



***Family Cyber Security  
Awareness Brief***

***UNCLASSIFIED***

***2015***



## *Sources*

**[www.joyoftech.com](http://www.joyoftech.com) – archived photos**

**United States Strategic Command Cyber Portal**

**[https://vela.stratcom.mil/sites/cyber\\_gateway/default.aspx](https://vela.stratcom.mil/sites/cyber_gateway/default.aspx)**

**The Internet of Things**

**<http://blog.surveyanalytics.com>**



# *Cyber User Awareness*

Cybersecurity has become an integral part of society with the growth of mobile electronic devices and the mass utilization of the Internet via social media.

There are inherent dangers when participating in any social media or utilizing any commercial email account.

As with any medium that involves passing personal or professional information, caution should be used

***Applying practical security safeguards is paramount in protecting your information and identity.***



## *Digital ID*



**A digital identification or footprint is the record or trail left by the things you do online. Your social media activity, the information on your personal website, your browsing history, online subscriptions, any photo galleries and videos you've uploaded.**



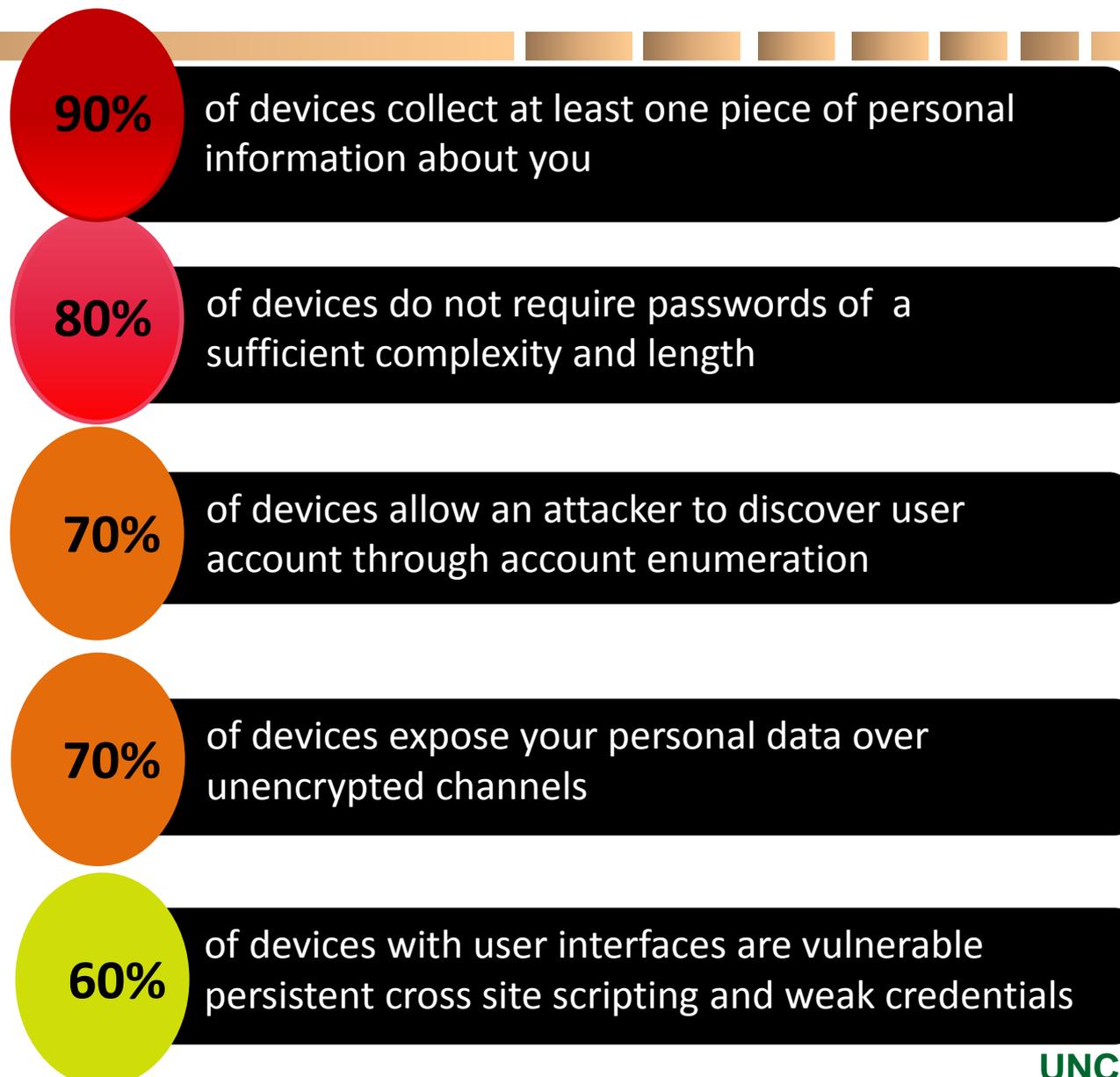
# *“The Internet of Things”*

The **“Internet of things”** refers to devices other than computers, smart phones, or tablets that have the ability to connect to the internet and communicate with other connected devices.

