

Exponential Threats to a Digital Age

CISO Forum – Jan. 25, 2011

“Hackers costing enterprises billions”

“Computer hackers could disable military”

“Hackers breach clusters of U.S. supercomputers”

“St. Pete Breeding Ground for World Class Hackers”

“Telenor takes down 'massive' botnet”

“Computer 'phishing' fraud worms way into Kentucky”

“Hackers hijack federal computers”

“Eerie virus sweeps through Internet”

“Microsoft hackers had access for weeks”

“Hackers attack U.S. government Web sites”

“MSBlast picks on vulnerable computers. Don't fall prey!”

“Hackers make the headlines on USA Today”

“Hackers hit Hotmail”

Threats Out-Pace the Informed

Threats Out-Pace the Informed

- **InfoSec Pros Get Compromised**

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised

Security Gurus Owned by Black Hats



Adjust text size: **A-** **A+**

July 30th, 2009, 11:06 GMT | By [Lucian Constantin](#)



Be the first of your friends to like this



ENLARGE

The websites and servers of reputed security experts and popular online hacking communities have been compromised by a group [called](#) ZFO (Zero for Owned), which released a big text file containing a wealth of info extracted during the hacks. According to its manifesto, ZFO opposes full-disclosure practices and thinks that the security industry is failing.

The file left behind by the black hats, called ZFO5.txt, which is supposed to signify issue five of the Zero for Owned zine (magazine), contains attack logs sprinkled with the hackers' comments, as well as personal emails, [chats](#) and other data belonging to those compromised.

The hacked security websites include the ones belonging to Kevin Mitnick, Dan Kaminsky, Ralph von der Heyden, Julien Tinnes, as well as darkmindz, elitehackers, hak5, binrev, and blackhat-forums. The group decided to break out the news on the eve of the Black Hat Briefings, one of the biggest security conferences where the industry's elite gathered.

Dan Kaminsky in particular seems to have had it worse, with many of his personal emails and chats with other white hats being exposed. ZFO claims to have 1.5gb of them dating as far back as 2005. "Dan Kaminsky got owned. Everything. Blackhats have been passing around his personal emails for months. He's only famous because his ego is so bloated that he attacks the world with his pointless ramblings," the group writes.

Ads by Google

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised
- **Thousands of new viruses per month**



Mcafee Threats Report 2010:

Even though spam declined, an average of 60,000 new malware threats were identified each day, nearly four times the 16,000 detected per day in 2007.

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised
 - Thousands of new viruses per month
 - **Growing complexity of attack vectors**
- March 2010
 - AV Detects KNOWN attacks.
 - AV vendors can't agree on Virus: name, effect, taxonomy or if it is even a virus

Tech Center: Vulnerability Manage

 E-mail this page |  Print this page |  BOOKMARK 

Only One In Seven Consumer AV Tools Catch New 'Aurora' Variants

NSS Labs says its new test shows emphasis on antivirus exploit detection flawed, but others disagree

Mar 11, 2010 | 04:20 PM

By Kelly Jackson Higgins
DarkReading

Most antivirus products don't detect new variants of the exploit used in the so-called "Operation Aurora" attacks on Google, Adobe, and other U.S. companies, according to a new test conducted by NSS Labs.

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised
- Thousands of new viruses per month
- Growing complexity of attack vectors
- **Integration of services/apps/companies**

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised
- Thousands of new viruses per month
- Growing complexity of attack vectors
- Integration of services/apps/companies
- **Social Networking/Engineering**

Threats Out-Pace the Informed

Glut of Stolen Banking Data Trims Profits for Thieves

A massive glut in the number of credit and debit cards stolen in data breaches at financial institutions last year has flooded criminal underground markets that trade in this material, driving prices for the illicit goods to the lowest levels seen in years, experts have found.

For a glimpse of just how many financial records were lost to hackers last year, consider [the stats released this week by Verizon Business](#). The company said it responded to at least 90 confirmed data breaches last year involving roughly 285 million consumer records, a number that exceeded the combined total number of breached records from cases the company investigated from 2004 to 2007. Breaches at banks and financial institutions were responsible for 93 percent of all such records compromised last year, Verizon found.

As a result, the stolen identities and credit and debit cards for sale in the underground markets is outpacing demand for the product, said Bryan Sartin, director of investigative response at Verizon Business.

Verizon found that profit margins associated with selling stolen credit card data have dropped from \$10 to \$16 per record in mid-2007 to less than \$0.50 per record today.

- April 2009
- Our data for sale
- Stolen credit card profit margins have dropped
 - 2007 - \$10-16
 - 2009 - \$0.50
 - 2010 - \$0.06*

* Bulk Pricing Available

Threats Out-Pace the Informed

- InfoSec Pros Get Compromised
- Thousands of new viruses per month
- Growing complexity of attack vectors
- Integration of services/apps/companies
- Social Networking/Engineering

No One Can Keep Up

Who **hasn't** experienced fraud or loss of an asset or identity for themselves or family?

HACK

ID: 1518: Malicious Software/Hack compromises unknown number of credit cards at fifth largest credit card processor

Date: 2009-01-20 Records Lost: 130,000,000 Source: Outside Submitted by: michaelcordes Location: Princeton NJ, US
Organizations: Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank

HACK

ID: 548: Hack exposes 94 million credit c

Date: 2007-01-17 Records Lost: 94,000,000 Sc
Organizations: TJX Companies Inc.

HACK

ID: 2061: Hackers access credit-reporting

Date: 1984-06-01 Records Lost: 90,000,000 Sc
Organizations: TRW, Sears Roebuck

**DISPOSAL
DISK
DRIVE**

ID: 2382: Veterans records on improperl

Date: 2009-10-05 Records Lost: 76,000,000 Sc
Organizations: National Archives and Records Adm

HACK

ID: 110: Major card processor breached

Date: 2005-06-19 Records Lost: 40,000,000 Sc
Organizations: CardSystems, Visa, MasterCard, Am

**STOLEN
COMPUTER**

ID: 289: Names, Social Security numbers

Date: 2006-05-22 Records Lost: 26,500,000 Sc
Organizations: U.S. Department of Veterans Affairs

**LOST
MEDIA**

ID: 841: HMRC

Date: 2007-11-20 Records Lost: 25,000,000 Sc
Organizations: HM Revenue and Customs, TNT

**LOST DISK
DRIVE**

ID: 1172: T-Mobile lost disk containing data on 17 million customers

Date: 2008-10-06 Records Lost: 17,000,000 Source: Inside Submitted by: jkouns Location: DE
Organizations: T-Mobile, Deutsche Telekom

Hundreds of millions of “reported” records lost in the last few years just in the US.

