Lecture 23 – U-Pick-Em
How Bailey Secures Himself

Michael Bailey
University of Illinois
ECE 422/CS 461 – Spring 2018

Thinking as a Defender

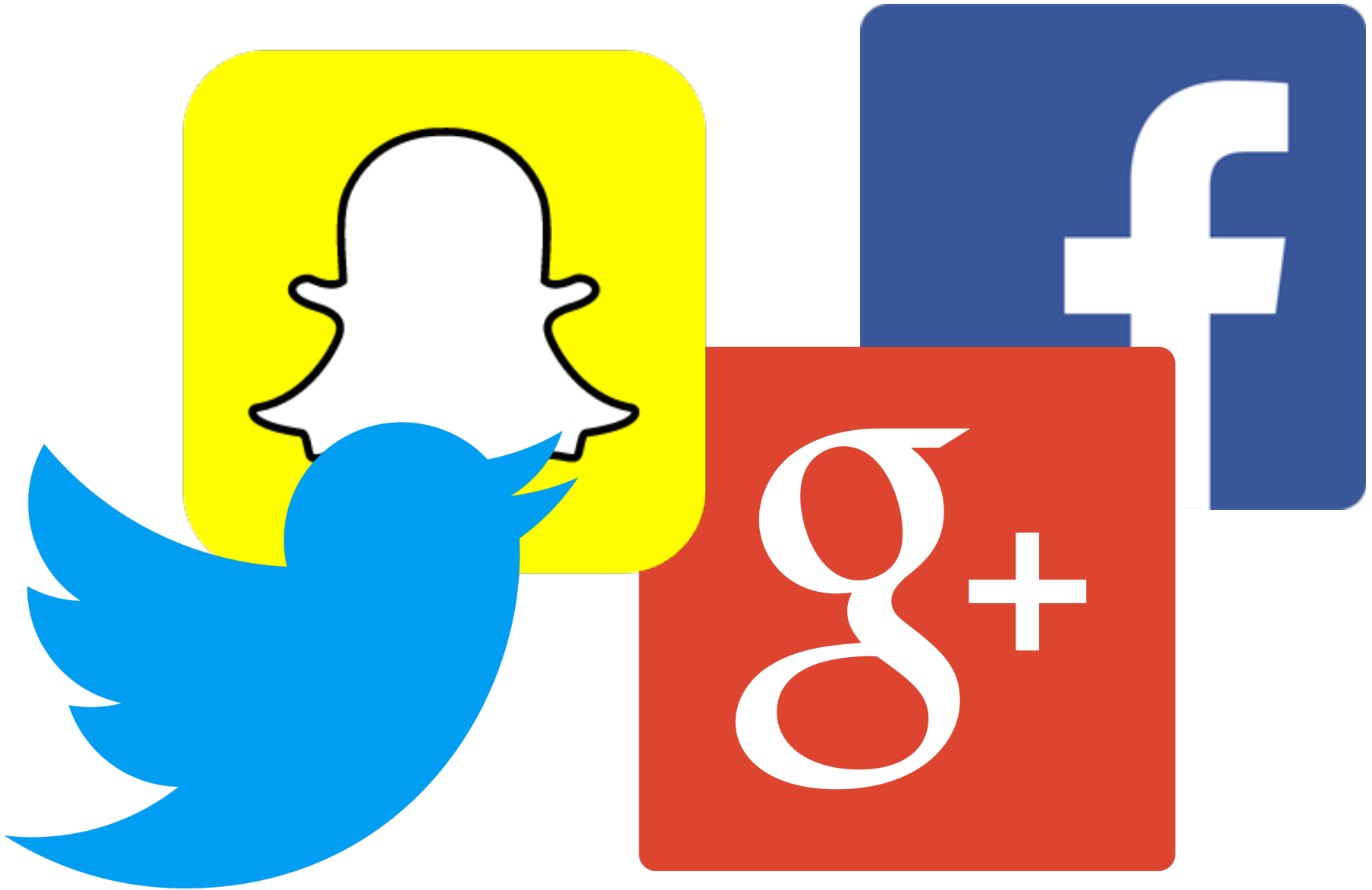
- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers?
  - What are their Capabilities? Motivations?
- Risk assessment
  - What are the weaknesses of the system?
  - How likely?
- Countermeasures
  - Technical vs. nontechnical?
  - How much do they cost?

Challenge is to think rationally and rigorously about risk. *Rational paranoia.*

What am I trying to protect?

What am I trying to protect?

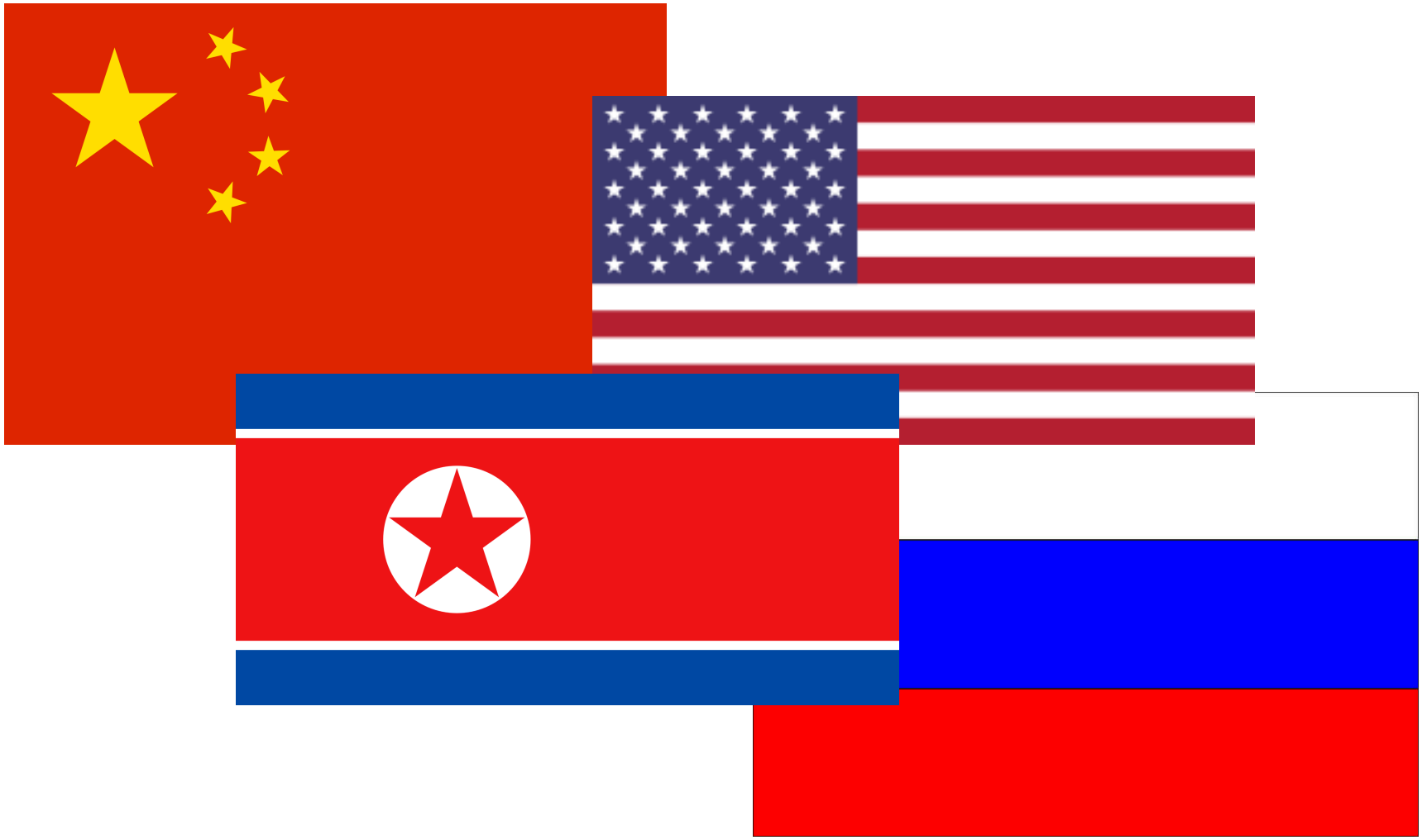
What am I trying to protect?



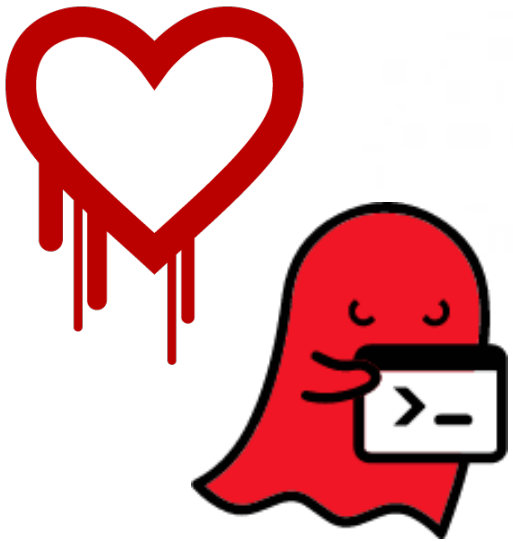
Who am I protecting it from?

Who am I protecting it from?

Who am I NOT protecting it from?

