

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?



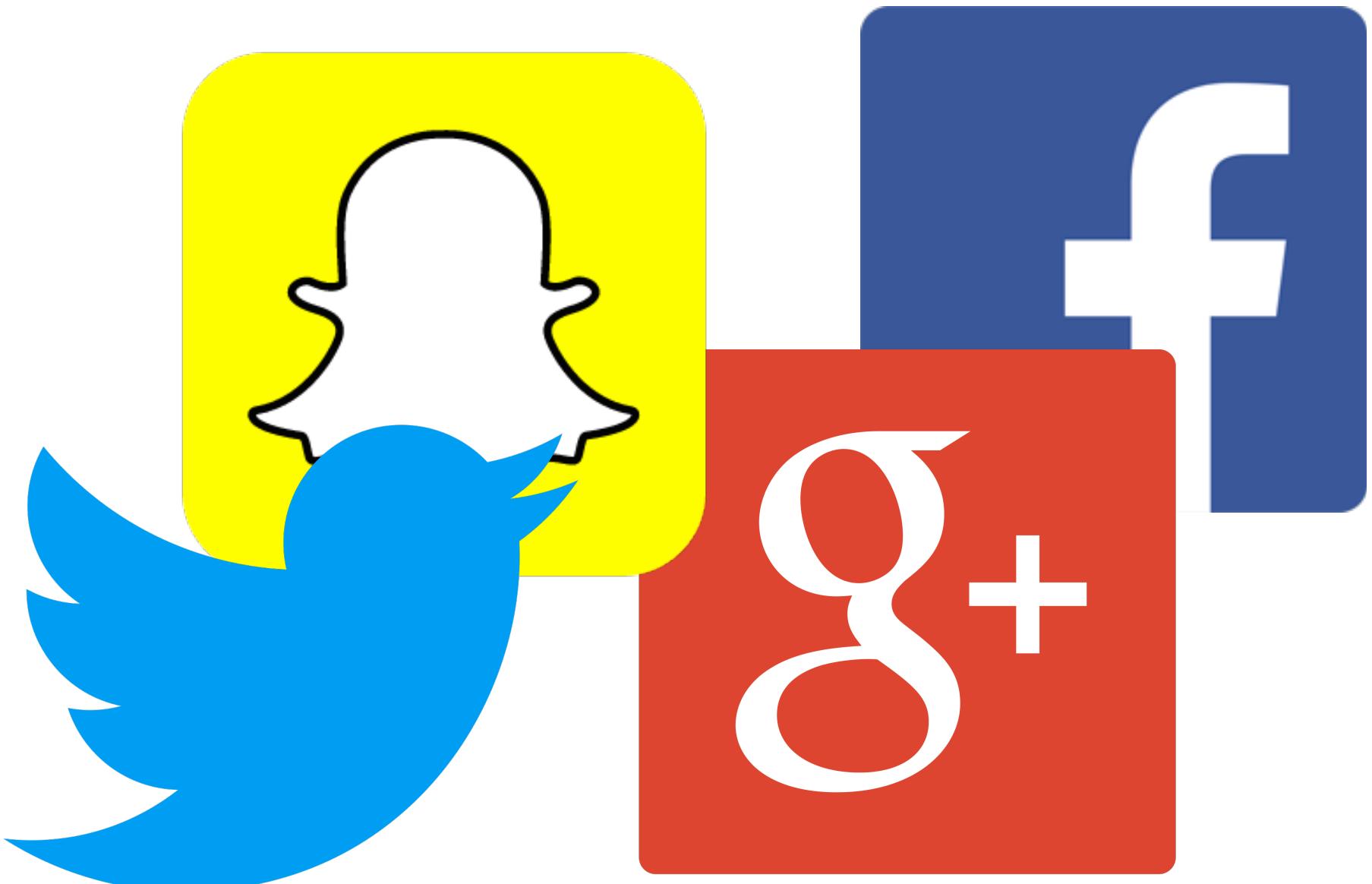
What am I trying to protect?



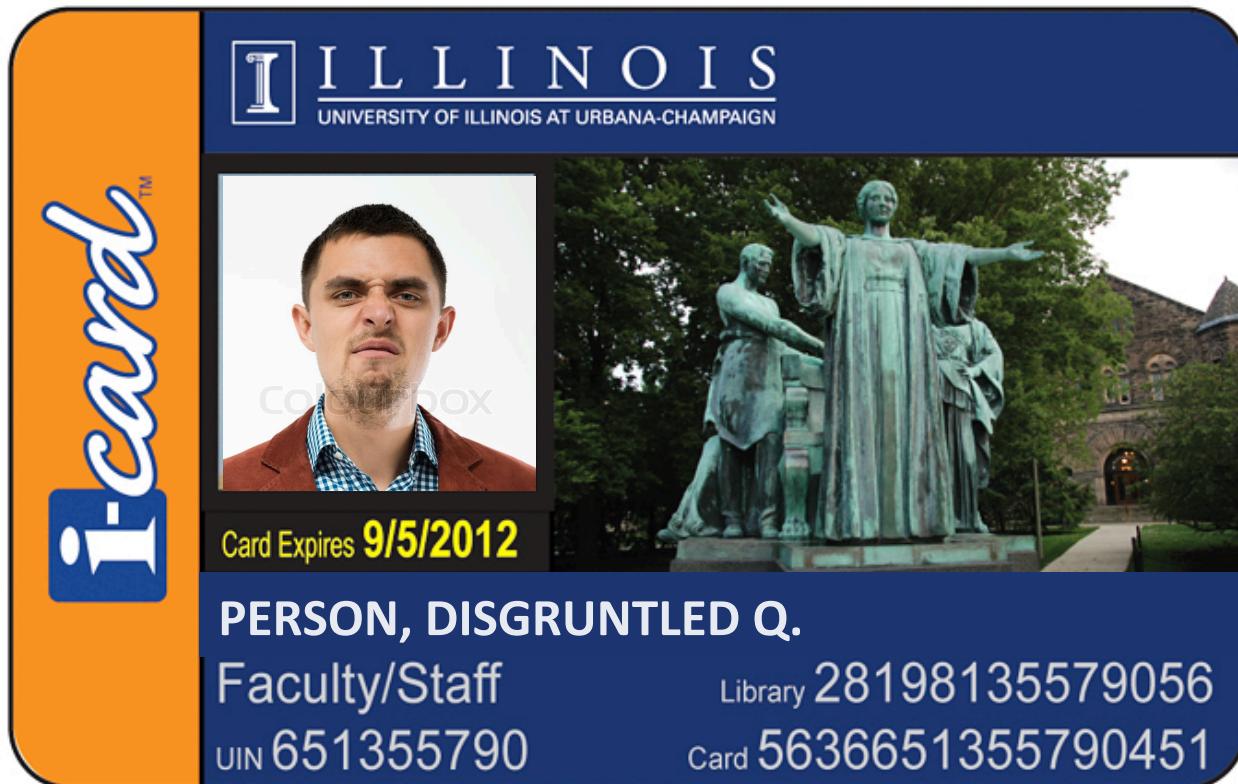
Bank of America



What am I trying to protect?



Who am I protecting it from?



Who am I protecting it from?

