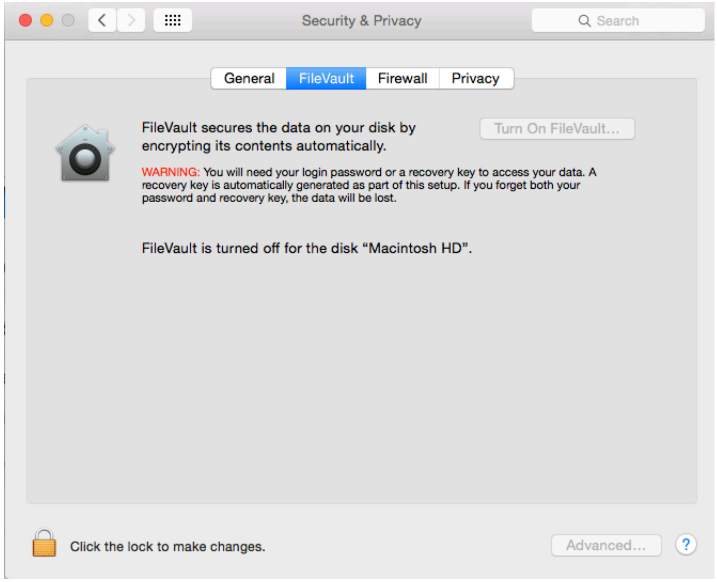
BitLocker Drive Encryption - Hard Disk Drives

C:
Off

Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

Insert a removable drive to use BitLocker To Go.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

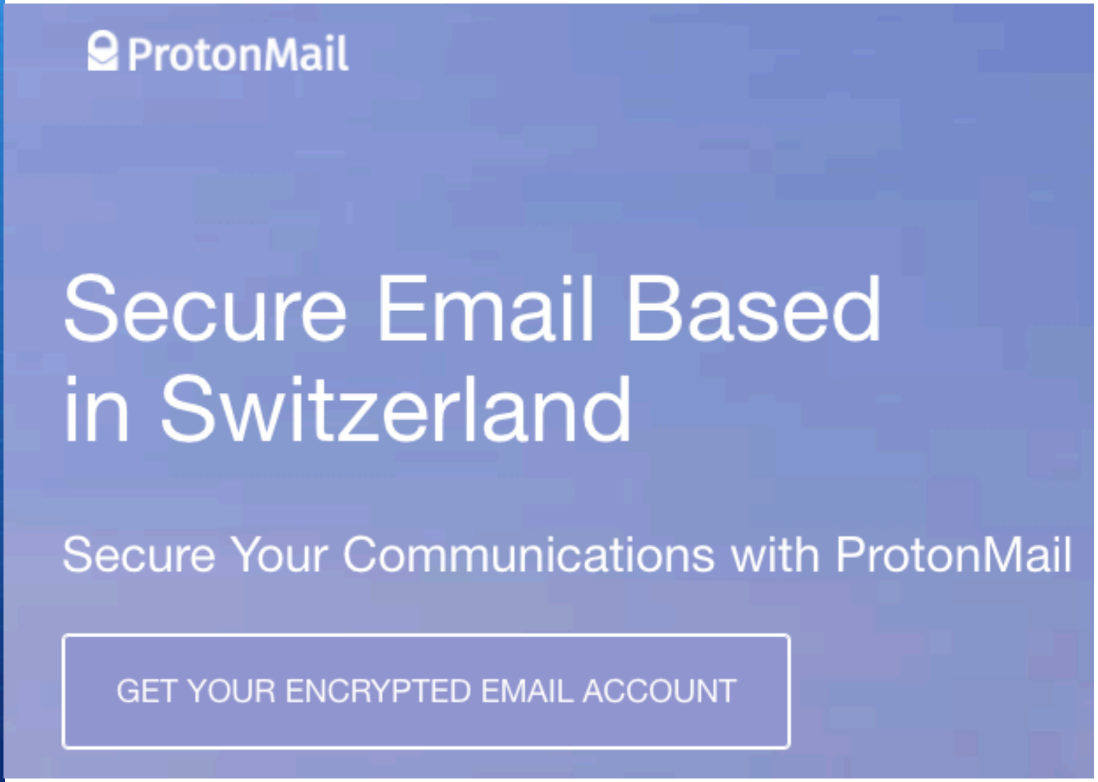
FileVault is turned off for the disk “Macintosh HD”.

Click the lock to make changes.

Enabling Bitlocker https://uit.stanford.edu/service/encryption/wholedisk/bitlocker

