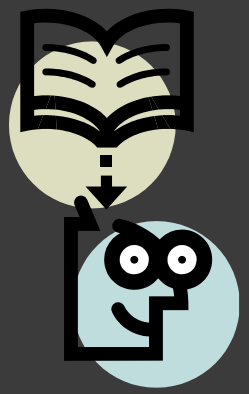
Western Intergovernmental Audit Forum
September 13, 2013

IT SECURITY AWARENESS

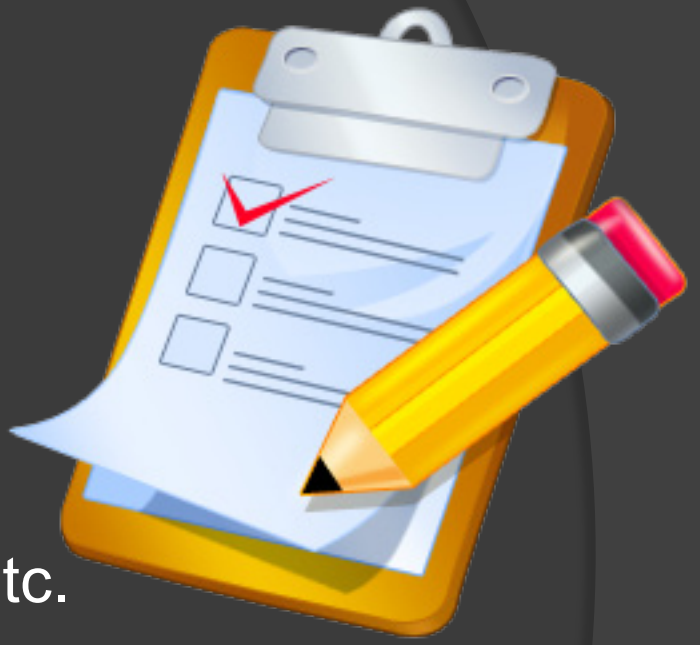
Melinda Gardner, CISA
- Senior IT Auditor
- Office of the Auditor General, AZ

Objectives



- Attendees will:
  - Understand security
  - Be familiar with current attack vectors
  - Learn practical steps to promote security

Agenda



- Importance?
- Attack Vectors
  - Mobile devices, social media
  - Passwords, social engineering, etc.
- Security Myths
- Q & A

Why should I care about computer security?

- Secure your personal/business info
- Bad guys go for low hanging fruit
- Increased dissemination of personal information
- Mobile transactions/devices

Article – hackers learned who friends were and sent IM's from friends names

Topic: Malware

Follow via:

Report: Cyberattackers hit Google staff via friends

Summary: *People behind the China-based online attacks of Google and other companies looked up key employees on social networks and contacted them pretending to be their friends to get the workers to click on links leading to malware, according to a report.*

By Elinor Mills | January 26, 2010 -- 06:40 GMT (22:40 PST)

Comments 17 Votes 0 Share more +

People behind the China-based online attacks of Google and other companies looked up key employees on social networks and contacted them pretending to be their friends to get the workers to click on links leading to malware, according to a published report on Monday.

"The most significant discovery is that the attackers had selected employees at the companies with access to proprietary data, then learned who their friends were," the Financial Times reported. "The hackers compromised the social network accounts of those friends, hoping to enhance the probability that their final targets would click on the links they sent."

The attackers used a popular instant-messaging program to distribute the malware link to target employees, George Kurtz, chief technology officer at security firm McAfee, told the Financial Times. The malware exploited a hole in Internet Explorer that Microsoft patched just last week.

For more on this story, read "Report: Attackers sent Google workers IMs from 'friends'" on CNET News.

Security Topics

- Mobile Devices
- Public Wi-Fi
- Social Media
- Passwords
- Social Engineering - Spearfishing
- Common Myths

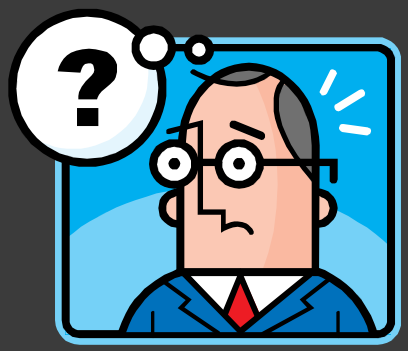
Mobile Device Security

- Mobile Devices
  - Laptops
  - Tablets
  - Smart Phones
- Threats
  - Theft
  - Data Leakage
  - Malware

Mobile Devices

- **Protect the Device**

- **Avoid questionable Apps!!!**



App Stores

	Android	Apple	Windows
Vet programs (review/ test code/ permissions)	X		
Show Permissions?		X	
Market Share	68%	17%	3%

App Questions to ask yourself

- Is this app from a trust worthy developer?
  - Lots of reviews?
- Does it look like Malware?
  - Bad reviews?
  - “Google” it

- Do I understand why this app needs these permissions?
- Does the developer explain to me why they need these permissions?

★★★★★ (159)

INSTALL

More from developer

Block Mania Free
HANA MOBILE LLC
★★★★½ (71)
Free

English-Chinese Dict
HANA MOBILE LLC
★★★☆☆ (149)
Free

Backgrounds
HANA MOBILE LLC
★★★½☆ (150)
Free

Tiny Dream Tower
HANA MOBILE LLC
★★★★☆ (261)
Free

See more ›

Users who viewed this also viewed

Aladdin & Wonderful Lamp
PLAYTALES BOOKS
★★★★☆ (20)
Free

Advanced Task Killer
RECHILD
★★★★½ (431,270)
Free

Permissions

THIS APPLICATION HAS ACCESS TO THE FOLLOWING:

YOUR LOCATION

APPROXIMATE LOCATION (NETWORK-BASED)

Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.

NETWORK COMMUNICATION

FULL NETWORK ACCESS

Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.

PHONE CALLS

READ PHONE STATUS AND IDENTITY

Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.

STORAGE

MODIFY OR DELETE THE CONTENTS OF YOUR USB STORAGE

Allows the app to write to the USB storage.

SYSTEM TOOLS

PREVENT DEVICE FROM SLEEPING

Allows the app to prevent the device from going to sleep.

Hide

NETWORK COMMUNICATION

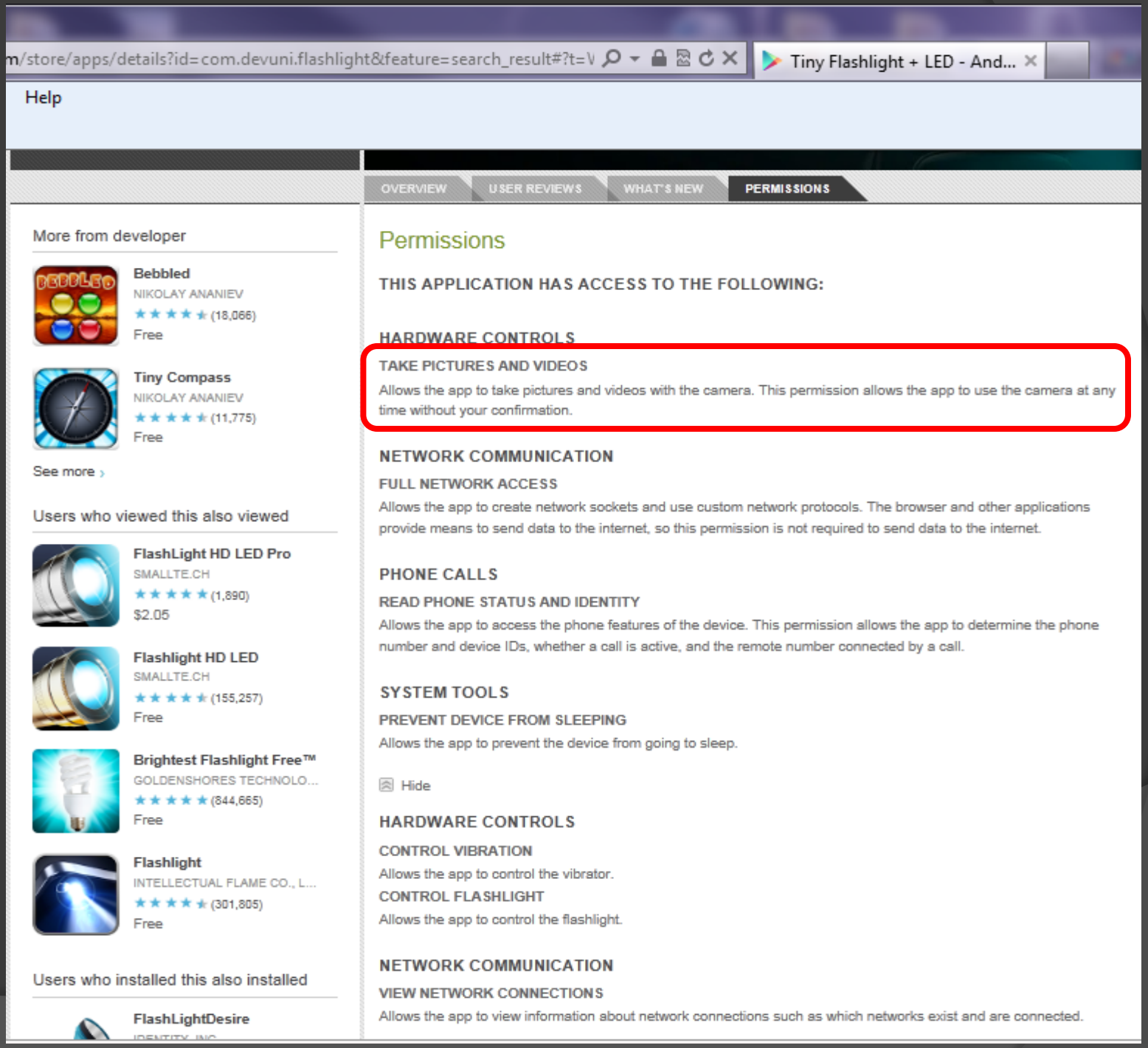
VIEW NETWORK CONNECTIONS

Allows the app to view information about network connections such as which networks exist and are connected.