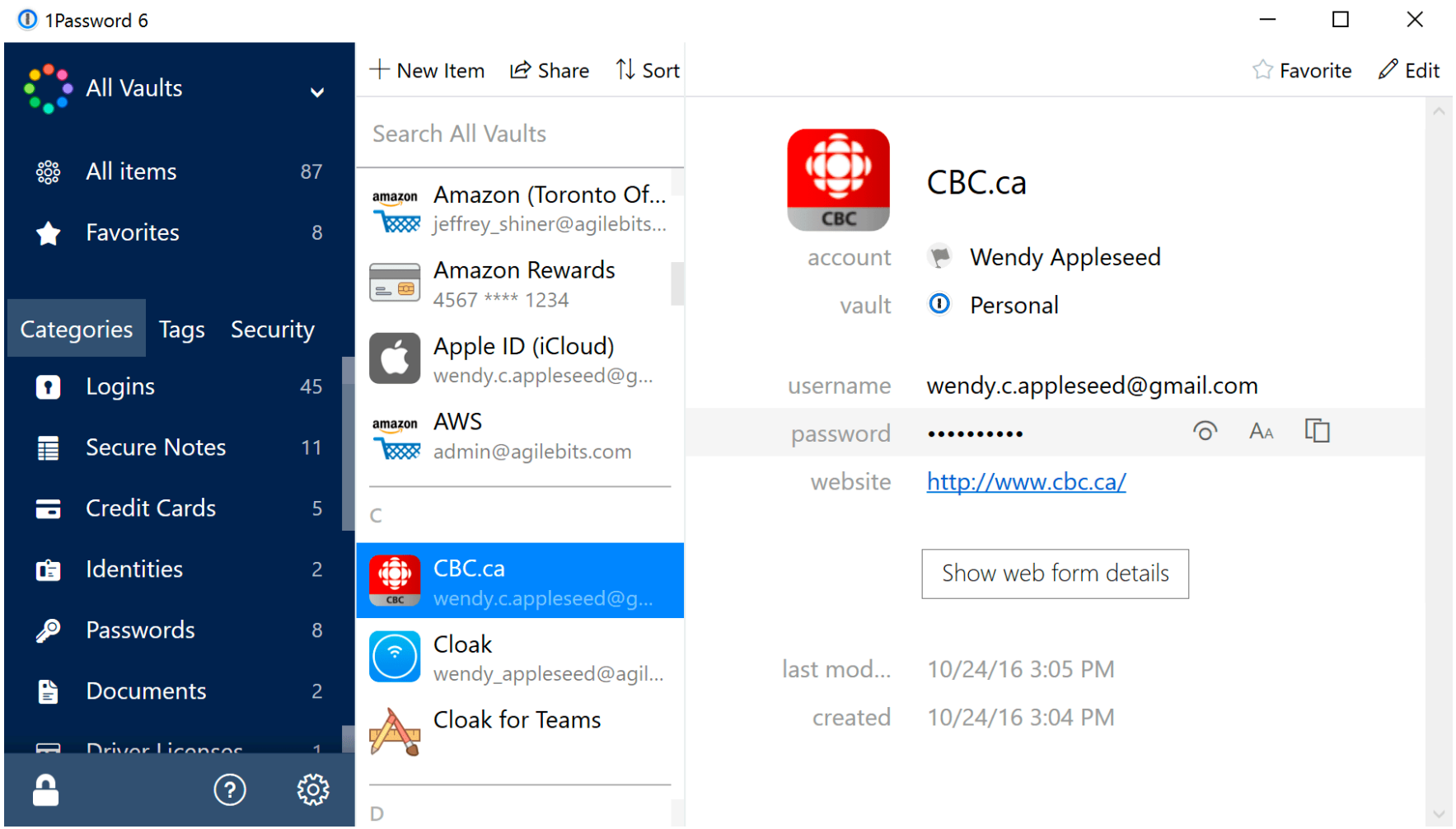


How will I lose it?



Questions?

1. Password Manager



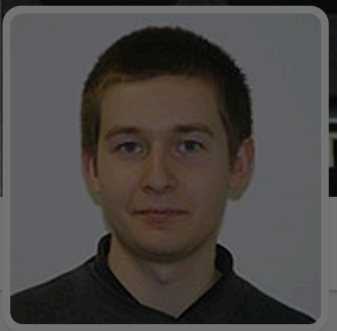

CLOUDFLARE

Tavis Ormandy on Twitter: "Ah

Twitter, Inc. [US] https://twitter.com/taviso/status/845717082717114368?lang=en

Research Ideas -... Science of Securit... https://raid2017.ho... Coinscope: A Cryp... USENIX Security '17 CIS 556: Cryptogr... https://sites.googl... sgx_bh16.pdf

Home Moments Search Twitter Have an account? Log in



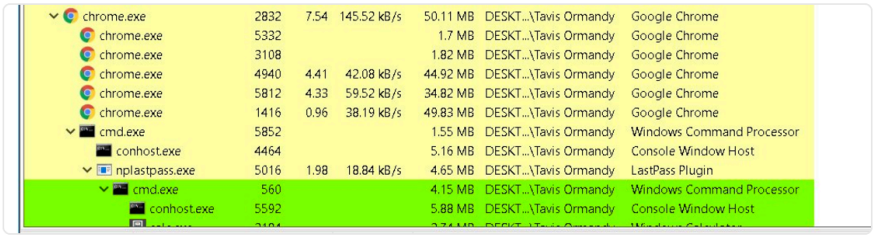
Tavis Ormandy
@taviso

Vulnerability researcher at Google. This is a personal stream, opinions expressed are mine.

California
taviso.decsystem.org
Joined April 2008

Tavis Ormandy @taviso
Follow

Ah-ha, I had an epiphany in the shower this morning and realized how to get codeexec in LastPass 4.1.43. Full report and exploit on the way.



RETWEETS 923 LIKES 1,736

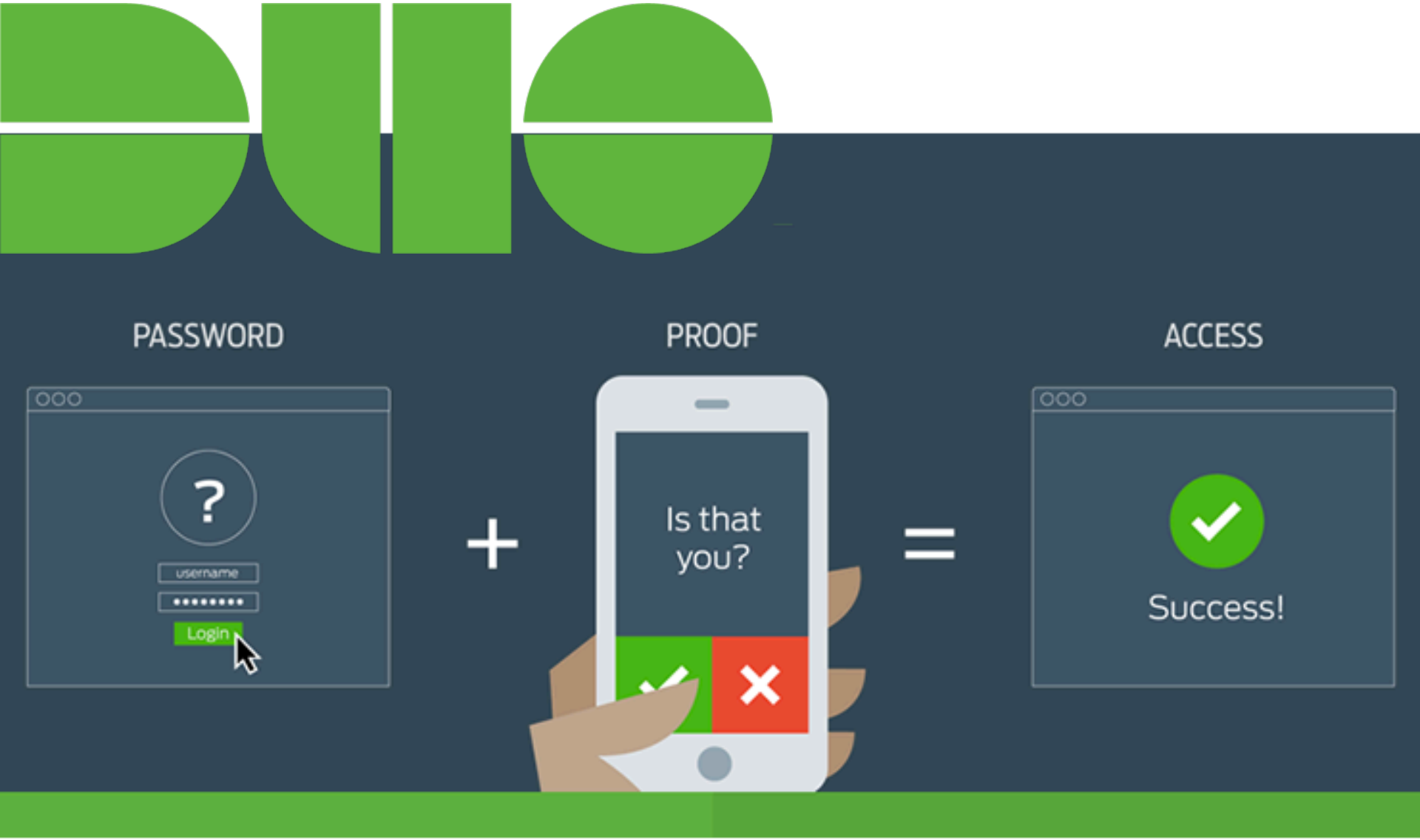
12:20 PM - 25 Mar 2017

87 923 1.7K

Tavis Ormandy @taviso · Mar 25
Replying to @taviso
OK, exploit working and full report sent to LastPass. Now time to put some pants on.

21 95 606

2. Two Factor Authentication



The very four digits that Amazon considers unimportant enough to display in the clear on the Web are precisely the same ones that Apple considers secure enough to perform identity verification.

3. Automatic Updates

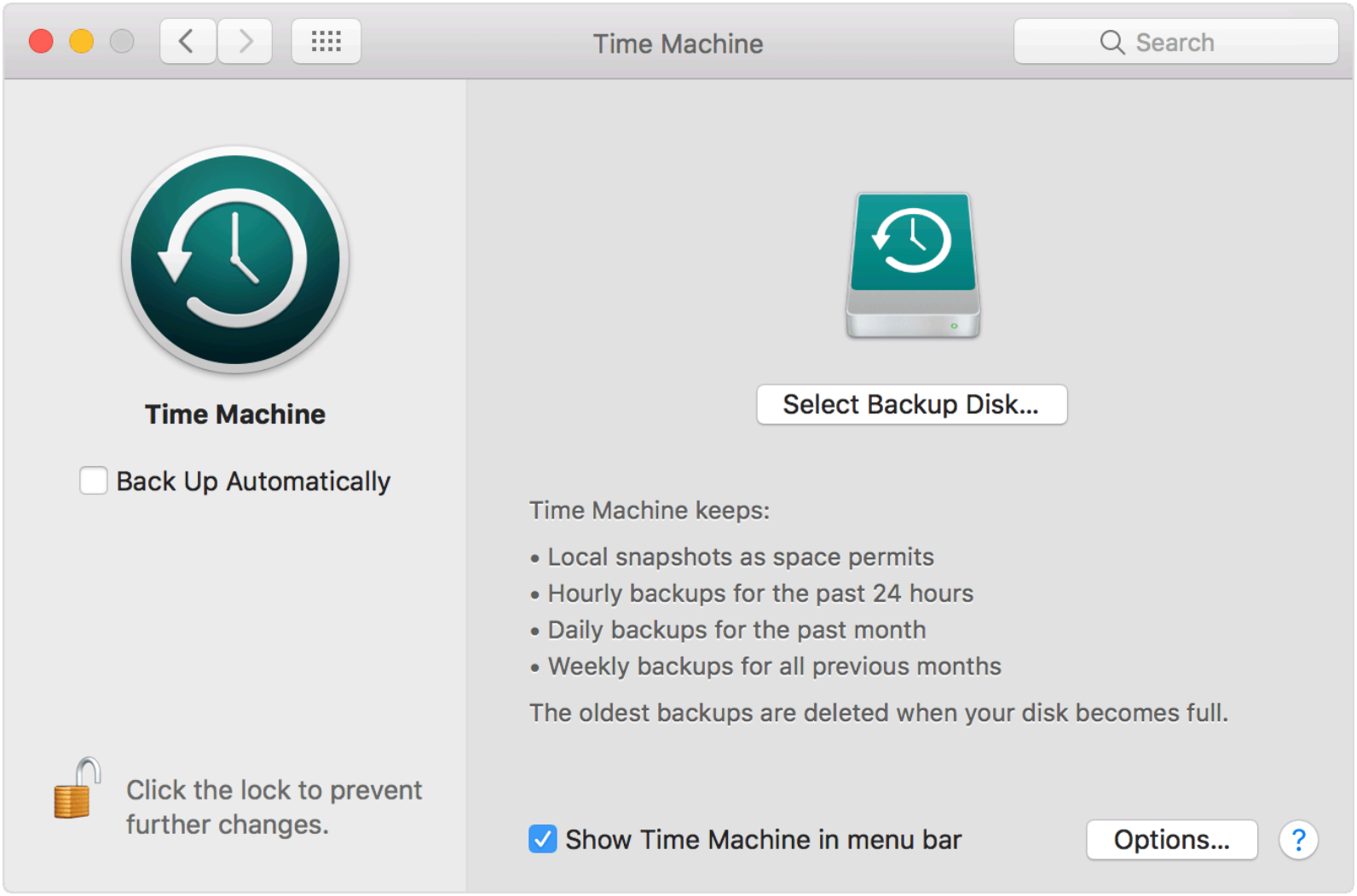
The App Store keeps OS X and apps from the App Store up to date.