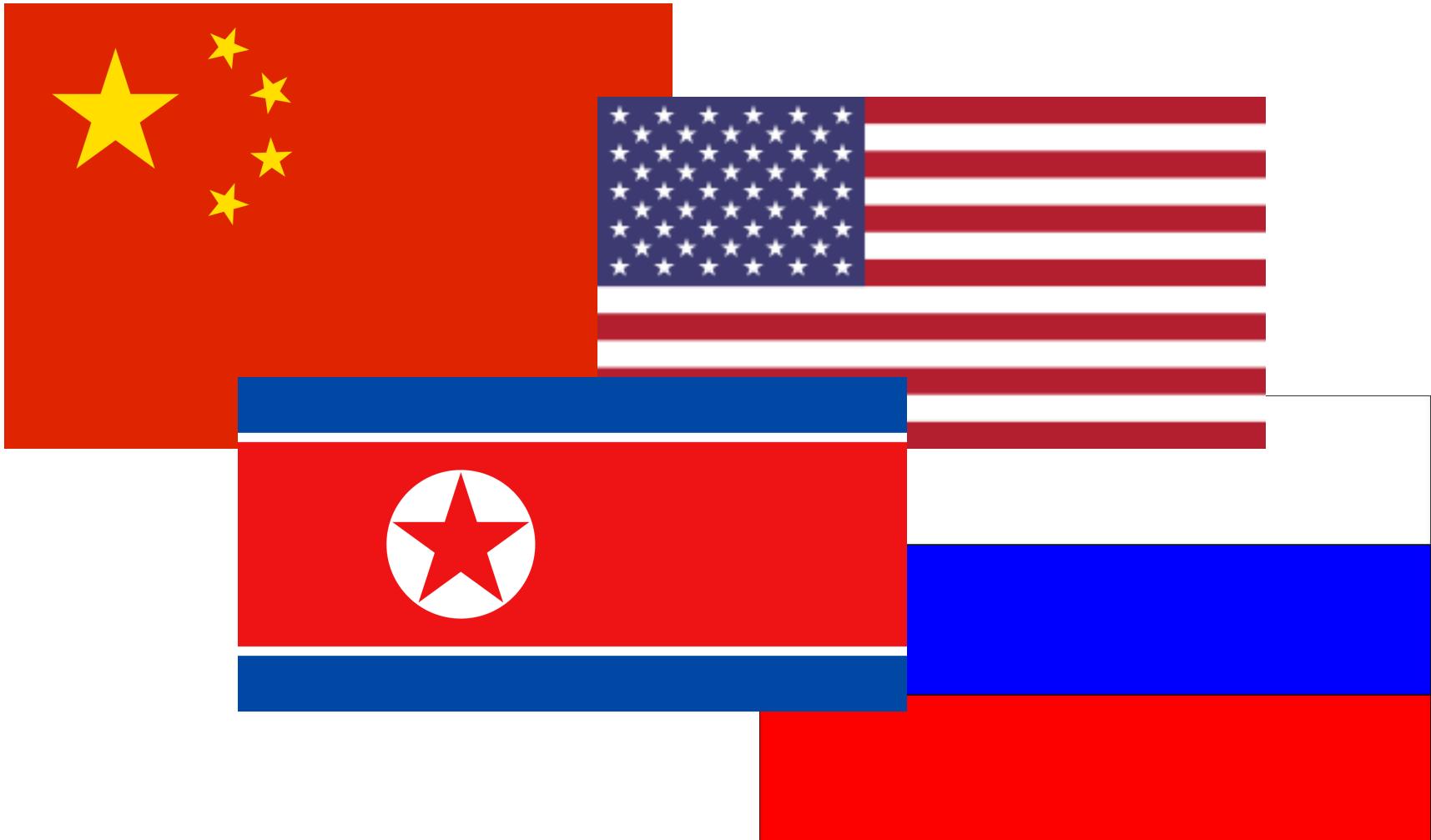


```
10000001
...1001110010...
010000001101111011C_1
001011011100110010...
101001011001010111011001...
10010000001101000110000101...
100110010000100000010010010C...
1001011011100010000001110100C...
01111011011100010111000100000010...
1000100111010101110100001010000...
1001110100...
001110110010101101110...
0001110100001101001011011010111...
01010010111000100000010010010...
0100011011101011110001000010...
1000111101100010...
001110111100101111001...
1001110110001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
```

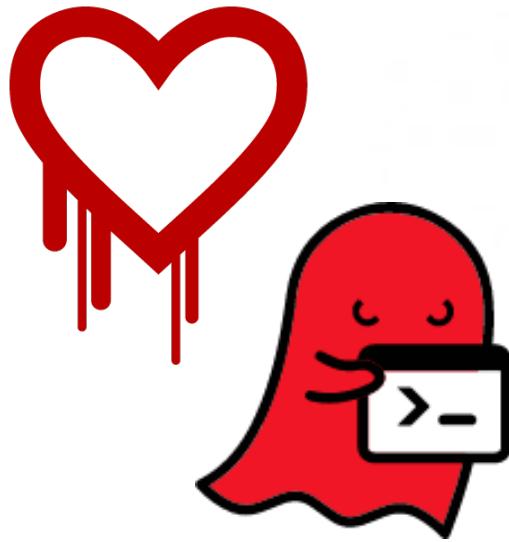
```
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
0011101111001011110001...
```



Who am I NOT protecting it from?



How will I lose it?



Questions?

1. Password Manager

1Password 6

The screenshot shows the 1Password 6 application window. On the left is a dark sidebar with a circular logo at the top. Below it are sections for 'All Vaults' (with a dropdown arrow) and 'Categories'. Under 'Categories', there are six items: Logins (45), Secure Notes (11), Credit Cards (5), Identities (2), Passwords (8), and Documents (2). At the bottom of the sidebar are icons for Help, Settings, and a gear.

+ New Item Share Sort

Search All Vaults

amazon Amazon (Toronto Of...

Amazon Rewards

4567 **** 1234

Apple ID (iCloud)

wendy.c.appleseed@g...

amazon AWS

admin@agilebits.com

CBC.ca

wendy.c.appleseed@g...

Cloak

wendy_appleseed@agil...

Cloak for Teams



CBC.ca

account

Wendy Appleseed

vault

Personal

username

wendy.c.appleseed@gmail.com

password

.....

website

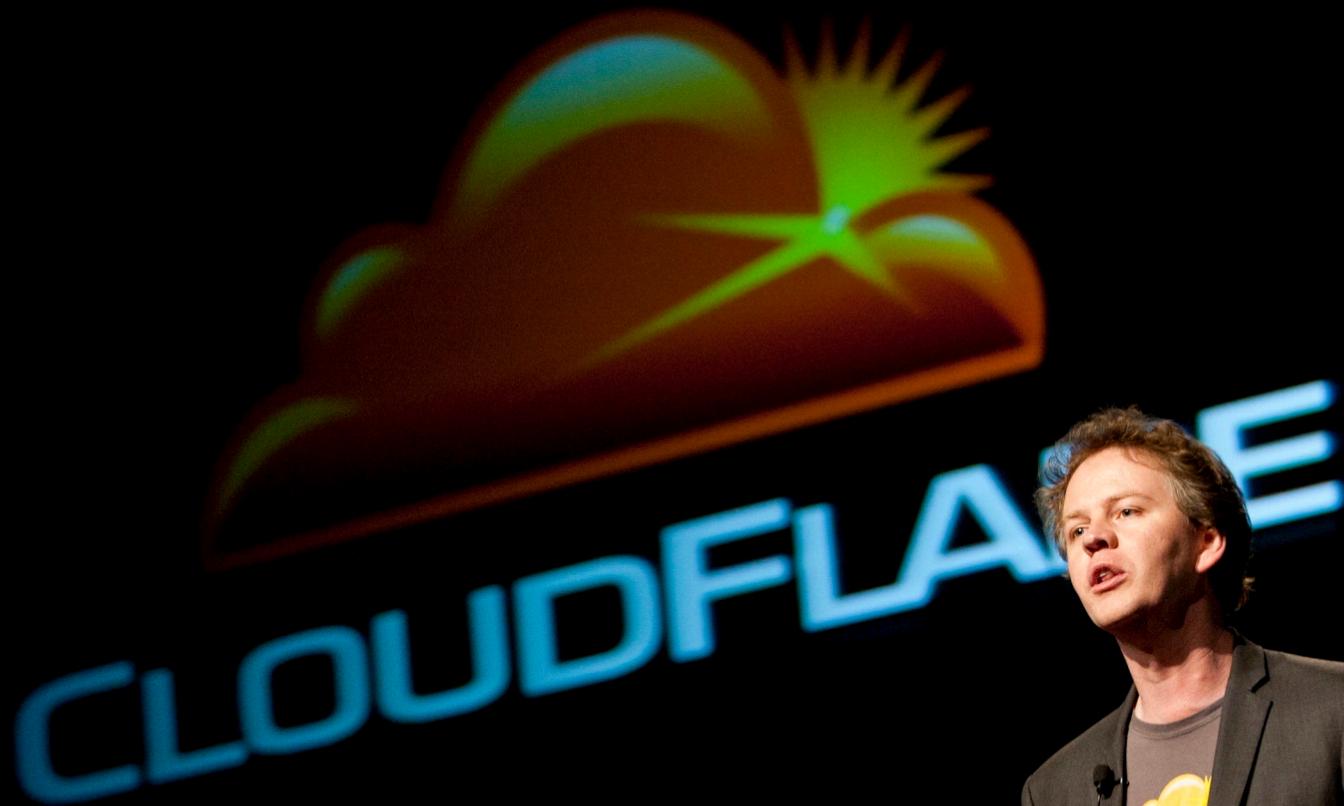
<http://www.cbc.ca/>



Show web form details

last mod... 10/24/16 3:05 PM

created 10/24/16 3:04 PM





Tavis Ormandy

@taviso

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.