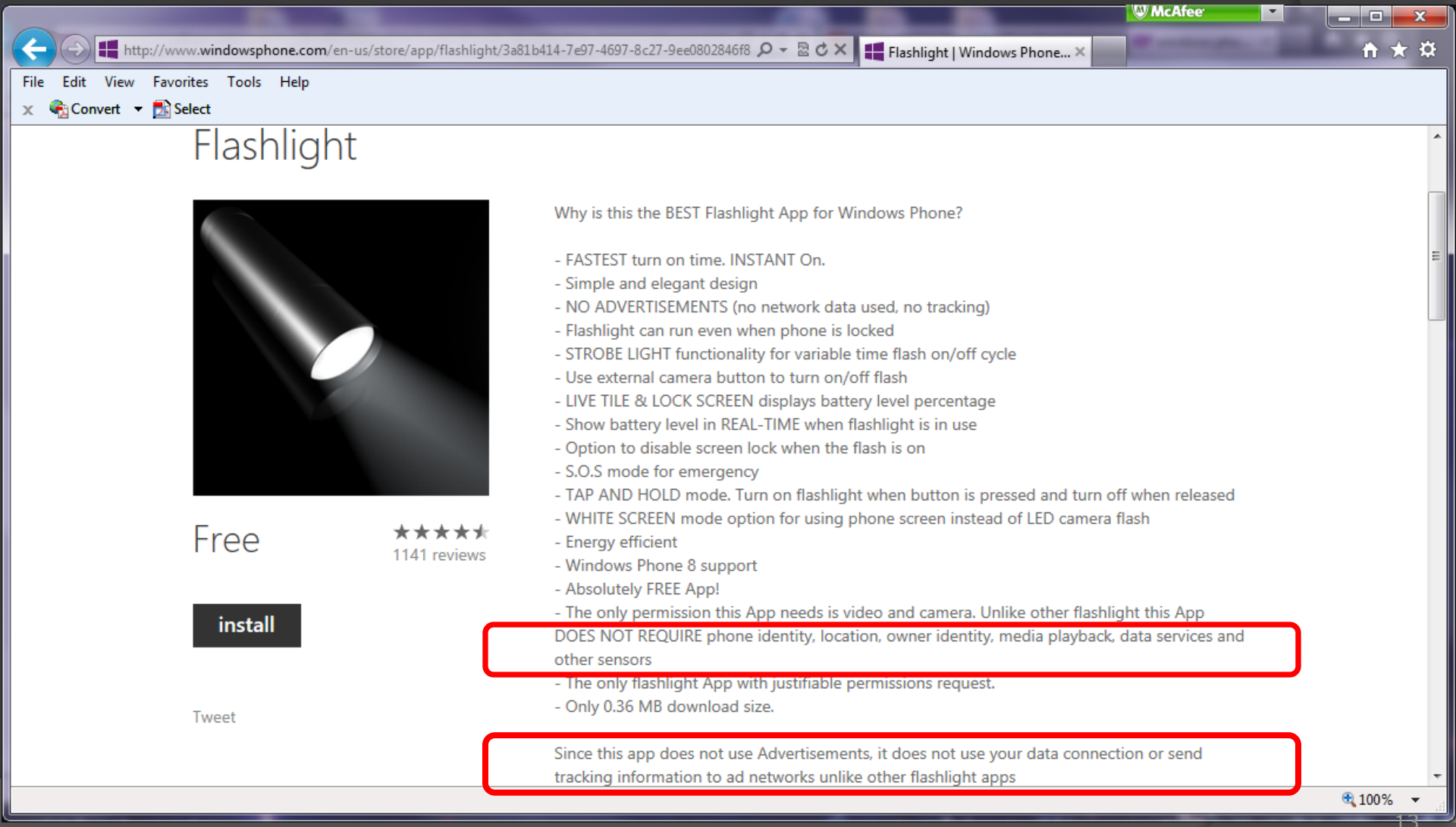
DEFAULT

TEST ACCESS TO PROTECTED STORAGE

Allows the app to test a permission for USB storage that will be available on future devices.


m/store/apps/details?id=com.devuni.flashlight&feature=search_result#?t=V
Tiny Flashlight + LED - And...
Help
OVERVIEW
USER REVIEWS
WHAT'S NEW
PERMISSIONS
More from developer
Bebbled
NIKOLAY ANANIEV
(18,066)
Free
Tiny Compass
NIKOLAY ANANIEV
(11,775)
Free
See more
Users who viewed this also viewed
FlashLight HD LED Pro
SMALLTE.CH
(1,890)
$2.05
Flashlight HD LED
SMALLTE.CH
(155,257)
Free
Brightest Flashlight Free™
GOLDENSHORES TECHNOLO...
(844,665)
Free
Flashlight
INTELLECTUAL FLAME CO., L...
(301,805)
Free
Users who installed this also installed
FlashLightDesire
Permissions
THIS APPLICATION HAS ACCESS TO THE FOLLOWING:
HARDWARE CONTROLS
TAKE PICTURES AND VIDEOS
Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.
NETWORK COMMUNICATION
FULL NETWORK ACCESS
Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.
PHONE CALLS
READ PHONE STATUS AND IDENTITY
Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.
SYSTEM TOOLS
PREVENT DEVICE FROM SLEEPING
Allows the app to prevent the device from going to sleep.
Hide
HARDWARE CONTROLS
CONTROL VIBRATION
Allows the app to control the vibrator.
CONTROL FLASHLIGHT
Allows the app to control the flashlight.
NETWORK COMMUNICATION
VIEW NETWORK CONNECTIONS
Allows the app to view information about network connections such as which networks exist and are connected.

Apps


http://www.windowsphone.com/en-us/store/app/flashlight/3a81b414-7e97-4697-8c27-9ee0802846f8
Flashlight | Windows Phone...
File Edit View Favorites Tools Help
Convert Select
Flashlight
Free
1141 reviews
install
Tweet
Why is this the BEST Flashlight App for Windows Phone?
- FASTEST turn on time. INSTANT On.
- Simple and elegant design
- NO ADVERTISEMENTS (no network data used, no tracking)
- Flashlight can run even when phone is locked
- STROBE LIGHT functionality for variable time flash on/off cycle
- Use external camera button to turn on/off flash
- LIVE TILE & LOCK SCREEN displays battery level percentage
- Show battery level in REAL-TIME when flashlight is in use
- Option to disable screen lock when the flash is on
- S.O.S mode for emergency
- TAP AND HOLD mode. Turn on flashlight when button is pressed and turn off when released
- WHITE SCREEN mode option for using phone screen instead of LED camera flash
- Energy efficient
- Windows Phone 8 support
- Absolutely FREE App!
- The only permission this App needs is video and camera. Unlike other flashlight this App DOES NOT REQUIRE phone identity, location, owner identity, media playback, data services and other sensors
- The only flashlight App with justifiable permissions request.
- Only 0.36 MB download size.
Since this app does not use Advertisements, it does not use your data connection or send tracking information to ad networks unlike other flashlight apps
100%

Mobile Devices

- Security Methods
  - **Protect the data**
    - Lock
    - Encrypt
      - Lots of Apps
    - Backup
      - Android – Back up to Google servers, install app
      - Apple – Backup to iTunes account (iCloud)

Mobile Devices

- Security Methods
  - **Protect the Apps**
    - Review your apps
    - Don't root/jailbreak device

    - Install Antivirus
      - Android – Multiple apps in Google Play
      - Apple - built-in security features, but antivirus still a good idea

http://www.pcadvisor.co.uk/features/security/3418367/do-apple-macs-need-antivirus-os-x-security-explained/

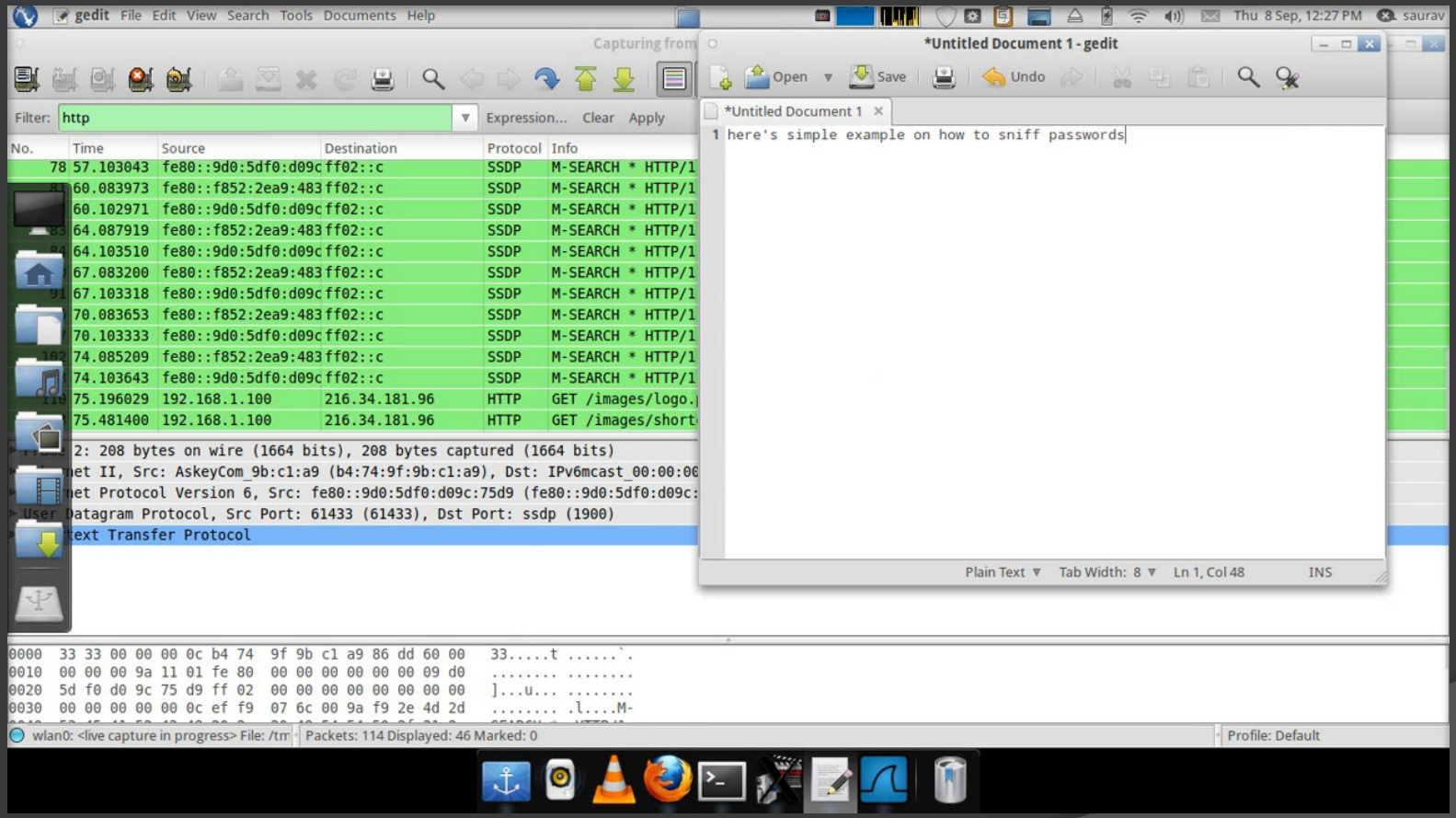
Mobile Devices - Demo

- Apple
  - Find My iPhone - http://howto.cnet.com/8301-11310_39-20078442-285/how-to-set-up-find-my-iphone-on-your-ios-device/
- Android
  - Bitdefender Anti-Theft
  - DEMO