- [x] Automatically check for updates
  - [x] Download newly available updates in the background
    You will be notified when the updates are ready to be installed
  - [x] Install app updates
  - [ ] Install OS X updates
  - [x] Install system data files and security updates
- [–] Automatically download apps purchased on other Macs
  Can't determine if automatic downloads are enabled due to a network problem

Last check was Thursday, December 1, 2016 | Check Now

?

4. Backups


Time Machine
Search
Time Machine
Back Up Automatically
Select Backup Disk...
Time Machine keeps:
• Local snapshots as space permits
• Hourly backups for the past 24 hours
• Daily backups for the past month
• Weekly backups for all previous months
The oldest backups are deleted when your disk becomes full.
Click the lock to prevent further changes.
Show Time Machine in menu bar
Options...
?

YOUR BROWSER HAS BEEN LOCKED

fbi.gov.id657546456-3999456674.k8381.com

Reader

Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular

THE FBI CYBER DEPARTMENT
FEDERAL BUREAU OF INVESTIGATION

All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

Your IP:

Location:

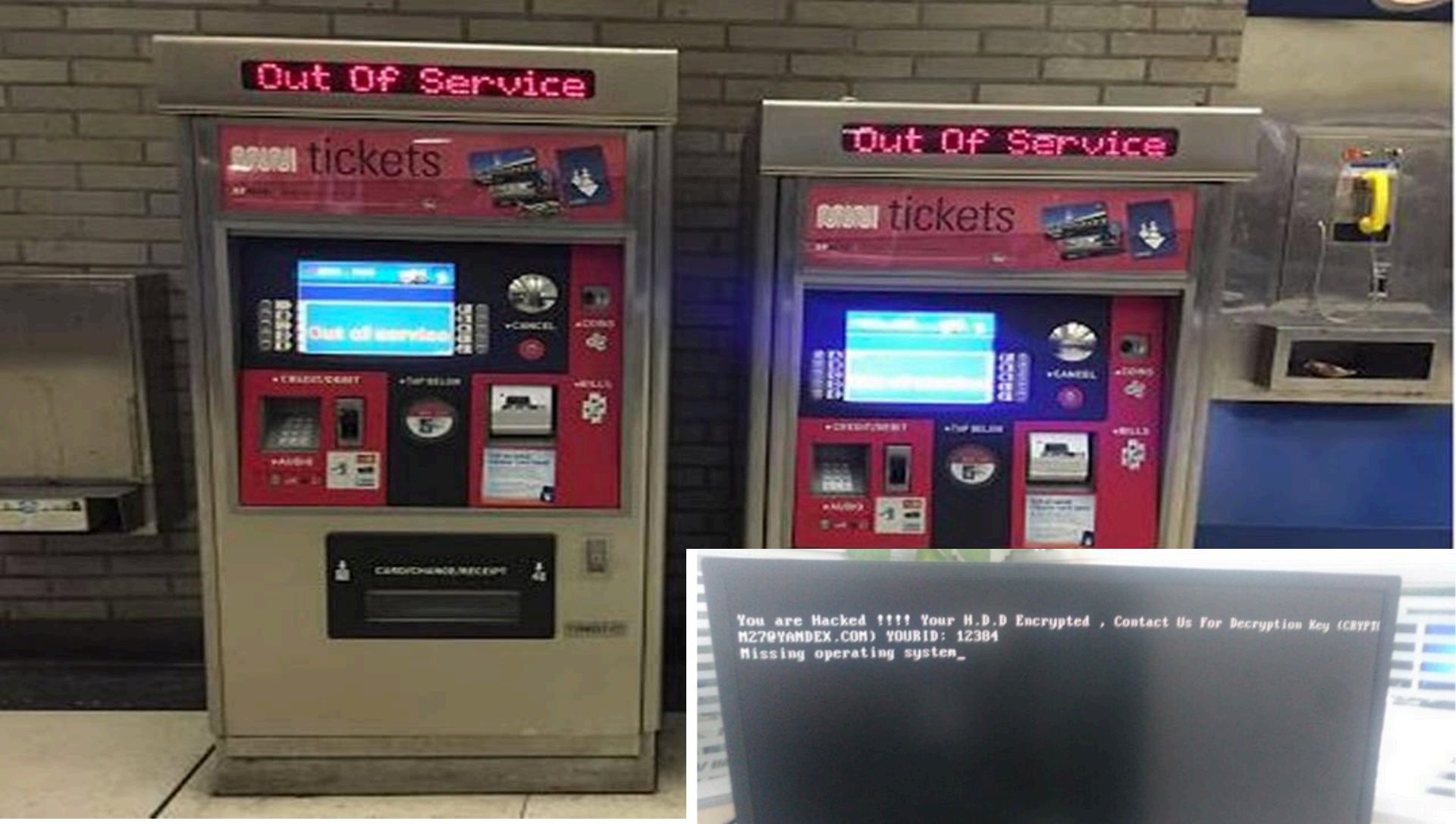
SECURE PAYMENT FORM

Enter the code MoneyPak

Please enter MoneyPack code using pin pad below.

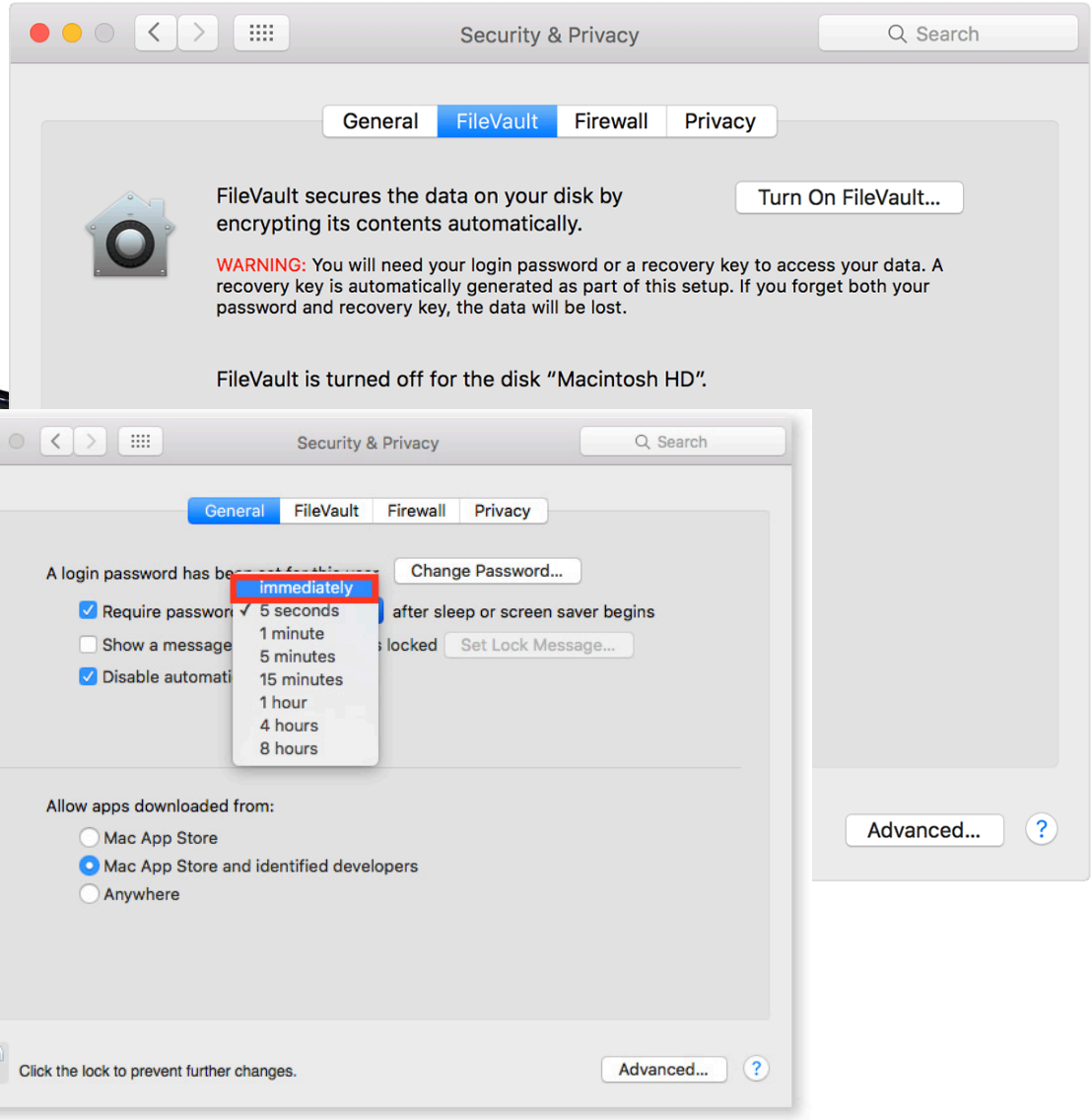
1 2 3 4 5 6 7 8 9 0 Clear

UNLOCK YOUR PC NOW!