Enabling FileVault https://support.apple.com/en-us/HT204837

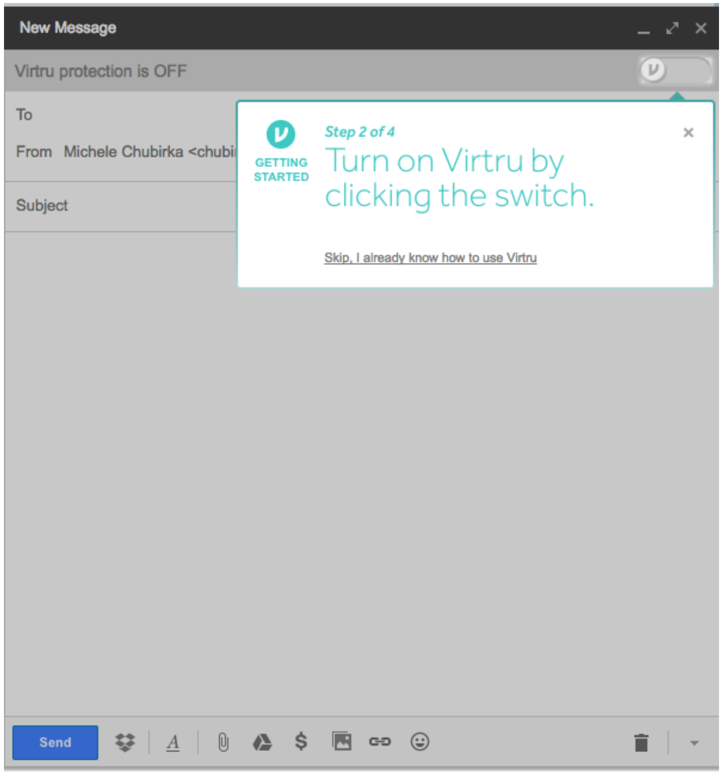
ProtonMail and Virtru



ProtonMail

Secure Email Based in Switzerland

Secure Your Communications with ProtonMail



New Message

Virtru protection is OFF

To

From Michele Chubirka <chubi

Subject

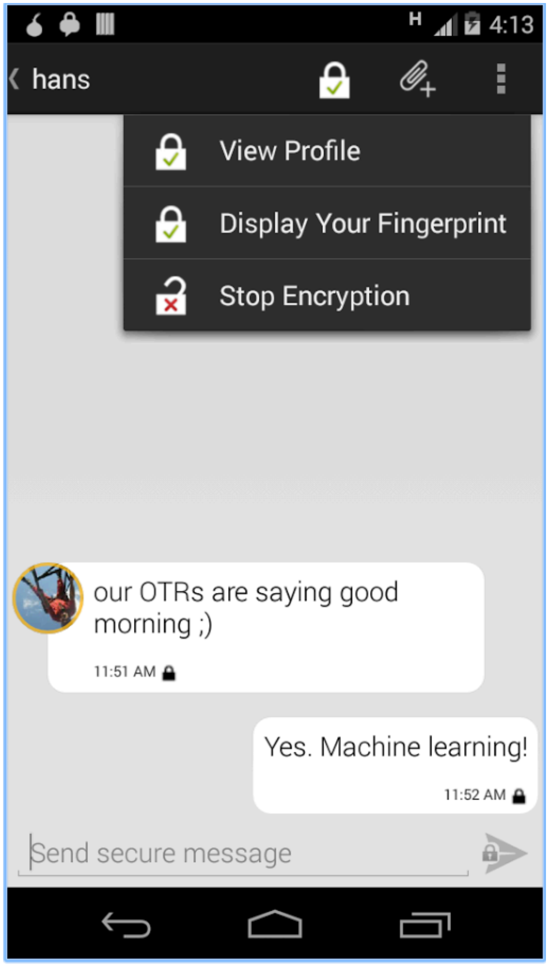
GETTING STARTED

Step 2 of 4

Turn on Virtru by clicking the switch.