Public Wi-Fi

- Public WiFi Locations
  - Hotels
  - Coffee Shops
  - Airports
  - Neighbors
- Threats
  - Sniffers:
    - Demo (Videos)
  - Shared Files/Folders

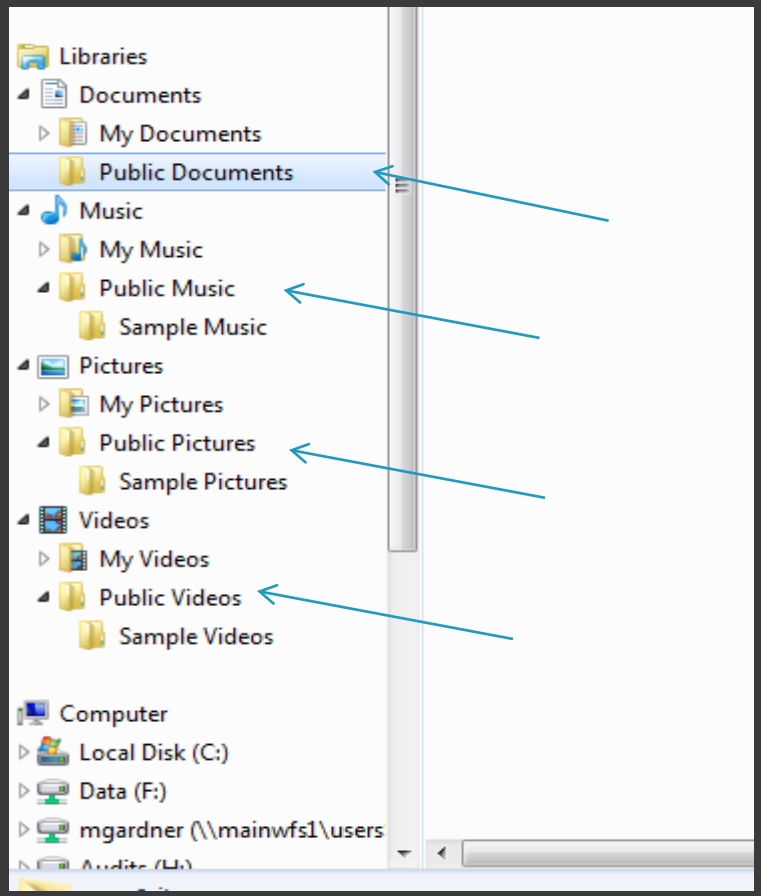
Sniffer - Wireshark



Firesheep


Firefox File Edit View History Bookmarks Tools Window Help
Twitter
http://twitter.com/
Firesheep
Start Capturing
A new Twitter experience is coming! Learn more about it... #NewTwitter
twitter
Search
The best way to discover what's new in your world.
Have an account? Sign in
New to Twitter?
Easy, free, and instant updates. Get access to the information that interests you most.
Sign Up ›
A #NewTwitter
Catch a glimpse of the new Twitter.com.
Marcelino Camacho Barnes & Noble Ceuta Marie Claire Nook Color Pound Drop TRENDING TOPICS
See who's here
Friends and industry peers you know. Celebrities you watch. Businesses you frequent. Find them all on Twitter.
Top Tweets View all ›
SeaShepherd We are getting reports that the dolphin slaughter has begun in the cove in Taiji, Japan. More information coming soon. #seashepherd #thecove
33 minutes ago
jelani9 I find it odd when black people say "voting doesn't matter." I usually ask "Then why did they fight so hard to keep us from doing it?"
4 hours ago
CHSpurgeon Whether we teach young Christians truth or not, the devil will be sure to teach them error.
4 hours ago
Waiting for s3.amazonaws.com...

Shared Docs



These will be seen by anyone on the public wifi you connect to

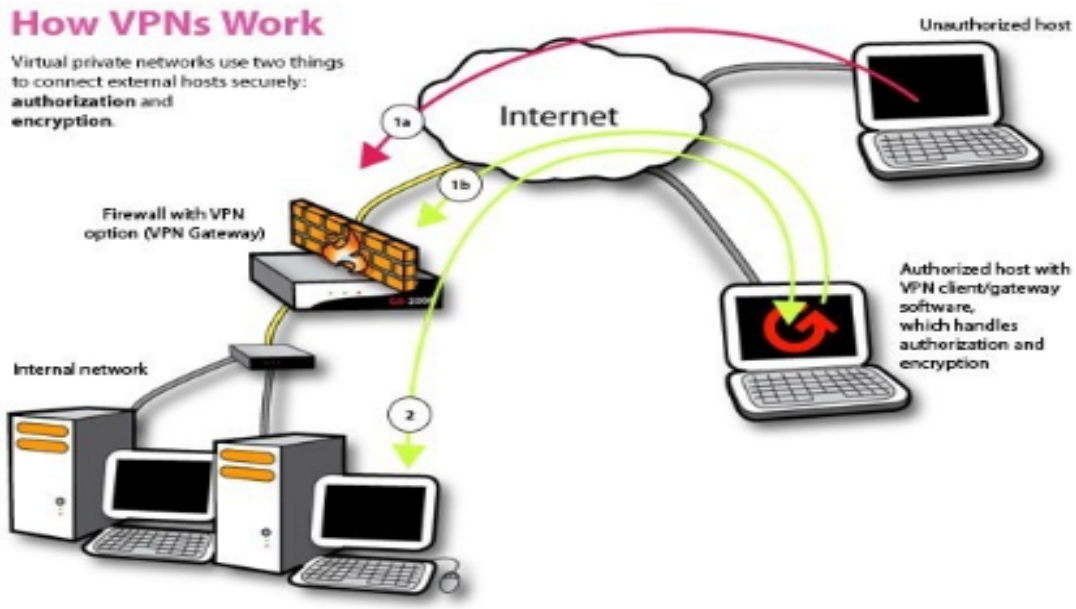
Public Wi-Fi

- Protecting Yourself
  - Disable – “Automatically connect to non-preferred networks” (Some windows versions)
  - Enable “https” and “SSL” in app settings
  - Use a VPN
    - CNET download of spotfly- free VPN

6 Best Free VPN Services to Protect Your Privacy

Posted on August 10, 2012 by Squad Admin in Websites with 2 Comments

With the expansion of Internet service, many of the websites have been banned in many countries and even in schools and offices. There are many instances where some services are available only in selected countries like US and UK. If you are facing these issues, a Free VPN (Virtual Private Network) will help you solve these problems. Apart from these VPN services allows you to browse the web anonymously. Here is a list of services offering FREE VPN accounts.



1. HideIPVPN: This service offers FREE VPN accounts on servers located in United States and United Kingdom. You can access blocked sites using this VPN service. The service offers 100 new free accounts per month, so follow their website to know when the free account giveaway starts.

2. USA IP: You can get free PPTP, L2TP and OpenVPN testing account compatible with Mac OS, Windows 7, Vista, XP, Linux from USA IP. The demo access is unlimited in time but you are required to reconnect after every 7 minutes.

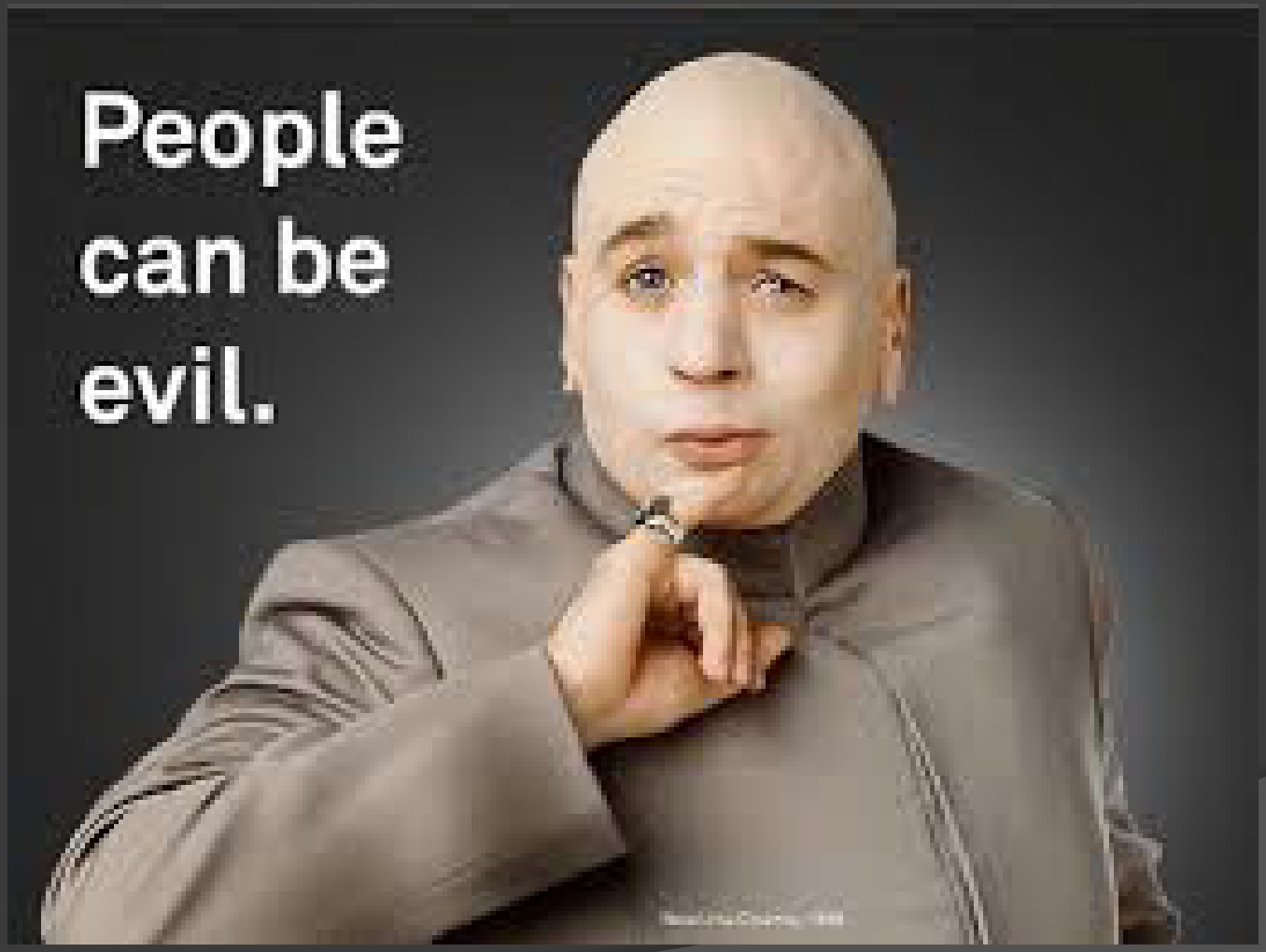
3. MacroVPN: This is another service offering FREE VPN, but with restrictions. The free account is limited