| ▼ | chrome.exe | 2832 | 7.54 | 145.52 kB/s | 50.11 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
|---|------------------|------|------|-------------|----------|------------------------|---------------------------|--|--|--|--|
| | chrome.exe | 5332 | | | 1.7 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
| | chrome.exe | 3108 | | | 1.82 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
| | chrome.exe | 4940 | 4.41 | 42.08 kB/s | 44.92 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
| | chrome.exe | 5812 | 4.33 | 59.52 kB/s | 34.82 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
| | chrome.exe | 1416 | 0.96 | 38.19 kB/s | 49.83 MB | DESKT... Tavis Ormandy | Google Chrome | | | | |
| ▼ | cmd.exe | 5852 | | | 1.55 MB | DESKT... Tavis Ormandy | Windows Command Processor | | | | |
| | conhost.exe | 4464 | | | 5.16 MB | DESKT... Tavis Ormandy | Console Window Host | | | | |
| | ▼ nplastpass.exe | 5016 | 1.98 | 18.84 kB/s | 4.65 MB | DESKT... Tavis Ormandy | LastPass Plugin | | | | |
| | cmd.exe | 560 | | | 4.15 MB | DESKT... Tavis Ormandy | Windows Command Processor | | | | |
| | conhost.exe | 5592 | | | 5.88 MB | DESKT... Tavis Ormandy | Console Window Host | | | | |
| | cmd.exe | 2124 | | | 2.74 MB | DESKT... Tavis Ormandy | Windows Command Processor | | | | |

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

Tavis Ormandy

@taviso

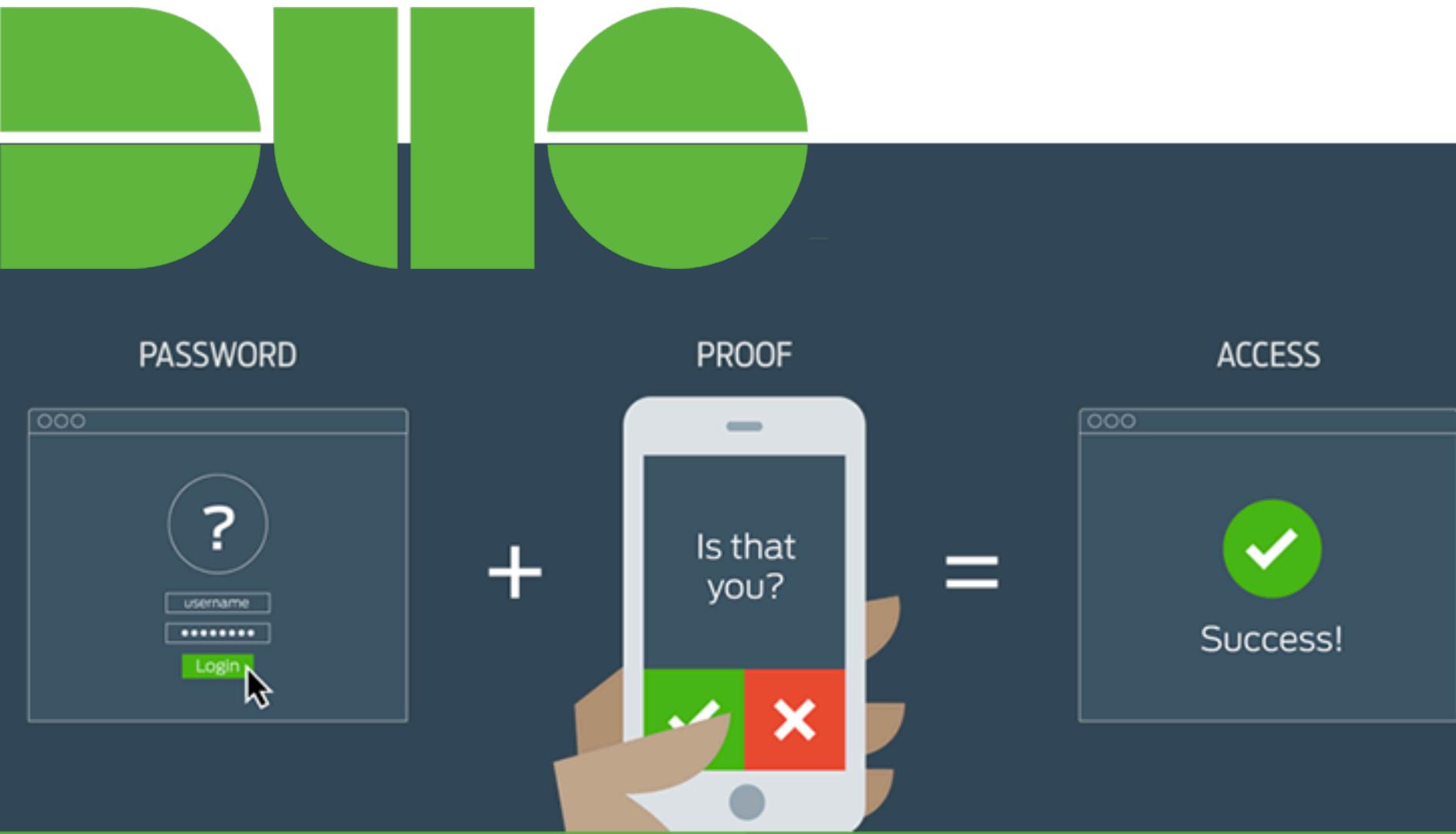
Vulnerability researcher at Google. This is a personal stream, opinions expressed are mine.

California

taviso.decsystem.org

Joined April 2008

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.

Automatically check for updates

- Download newly available updates in the background
You will be notified when the updates are ready to be installed