Out Of Service
tickets
Out of service
Out Of Service
tickets

You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (CRYPT
MZ70YANDEX.COM) YOURID: 12304
Missing operating system_
AOC

5. Disk Encryption, Physical Security



Data on millions of vets stolen from VA employee's home - News - GovExec.com

www.govexec.com/federal-news/2006/05/data-on-millions-of-vets-stolen-from-va-employees-home/2

Government Executive

Data on millions of vets stolen from VA employee's home

By David Perera

May 22, 2006

Personal information, including Social Security numbers, of possibly every living U.S. veteran discharged since 1975 was stolen earlier this month from the home of a Veterans Affairs employee, the department announced Monday.

The employee took the electronic data without authorization, Veterans Affairs Secretary Jim Nicholson said. Sources said the employee, now placed on administrative leave, worked in the Policy and Planning Group at department headquarters and was performing a statistical analysis on the data as part of an annual department study on veteran population demographics.

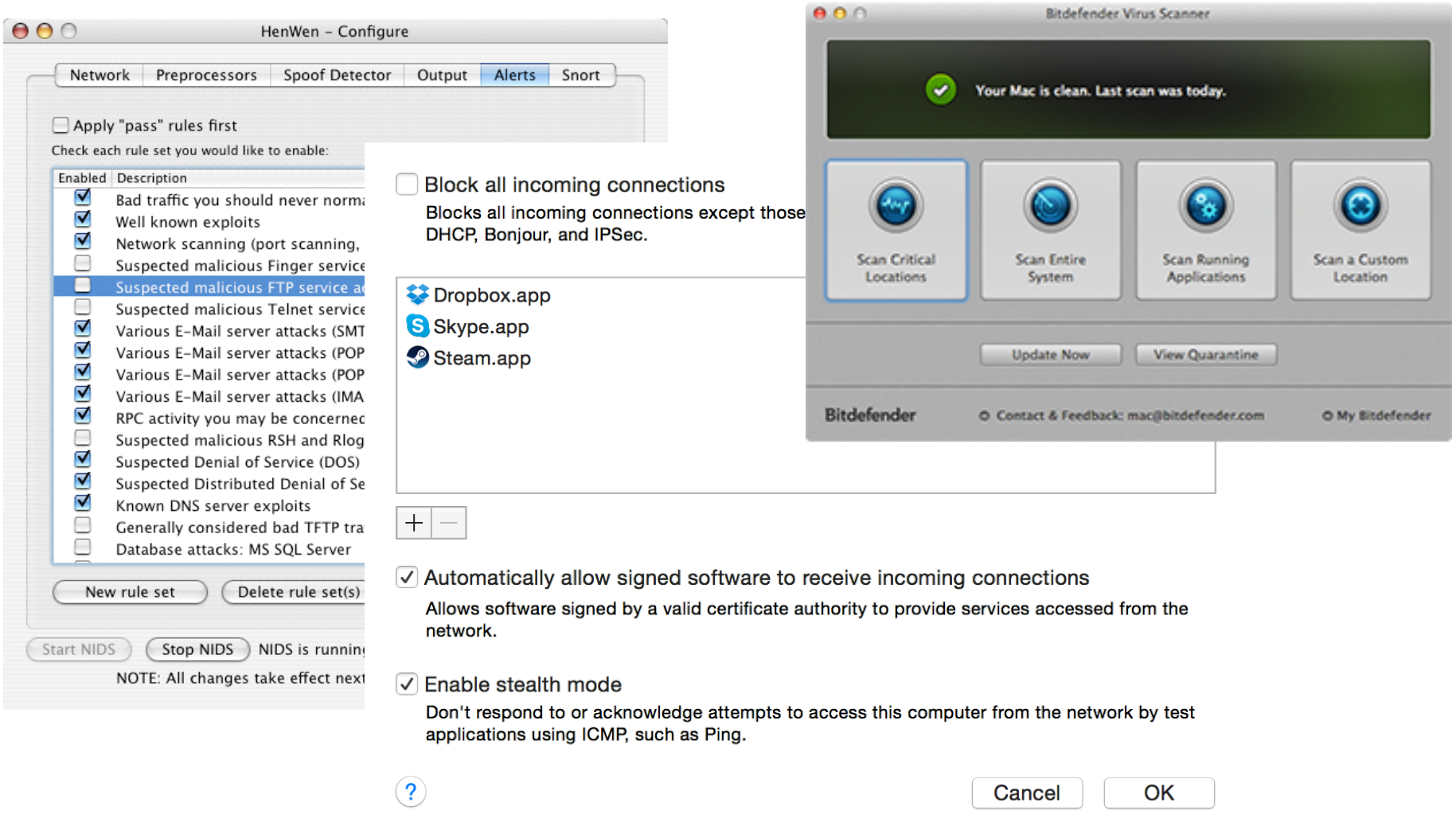
The data also contained the names, dates of birth and some disability ratings for up to 26.5 million veterans and some of their spouses, according to a VA statement. The stolen data does not contain medical records, the