Social Media

- **Social media** refers to the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks.

Social Media Sites

Social Media



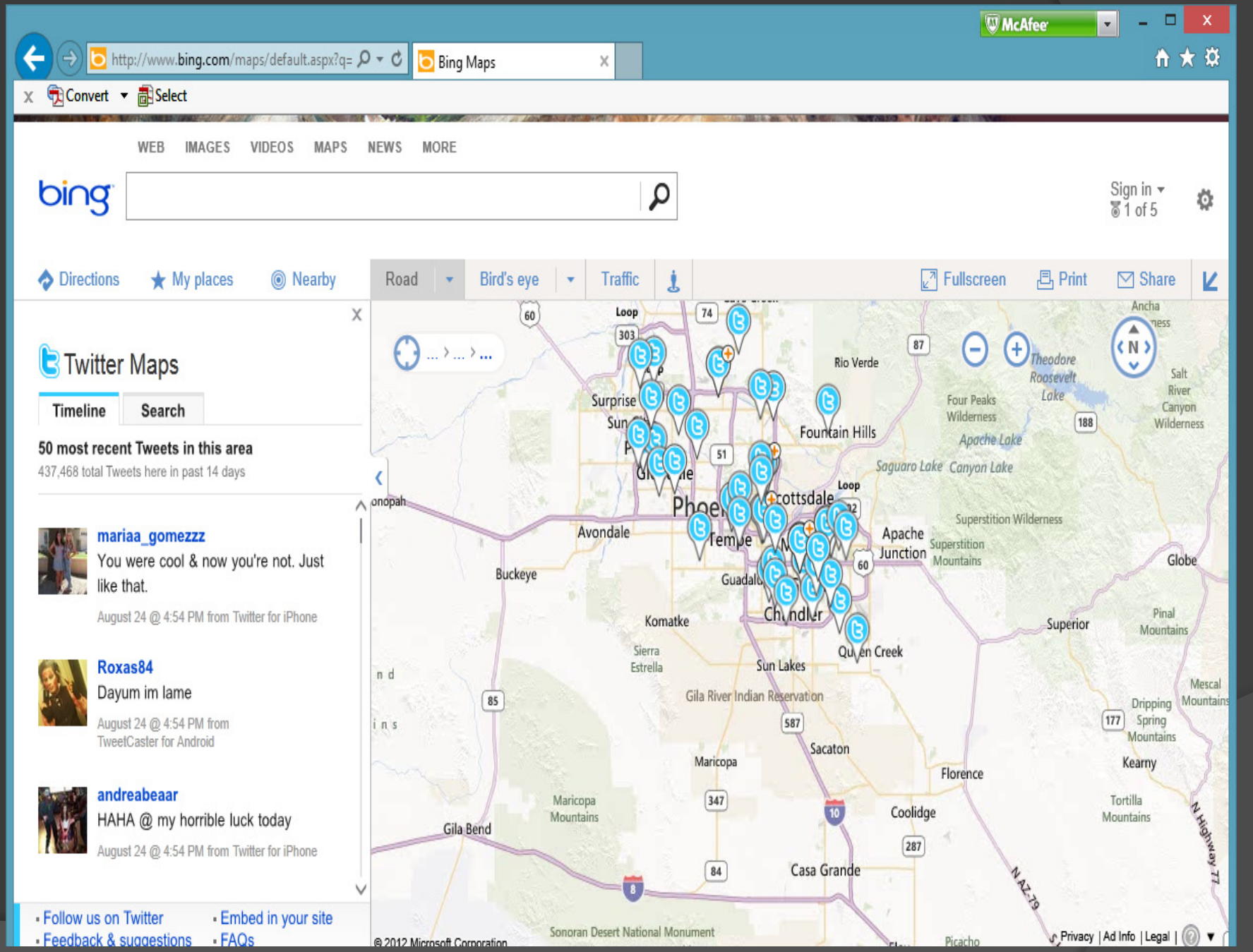
Social Media

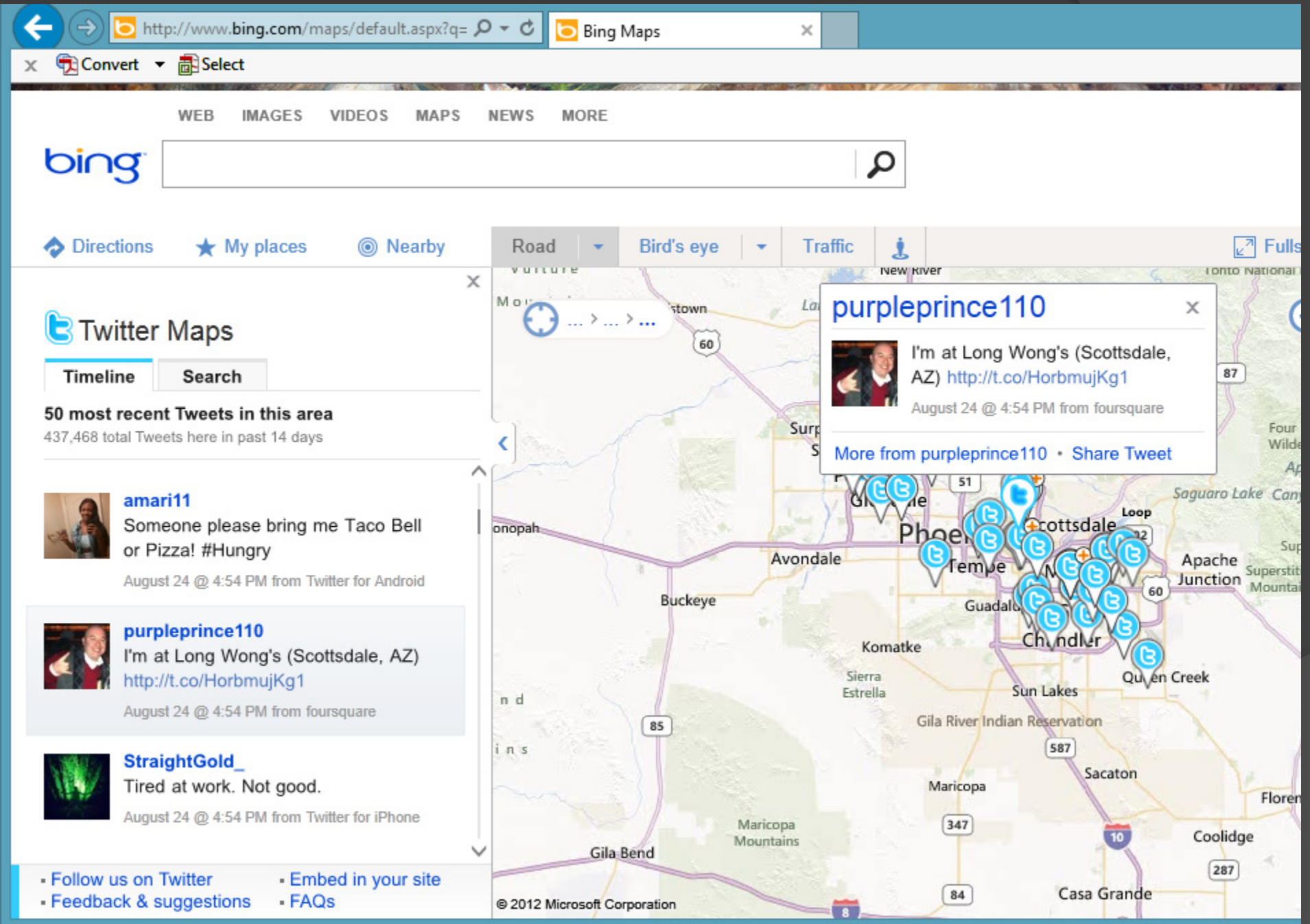
- http://www.geoimgr.com/

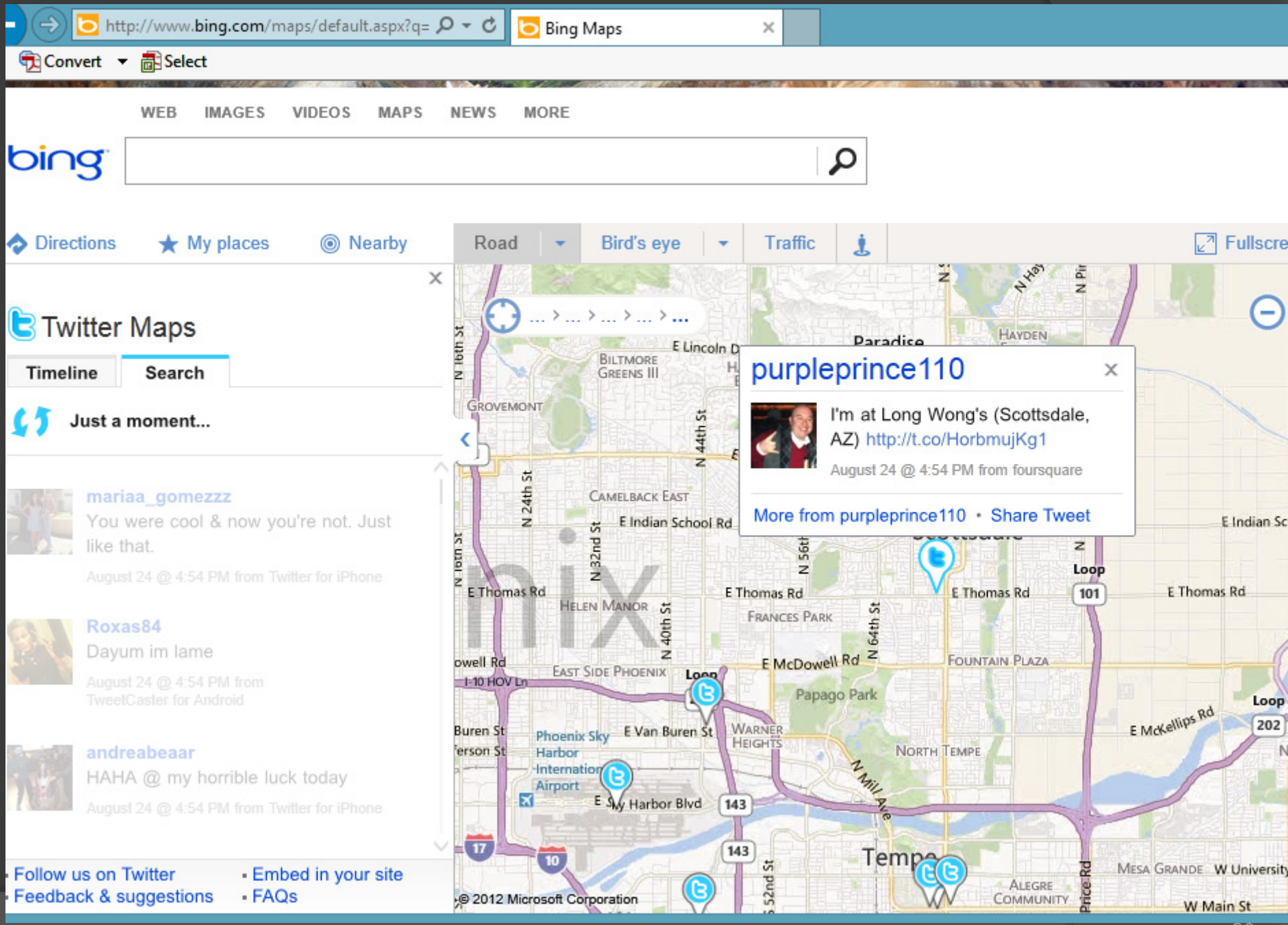
GPS

Social Media

- Bing Maps
  - Application – Twitter Maps
    - Pulls information from different sources
      - Twitter/Foursquare/Instagram/Snapseed
- Bing → Maps→ Explore more maps → twitter maps
- TMI- posting too much information!


McAfee
http://www.bing.com/maps/default.aspx?q=
Bing Maps
Convert
Select
WEB
IMAGES
VIDEOS
MAPS
NEWS
MORE
bing
Sign in
1 of 5
Directions
My places
Nearby
Road
Bird's eye
Traffic
Fullscreen
Print
Share
Twitter Maps
Timeline
Search
50 most recent Tweets in this area
437,468 total Tweets here in past 14 days
mariaa_gomezzz
You were cool & now you're not. Just like that.
August 24 @ 4:54 PM from Twitter for iPhone
Roxas84
Dayum im lame
August 24 @ 4:54 PM from TweetCaster for Android
andreabeaar
HAHA @ my horrible luck today
August 24 @ 4:54 PM from Twitter for iPhone
Follow us on Twitter
Embed in your site
Feedback & suggestions
FAQs
Loop
Rio Verde
Surprise
Fountain Hills
Four Peaks Wilderness
Theodore Roosevelt Lake
Apache Lake
Saguaro Lake
Canyon Lake
Salt River Canyon Wilderness
Avondale
Tempe
Apache Junction
Superstition Wilderness
Superstition Mountains
Globe
Buckeye
Komatke
Chandler
Superior
Pinal Mountains
Sierra Estrella
Sun Lakes
Queen Creek
Gila River Indian Reservation
Mescal Mountains
Dripping Spring Mountains
Sacaton
Maricopa
Florence
Kearny
Maricopa Mountains
Coolidge
Tortilla Mountains
Gila Bend
Casa Grande
Sonoran Desert National Monument
© 2012 Microsoft Corporation
Privacy | Ad Info | Legal


http://www.bing.com/maps/default.aspx?q=
Bing Maps
Convert
Select
WEB
IMAGES
VIDEOS
MAPS
NEWS
MORE
bing
Directions
My places
Nearby
Road
Bird's eye
Traffic
Twitter Maps
Timeline
Search
50 most recent Tweets in this area
437,468 total Tweets here in past 14 days
amari11
Someone please bring me Taco Bell or Pizza! #Hungry
August 24 @ 4:54 PM from Twitter for Android
purpleprince110
I'm at Long Wong's (Scottsdale, AZ) http://t.co/HorbmujKg1
August 24 @ 4:54 PM from foursquare