Skip, I already know how to use Virtru

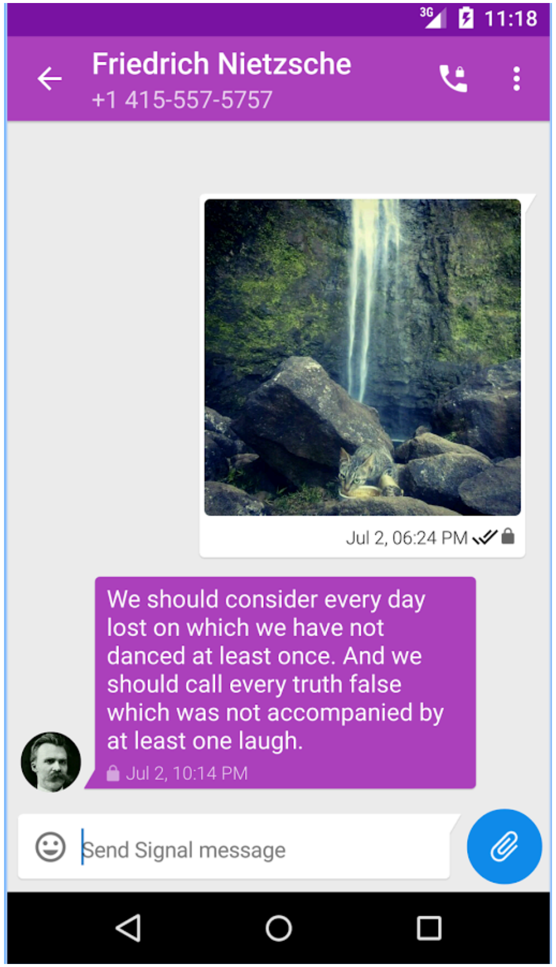
Chatsecure and Signal



our OTRs are saying good morning ;)
11:51 AM

Yes. Machine learning!
11:52 AM

Send secure message



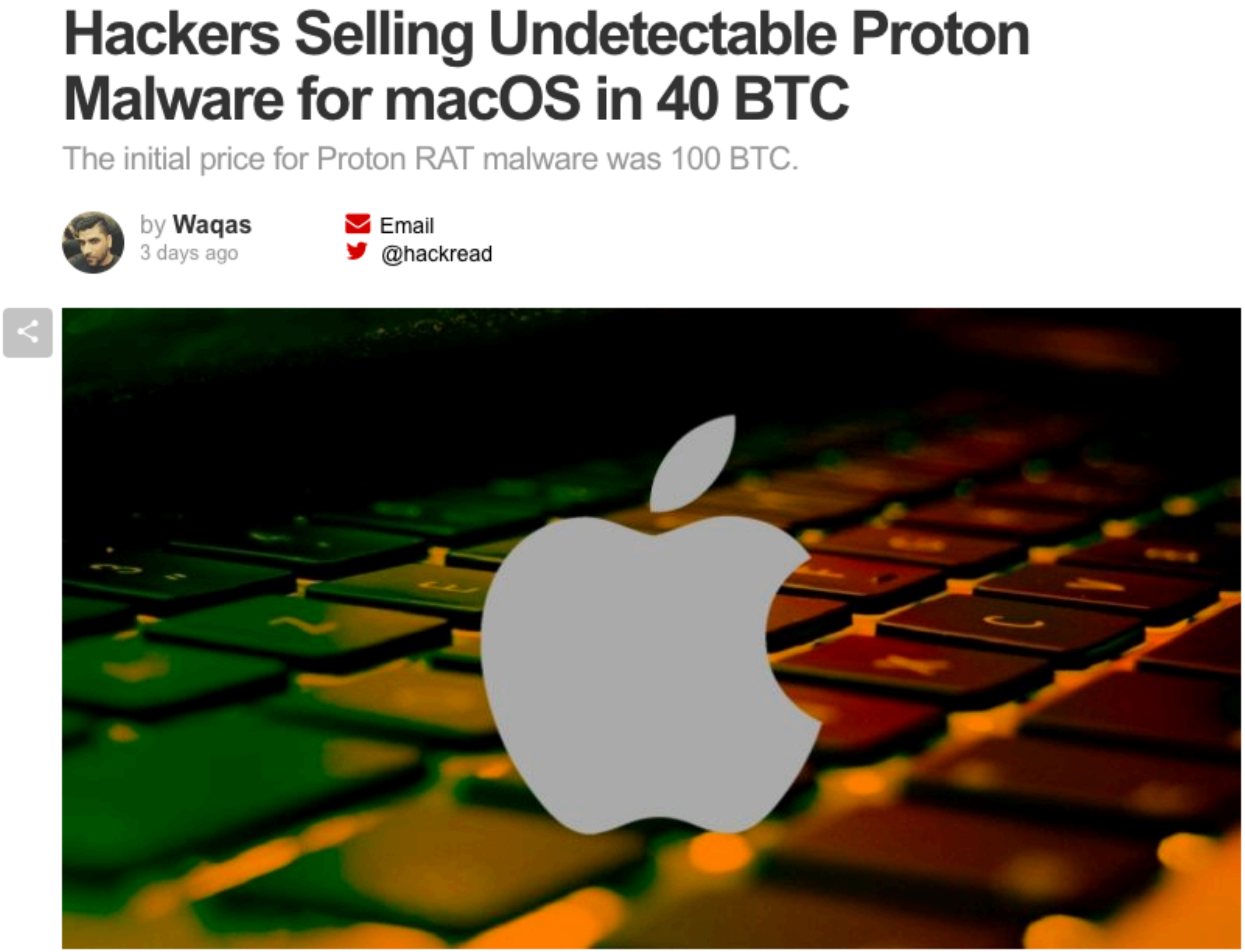
Jul 2, 06:24 PM

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.
Jul 2, 10:14 PM

Send Signal message

Endpoint Protection and Anti-Virus Software

- Yes, Macs get malware.
- Install or turn on your firewall. On OSX, it isn't enabled by default.
- Set boot and screensaver passwords.
- Apply all application patches and operating system updates.
- Make sure mobile devices (laptops, phones, tablets) have screen timeouts and are password protected. The fingerprint reader is okay, but avoid PINs.
- If your computer becomes infected with malware, reinstall it. Modern malware is difficult to remove completely.



Hackers Selling Undetectable Proton Malware for macOS in 40 BTC

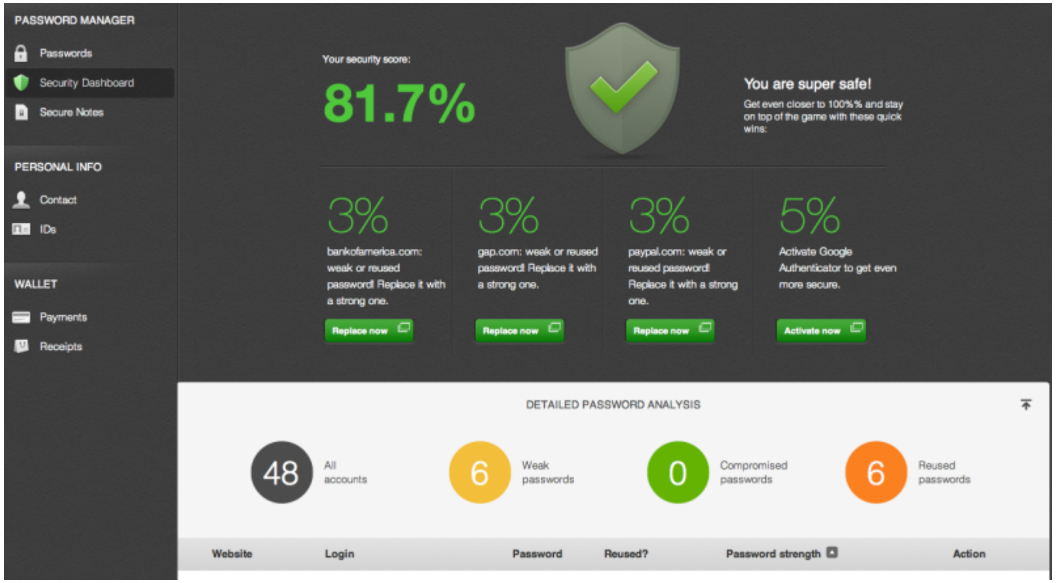
The initial price for Proton RAT malware was 100 BTC.

by **Waqas**
3 days ago

✉ Email
@hackread

https://www.hackread.com/hackers-selling-undetectable-proton-mac-malware/

Password Managers



Your security score:

81.7%

You are super safe!

Get even closer to 100%% and stay on top of the game with these quick wins:

3% bankofamerica.com: weak or reused password! Replace it with a strong one.

3% gap.com: weak or reused password! Replace it with a strong one.

3% paypal.com: weak or reused password! Replace it with a strong one.

5% Activate Google Authenticator to get even more secure.

DETAILED PASSWORD ANALYSIS

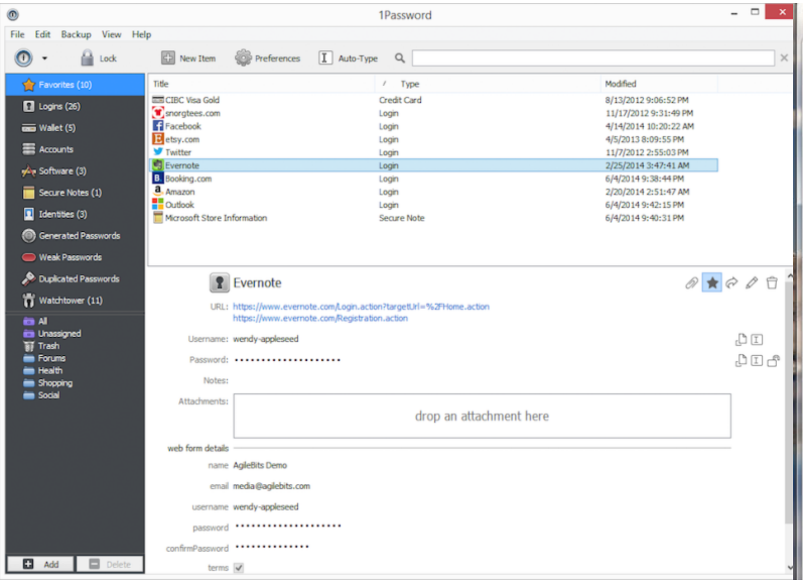
48 All accounts

6 Weak passwords

0 Compromised passwords

6 Reused passwords

Website	Login	Password	Reused?	Password strength	Action



Title	Type	Modified
CIBC Visa Gold	Credit Card	8/13/2012 9:06:52 PM
snorgtees.com	Login	11/17/2012 9:31:49 PM
Facebook	Login	4/14/2014 10:20:22 AM
etsy.com	Login	4/5/2013 8:09:55 PM
Twitter	Login	11/7/2012 2:55:03 PM
Evernote	Login	2/25/2014 3:47:41 AM
Booking.com	Login	6/4/2014 9:38:44 PM
Amazon	Login	2/20/2014 2:51:47 AM
Outlook	Login	6/4/2014 9:42:15 PM
Microsoft Store Information	Secure Note	6/4/2014 9:40:31 PM