Are you **sure** you or your family wasn't compromised?





Luck Favors the Prepared



Principles to Live By

- Least Privilege
 - Need-to-know
- Separation of Duties
- Minimize Threat Surface
 - Defense In Depth
 - Security Awareness
- Situational Awareness

Remember the Cobbler's Kids

- Best-practice principles...**are**
- Apply similar precautions at home



Least Privilege

*Do some who have access to your
sensitive assets shouldn't?*

2 Men Accused Of Swiping CC Numbers

Timothy Curley, Michael Thomas At Center Of Secret Service Investigation

Cara Liu
Reporter, KPHO.com

POSTED: 11:20 pm MST July 2, 2009

UPDATED: 9:01 am MST July 7, 2009

PHOENIX — Two Phoenix men are accused of stealing thousands of American Express card numbers and swindling more than a million dollars from customers.

Timothy Curley, of Phoenix, is at the center of the Secret Service investigation.

Curley was arrested June 24 at Sky Harbor Airport.

Court records obtained by CBS 5 News detail what police confiscated during the arrest: drugs, approximately \$5,000, fictitious Arizona driver's licenses, a laptop computer and more than 100 re-encoded credit cards.

Those bogus ci
police.

Police discover
who "could hav
various banks,"

Investigators le

No one answer

When investiga
Detectives also

Michael Thoma

Police said he t
Investigators al

A spokeswoma
accounts for fra

A Secret Service spokesperson would only confirm an ongoing investigation.

- July 2009
- AMEX Employee steals cardholder info to forge cards
- AMEX claims few had access to this information, making this a trusted-individual

Related To Story



Video: Secret Service: Investigation Ongoing
In CC Fraud Case

d, according to

one of the few
machines at

uck last August.

search warrants.

ress customers.

nonitors

Minimize Threat Surface

*Do you unnecessarily expose your
sensitive assets (e.g. SSN,
Location, Schedule, Family info)?*

- June 2009
- More laptops stolen with no encryption or protection
- This one from a bank.
- Every industry is at risk

BBC NEWS

Bank's details on stolen laptops

A laptop containing bank account details of 75,000 Irish gas board customers, has been stolen in Dublin.

The theft took place almost two weeks ago, but was not publicised until Wednesday because police were following "a particular line of inquiry".

The confidential information was not encrypted and was on one of four stolen laptops taken from Bord Gáis offices and nearby buildings on 5 June.

Bord Gáis said it will contact affected customers next week.

The company added that police and the Irish Data Protection Commissioner were immediately informed.

Bord Gáis, which has recently entered the electricity market, has attracted significant numbers of new customers who have changed their supplier.

The National Consumer Agency has described the lack of encryption as "unacceptable and a poor reflection on Irish business".

My name is Todd Davis
This is my social security number 457-55-5462

"I'm Todd Davis, CEO of LifeLock. Yes, that really is my social security number. No I'm not crazy. I'm just sure our system works. Just like we have with mine, LifeLock will make your personal information useless to a criminal. And it's **GUARANTEED.**"

Here at LifeLock, We Guarantee Your Good Name.
No one else does because no one else can.



More Testimonials:
Stop Junk Mail. Stop Credit Offers.
Stop Identity Theft. **Guaranteed.**



[Enroll Now ▶](#)

LifeLock Dinged \$12 Million for Deceptive Business Practices

By Kim Zetter  March 9, 2010 | 3:34 pm | Categories: [Crime](#), [Cybersecurity](#)



The CEO of Lifelock, Todd Davis, became famous for advertising his Social Security number on television ads and billboards promising his \$10 monthly service would protect consumers from identity theft.

The company also offered a \$1 million guarantee to compensate customers for losses incurred if they became a victim of identity theft after signing up for the service.

But the Federal Trade Commission said Tuesday that the [claims were bogus](#) (.pdf) and accused Lifelock, based in Arizona, of operating a scam and con operation. The commission announced, along with 35 state attorneys general, that it had levied a fine of \$12 million against the company for deceptive business practices and for failing to secure sensitive customer data. Of that amount, \$11 million will go to refund customers who subscribed to the service. Consumers will receive a letter from the FTC and their attorney general explaining how to take part in the settlement.

The FTC said that [Lifelock](#), which advertises itself as "#1 In Identity Theft Protection," engaged in false advertising by promising customers that if they signed up with its service their personal information would become useless to thieves.

"In truth, the protection they provided left such a large hole ... that you could drive that truck through it," said FTC Chairman Jon Leibowitz, referring to a Lifelock TV ad showing a truck painted with the CEO's Social Security number driving around city streets.

- March 2010
- FTC Accused of scam and con operation
- Forced to pay \$12M

Defense In Depth Minimize Threat Surface Security Awareness

*Have you disclosed unnecessary
information about
yourself/work/etc. online?*

Age of Information

- Reconnaissance Takes Just Button Clicks
- Entity Cooperations Can't Easily be Identified
- Information Posted on One Site Could be Queried from Another

Gawker Hack

- *Gawker* (gossip site) Raided Nov/Dec 2010
- 1.5M Accounts Compromised
- Feud Between *Gawker* and *Gnosis* Hackers
- *Gnosis* Had Access for Weeks
- *Gawker* Made Many Errors
- Compromised Accounts includes staff from SSA, NASA, FTC, NARA, USDA, FDA, LoC, US Senate, DoD

What Can We Learn?

- Never Underestimate Your Opponent
- A Site's Insecure cred Mgmt. Can Harm You
- You Never Know a Site's Affiliates or Enemies
- Account and Password Reuse is Dangerous
- There is a Saying: *A smart man puts all of his eggs in one basket, then watches that basket*

What Can We Learn?

- Never Underestimate Your Opponent
- A Site's Insecure cred Mgmt. Can Harm You
- You Never Know a Site's Affiliates or Enemies
- Account and Password Reuse is Dangerous
- There is a Saying: *A smart man puts all of his eggs in one basket, then watches that basket*
- **How do you watch something that you don't know exists and have no ability to watch?**

What Did “They” Learn?

- *Gawker* Sourcecode
- *Gawker* and Affiliate Business Practices
- Admin/Mgmt Accounts for Many Affiliate Sites
- *Gawker*-Internal Correspondence
- All User Credentials
- Knowledge of How Users Create Passwords

What Did “They” Learn?