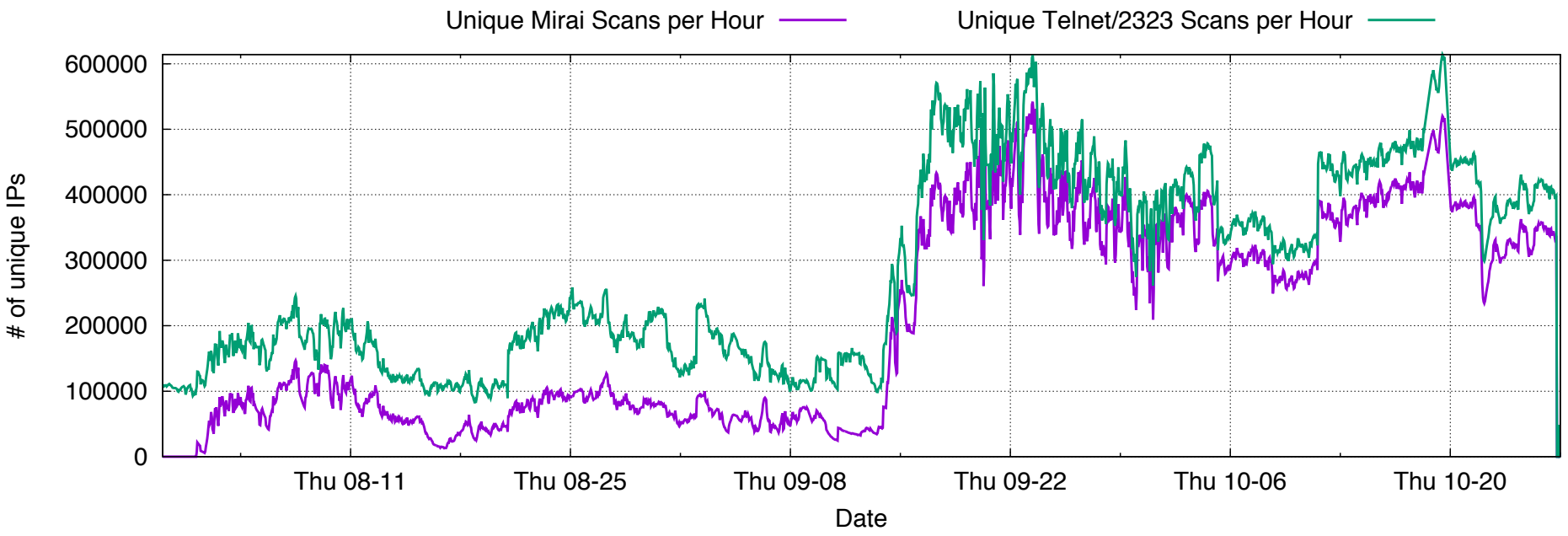
Privacy Impact Assessment
for the

Border Searches of Electronic Devices

August 25, 2009

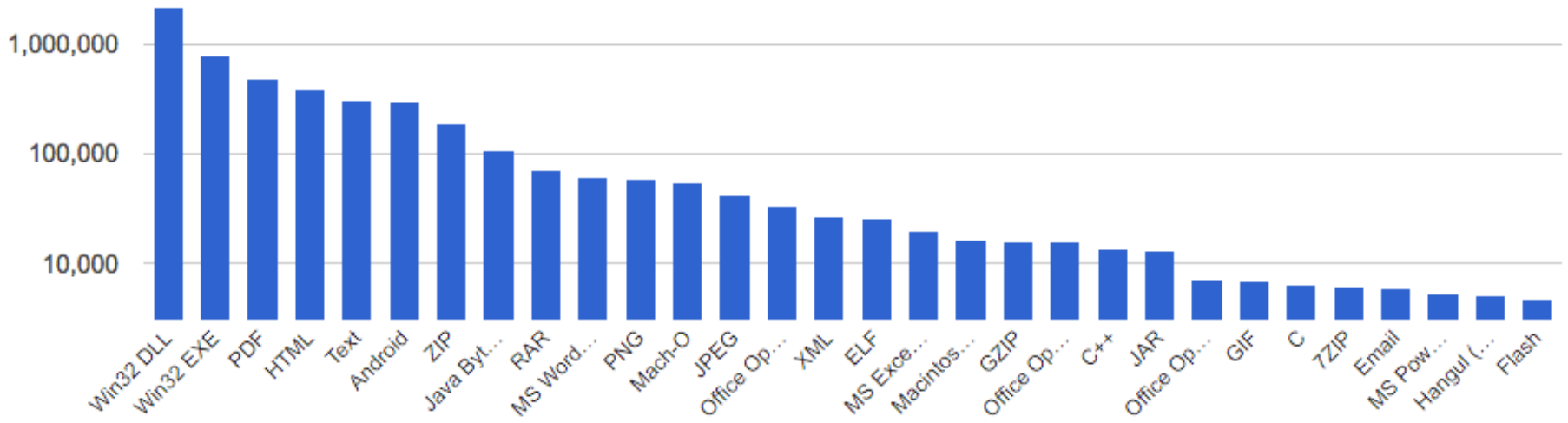
6. Firewall, IDS, AV



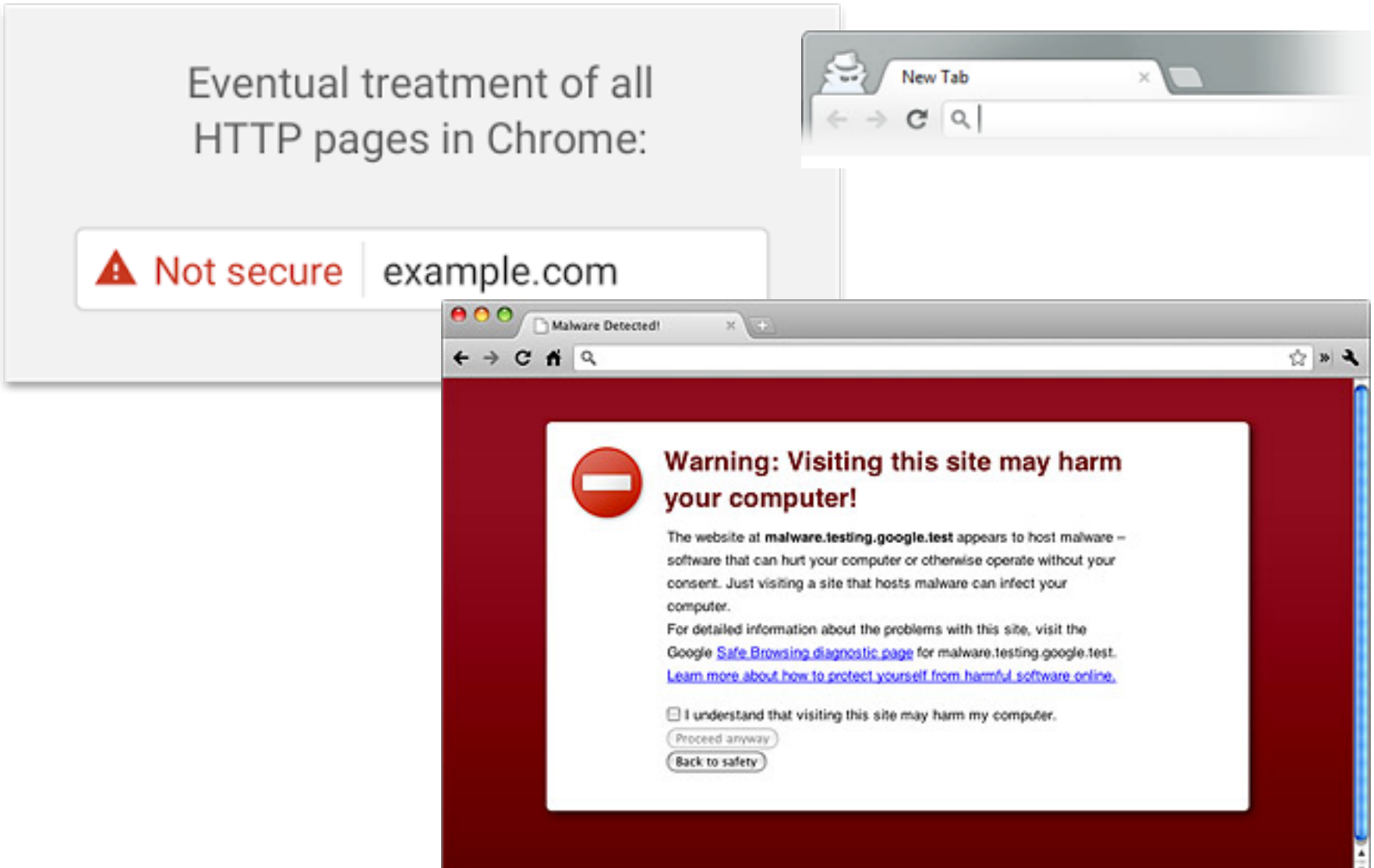

Unique Mirai Scans per Hour
Unique Telnet/2323 Scans per Hour
# of unique IPs
600000
500000
400000
300000
200000
100000
0
Thu 08-11
Thu 08-25
Thu 09-08
Thu 09-22
Thu 10-06
Thu 10-20
Date