Evernote

URL: https://www.evernote.com/Login.action?targetUrl=%2FHome.action
https://www.evernote.com/Registration.action

Username: wendy-appleseed

Password: ••••••••••••••••••••

Notes:

Attachments: drop an attachment here

web form details

name AgileBits Demo

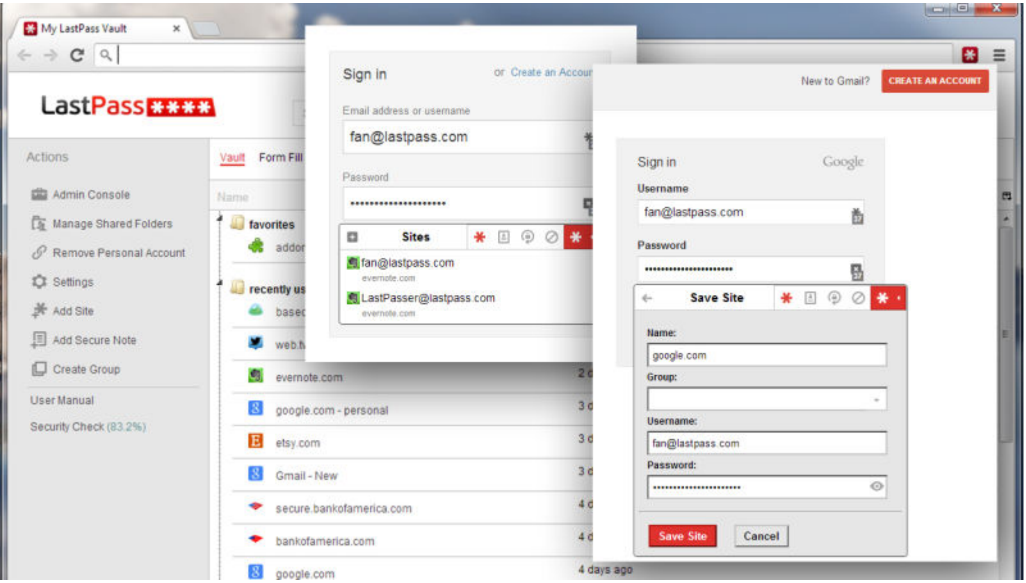
email media@agilebits.com

username wendy-appleseed

password ••••••••••••••••••••

confirmPassword ••••••••••••••

terms ☑



addor

based

web.t

evernote.com 2 d

google.com - personal 3 d

etsy.com 3 d

Gmail - New 3 d

secure.bankofamerica.com 4 d

bankofamerica.com 4 d

google.com 4 days ago

Sign in or Create an Accour

Email address or username

fan@lastpass.com

Password

••••••••••••••••••••

fan@lastpass.com
evernote.com

LastPasser@lastpass.com
evernote.com

Sign in

Username

fan@lastpass.com

Password

••••••••••••••••••••••

Name: google.com

Group:

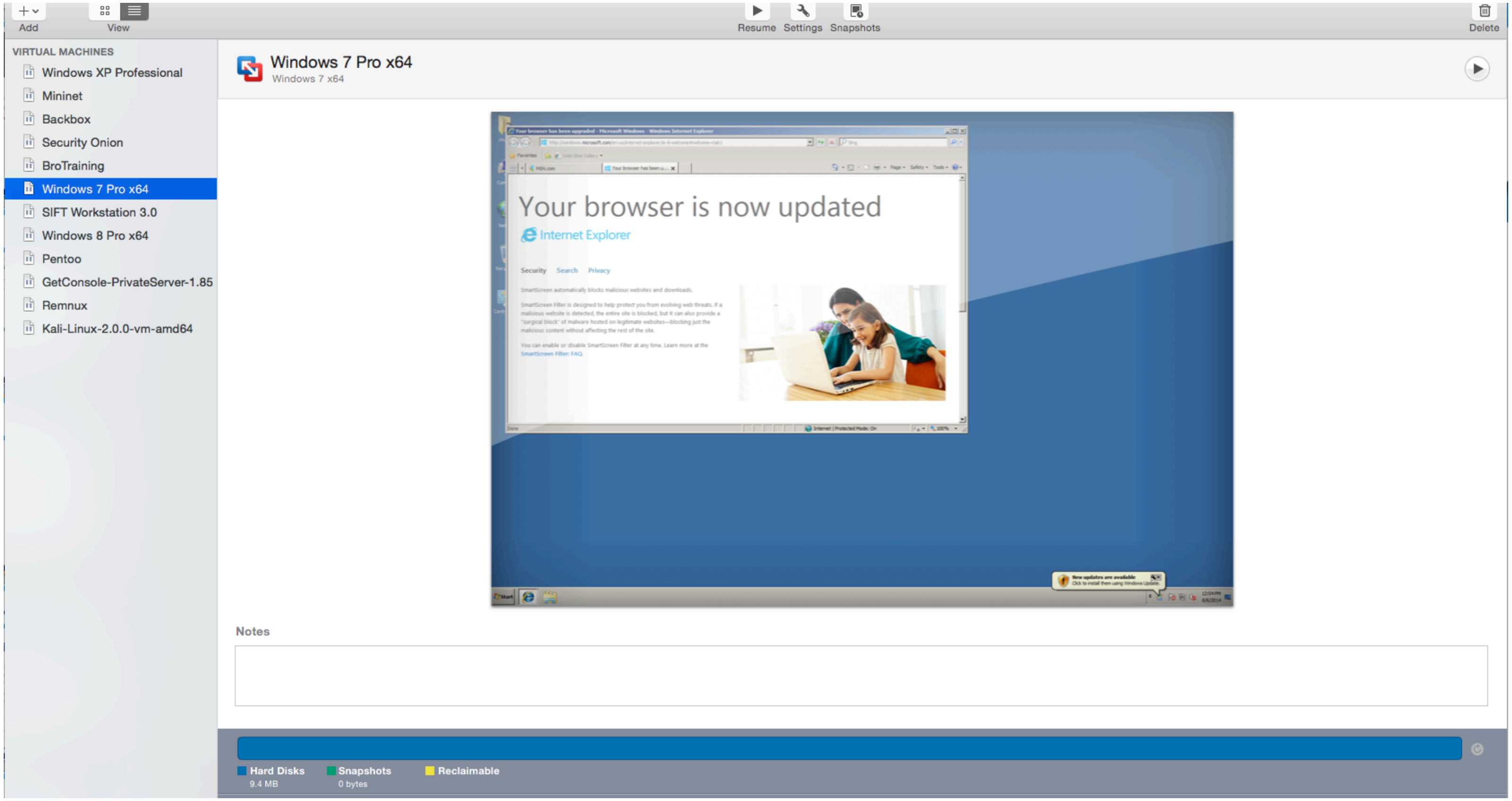
Username: fan@lastpass.com

Password: ••••••••••••••••••••••

Going Off The Grid

- Use dedicated devices prepaid phones and laptops without any personal information or accounts.
- Use special software that runs a virtualized computer image on your system and can be easily destroyed.
  - Vmware Fusion
  - Parallels
  - VirtualBox
- Boot from a read-only OS, run applications from a USB drive or a sandbox environment.
  - Tails
  - Portable Apps
  - Qubes OS

VMware Fusion: Windows on Mac



VIRTUAL MACHINES

- Windows XP Professional
- Mininet
- Backbox
- Security Onion
- BroTraining
- Windows 7 Pro x64
- SIFT Workstation 3.0
- Windows 8 Pro x64
- Pentoo
- GetConsole-PrivateServer-1.85
- Remnux
- Kali-Linux-2.0.0-vm-amd64

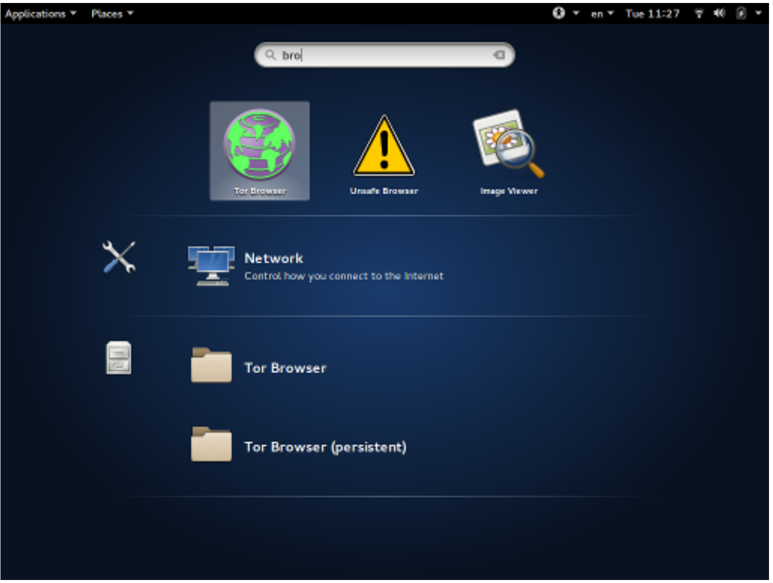
Windows 7 Pro x64
Windows 7 x64

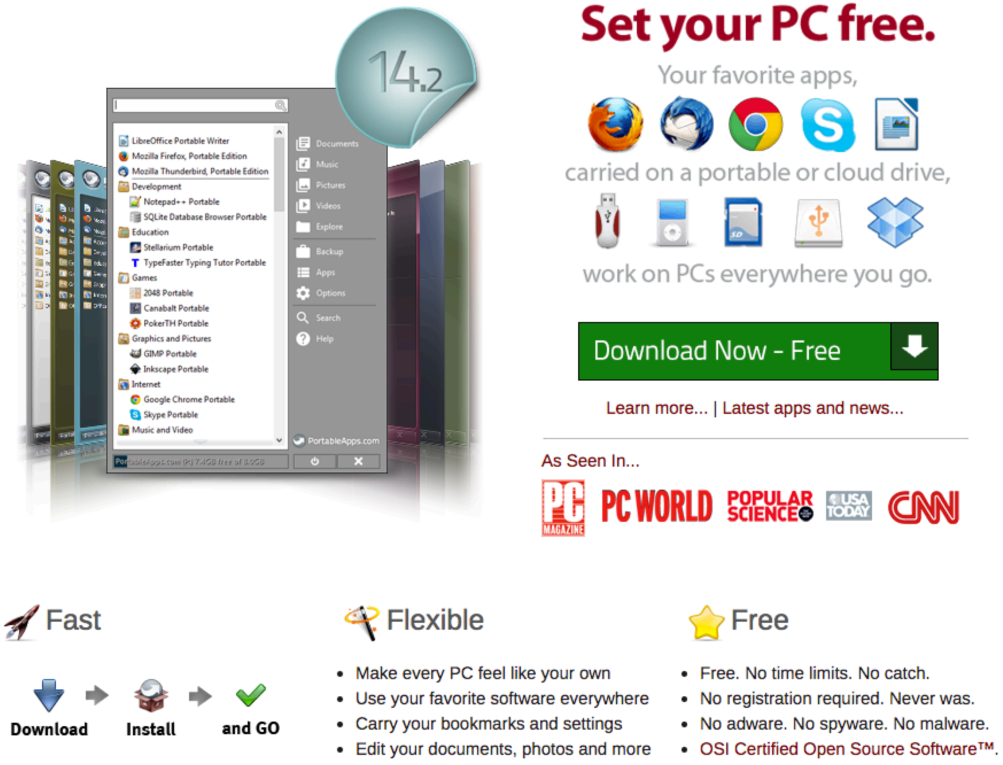
Your browser is now updated
Internet Explorer

Notes

Hard Disks 9.4 MB
Snapshots 0 bytes
Reclaimable

Tails and PortableApps





Set your PC free.