- *Gawker* Sourcecode
- *Gawker* and Affiliate Business Practices
- Admin/Mgmt Accounts for Many Affiliate Sites
- *Gawker*-Internal Correspondence
- All User Credentials
- Knowledge of How Users Create Passwords

The Worst isn't Over ...

Technology News

Security risk as people use same password on all websites

More than 1.7 million people are at risk of falling victim to internet fraud because they use exactly the same password every time they go online, a new report warns.



How to choose a secure password Photo: GETTY

7:05AM BST 02 Sep 2009

The latest research by insurer CPP reveals that many people admit to using easy-to-guess passwords, such as memorable dates, the names of their children or pets and share them with partners, friends and colleagues.

Most People
use the Same
Password on
all Websites

What can an attacker do with your
username/password recovered from a
compromised site?

What can an attacker do with your
username/password recovered from a
compromised site?

Reconnaissance!!



username

[SIGN UP](#) [SIGN IN](#)

Remember me ☐

**RESERVE YOUR NAME
ON HUNDREDS OF SITES**
[CLICK HERE](#)

Need Help?
Have Questions?
(800) 691-KNOW
(5669)

- [Check Username](#)
- [Create Profile](#)
- [Community](#)
- [Networks](#)
- [About](#)

Feedback



Search over 470 popular social networks and over 40 domain names to instantly secure your brand across the social web.

[Check It](#)

What is this?

KnowEm allows you to check for the use of your brand, product, personal name or username instantly on over 470 popular and emerging social media websites. Grab your name and secure your brand before someone else does. [Learn more](#)

KnowEm for the Enterprise

[KnowEm Enterprise Dashboard](#)
[CLICK HERE](#)

KnowEm now offers an [Enterprise Dashboard](#) for Trademark Protection, Search Engine Marketing and SEO Agencies.

As Featured In



The Washington Post





type username here

chk

Show Most Popular Sort by Name

Check to see if your desired *username* or *vanity url* is still available at dozens of popular Social Networking and Social Bookmarking websites. Promote your brand consistently by registering a username that is still available on the majority of the most popular sites. Find the best username with **namechk**.

Google	hi5	eSnips	Jamendo
Facebook	newsvine	Snooth	brightkite
YouTube	bebo	ThisNext	Virb
eBay	funnyordie	mixx	tipd
wikipedia	Gather	DailyBooth	Corkd
MySpace	Good Reads	PictureTrail	12seconds.tv
Wordpress	Kongregate	diigo	CopyTaste
eHow	reddit	Blip.fm	Dropjack
twitter	delicious	Revver	WUAH
photobucket	Posterous	Families.com	Jaiku
Flickr	foursquare	blogTV	Picasa
LinkedIn	Viddler	FFFFFound!	Elgg.org
Hulu	plaxo	Soup.io	Odeo
Vimeo	Current	Aviary	Blogmarks
Blogger	Vox	Qik	AudioBoo
tumblr	Xanga	Tripit	ryze
ning	blip.tv	vi.sualize.us	Skribit
Digg	Multiply	Zoomr	Plime
Squidoo	Technorati	Shelfari	Bambuser
DailyMotion	SoundCloud	ibibo	claimid
LiveJournal	Livevideo	netvibes	Gnolia



NAME

EMAIL

PHONE

USERNAME

FRIENDS

Enter a first and last name Example: John Doe or Jane Doe, Los Angeles, CA

Not your grandma's phonebook.



Defense in Depth Situational Awareness

*Would a single exploit
compromise your critical assets
(e.g. bank, mortgage-payment,
records)?*

NY Times Website Infected With Fake Antivirus

Posted by [John Sawyer](#), Sep 15, 2009 10:45 AM



The New York Times Website became the victim of a malicious Internet-based advertisement over the weekend. Users of certain sections of NYTimes.com encountered notifications that they were infected with malware and needed to install the antivirus software linked from the notification. And if you've dealt with a user, friend, or family member who's fallen for this sort of ruse, then you know the AV software is really just malware posing as AV.

Computerworld had a [good story](#) on the incident and Dancho Danchev, as always, has a [good analysis](#) of some background sites and IPs associated with the attack that link to other known fake AV and "malvertisement" campaigns.

I've discussed how one of the major flaws with antivirus is the fact it relies on blacklisting, or blocking known bad things. A [recent study](#) shows I'm not alone, but blacklisting isn't

There are many reasons why this is a problem. It's based on the assumption that

One of the rules of security is to read the fine print. take the

If you were using the New York Times (this morning). ing from list this

So while many will still say blacklists are not effective, they do help in cases like these. Would your IPS or AV have blocked the attack? If so, do you know if it did it because it identified the attack, or because it knew it was coming from an RBN IP?

John H. Sawyer is a senior security engineer on the IT Security Team at the University of Florida. The views and opinions expressed in this blog are his own and do not represent the views and opinions of the UF IT Security Team or the University of Florida. When John's not fighting flaming, malware-infested machines or performing autopsies on blitzed boxes, he can usually be found hanging with his family, bouncing a baby on one knee and balancing a laptop on the other. Special to Dark Reading.

- March 2010
- Energizer Bunny Infects
- Trojan horse grants access
- Company had no idea

Energizer Bunny's software infects PCs

USB battery recharger status software contains Trojan, says US-CERT

By Gregg Keizer

March 7, 2010 10:17 PM ET

 Comments (23)  Recommended (17)    Share

Computerworld - The Energizer Bunny infects PCs with backdoor malware, the Department of Homeland Security's US-CERT said Friday.

According to researchers at US-CERT (United States Computer Emergency Readiness Team), software that accompanies the Energizer DUO USB battery charger contains a Trojan horse that gives hackers total access to a Windows PC.

The Energizer DUO, a USB-powered nickel-metal hydride battery recharger, has been discontinued, said Energizer Holdings, which late Friday confirmed that the software contains malicious code. The company has not said how the Trojan made its way into the software, however. "Energizer is currently working with both CERT and U.S. government officials to understand how the code was inserted in the software," Energizer said in a statement.

Energizer's DUO was sold in the U.S., Latin America, Europe and Asia starting in 2007.

The Windows software included with the charger is designed to show battery-charging status. When the software is installed, it creates the file "Arucer.dll," which is actually a Trojan that listens for commands on TCP port 7777. Upon

Entrusted Handling Theft

*Do you have any protections at all
for risks to entrusted handling?*

Why Now?