StraightGold_
Tired at work. Not good.
August 24 @ 4:54 PM from Twitter for iPhone
Follow us on Twitter
Embed in your site
Feedback & suggestions
FAQs
purpleprince110
I'm at Long Wong's (Scottsdale, AZ) http://t.co/HorbmujKg1
August 24 @ 4:54 PM from foursquare
More from purpleprince110 • Share Tweet
Avondale
Buckeye
Komatke
Sierra Estrella
Sun Lakes
Gila River Indian Reservation
Maricopa
Sacaton
Maricopa Mountains
Gila Bend
Casa Grande
Coolidge
Apache Junction
Saguaro Lake
Loop
© 2012 Microsoft Corporation

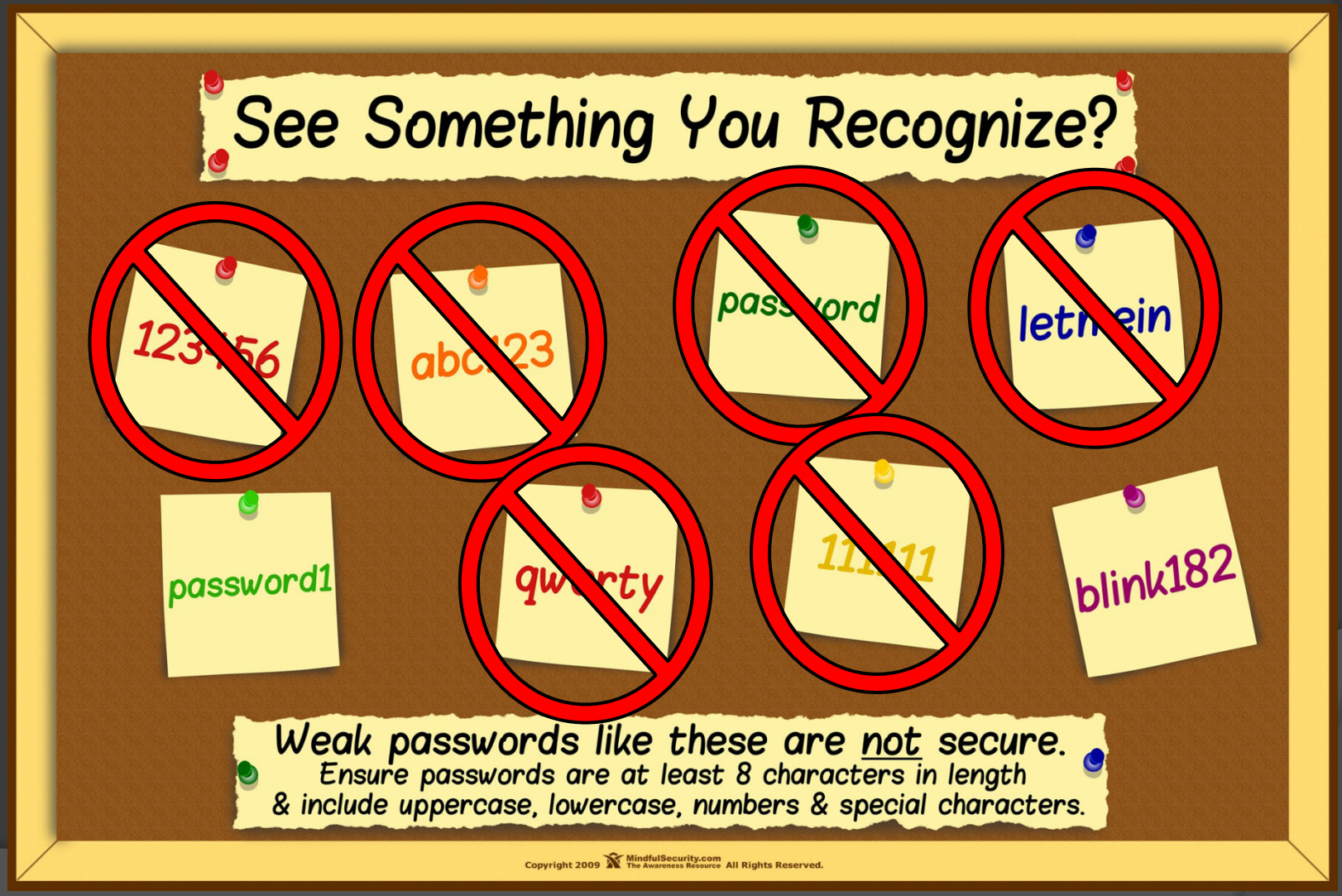

http://www.bing.com/maps/default.aspx?q=
Bing Maps
Convert
Select
WEB
IMAGES
VIDEOS
MAPS
NEWS
MORE
bing
Directions
My places
Nearby
Road
Bird's eye
Traffic
Fullscre
Twitter Maps
Timeline
Search
Just a moment...
mariaa_gomezzz
You were cool & now you're not. Just like that.
August 24 @ 4:54 PM from Twitter for iPhone
Roxas84
Dayum im lame
August 24 @ 4:54 PM from TweetCaster for Android
andreabeaar
HAHA @ my horrible luck today
August 24 @ 4:54 PM from Twitter for iPhone
Follow us on Twitter
Feedback & suggestions
Embed in your site
FAQs
purpleprince110
I'm at Long Wong's (Scottsdale, AZ) http://t.co/HorbmujKg1
August 24 @ 4:54 PM from foursquare
More from purpleprince110 • Share Tweet
Paradise
Hayden
Biltmore Greens III
Grovemont
Camelback East
E Indian School Rd
E Thomas Rd
Helen Manor
Frances Park
E McDowell Rd
Fountain Plaza
East Side Phoenix
Papago Park
Warner Heights
North Tempe
Phoenix Sky Harbor International Airport
E Van Buren St
E Sky Harbor Blvd
Tempe
Mesa Grande
Alegre Community
W Main St
Loop
101
143
202
17
10
© 2012 Microsoft Corporation

Social Media

- Security Methods

  - Turn off GeoTagging on your devices
  - Be guarded on what you post
  - Remove Geotagging information
  - If you do post use the most stringent privacy settings to cut down on who see information
  - Ask friends and family to not tag you in photos and be aware of what they are posting about you

Passwords


See Something You Recognize?
password1
blink182
Weak passwords like these are not secure.
Ensure passwords are at least 8 characters in length
& include uppercase, lowercase, numbers & special characters.
Copyright 2009 MindfulSecurity.com The Awareness Resource All Rights Reserved.