Submissions

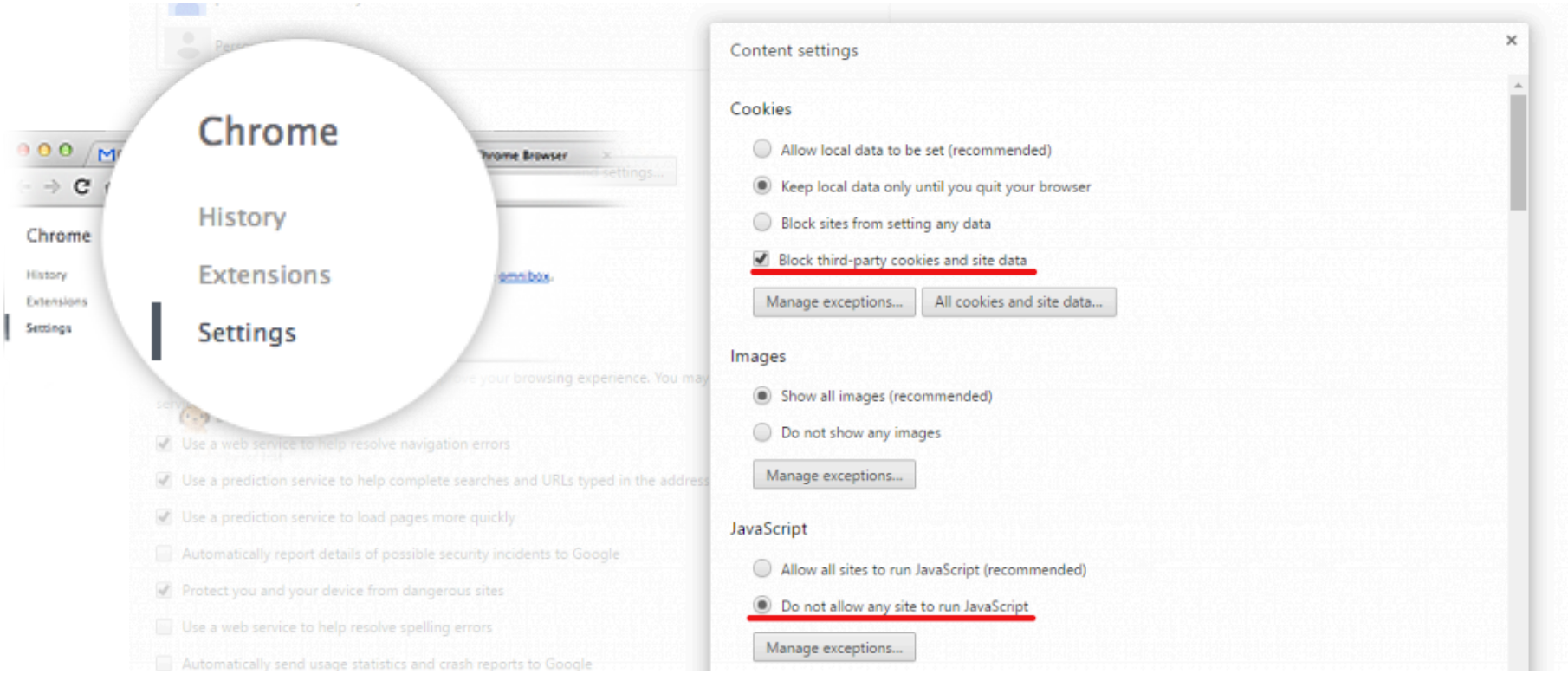
File types



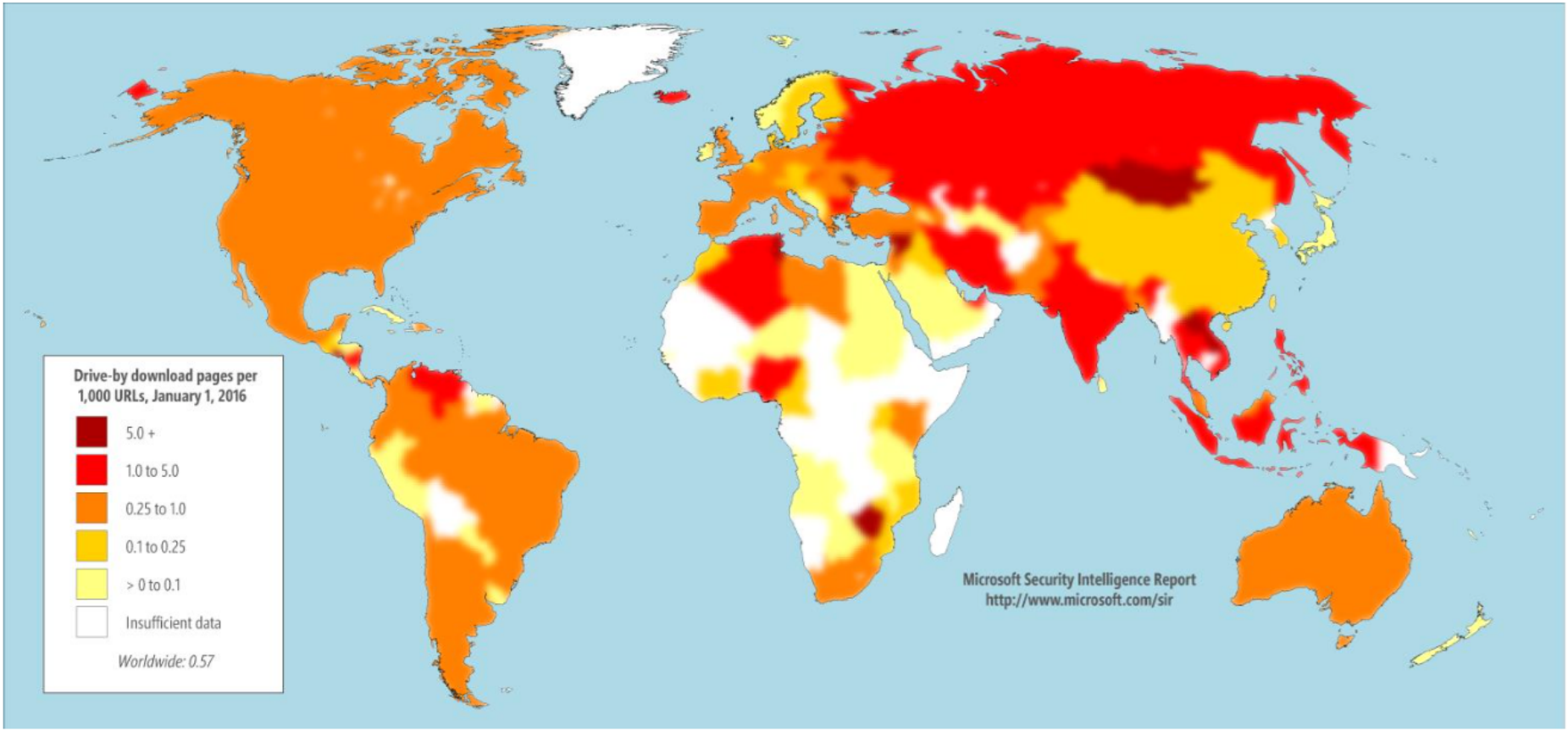
7. Safe Browsing



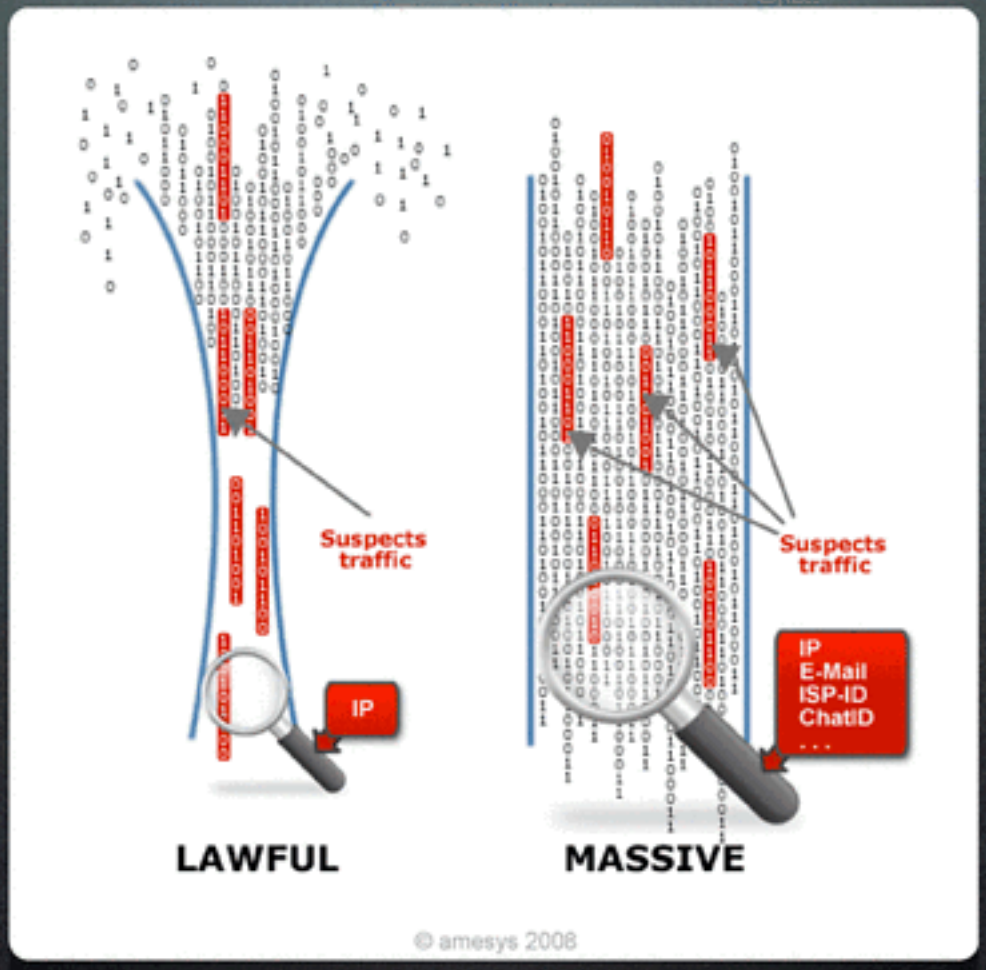
7. Safe Browsing



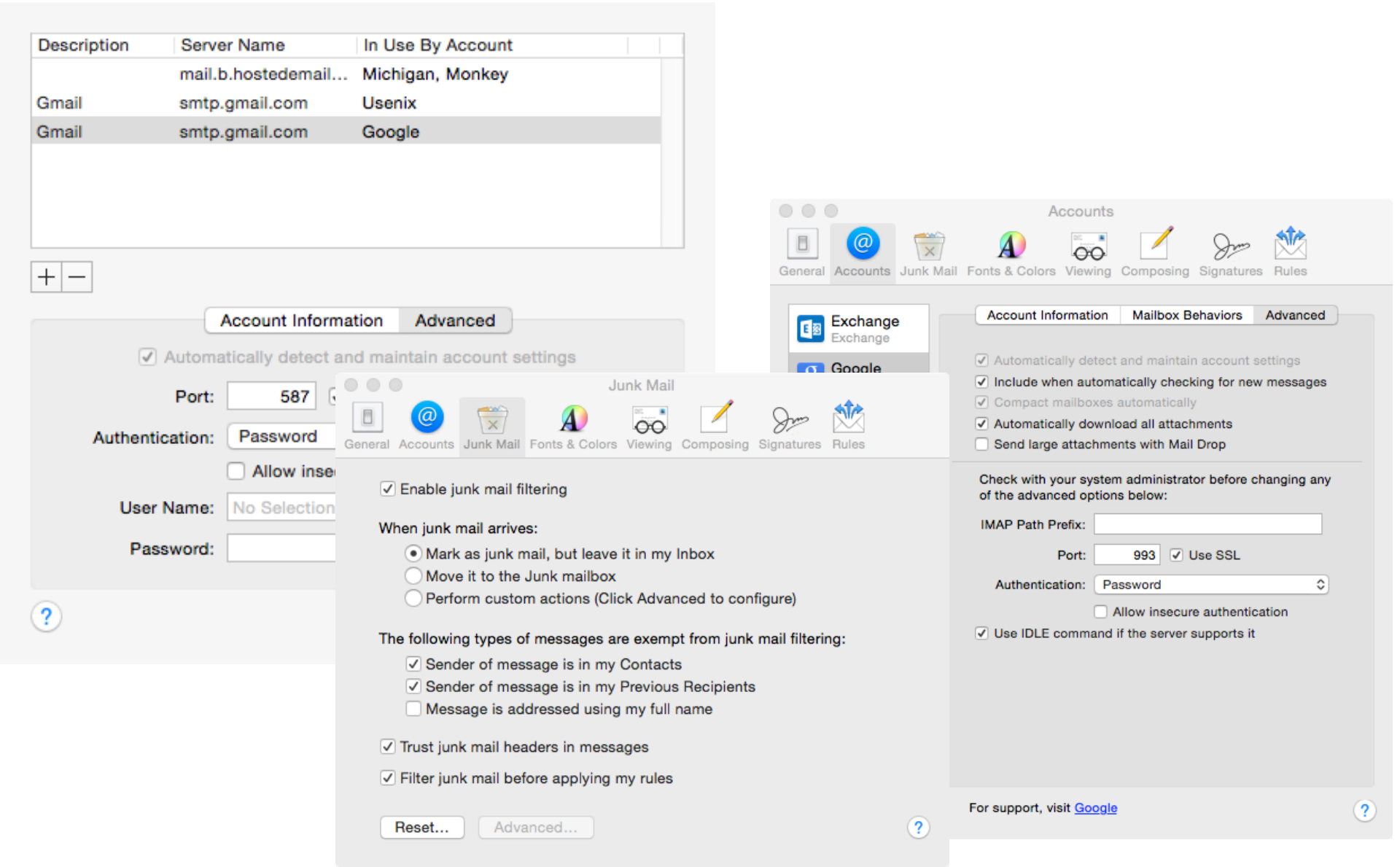
7. Safe Browsing


Drive-by download pages per 1,000 URLs, January 1, 2016
5.0 +
1.0 to 5.0
0.25 to 1.0
0.1 to 0.25
> 0 to 0.1
Insufficient data
Worldwide: 0.57
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

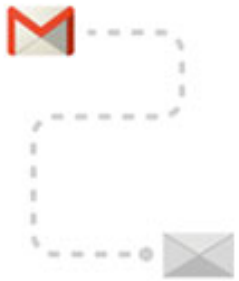
Lawful vs Massive



8. Safe Communication

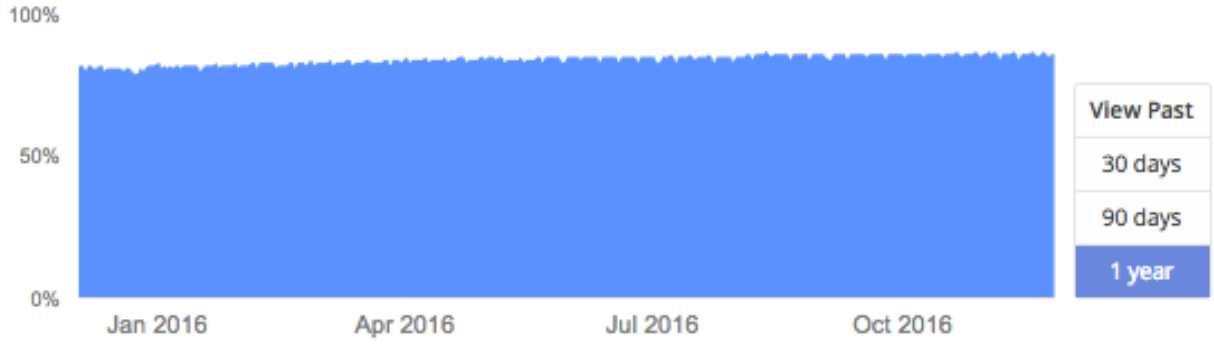


Outbound

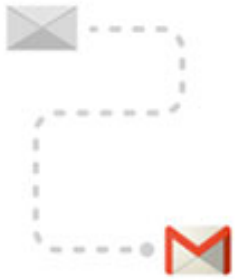


86%

Messages from Gmail to other providers.