- Entrusted Handling Has Always Been a Risk
- Accessibility of Money-Movers Never Higher
- Anyone With Physical Access Can Win


ATM Skimming



Howard County Police looking for suspects who have been skimming from an ATM

Ellicott City ATM hit by skimmers



 Be the first of your friends to recommend this.

Posted: 11/30/2010

ELLCOTT CITY, Md. - Howard County Police are looking for two men who they believe rigged an Ellicott City ATM so that they could steal thousands of dollars out of the bank accounts of strangers.

Police think the suspects installed a skimming device on the ATM at the Columbia Bank on the 4400 block of Long Gate Parkway and then recorded customer's bank card information and

Entrusted Handling Thoughts

- ATM/Gas-Pump Skimming On the Rise
- Hotel Check-in CC Theft on the Rise
- Restaurant-Server CC Theft on the Rise
- Insecure CC Handling With Websites is STILL a Big Problem
- How Can Best Practice Principles be Applied to Reduce Your Risk of Exposure?

Security Awareness

Situational Awareness

Do your online habits elevate the risk to your employer or friends?

Corporate Breach via Facebook

How Facebook phishers breached a corporate network

Posted on | March 4, 2010 | 4 comments

By Byron Acohido

USA TODAY P. 1A 04Mar2010

SAN FRANCISCO — "Hey Alice, look at the pics I took of us last weekend at the picnic. Bob"

That Facebook message, sent last fall between co-workers at a large U.S. financial firm, rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page.

So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from

- March 2010
- Facebook network used to gain access to corporate network
- Corporate Policy?
- Controls?
- Stories like this are becoming common



thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

Sidebar: How the Koobface worm is evolving to keep bad guys ahead

Report: Facebook Served As Primary Distribution Channel For Botnet Army

Posted by [Raj Dash](#) on February 18th, 2010 4:35 PM

[Share](#) [2 Comments](#)

Internet security company NetWitness has just published a report that reveals an 18-month-long widespread hacker attack on computers worldwide whose topmost method of malware delivery was Facebook. However, while over 3500 Facebook login credentials were stolen, that's a very tiny percentage given there are over 400 million users of this social media site. Yahoo and Hi5 came in 2nd and 3rd, respectively, for stolen credentials.

A NetWitness engineer found evidence of the hacker operation in late January 2010, while installing security software for a company. Additional evidence suggests that an Eastern Euro group is possibly behind the attack, and used both German and Chinese as the latter because of the ease of operation and reduced chance of detection. The effort likely exposed login credentials — for online banking, social networking sites and email — over 2,400 companies and government agencies. The effort likely exposed corporate data and secrets, including credit card transaction info and intel from American companies whose computers were attacked span a range of industries including entertainment, technology, finance, energy, Internet providers, and education. Currently, there is no indication of how much data was stolen or how it was used.

Initially, it's believed that hackers in Germany started the operation in late January 2010 by convincing employees of one organization into clicking on links via contaminated website attachments or "virus cleaning" ads. Part of the effort also involved fooling officials into installing spyware. Computers at as many as 10 U.S. government agencies were compromised, and even one soldier's login info was stolen. At least one online payments processing server was accessed. In one case, an employee was involved in allowing hackers to gain access to corporate servers.

Number of credentials stolen via the ZeuS spyware virus by site



Source: NetWitness
Erik Brynildsen and
The Wall Street Journal

- February 2010
- Botnet controlled from facebook app
- 68,000 credentials stolen from 2,400 companies and Gov't agencies