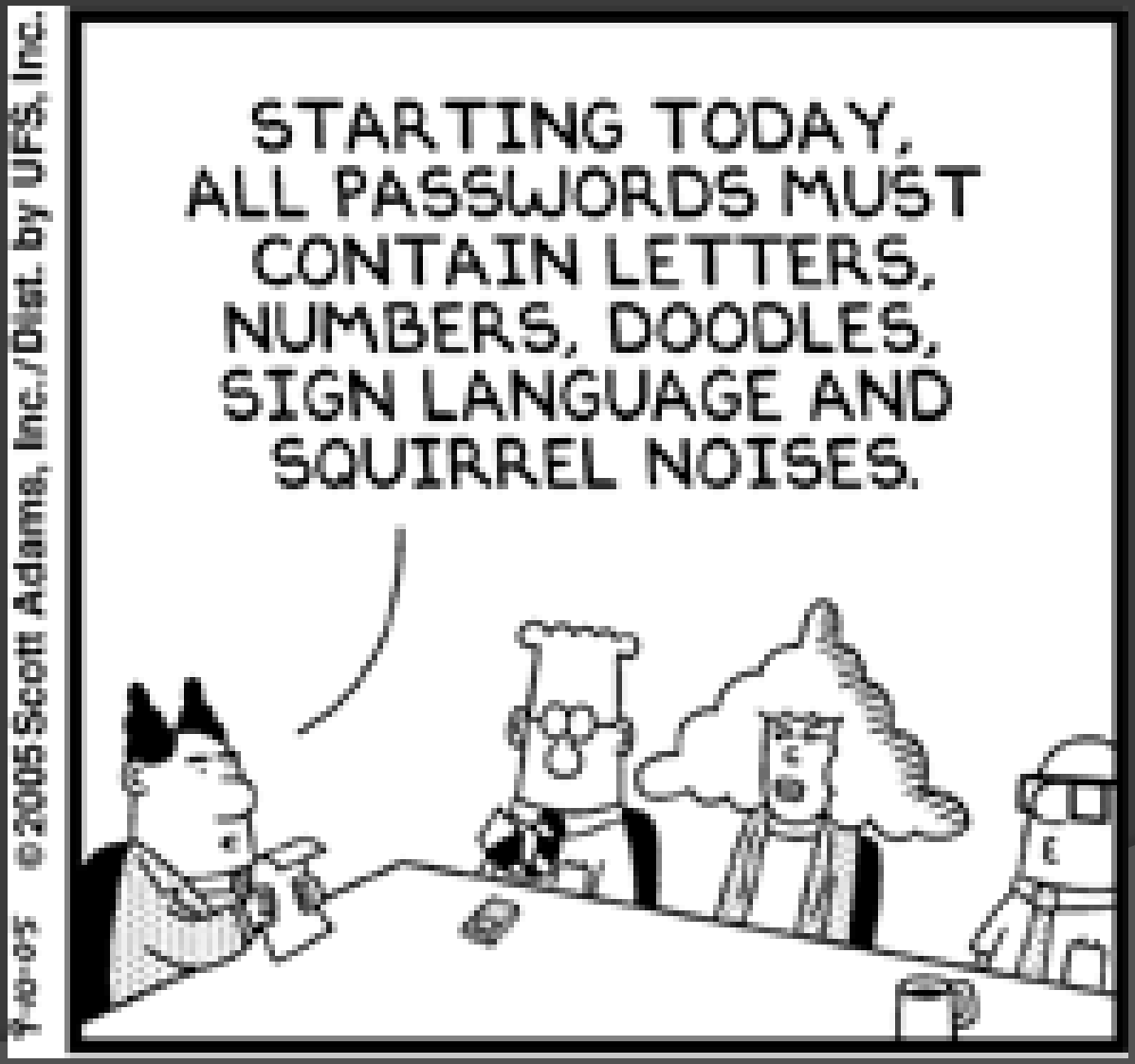
Why Password Management Matters

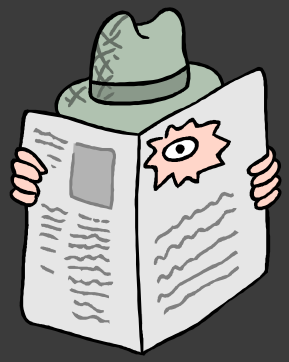
- Dangers
  - Default, common, or guessable
  - Free software and new technologies computes passwords quickly! (3.3B/sec)

Weak Passwords	Strong Passwords
Short (< 15 characters)	Long **OR** Complex
OR, no special characters (e.g. !@#)	Not in dictionary (e.g. nonsensical)
Default OR guessable	Used on 1 system
	Changed regularly

If every possible password is tried, sooner or later yours **will** be found.

Dilbert on Passwords





Strong Password

#4focf43hC#@j390

Facebook

#4focf43hC#@j390

Online Bank #1

#4focf43hC#@j390

Twitter

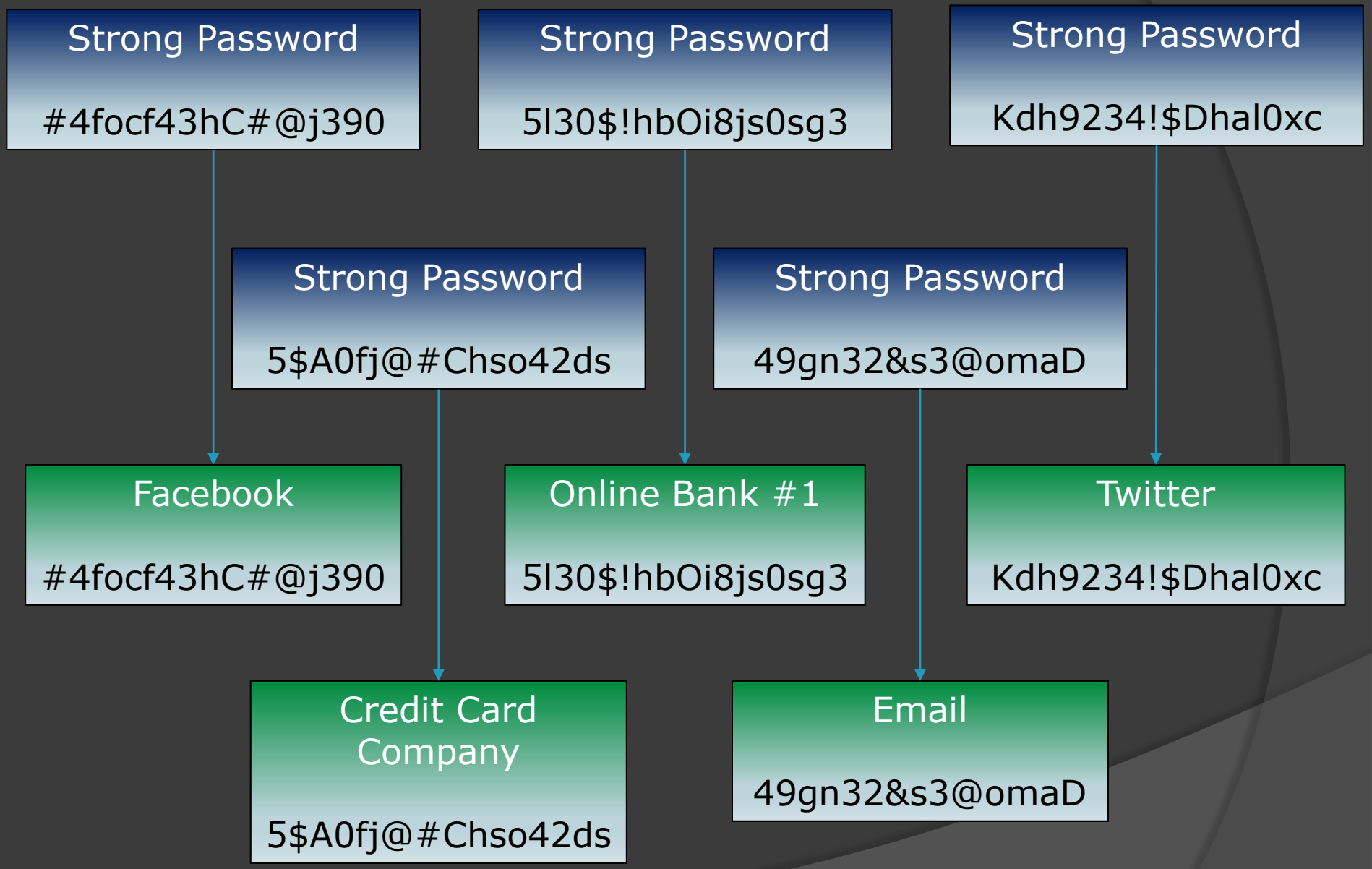
#4focf43hC#@j390

Credit Card Company

#4focf43hC#@j390

Email

#4focf43hC#@j390


Strong Password
#4focf43hC#@j390
Strong Password
5l30$!hbOi8js0sg3
Strong Password
Kdh9234!$Dhal0xc
Strong Password
5$A0fj@#Chso42ds
Strong Password
49gn32&s3@omaD
Facebook
#4focf43hC#@j390
Online Bank #1
5l30$!hbOi8js0sg3
Twitter
Kdh9234!$Dhal0xc
Credit Card Company
5$A0fj@#Chso42ds
Email
49gn32&s3@omaD