These devices collect data using small sensors and communicate the data to other devices, databases, or the user via the internet. By communicating this data between devices almost everything in your home, in a city, and around the world can be controlled and operate in unison to adjust for any situation based on data collected near or far.



# Internet Security Concerns





# *Security Concerns*

As with any connected device, security is a big concern when it comes to the **Internet of Things**. When considering the massive amounts of data these devices will be collecting, one must wonder where all that data goes, who has access to it, and how can cyber criminals use the data to damage a person's financials or reputation. Other devices, such as "smart watches" will collect data on the user's location, activity, and even health or mood information.



# Wi-Fi /Gaming Consoles

- Change default passwords / do not utilize simple passwords for game accounts.
- Restrict access
- Encrypt your data (enable WPA/WPA2)
- Protect your SSID (don't advertise the unique identifier)
- For added security, install a firewall
- For online-gaming purchases, utilize a pre-paid gaming card rather than using a bank credit card





# Increase Password complexity

- *Do not share your passwords with anyone (create separate accounts for the kids)*
- *Change passwords on a regular basis (recommended every 3-6 months)*
- *Do not use the same password for multiple accounts*
- *Ensure passwords characters have a combination of upper and lower case letters, numbers, and special characters*
- *Passwords should NOT stored on paper accessible to everyone or stored electronically on your personal computer*
- *Don't use passwords that are based on personal information that can be easily accessed or guessed*
- *Don't use words that can be found in any dictionary of any language*
- *Use passphrases when you can (ex: !L1keTh3c@ndybarReese\$ )*

**\* Don't forget about your wireless router – this should be an extremely complicated password...it's the gateway into your home network.**



# Social Media Security





# Social Networks

- Social Media Integration – The nearly universal “Like” button



- Logins maintained through cookies, sometimes flash
- Third parties can see login, compromise privacy
- Search engines link your search terms to your social media profile for extra personalization
- Bottom Line....Good idea to log out of your social media accounts when searching for information on Google, Yahoo, Bing etc.



## *Social Media Best Practices*

- **Utilize the privacy and security settings on social networks—reduce what others can see or collect on your family.**
- **Keep personal information personal: Be cautious about how much personal information you provide on social networking sites. Information can be used to steal your identity, access your data or even lead to stalking.**
- **Be careful not to divulge any sensitive information. This can also lead to you being a target for social engineering or possible collection of information.**
- **Don't reveal information (even innocently) about military activity, operations or CENTCOM affiliation**