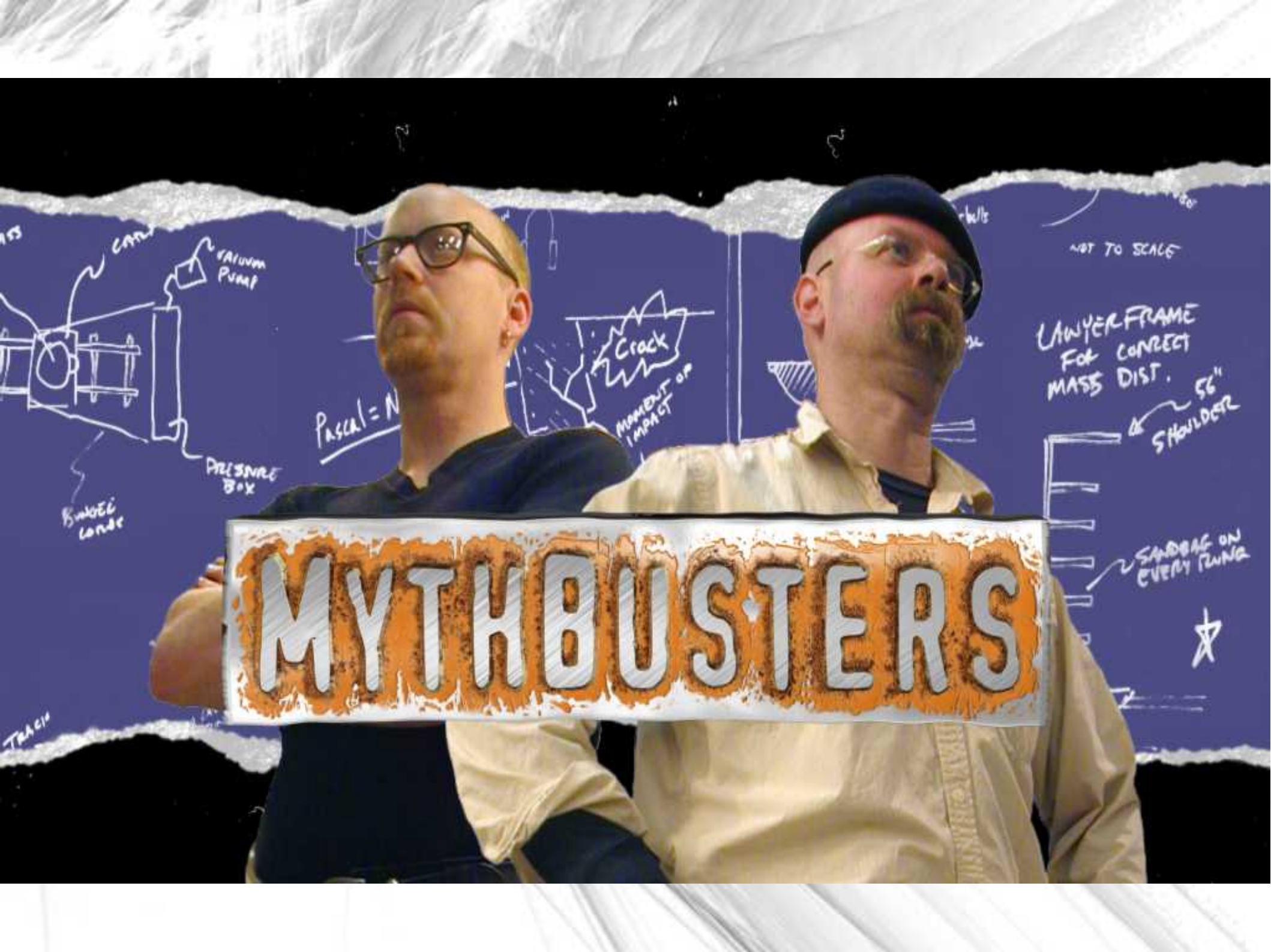
Need to Know Security Awareness

*Do you know what that 'tech' (e.g.
your fancy smartphone) is really
doing?*



Who is this guy?





MYTHBUSTERS





@donttrythis

Adam Savage

<http://twitpic.com/128p1b> - Now it's off to work in my beast. Wait... How'd that DOG get in there?

9 Feb via [TwitPic](#) ☆ [Favorite](#) ↻ [Retweet](#) ↩ [Reply](#)

<http://twitter.com/#!/donttrythis/status/886090735>



Posted on February 9, 2010
by [dontrythis](#)

Interest Based Ads

Now it's off to work in my beast. Wait... How'd that DOG get in there?

<http://twitpic.com/128p1b>

49 Comments



[zachamey](#) 156 days ago

nice house adam!! <http://yhoo.it/9W6mGD>



[MrPacMan36](#) 164 days ago

More photos by dontrythis



Share this photo

Put this photo on your website

Views 22,925

Events

Tags



What's EXIF?



Image Properties

General

Metadata

Details

Tag	Value
▶ Camera	
▼ Image Data	
DateTime	2010:02:09 08:26:14
YCbCrPositioning	centered
ISOSpeedRatings	70
DateTimeOriginal	2010:02:09 08:26:14
DateTimeDigitized	2010:02:09 08:26:14
PixelXDimension	800
PixelYDimension	600
▶ Image Taking Conditions	
Maker Note	
▼ Other	
FlashPixVersion	FlashPix Version 1.0
ColorSpace	sRGB
GPSLongitudeRef	W
GPSLongitude	122.00, 26.71, 0.00
GPSAltitudeRef	Sea level
GPSAltitude	34.00
GPSTimeStamp	08:26:13.98
GPSDOP	5.00
GPSImgDirectionRef	M
GPSImgDirection	37.00
XMP Exif	

◀ Previous

Next ▶

Close

This is EXIF -->

And thanks to
GeoTagging we have
the image's
coordinates:
37.728333,-
122.445167



Image Properties

General Metadata Details

Tag	Value
► Camera	
▼ Image Data	
DateTime	2010:02:09 08:26:14
YCbCrPositioning	centered
ISOSpeedRatings	70
DateTimeOriginal	2010:02:09 08:26:14
DateTimeDigitized	2010:02:09 08:26:14
PixelXDimension	800
PixelYDimension	600
► Image Taking Conditions	
Maker Note	
Other	
FlashPixVersion	FlashPix Version 1.0
ColorSpace	sRGB
GPSLongitudeRef	W
GPSLongitude	122.00, 26.71, 0.00
GPSAltitudeRef	Sea level
GPSAltitude	34.00
GPSTimeStamp	08:26:13.98
GPSDOP	5.00
GPSImgDirectionRef	M
GPSImgDirection	37.00
XMP Exif	

◀ Previous Next ▶ Close

Exif Viewer

Please select your image and set the desired options, then click on the "Display EXIF Data" button.

Local File:

Select file...

Remote URL:

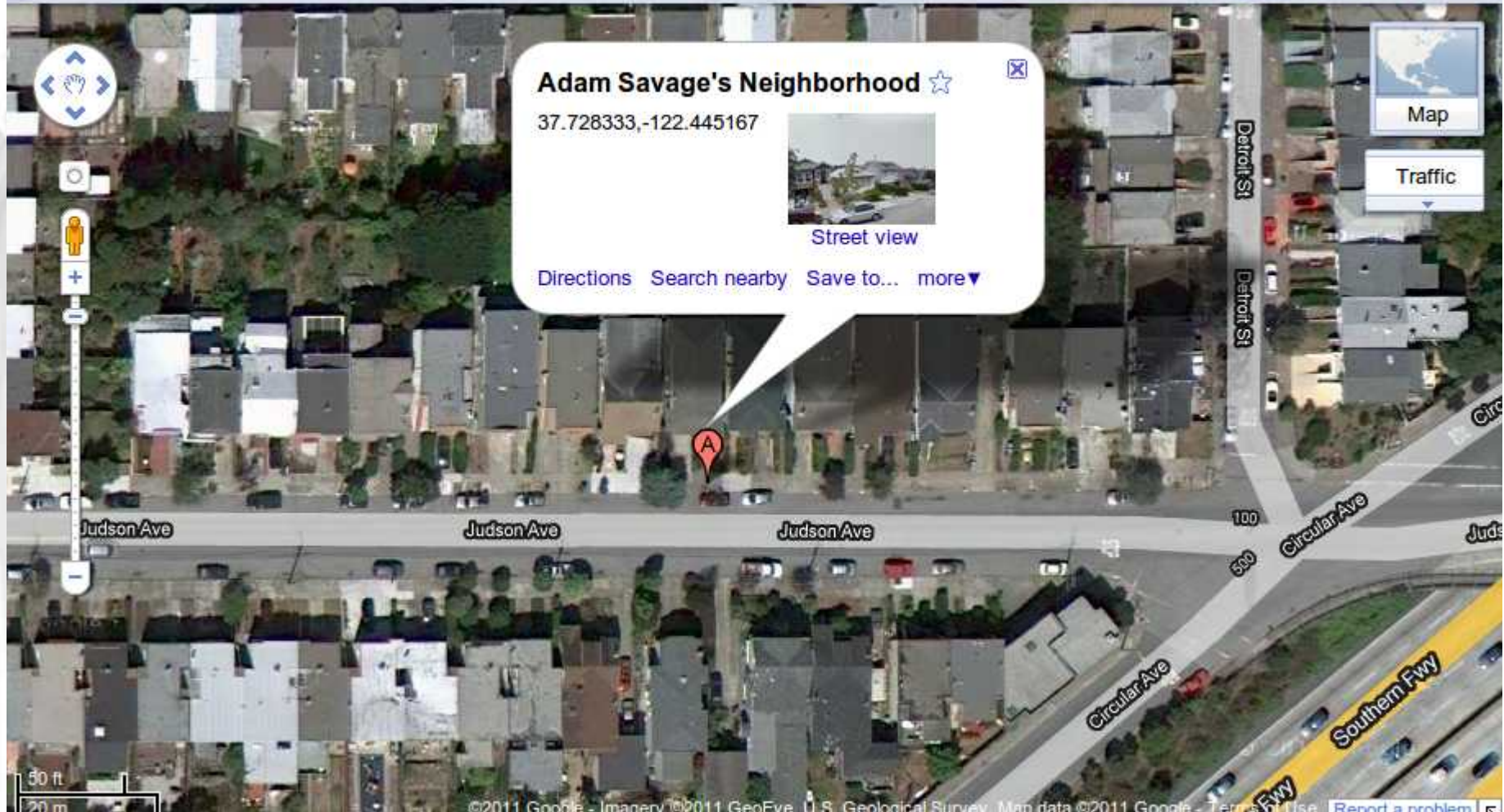
Display EXIF Data

- ☐ Basic information only
- ☐ Display Maker Note (if available)
- ☐ Suppress image display
- ☐ Use tables rather than lists
- ☒ Display EXIF tag ID

/home/sean/aplura/papers/threat/201101-CMS-Exponential_Threats_to_a_Digital_Age/images
/adam_savage_truck_image

EXIF GPS IFD

- GPS Latitude Reference {0x01} = N
- GPS Latitude {0x02} = 37/1,4370/100,0/1 [degrees, minutes, seconds] ==> 37° 43.7' == 37.728333°
- GPS Longitude Reference {0x03} = W
- GPS Longitude {0x04} = 122/1,2671/100,0/1 [degrees, minutes, seconds] ==> 122° 26.71' == 122.445167°
- Links to online mapping websites:
 - [Google™ Maps](#)
 - [Yahoo!® Maps](#)
 - [MSN® Maps & Directions](#)
 - [Mapquest®](#)
 - [Open KML data with Google™ Earth](#)
 - [Save KML data to file](#)
 - [Save KML data to file and open with Google™ Earth](#)
- GPS Altitude Reference {0x05} = sea level reference (negative value)
- GPS Altitude {0x06} = 34/1 m ==> 34 m
- GPS Time Stamp / UTC Time {0x07} = 8/1,26/1,1398/100 [hours, minutes, seconds] ==> 8h 26m 13.98s
- GPS Measure Mode {0x0B} = 5/1
- GPS Image Direction Reference {0x10} = magnetic direction
- GPS Image Direction {0x11} = 37/1 degrees





What Can Any Web User Know?

- Where Adam lives: **37.728333,-122.445167**
- Adam's Car: **Beige Toyota Landcruiser**
- What the house across the street looks like
- That he leaves for work around: **8:26 AM**
- That he is a dog-owner
- The dog may or may not be at home all day
- His phone: **iPhone 3GS ver:3.1.3**

And What is Adam's Address?

After this **incident** he moved, so we don't know.

Can you afford to move after sending a 140-character message to twitter?



[Sign In](#)

[Create Your Account](#)

Share your photos.
Watch the world.

AND
VIDEO

SEARCH

5,008 uploads in [the last minute](#) · 71,248 things tagged with [jump](#) · 4.3 million things [geotagged](#) this month · [Take the tour](#)



[Add George as a contact?](#)

Share & stay in touch



Upload & organize



Make stuff!



Explore...



[Take the Tour](#)

Explore [Flickr Blog](#), the [World Map](#), [Camera Finder](#) or interesting uploads from [the last 7 days](#).



[Sign In](#)

[Create Your Account](#)

**Share your photos.
Watch the world.**

AND
VIDEO

SEARCH

5,008 uploads in [the last minute](#) · 71,248 things tagged with [jump](#) · 4.3 million things [geotagged](#) this month · [Take the tour](#)

pensuncle

5,008 uploads in [the last minute](#) · 71,248 things tagged with [jump](#) · 4.3 million things [geotagged](#) this month



Make stuff!