Practical Solutions

- Password Safe (e.g. KeePass http://keepass.info)

  - Free tool (DEMO)
  - Encrypts entire database
    - User names, passwords, notes, links, etc
  - Portable, no installation required

- Use a Password Formula/trick to remember
  - Base password + use
  - e.g. phx#85018gmail, phx#85018bank

Social Engineering

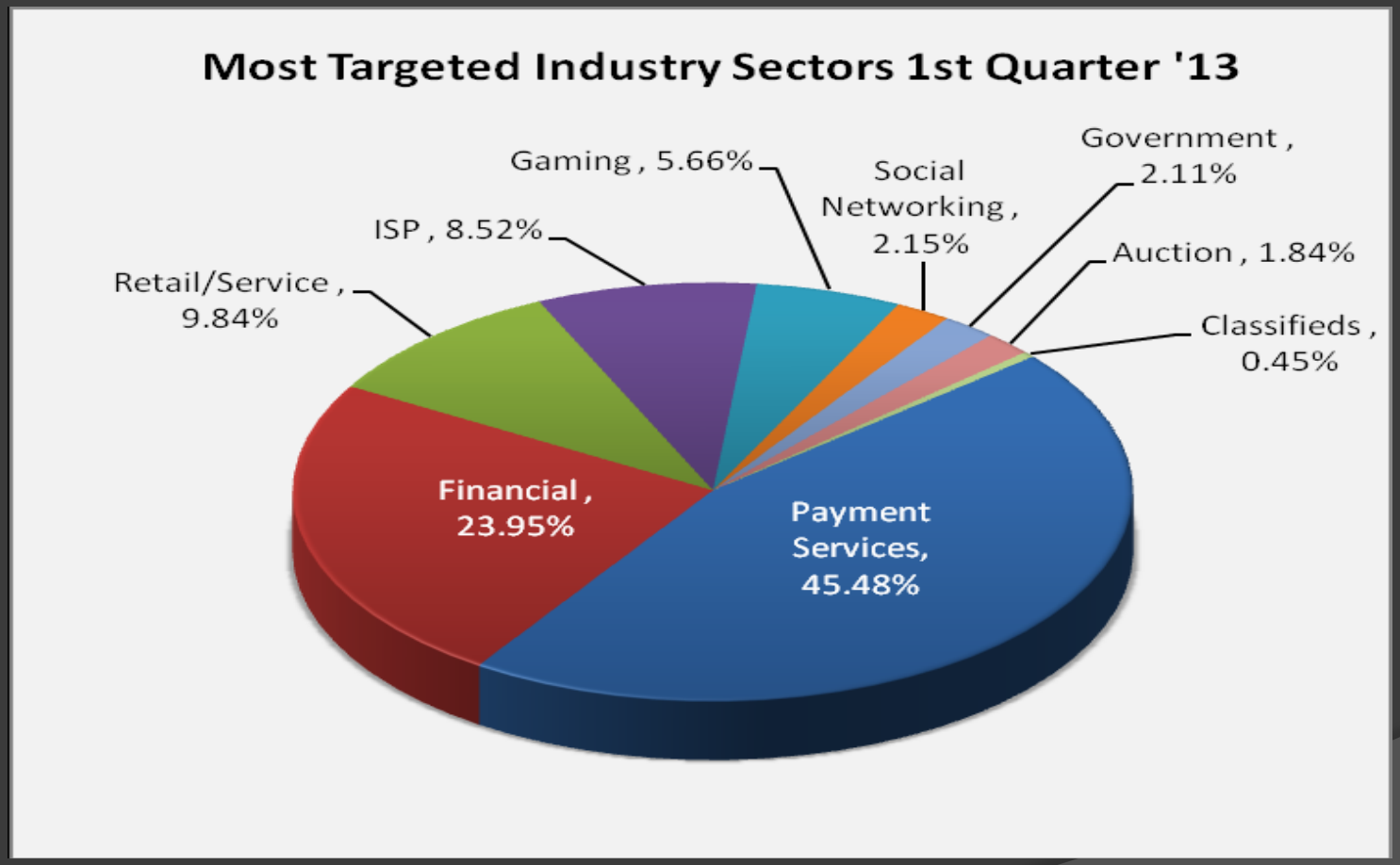
- Practice of obtaining confidential information by manipulating users
  - In person
  - Phone
  - Phishing
    - Email/ text/ call
      - Attachments
      - Giveaways

Phishing

- “Attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.”
- http://www.antiphishing.org

Phishing Statistics (2013 January only)	
# of new/unique phishing sites	46,066
# of brands hijacked	402
Country hosting most sites	United States
Proportion of infected computers	27.79% (China has 53%)

Phishing


Most Targeted Industry Sectors 1st Quarter '13
Gaming , 5.66%
Social Networking , 2.15%
Government , 2.11%
ISP , 8.52%
Auction , 1.84%
Retail/Service , 9.84%
Classifieds , 0.45%
Financial , 23.95%
Payment Services, 45.48%

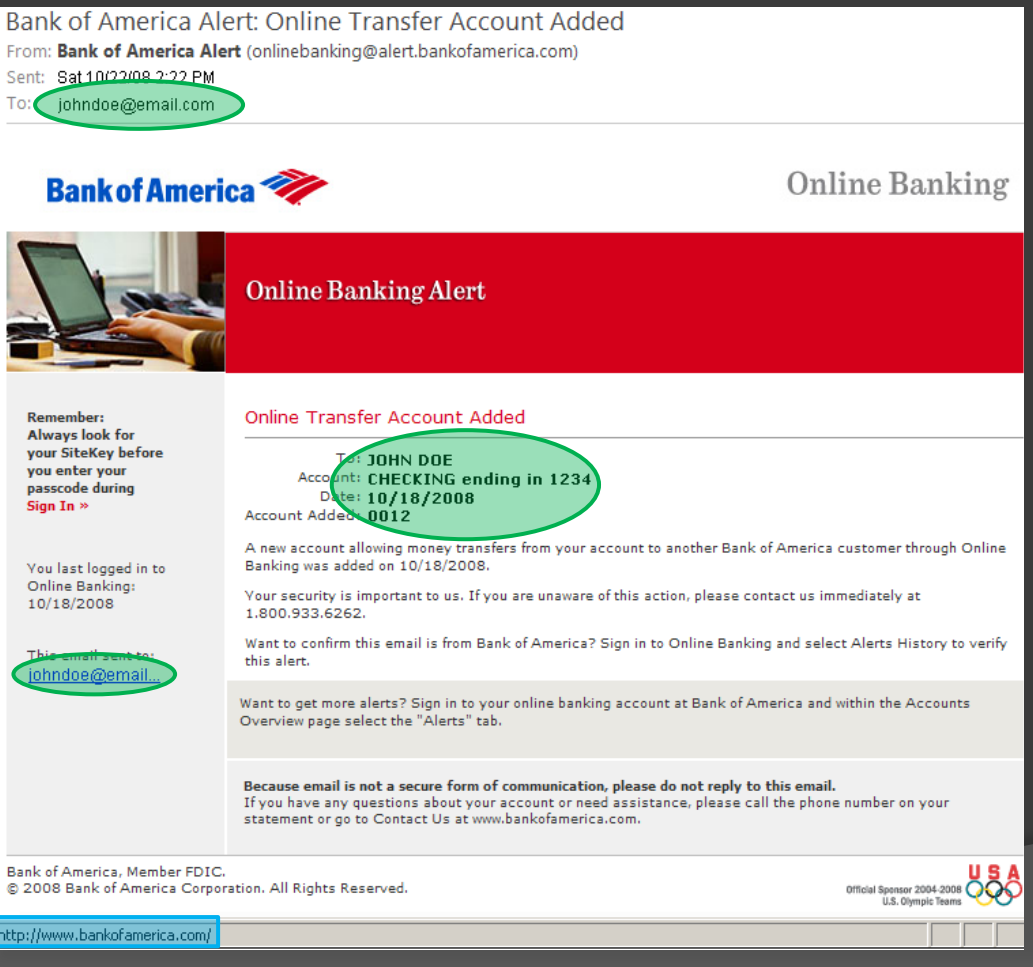
Can You Detect Phishing?