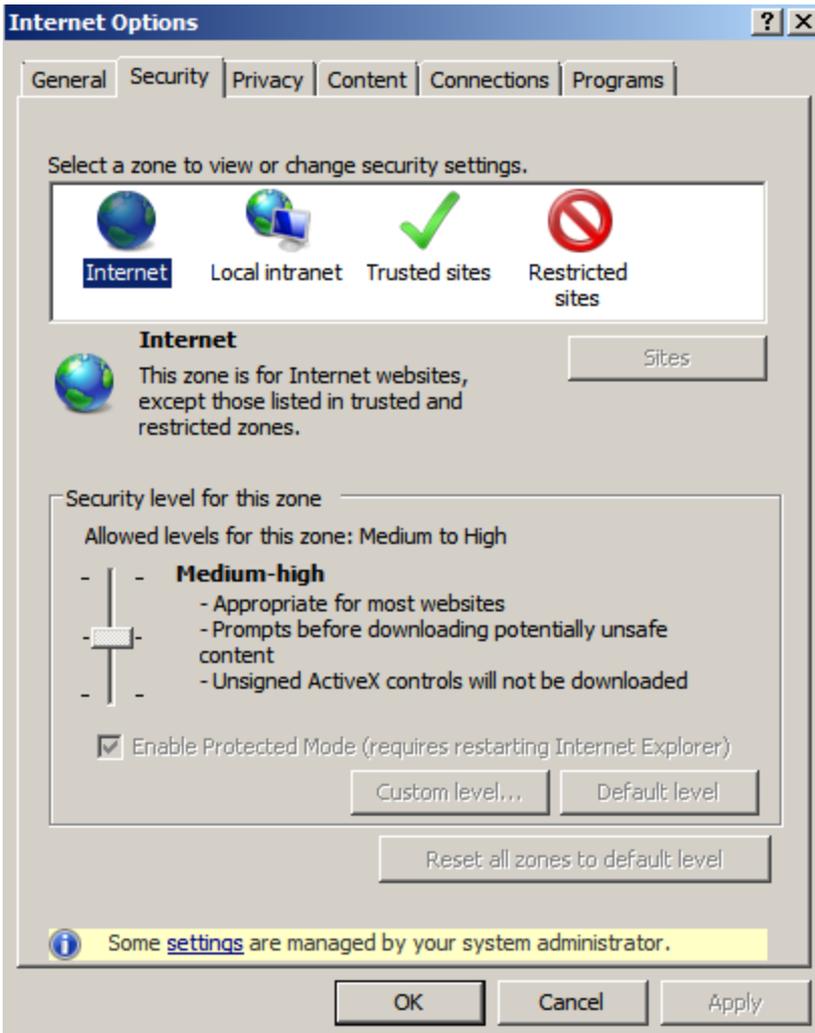
# Web Security



<https://www.>



# Web Browser Security



## ZONES

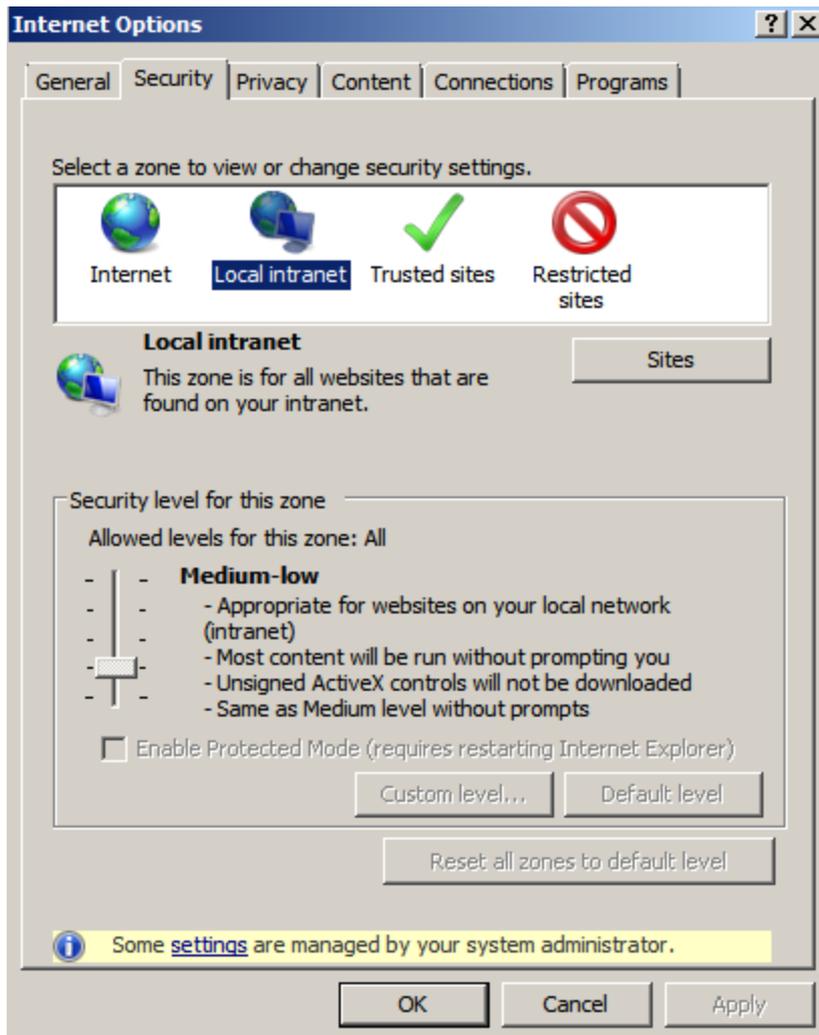
*Your browser may give you the option of putting web sites into different segments or zones and allow you to define different security restrictions for each zone.*

## Internet Zone

*When you browse the Internet, the settings for this zone are automatically applied to the sites you visit. For best protection as you browse you should set the security to the highest level or at least maintain at a medium level.*