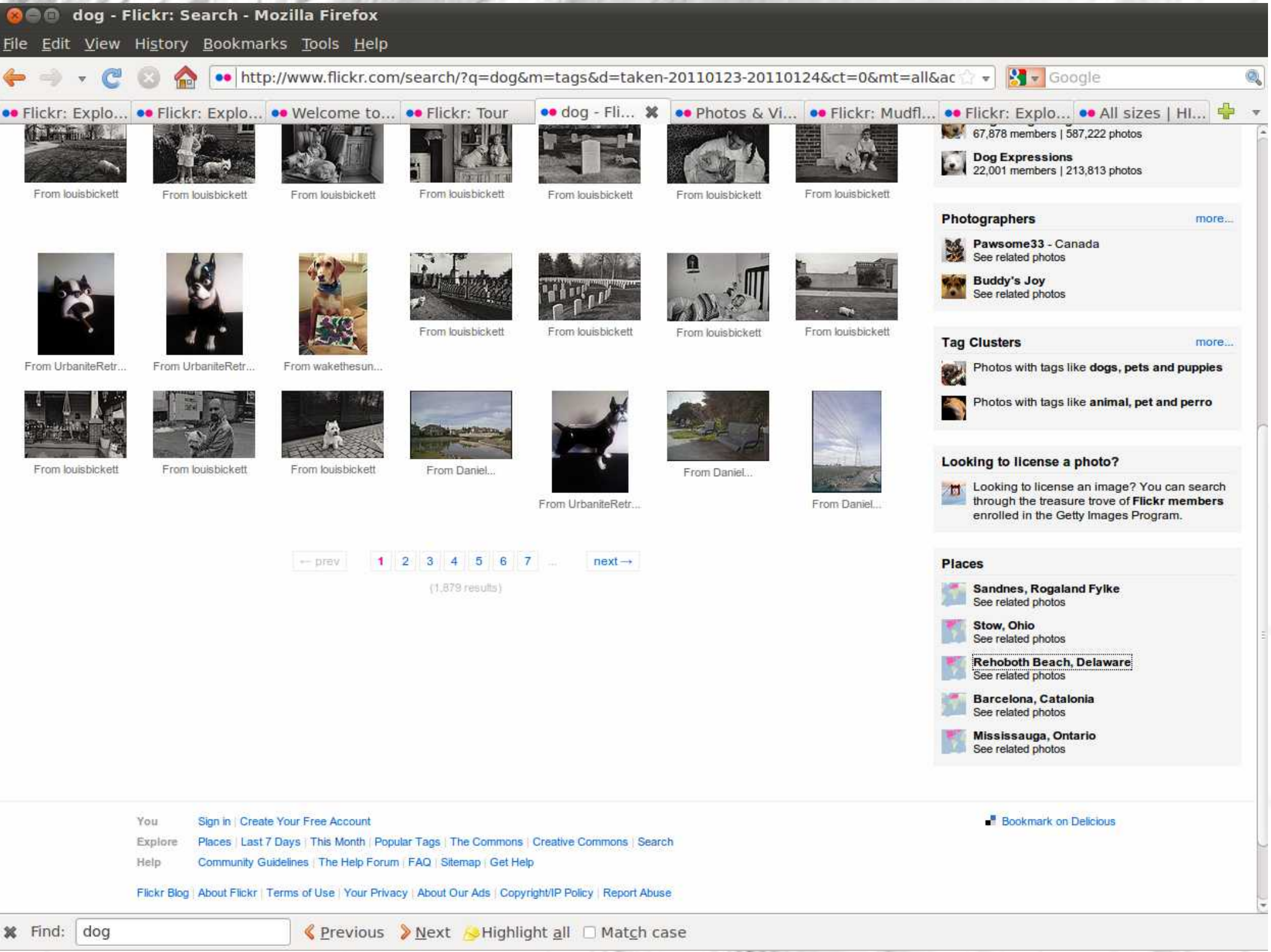


Explore...



Take the Tour

Explore [Flickr Blog](#), the [World Map](#), [Camera Finder](#) or interesting uploads from [the last 7 days](#).



flickr from YAHOO!

Home The Tour Sign Up Explore Upload

You aren't signed in Sign In Help

Find a place Search



Places / United States / Delaware /

Rehoboth Beach



Search for

Excellent Photos GO

All time popular tags

beach, delaware, rehoboth, sand, ocean, boardwalk, fence, dolles, water, sunrise, de, sun, night, bird, summer, oceanbeach, wave, waves, carousel, sign

Local time is 8.25pm Colour provided by Dopplr



20110123-DSC_1696 by MudflapDC

Interesting

Recent



From Emmott



From MudflapDC



From MudflapDC



From MudflapDC



From MudflapDC

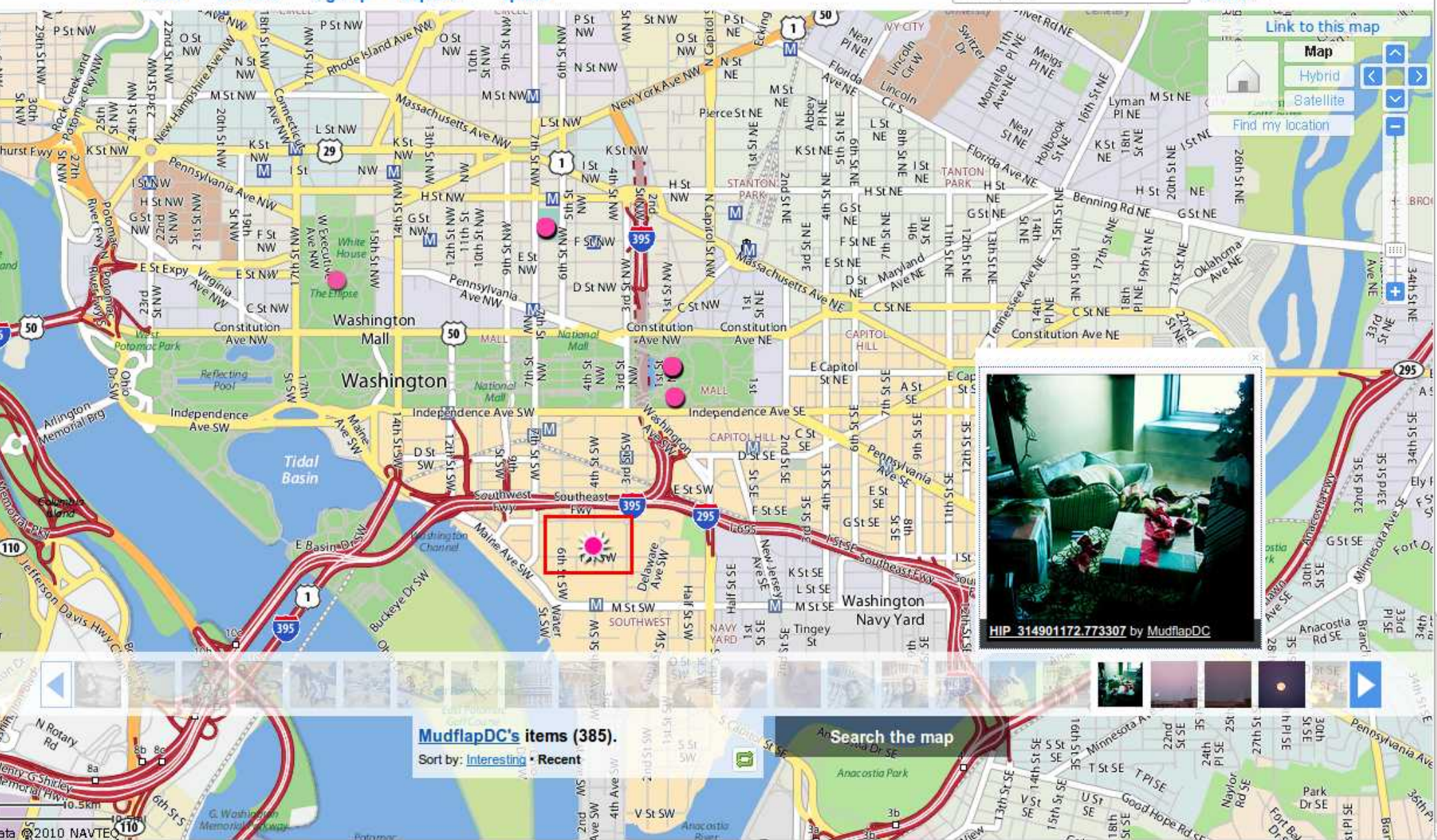


From MudflapDC

flickr from YAHOO!