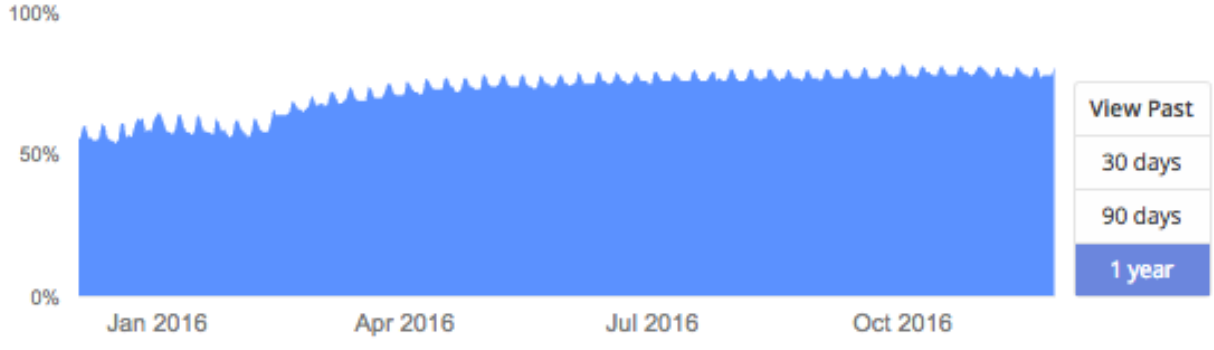


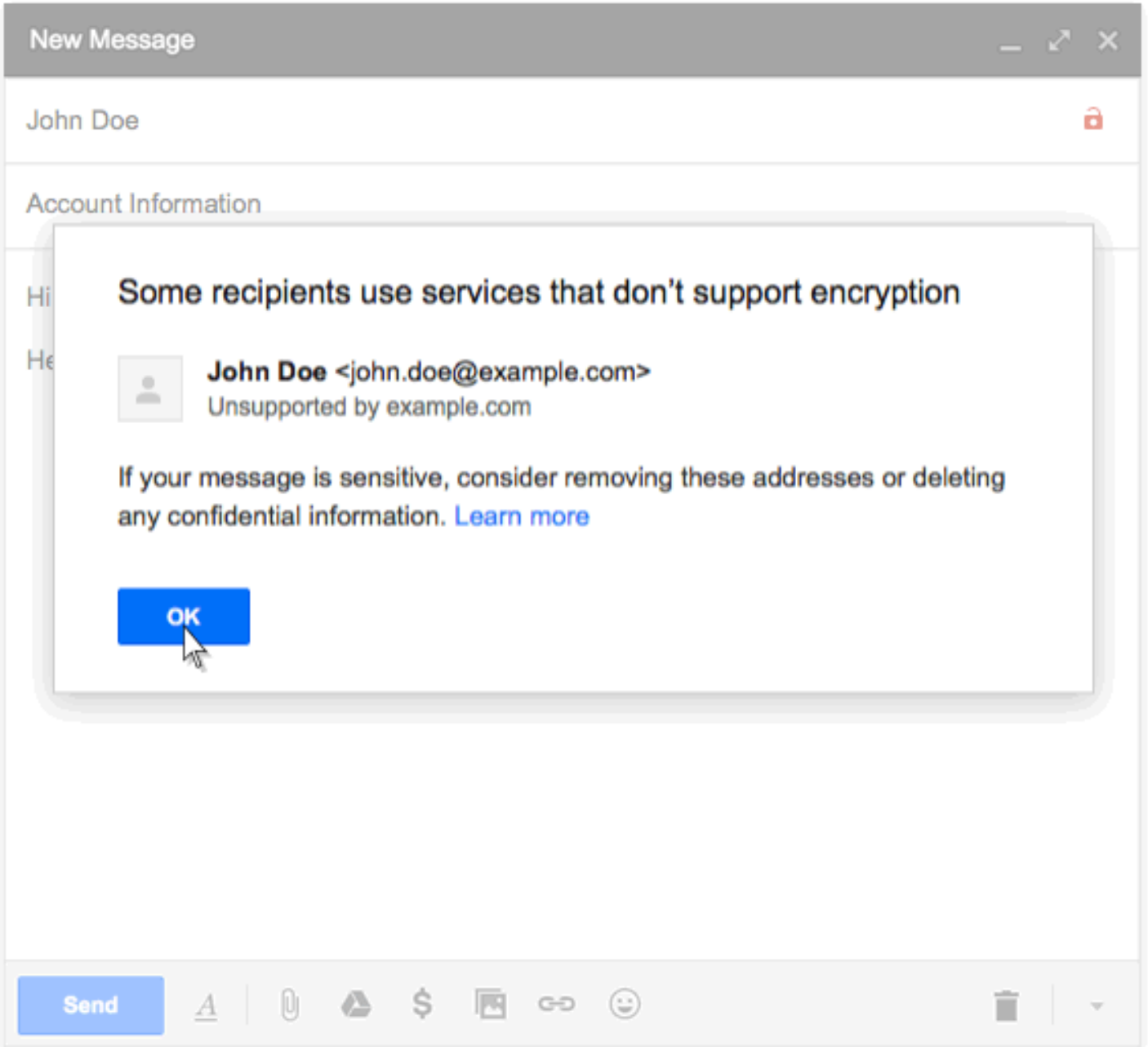
Inbound

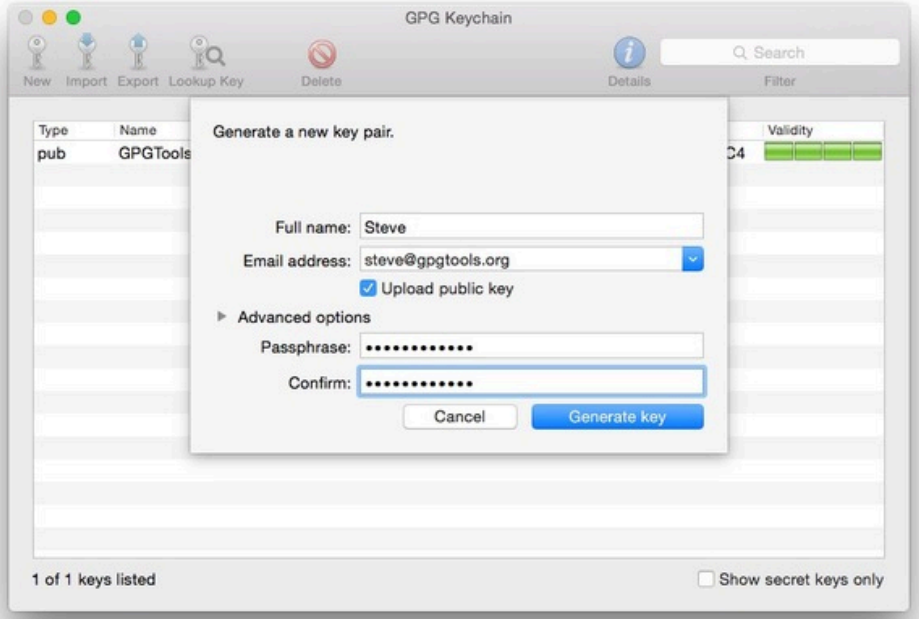


81%

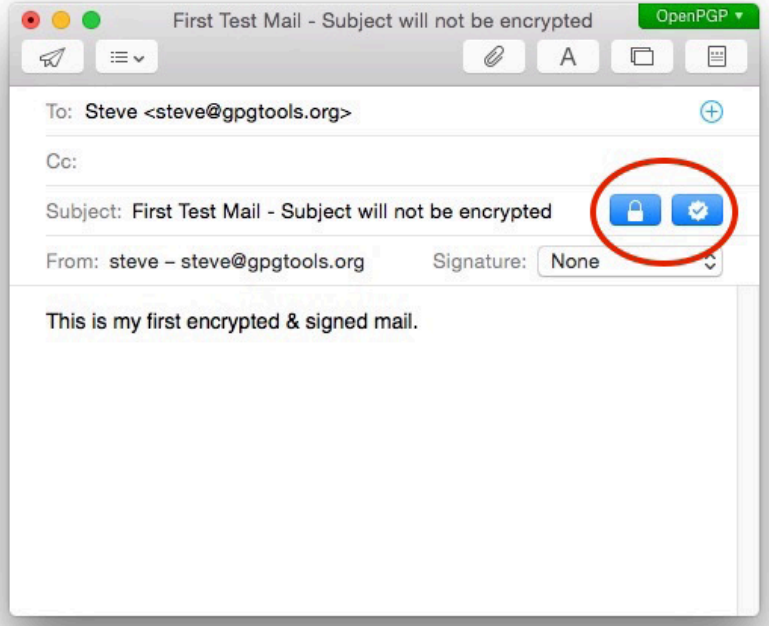
Messages from other providers to Gmail.

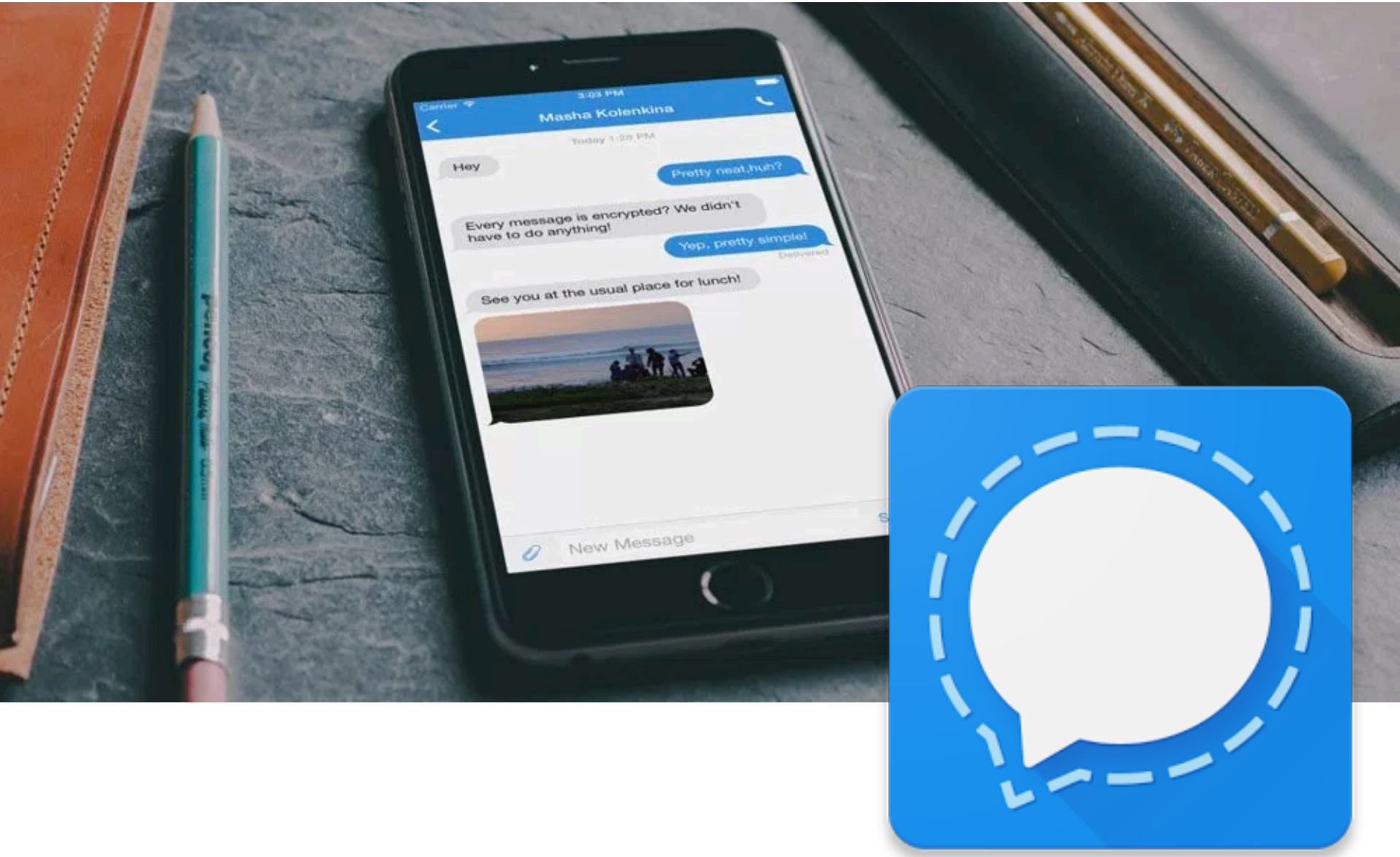



New Message
John Doe
Account Information
Hi
He
Some recipients use services that don't support encryption
John Doe <john.doe@example.com>
Unsupported by example.com
If your message is sensitive, consider removing these addresses or deleting any confidential information. Learn more
OK
Send