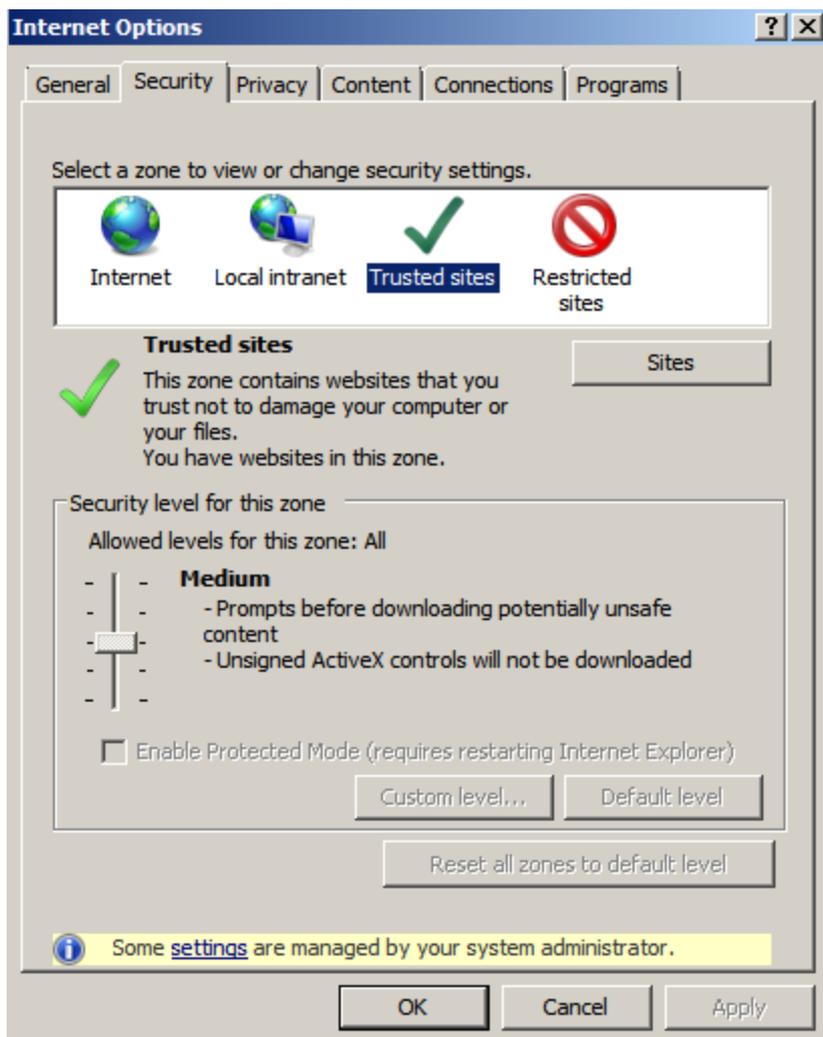
## Local Intranet



*If you are in an office setting that has its own intranet, this zone contains those internal pages.*