- Install app updates

- Install OS X updates

- Install system data files and security updates

Automatically download apps purchased on other Macs

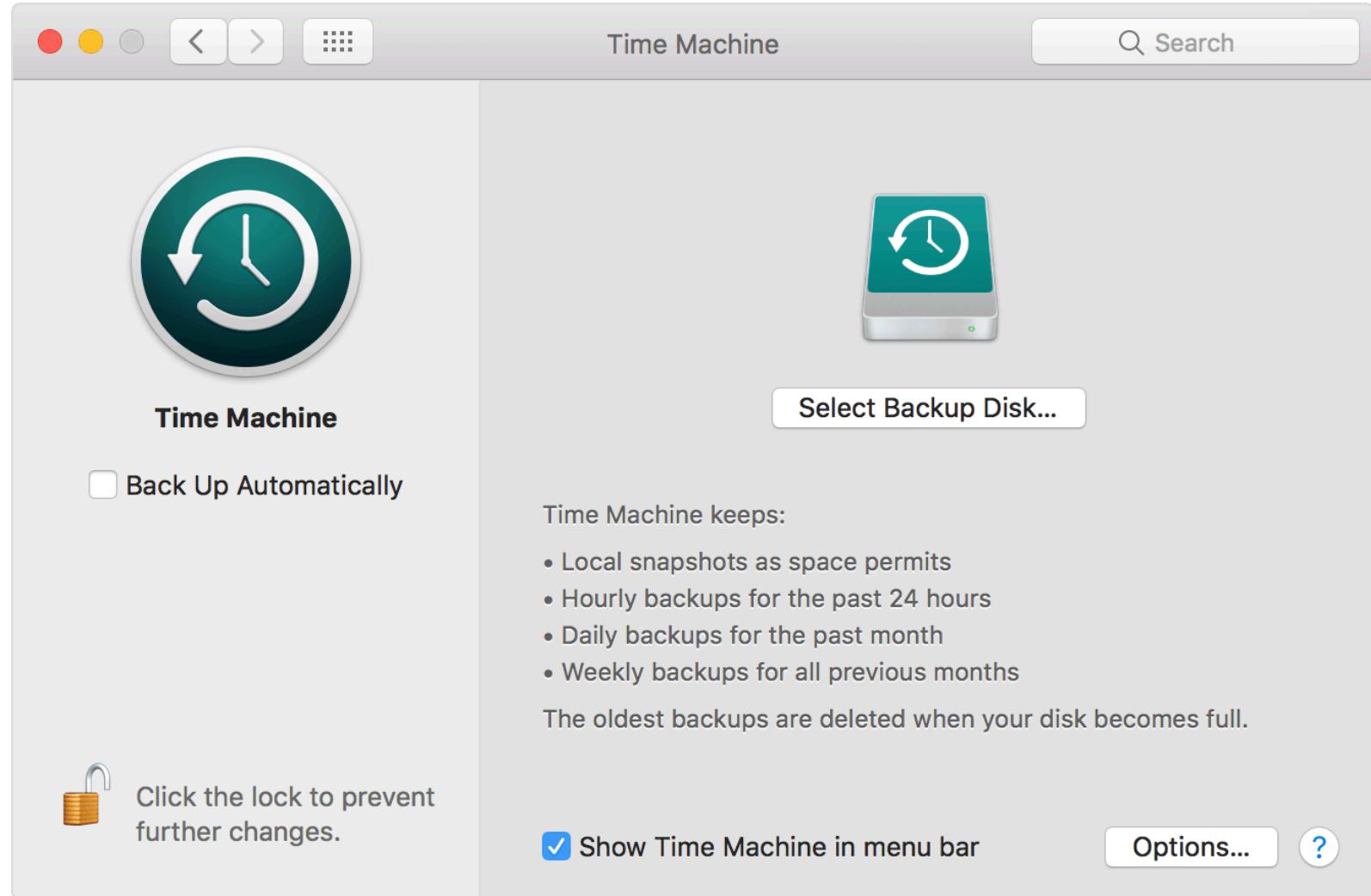
Can't determine if automatic downloads are enabled due to a network problem

Last check was Thursday, December 1, 2016

Check Now



4. Backups





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:

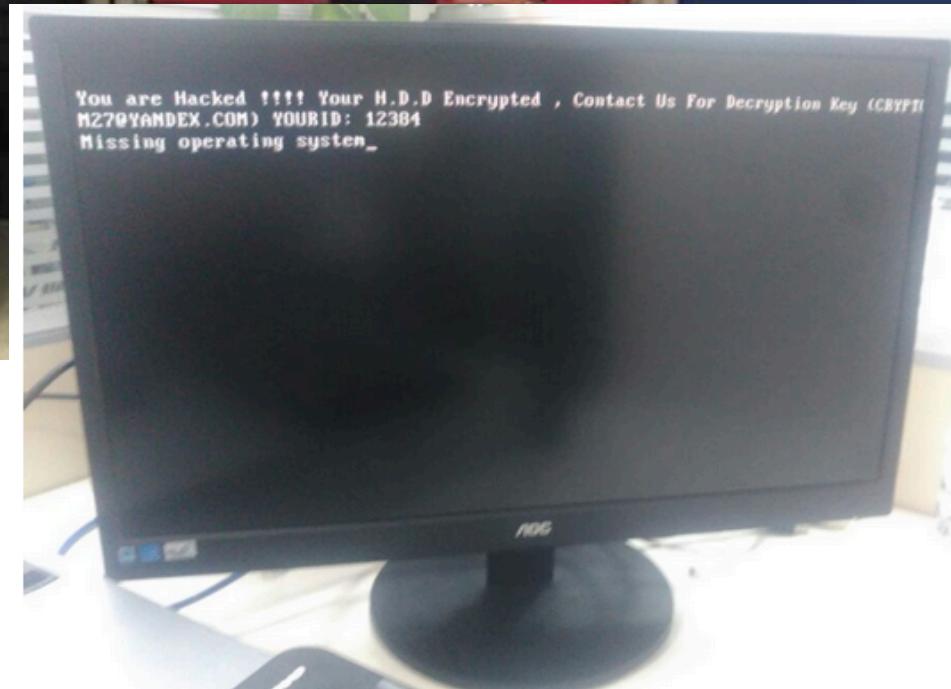
SECURE PAYMENT FORM

Enter the code MoneyPak

Please enter MoneyPak code
using pin pad below.

1 2 3 4 5 6 7 8 9 0 Clear

UNLOCK YOUR PC NOW!



5. Disk Encryption, Physical Security



Security & Privacy

General FileVault Firewall Privacy

 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".

Turn On FileVault...

Security & Privacy

General FileVault Firewall Privacy

A login password has been set for this user: **immediately** Change Password...

Require password 5 seconds after sleep or screen saver begins
 Show a message 1 minute
 Disable automatic login 5 minutes
Set Lock Message...
 15 minutes
 1 hour
 4 hours
 8 hours

Allow apps downloaded from:

Mac App Store Mac App Store and identified developers Anywhere

Advanced... ?

Click the lock to prevent further changes.

Advanced... ?

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.

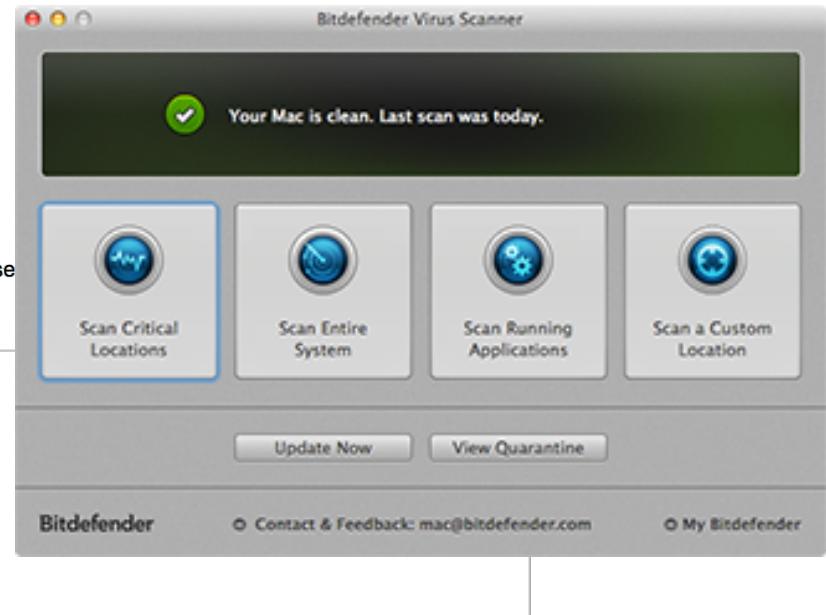
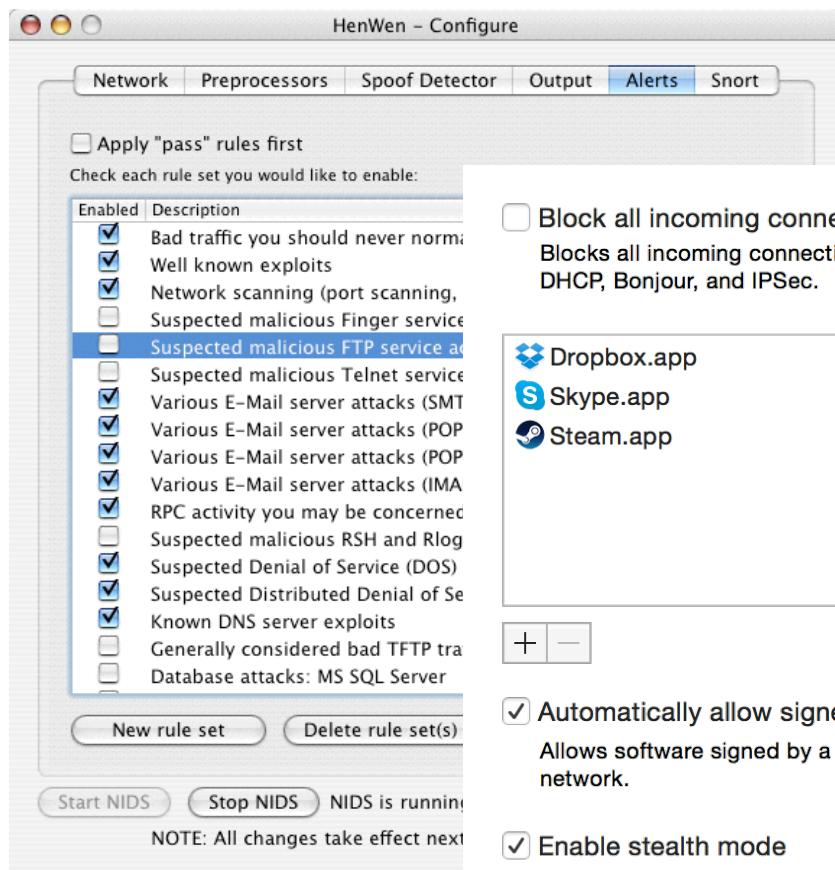
The data also contained the names, dates of birth and some disability ratings for up to 26.5 million veterans and some of their spouses, according to a VA statement. The stolen data does not contain medical records, the