Your favorite apps,

carried on a portable or cloud drive,

work on PCs everywhere you go.

Download Now - Free

Learn more... | Latest apps and news...

As Seen In...

Fast

Download → Install → and GO

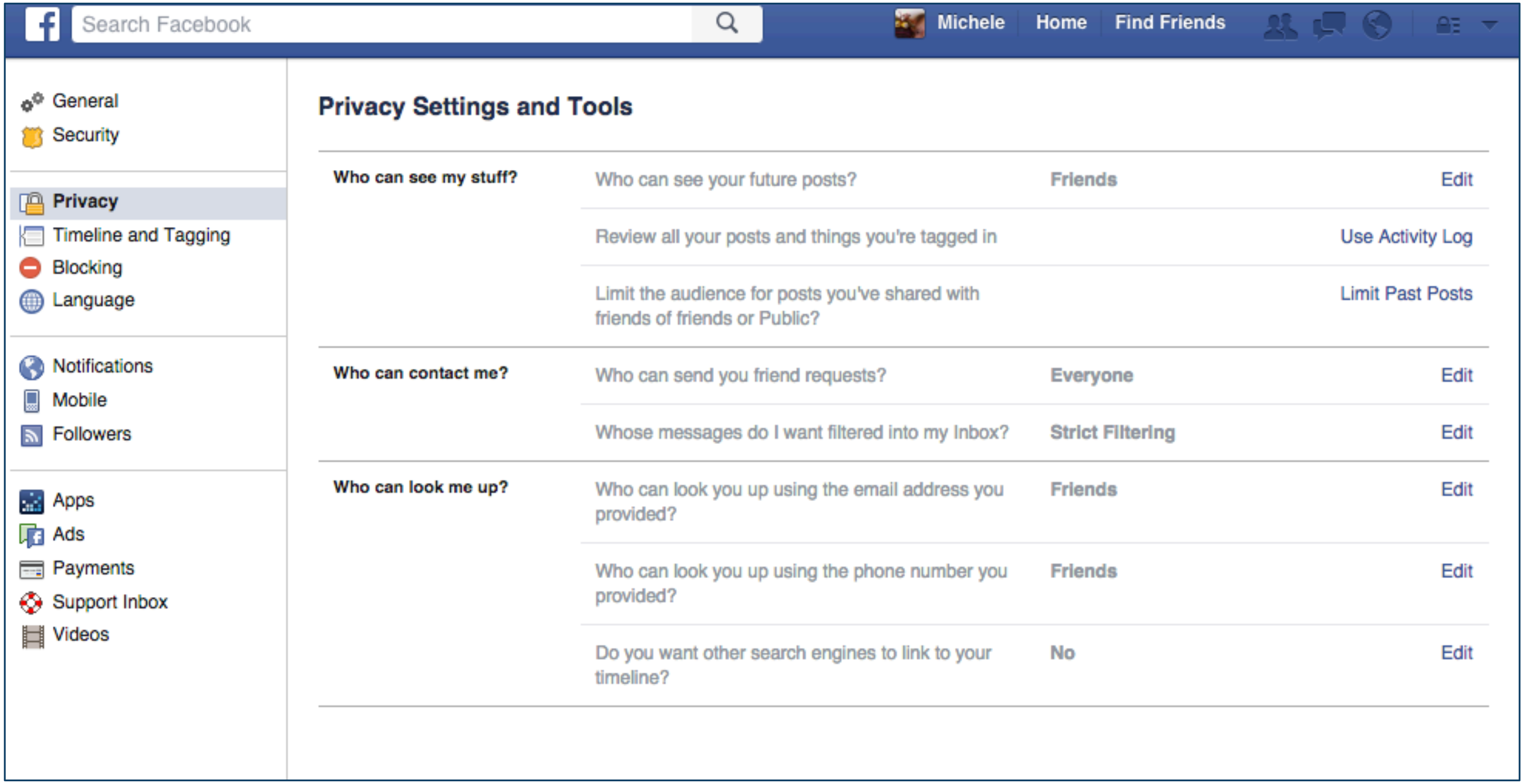
Flexible

- Make every PC feel like your own
- Use your favorite software everywhere
- Carry your bookmarks and settings
- Edit your documents, photos and more

Free

- Free. No time limits. No catch.
- No registration required. Never was.
- No adware. No spyware. No malware.
- OSI Certified Open Source Software™.

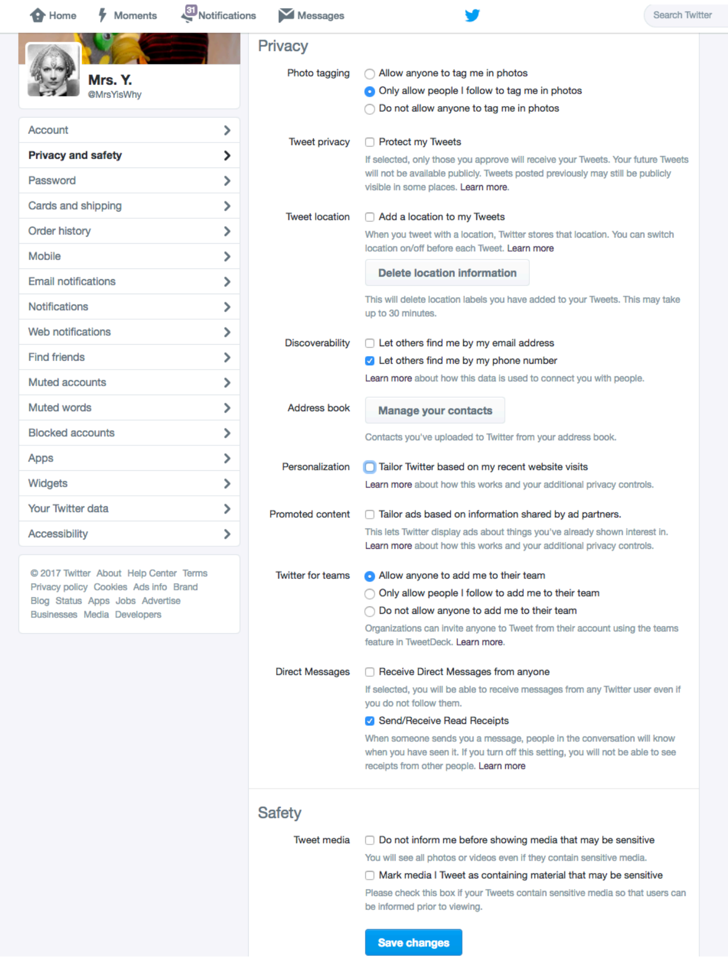
Facebook Privacy and Security Options



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose messages do I want filtered into my Inbox?	Strict Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want other search engines to link to your timeline?	No	Edit

Twitter and LinkedIn Privacy Options



Privacy

Photo tagging
- ○ Allow anyone to tag me in photos
- ● Only allow people I follow to tag me in photos
- ○ Do not allow anyone to tag me in photos

Tweet privacy
- □ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location
- □ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

Delete location information

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Discoverability
- □ Let others find me by my email address
- ☑ Let others find me by my phone number

Learn more about how this data is used to connect you with people.