Home The Tour Sign Up Explore Upload

Find a place Search





MudflapDC's photostream pro

[Collections](#) [Sets](#) [Galleries](#) **Tags** [People](#) [Archives](#) [Favorites](#) [Profile](#)

Jump to:

GO

06042010 4th against arboretum arlington army art atlanta atlantic **ave** ballpark baltimore band
baseball beach beer brain braves **bride** building bw cancer capitol cemetery center charity
charleston cheerleaders christmas colbert concert constitution create d3000 day **dc**
dcist de delaware **dog** dusk earl east **erie** fall fear fireworks footprints francisco friday
friends fun fundraiser funeral garden giants grass **groom** holiday hot hurricane independance
jose july laborday leaves lights mall marlins me **melissa** military **mlb** monument music
national nationals **nats** newyork night **nikon** nw ny nyc ocean october or
oregon orioles **pa** parade **park** pennsylvania pitcher pitching portland potomac pug rain
rally rb red rehoboth restore san sand sanity se **seattle seattlest sedc** service shore
smithsonian st start stephen stephenstrasburg stewart storm **strasburg** strasmas summer sunset
sw **swdc** tree trip uniform va **vabc vacation victoria** virginia voices wa walk wash
washdc **washington** washingtondc wave wedding weekend welovedc win
wldc woods zoe **zoo**



MudflapDC's photostream pro

[Collections](#) [Sets](#) [Galleries](#) **Tags** [People](#) [Archives](#) [Favorites](#) [Profile](#)

Jump to: [GO](#)

06042010 4th against arboretum arlington **army** art atlanta atlantic ave ballpark baltimore band
baseball beach beer brain braves bride building bw **cancer** capitol cemetery center charity
charleston cheerleaders christmas colbert concert constitution create d3000 day dc
dcist de delaware **dog** dusk earl east erie fall fear fireworks footprints francisco friday
friends fun fundraiser funeral garden giants grass groom holiday hot hurricane independance
jose july laborday leaves lights mall marlins me **melissa** military **mlb** monument music
national nationals **nats** newyork night nikon nw ny nyc ocean october or
oregon orioles pa parade park pennsylvania pitcher pitching portland potomac pug rain
rally rb red rehoboth restore san sand sanity se **seattle** **seattlest** sedc service shore
smithsonian st start stephen stephenstrasburg stewart storm strasburg strasmas summer sunset
sw swdc tree trip uniform va vabc vacation victoria virginia voices wa walk wash
washdc **washington** washingtondc wave wedding weekend welovedc win
wldc woods zoe zoo

**What if The Attacker's Motives Were
More Sinister?**

**Could He Find a Mark On Flickr in a
Specific Location?**

You bet!

flickr® from YAHOO!

Home The Tour Sign Up Explore Upload

You aren't signed in Sign In Help

Find a place Search

Link to this map

Map Hybrid Satellite Find my location



36,905 results matching "beach" here.

Sort by: Interesting Recent

Search the map

Find a place

Link to this map

Map

Hybrid

Satellite

Find my location



15 results matching "tent" here.

Sort by: Interesting • Recent

Search the map

**Who here doesn't use
Social Networking,
Geotags, or
smartphones?**

Do you have kids?





What about a spouse?

PRINT THIS PAGE

From Times Online

July 5, 2009

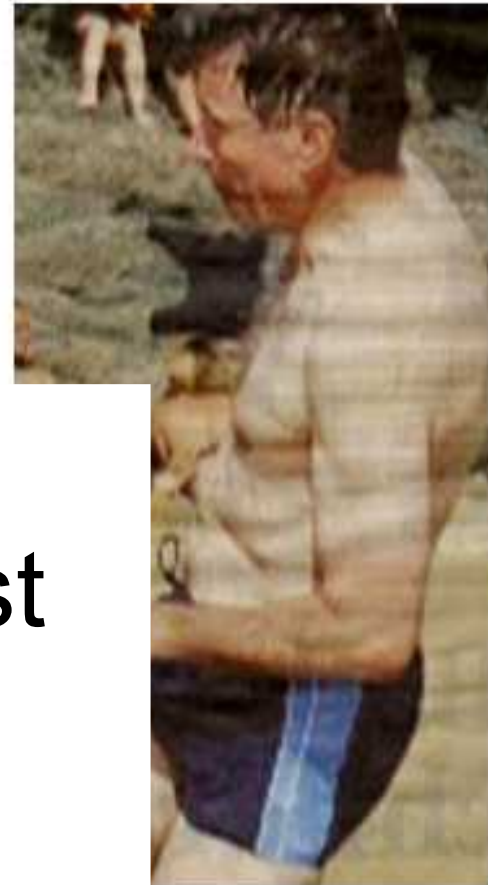
Wife blows MI6 chief's cover on Facebook

Nadia Gilani

The wife of the new head of MI6 has caused a major security breach and left his family exposed after publishing photographs and personal details on Facebook.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all of Britain's spying operations abroad.

But entries by his wife Shelley on the social networking site have exposed potentially compromising details about where they live and work, their friends' identities and where they spend their holidays. On the day her husband was appointed she congratulated him on the site using his codename "C".



Sawers on the beach in family photos

- July 2009
- England's MI6 chief's wife post sensitive info on Facebook
- Family, friends, and national security at risk

**Unintentional Information Disclosure of
Sensitive Personal Information Might
Come from Those Closest To You**

Are SocNets Evil?

- There are dozens of location-aware social networking services
- There are hundreds of social-networking sites
- Yes it's nice to stay in touch with friends and family
- But, Understand your role:

You are the product
NOT the customer

Are SocNets Evil?

- There are dozens of location-aware social networking services
- There are hundreds of social-networking sites
- Yes it's nice to stay in touch with friends and family
- But, Understand your role:

You are the **product**
NOT the customer

Don't Live Life in Fear, but...

- Keep Private Information, Private
- Minimize Your Threat Surface
- Evaluate Risks
- Have a Backup Plan (What happens if...?)
- Be Educated
- Be **AWARE**

Take Your Work Home With You!

Defend yourself from becoming a victim/statistic

Protect your assets (this includes information)

InfoSec Best-Practice applies just as easily at home as in the office... or the battlefield

Presenter:
Sean Wilkerson
Aplura, LLC
swilkerson@aplura.com
Twitter [@sdwilkerson](https://twitter.com/sdwilkerson)