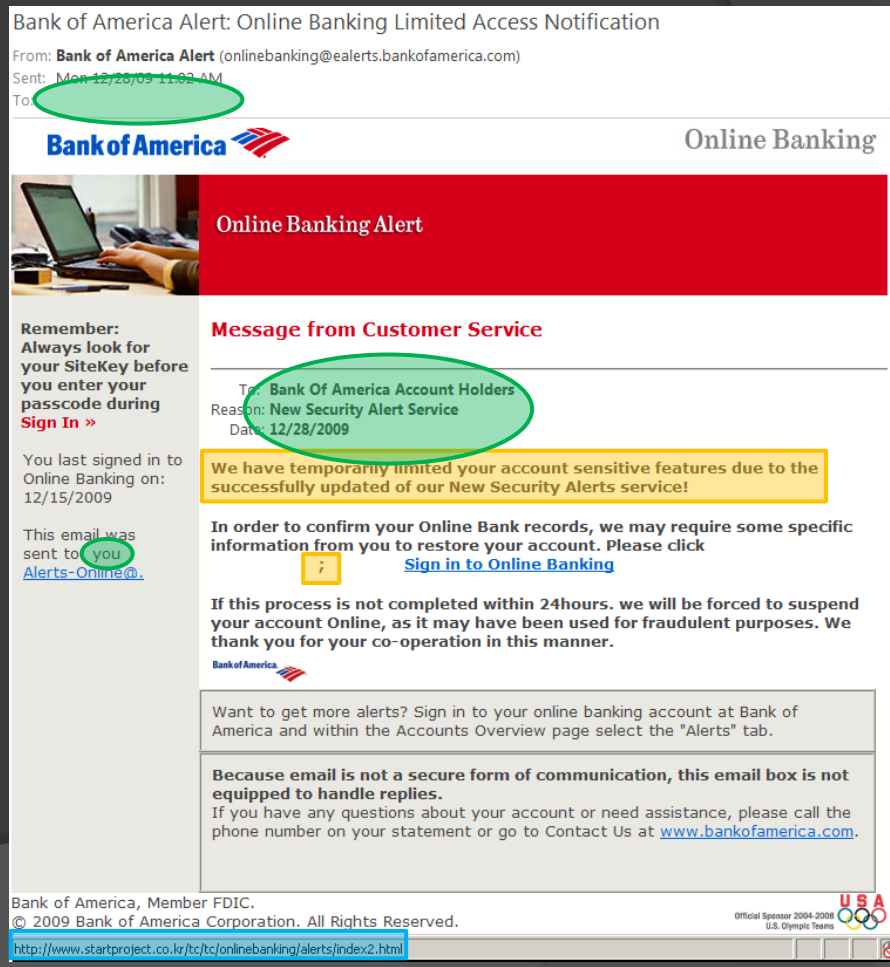
Greeting

Grammar/ punctuation

Status bar link

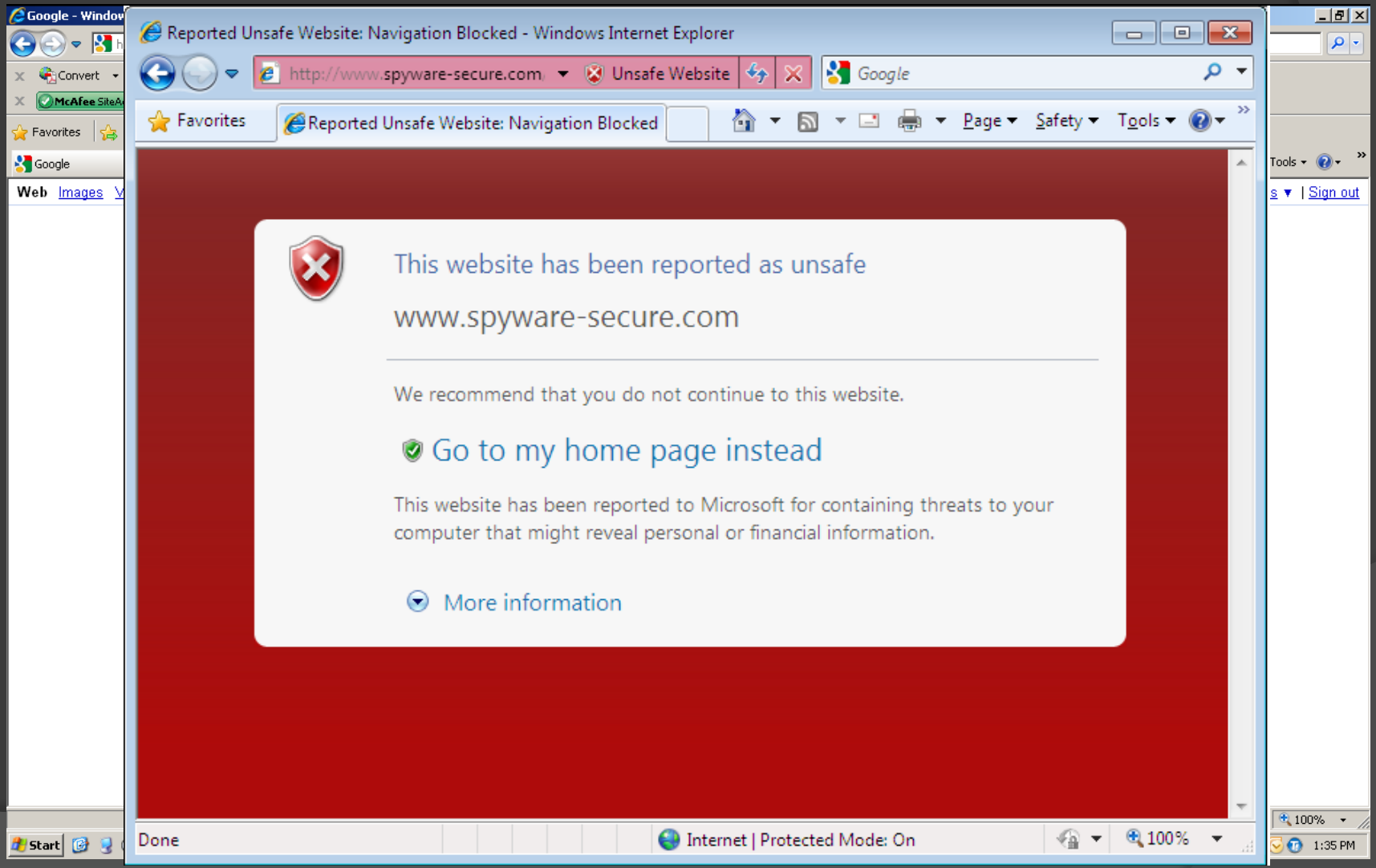
https





Phishing – IE Protection

SmartScreen Filter – Confirmed or suspicious



Phishing

- Safe Habits
  - Go directly to the source
  - http://whois.domaintools.com/
  - Research scams (snopes, ripoffreport)
    - US-CERT (Dept of Homeland Security)

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Debunking Common Myths

Myth: **Anti-virus software and firewalls are 100% effective**

- Zero-day attacks
- Phishing
- Attacks from trusted computers

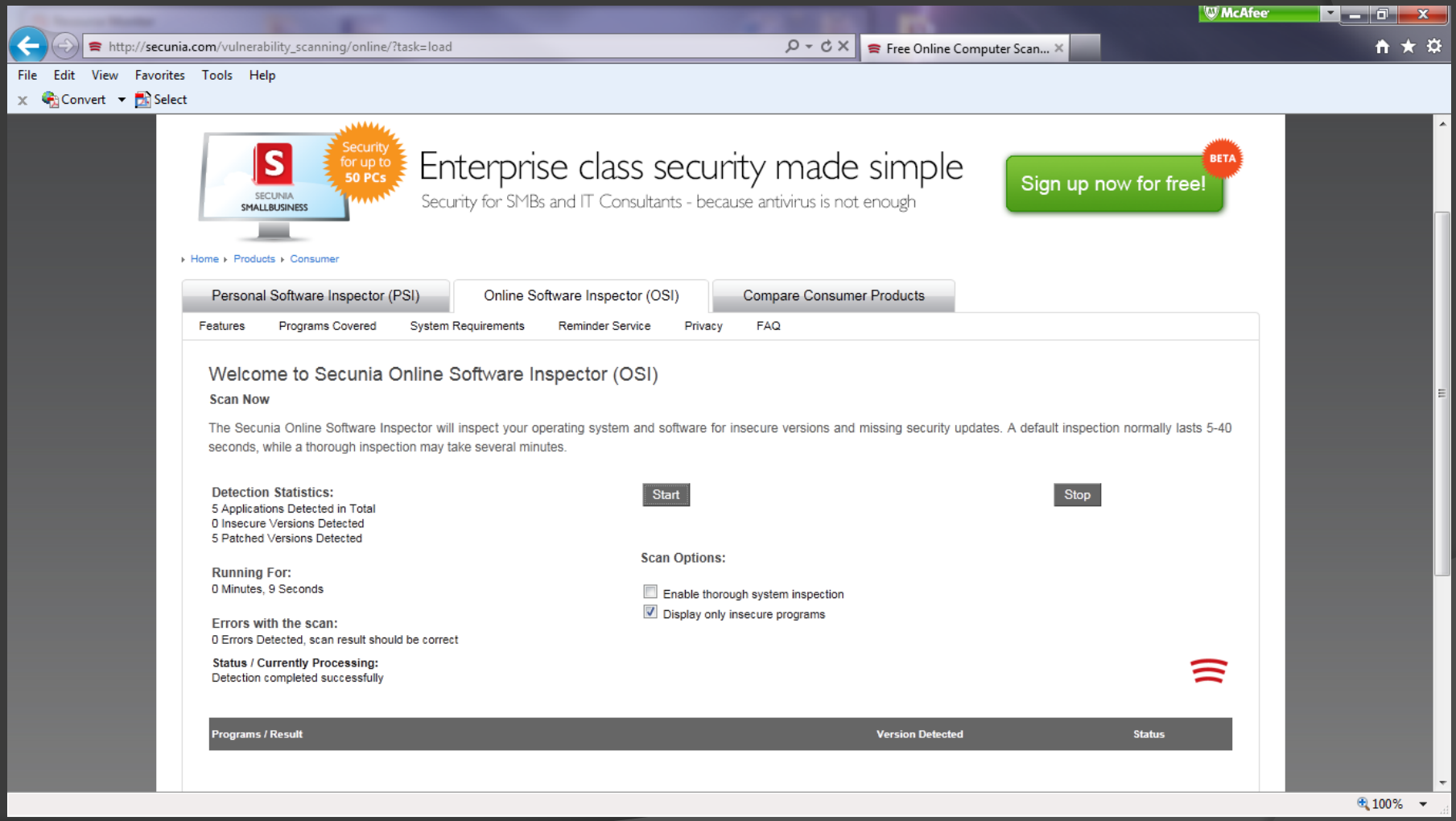
- Ex: Emails/Webpages with scripts

Debunking Common Myths

Myth: **Once software is installed on your computer, you don't have to worry about it anymore**

- Vulnerabilities
  - i.e. Acrobat, Internet Explorer, etc.
- Updates, patches
  - Automatic (Control Panel>>Security Center)
  - Microsoft Update (http://update.microsoft.com/microsoftupdate)
  - http://secunia.com/vulnerability_scanning/personal/screenshots/

Clean Bill of Health



Debunking Common Myths

Myth: **My chances of getting attacked are really slim**

- Targeted attacks
  - Social Engineering
  - Public PC's & Wireless Internet
- Mass attacks
  - Users of High-traffic Websites
  - Unpatched Computers
- Attack of organizations with your info
  - Attractive ROI
  - Trusted organizations

How likely is it?

To be struck by lightning?

- 1 in 750K

To be in a car accident?

- 1 in 52

To be bitten by rattlesnake?

- 1 in 37.5K

To be attacked online?

- 1 in 0.2

Security Solution?

Basic Security Makes a Difference

A little goes a long way

- Protect, discourage and deter
- Don’t be the Low hanging fruit

Criminals consider ROI

- Prioritize your efforts
- Not everything needs the same security

Don’t put all of your eggs in one basket

http:bcheck.scanit.be/bcheck/index.php

Thank You!

Questions?

Melinda Gardner, CISA
Arizona Auditor General's Office
mgardner@azauditor.gov
602.553.9815