Address book

Manage your contacts

Contacts you've uploaded to Twitter from your address book.

Personalization
- □ Tailor Twitter based on my recent website visits

Learn more about how this works and your additional privacy controls.

Promoted content
- □ Tailor ads based on information shared by ad partners.

This lets Twitter display ads about things you've already shown interest in. Learn more about how this works and your additional privacy controls.

Twitter for teams
- ● Allow anyone to add me to their team
- ○ Only allow people I follow to add me to their team
- ○ Do not allow anyone to add me to their team

Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. Learn more.

Direct Messages
- □ Receive Direct Messages from anyone

If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

- ☑ Send/Receive Read Receipts

When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see receipts from other people. Learn more

Safety

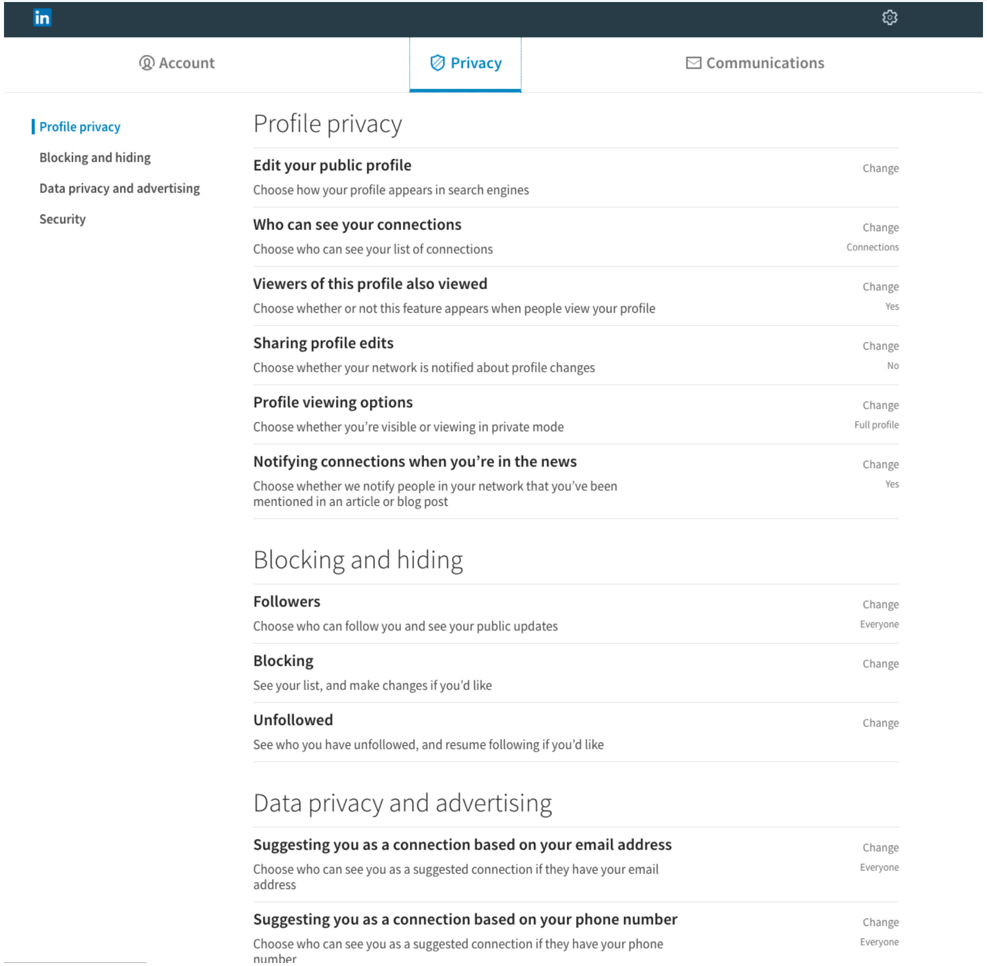
Tweet media
- □ Do not inform me before showing media that may be sensitive

You will see all photos or videos even if they contain sensitive media.

- □ Mark media I Tweet as containing material that may be sensitive

Please check this box if your Tweets contain sensitive media so that users can be informed prior to viewing.

Save changes



Profile privacy

Edit your public profile — Change
Choose how your profile appears in search engines

Who can see your connections — Change — Connections
Choose who can see your list of connections

Viewers of this profile also viewed — Change — Yes
Choose whether or not this feature appears when people view your profile

Sharing profile edits — Change — No
Choose whether your network is notified about profile changes

Profile viewing options — Change — Full profile
Choose whether you're visible or viewing in private mode

Notifying connections when you're in the news — Change — Yes
Choose whether we notify people in your network that you've been mentioned in an article or blog post

Blocking and hiding

Followers — Change — Everyone
Choose who can follow you and see your public updates