Privacy Impact Assessment for the Border Searches of Electronic Devices

August 25, 2009

6. Firewall, IDS, AV



Block all incoming connections
Blocks all incoming connections except those from DHCP, Bonjour, and IPSec.

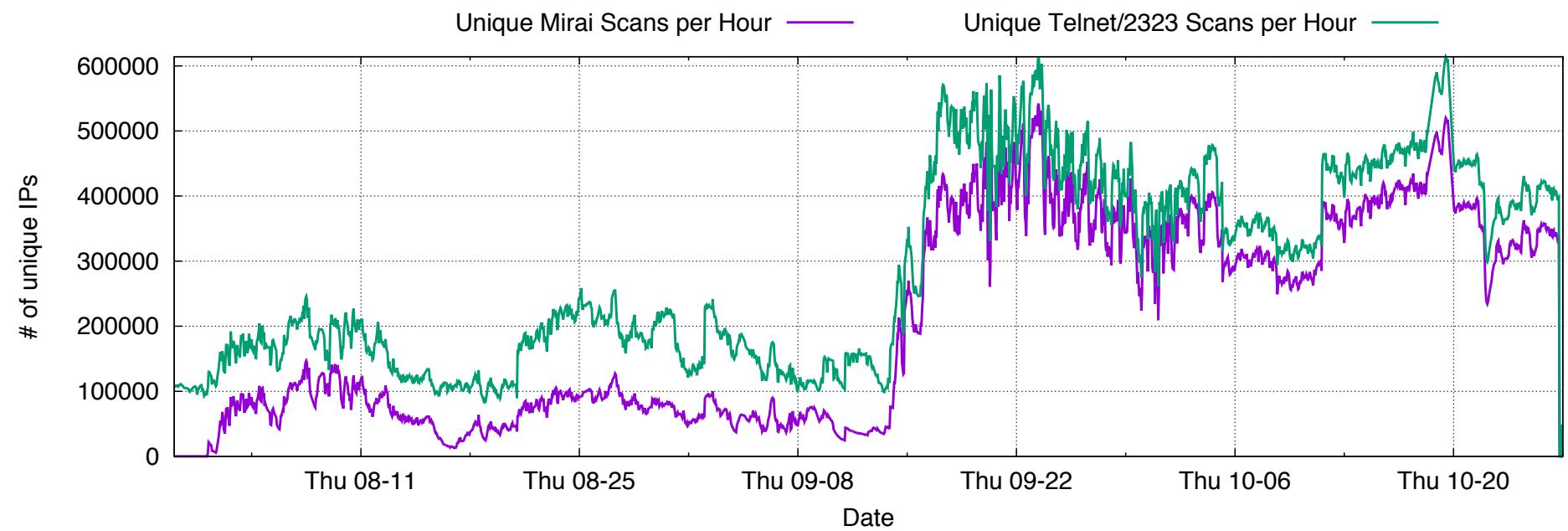
- Dropbox.app
- Skype.app
- Steam.app

Automatically allow signed software to receive incoming connections
Allows software signed by a valid certificate authority to provide services accessed from the network.