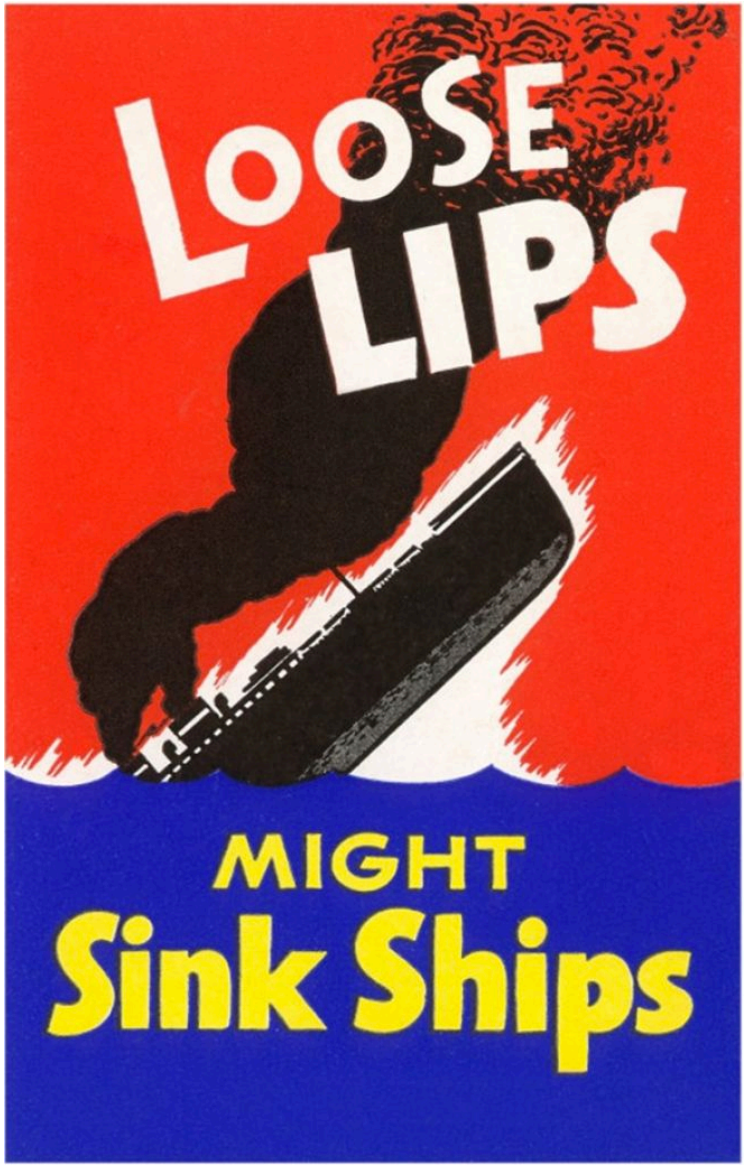

GPG Keychain
New
Import
Export
Lookup Key
Delete
Details
Search
Filter
Type
Name
Validity
pub
GPGTools
Generate a new key pair.
Full name: Steve
Email address: steve@gpgtools.org
Upload public key
Advanced options
Passphrase:
Confirm:
Cancel
Generate key
1 of 1 keys listed
Show secret keys only

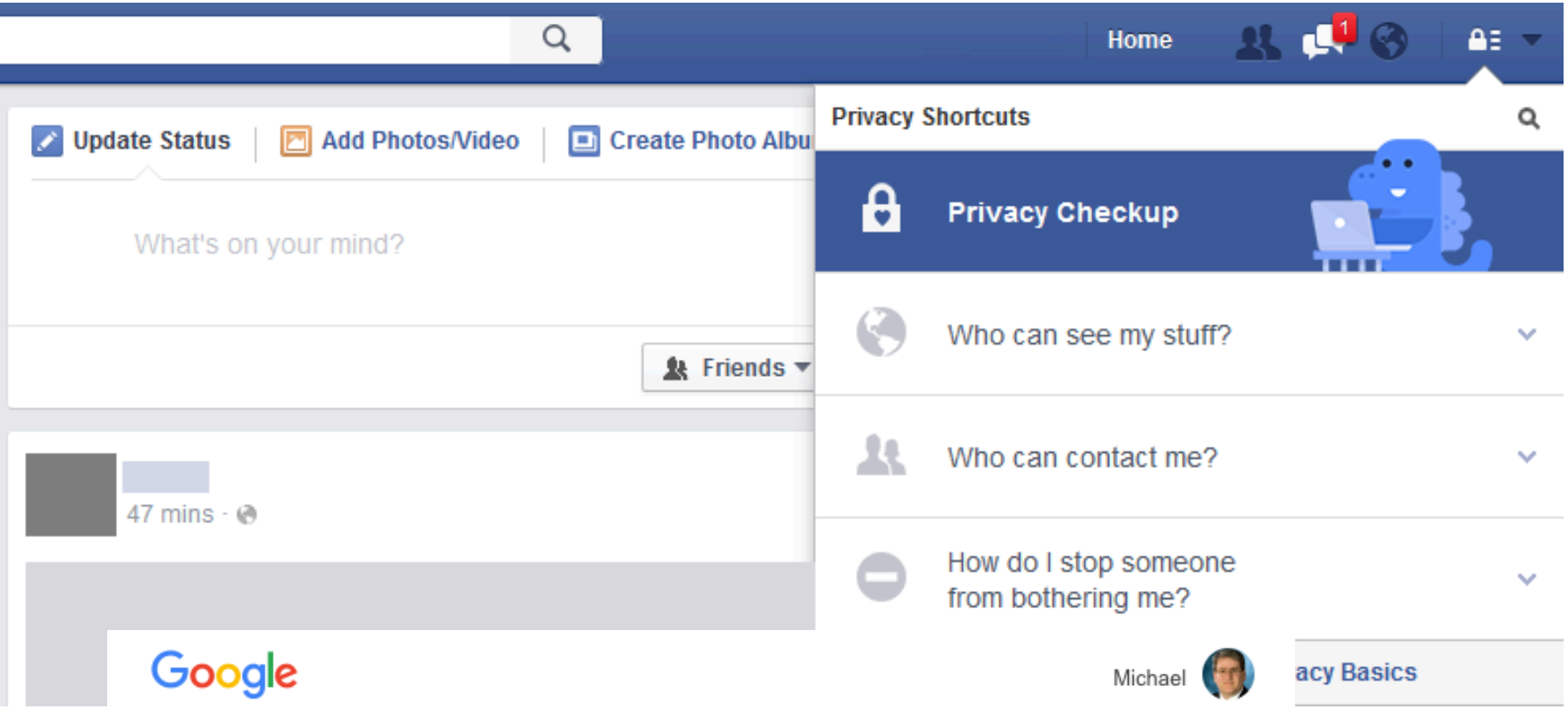

GPG Suite
GPG Suite
Install
Uninstall
GPGTOOLS

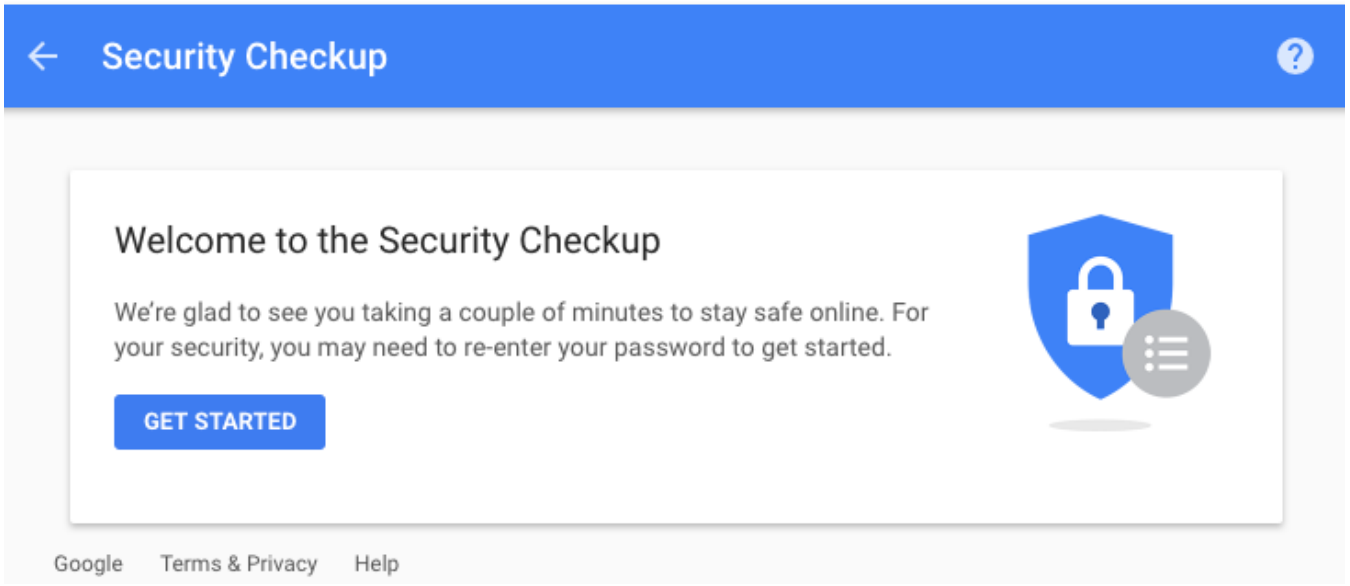

First Test Mail - Subject will not be encrypted
OpenPGP
To: Steve <steve@gpgtools.org>
Cc:
Subject: First Test Mail - Subject will not be encrypted
From: steve – steve@gpgtools.org
Signature: None
This is my first encrypted & signed mail.


Carrier
3:03 PM
Masha Kolenkina
Today 1:28 PM
Hey
Pretty neat,huh?
Every message is encrypted? We didn't have to do anything!
Yep, pretty simple!
Delivered
See you at the usual place for lunch!
New Message

9. Think Before You Share




Home
Update Status
Add Photos/Video
Create Photo Albu
What's on your mind?
Friends
47 mins
Privacy Shortcuts
Privacy Checkup
Who can see my stuff?
Who can contact me?
How do I stop someone from bothering me?
acy Basics


Google
Michael
Security Checkup
Welcome to the Security Checkup
We're glad to see you taking a couple of minutes to stay safe online. For your security, you may need to re-enter your password to get started.
GET STARTED
Google
Terms & Privacy
Help


Mr. Mark Zuckerberg

10. Security is a Process

Schneier on Security

KrebsonSecurity
In-depth security news and investigation

InformationWeek
DARKReading