Blocking — Change
See your list, and make changes if you'd like

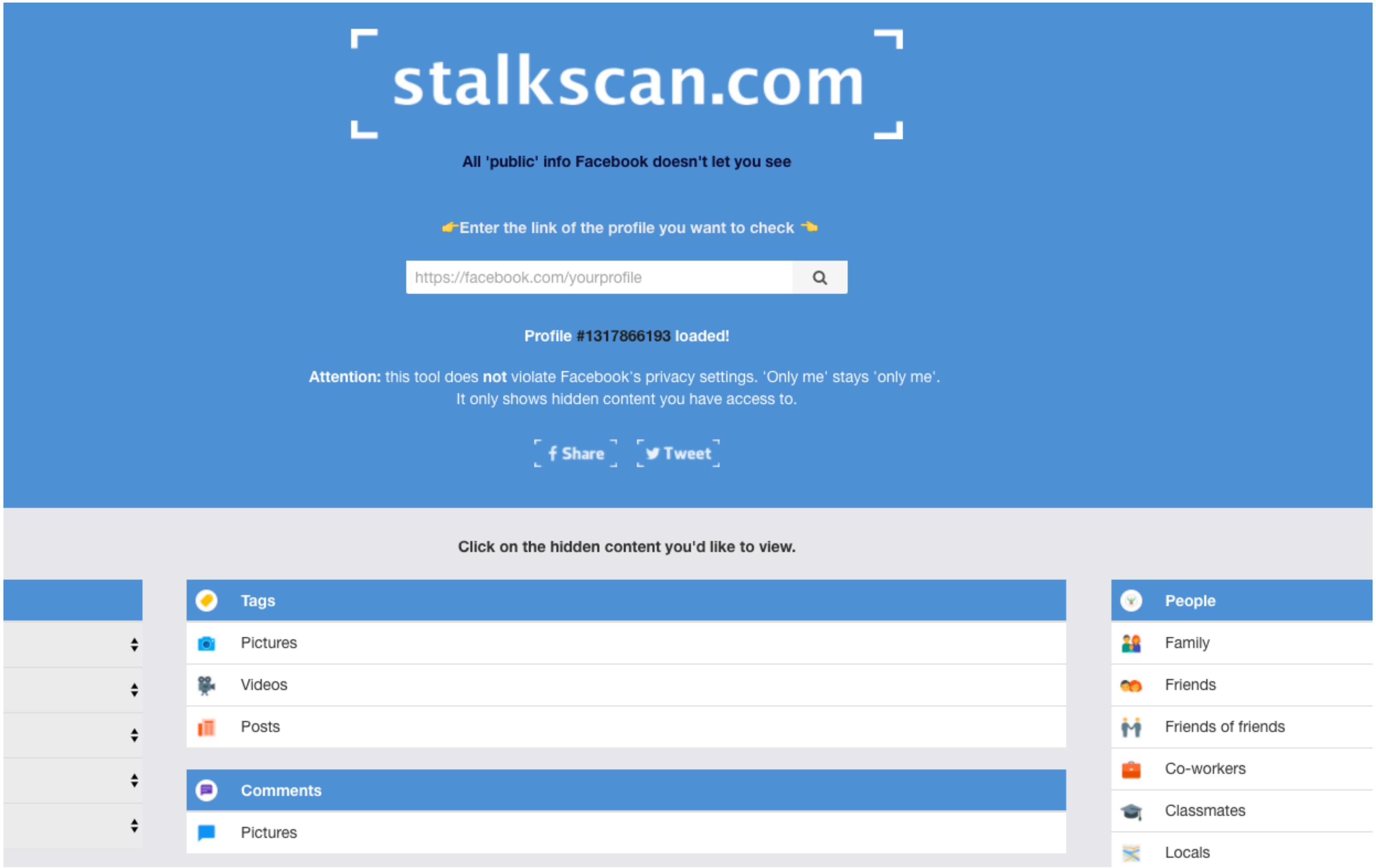
Unfollowed — Change
See who you have unfollowed, and resume following if you'd like

Data privacy and advertising

Suggesting you as a connection based on your email address — Change — Everyone
Choose who can see you as a suggested connection if they have your email address

Suggesting you as a connection based on your phone number — Change — Everyone
Choose who can see you as a suggested connection if they have your phone number

OSINT Tool: Stalkscan



stalkscan.com

All 'public' info Facebook doesn't let you see

👉Enter the link of the profile you want to check 👈

https://facebook.com/yourprofile

Profile #1317866193 loaded!

Attention: this tool does **not** violate Facebook's privacy settings. 'Only me' stays 'only me'.
It only shows hidden content you have access to.

Click on the hidden content you'd like to view.

- Tags
  - Pictures
  - Videos
  - Posts
- Comments
  - Pictures
- People
  - Family
  - Friends
  - Friends of friends
  - Co-workers
  - Classmates
  - Locals

Defense in Depth

- Enable multi-factor authentication on accounts, regularly change passwords and use a password safe to limit password reuse.
- Delete data securely.
- ENCRYPT: mobile devices, laptops, email, chat, messaging.
- Cover web cameras. Strip EXIF data from photos and configure your devices not to add location information.
- Turn off location tracking in your devices except when you need it.
- If you need to travel with an electronic device, consider using one dedicated for this purpose that has limited access to personal data. When crossing a border, always shut down devices completely.
- Never take an electronic device to a demonstration or consider purchasing a "burner" which isn't associated with any of your accounts.
- Use anti-virus, a firewall and *patch your devices regularly*. Secure your home network: encrypt wireless, change the default password on your router, configure the firewall. Remember, apply security in layers .
- Avoid unencrypted wireless. If you must use it, then only with a VPN.
- Enable privacy options in social media accounts and in your browser. Use search engines and other tools to validate your settings.
- Separate your social media personas, don't use real names if not required.

Trust No One

CAUTION:

There are limitations to any security tool. A dedicated adversary with the right resources (time and money) can bypass them.

LAYER YOUR DEFENSES!

Resources

- How Whole Disk Encryption Works https://www.symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_WP_21158817.en-us.pdf
- Chatting in Secret https://theintercept.com/2015/07/14/communicating-secret-watched/
- Enemies of the Internet http://surveillance.rsf.org/en/
- Me and My Shadow Project https://myshadow.org/
- Freedom on the Net https://freedomhouse.org/report-types/freedom-net
- Access Now Digital Security Helpline https://www.accessnow.org/help/
- EFF Surveillance Self Defense for tutorials on using security tools https://ssd.eff.org/
- Krebs On Security http://krebsonsecurity.com/
- Best VPN Services 2017 http://www.pcmag.com/article2/0,2817,2403388,00.asp
- Digital First Aid Kit https://www.digitaldefenders.org/digitalfirstaid/
- Tor Browser, Orbot or Onion Browser for mobile devices https://www.torproject.org/about/overview.html.en
- Burner Phone Best Practices http://www.b3rn3d.com/blog/2014/01/22/burnerphone/
- Password managers: Dashlane, 1Password, Lastpass