Enable stealth mode
Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

Cancel

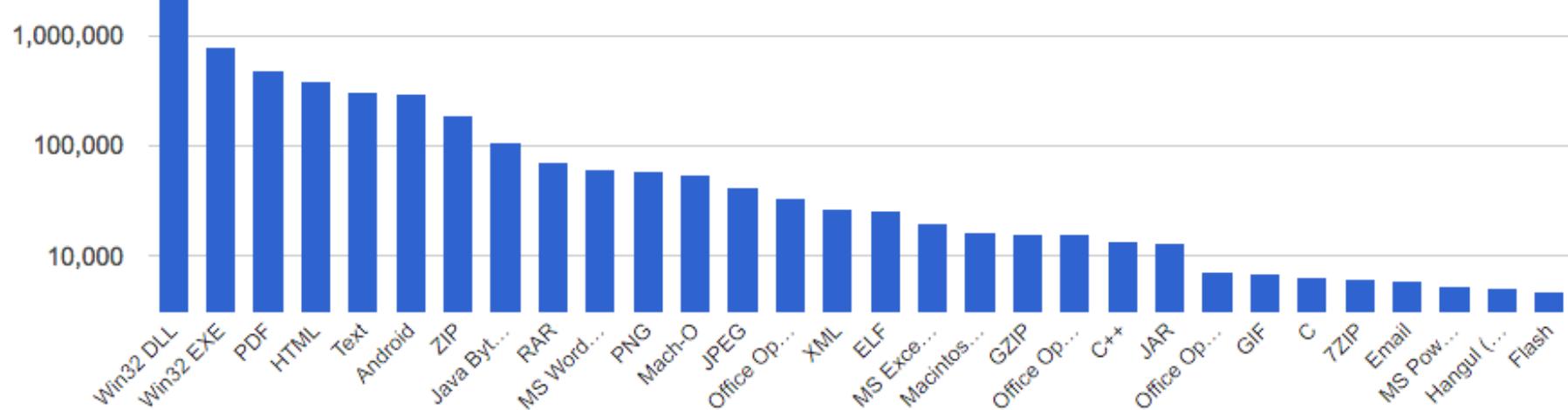
OK



Submissions

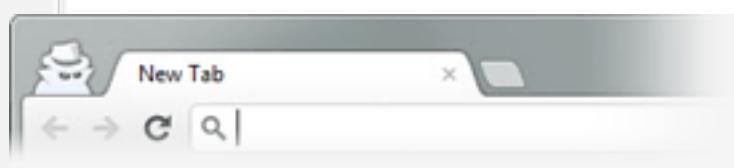


File types

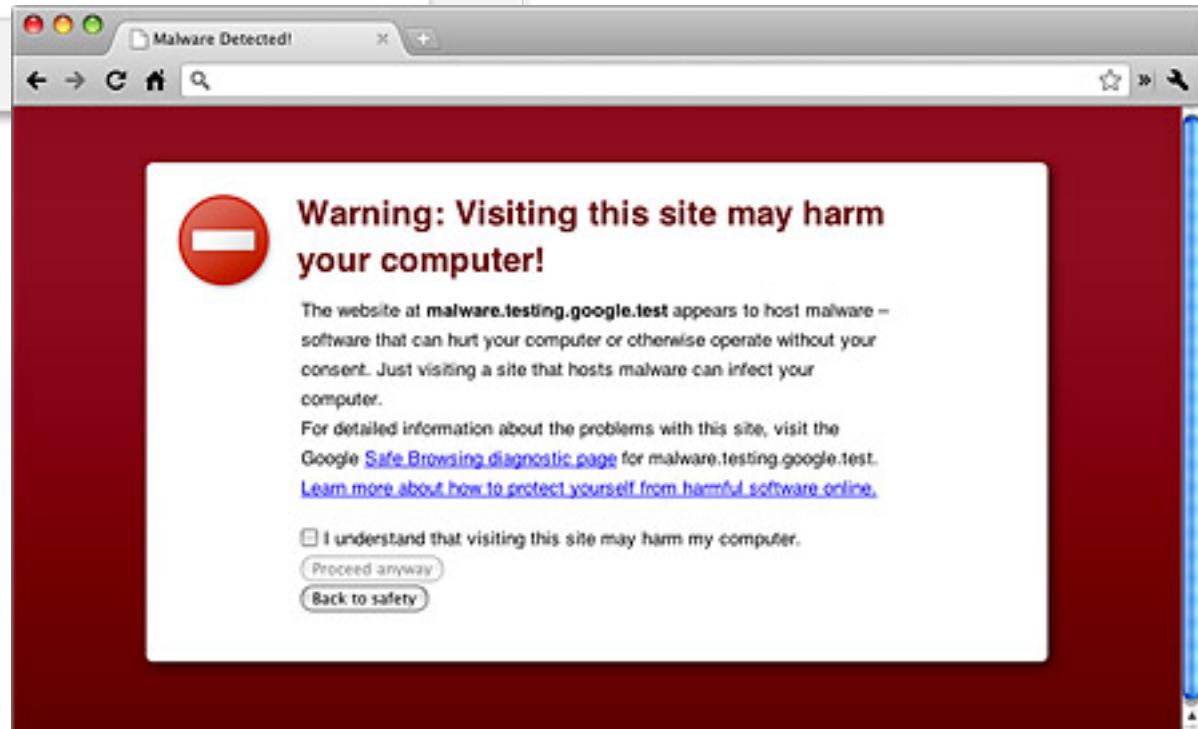


7. Safe Browsing

Eventual treatment of all
HTTP pages in Chrome:



 Not secure | example.com



7. Safe Browsing

The image shows a screenshot of the Google Chrome browser interface. On the left, a white circle highlights the 'Settings' option in the main navigation menu. To the right, a larger window displays the 'Content settings' dialog box.

Content settings

Cookies

- Allow local data to be set (recommended)
- Keep local data only until you quit your browser
- Block sites from setting any data
- Block third-party cookies and site data (highlighted)

Images

- Show all images (recommended)
- Do not show any images

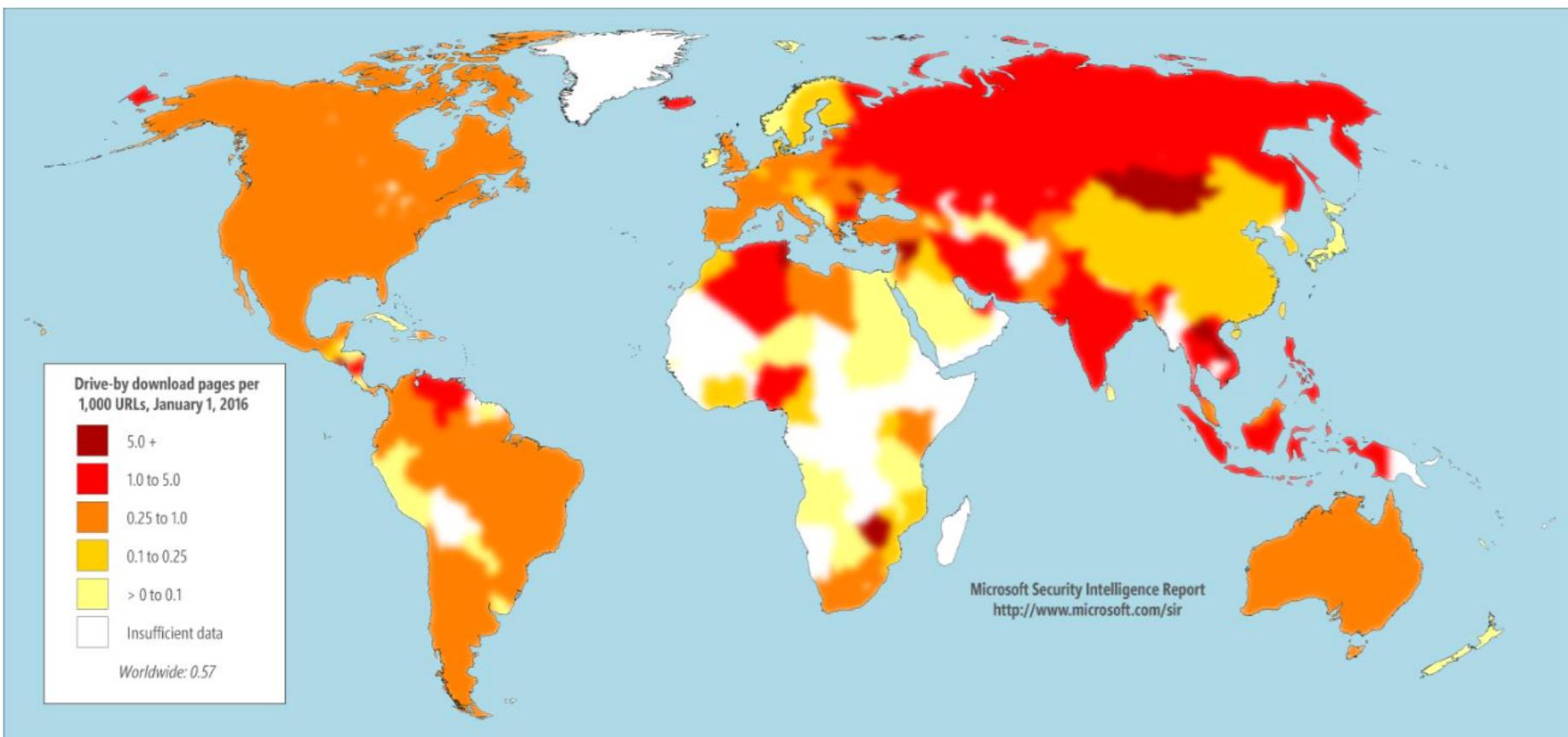
JavaScript

- Allow all sites to run JavaScript (recommended)
- Do not allow any site to run JavaScript (highlighted)

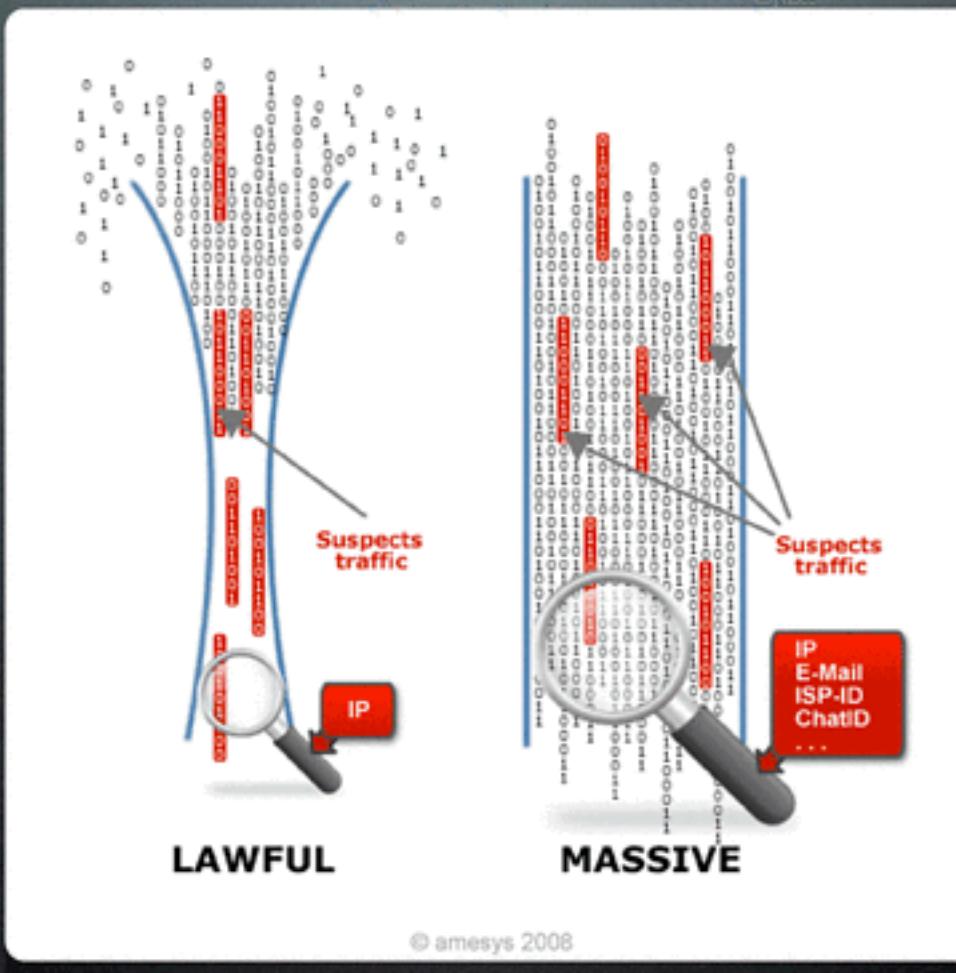
Buttons: Manage exceptions... All cookies and site data...

7. Safe Browsing





Lawful vs Massive



The Watershed Rehab

www.thewatershed.com/Help - Drug & Alcohol Rehabilitation Call Today For Help Now!

Ads by Google



8. Safe Communication

Screenshot of Mail.app settings showing multiple accounts and junk mail filtering options.

Accounts Overview:

| Description | Server Name | In Use By Account |
|-------------|-----------------------|-------------------|
| Gmail | mail.b.hostedemail... | Michigan, Monkey |
| Gmail | smtp.gmail.com | Usenix |
| Gmail | smtp.gmail.com | Google |

Account Information (Left Panel):

- Port: 587
- Authentication: Password
- Allow insecure connections
- User Name: No Selection
- Password: [redacted]

Advanced Tab Options:

- General
- Accounts
- Junk Mail
- Fonts & Colors
- Viewing
- Composing
- Signatures
- Rules

Advanced Tab Content (Left Panel):

- Automatically detect and maintain account settings
- Enable junk mail filtering
- When junk mail arrives:
 - Mark as junk mail, but leave it in my Inbox
 - Move it to the Junk mailbox
 - Perform custom actions (Click Advanced to configure)
- The following types of messages are exempt from junk mail filtering:
 - Sender of message is in my Contacts
 - Sender of message is in my Previous Recipients
 - Message is addressed using my full name
- Trust junk mail headers in messages
- Filter junk mail before applying my rules

Advanced Tab Content (Right Panel):

- Automatically detect and maintain account settings
- Include when automatically checking for new messages
- Compact mailboxes automatically
- Automatically download all attachments
- Send large attachments with Mail Drop

Check with your system administrator before changing any of the advanced options below:

- IMAP Path Prefix: [redacted]
- Port: 993 Use SSL
- Authentication: Password
- Allow insecure authentication
- Use IDLE command if the server supports it

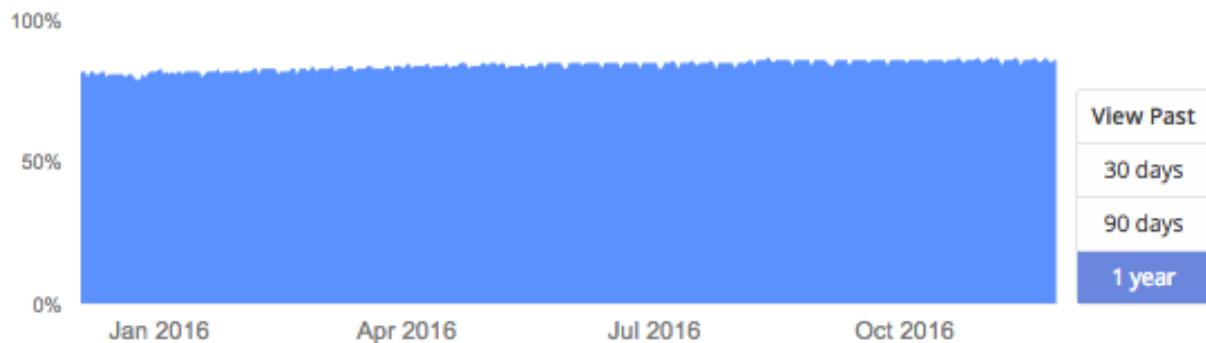
For support, visit [Google](#)

Outbound

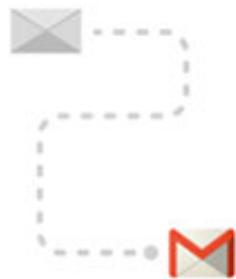


86%

Messages from
Gmail to other
providers.

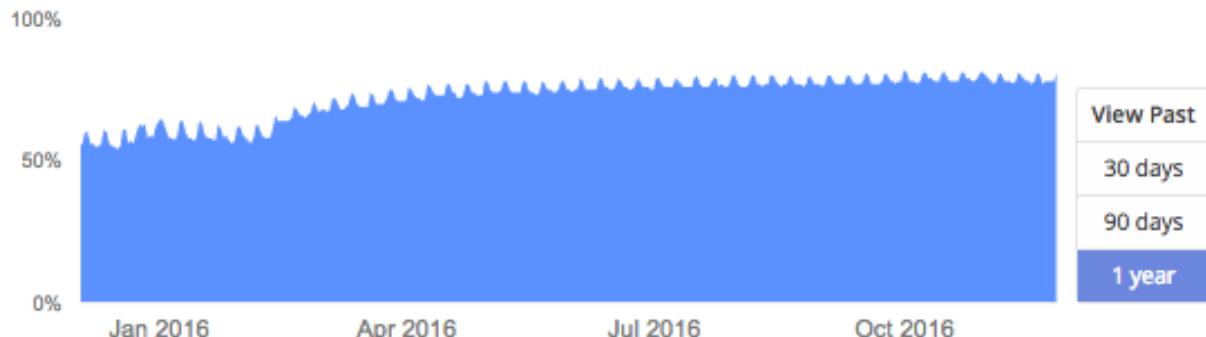


Inbound



81%

Messages from
other providers
to Gmail.



New Message

John Doe 

Account Information

Hi

Some recipients use services that don't support encryption

He



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



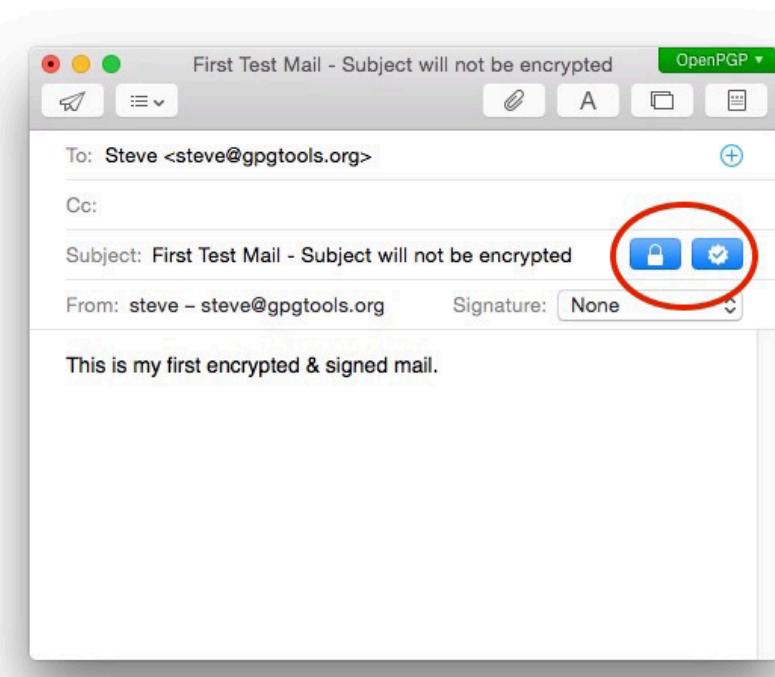
Send

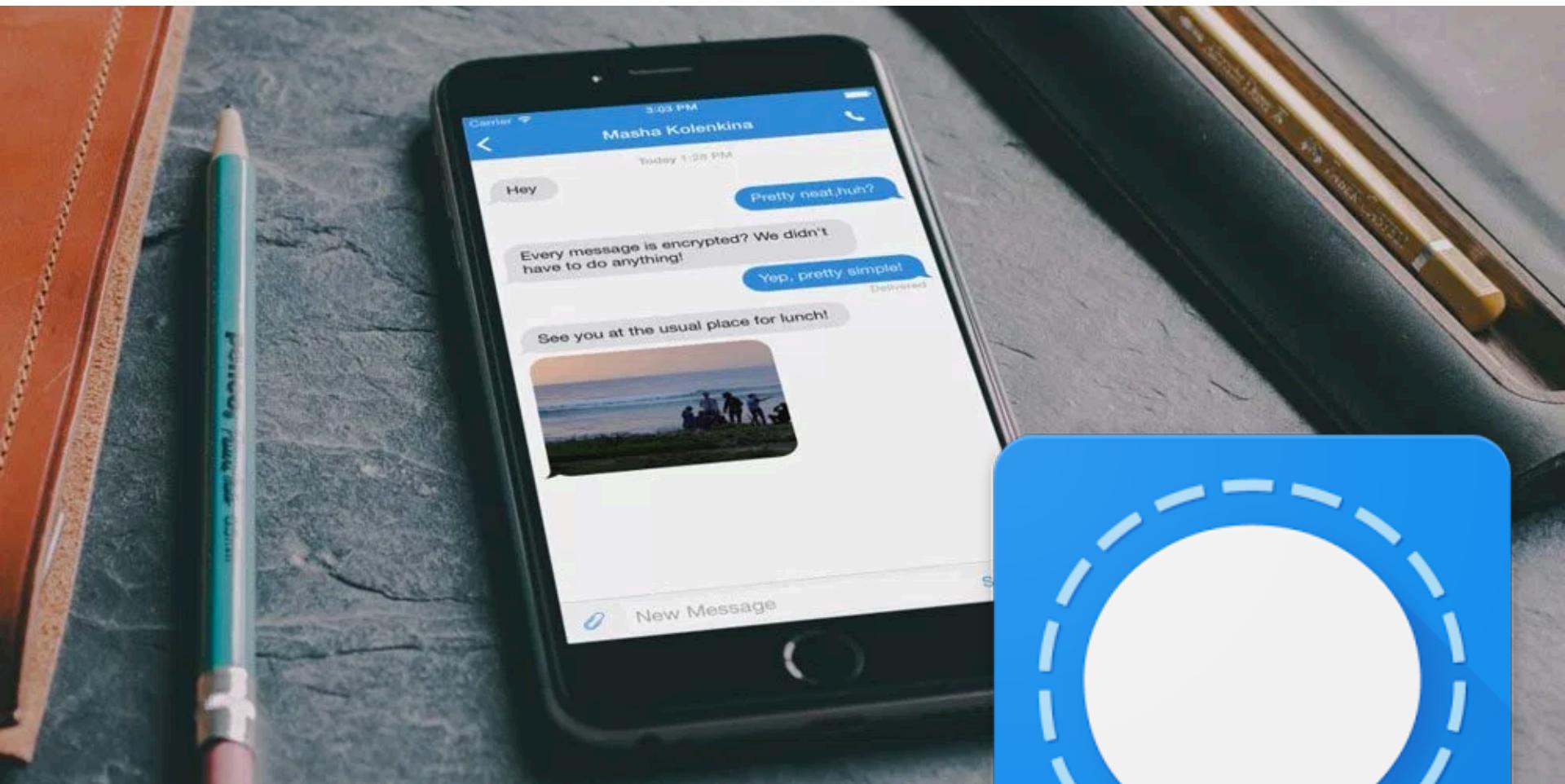
A



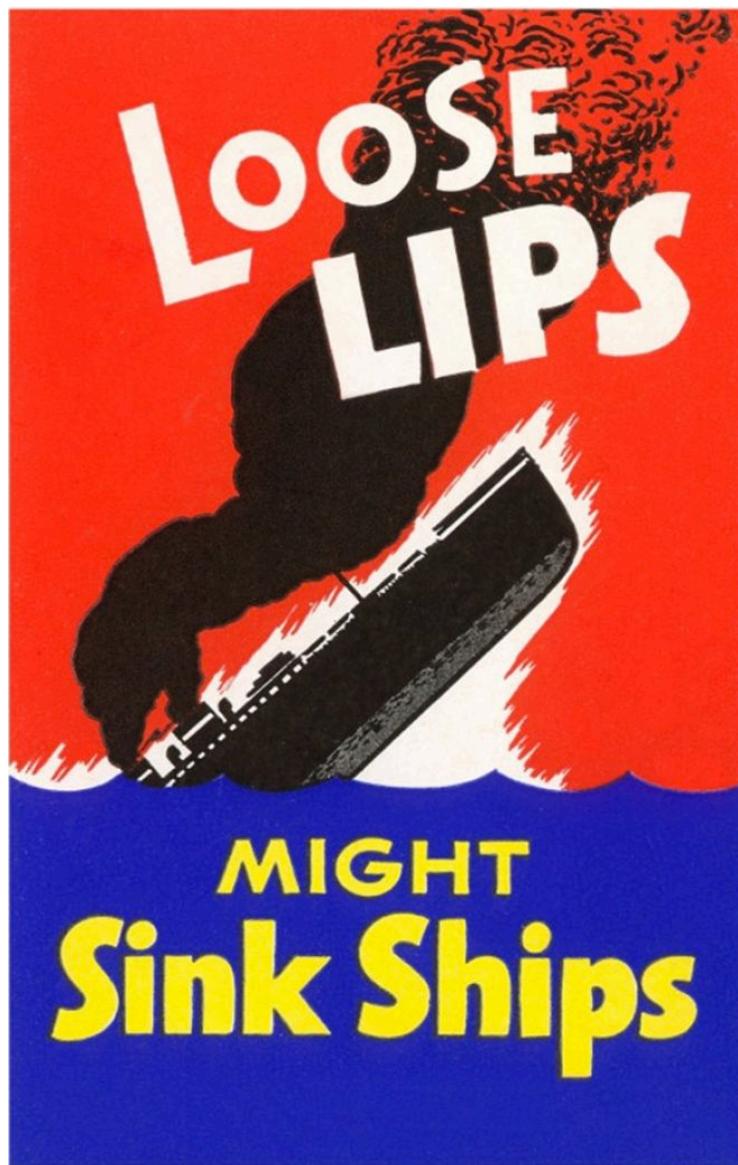
\$







9. Think Before You Share



Home 1

Update Status | Add Photos/Video | Create Photo Album

What's on your mind?

Friends ▾

47 mins ·

Google

Michael

Privacy Shortcuts

Privacy Checkup

Who can see my stuff?

Who can contact me?

How do I stop someone from bothering me?

← 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





10. Security is a Process

Schneier on Security



KrebsOnSecurity

In-depth security news and investigation



InformationWeek

DARKReading