## Trusted Sites

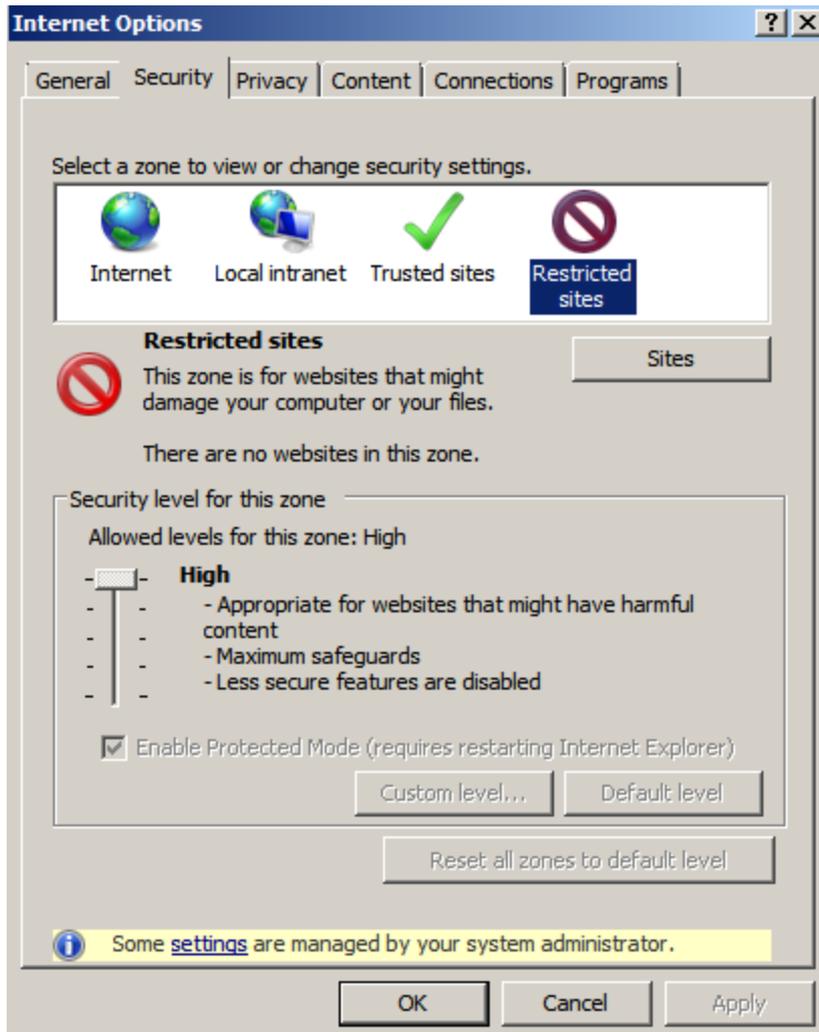


*If you believe that certain sites are designed with security in mind and you feel that content from the site can be trusted not to contain malicious material, you can add them to your trusted sites. Recommend you only add (\*SSL) enabled sites.*

*\*Sites in the URL title bar which start with https://*



## Restricted Sites



*If there are particular sites you think might not be safe, you can identify them and set heightened security settings.*

*Best precaution is to avoid going to sites that make you question whether or not they're safe.*

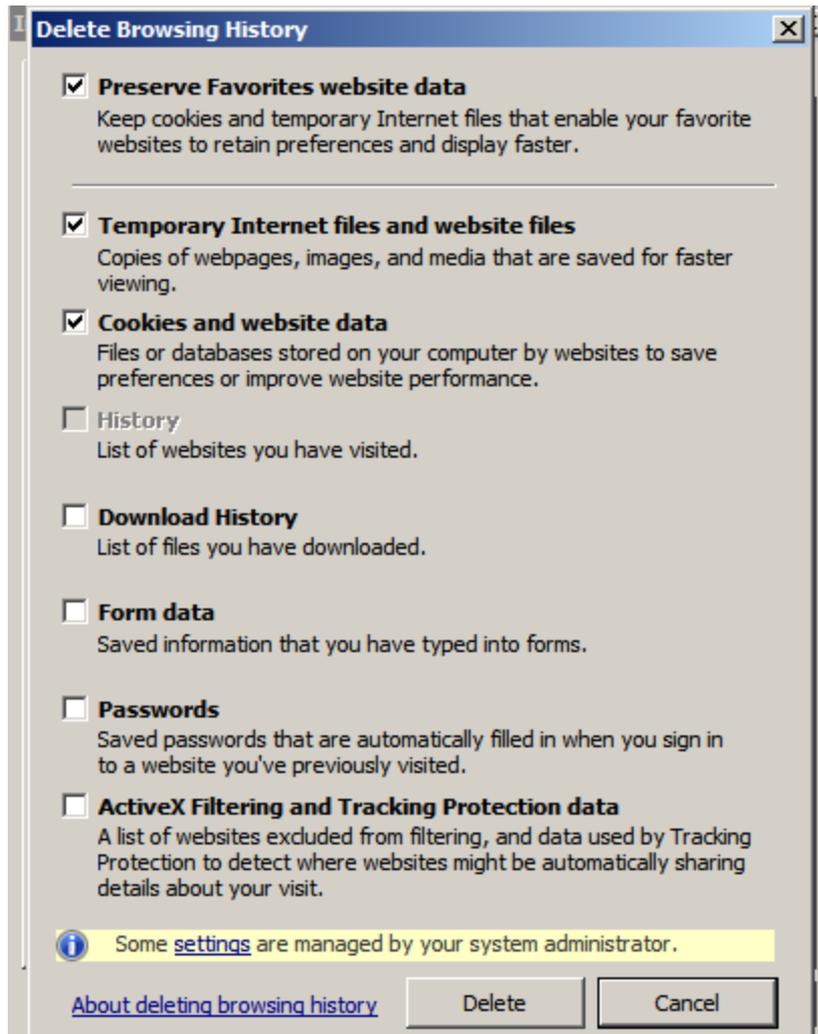


## References

Report online Internet complaints to FBI via  
<http://www.ic3.gov/default.aspx>

Cyber Security / Home Computer Security Information  
<http://www.us-cert.gov/home-and-business>

Computer Scams  
[http://www.fbi.gov/scams-safety/computer\\_protect](http://www.fbi.gov/scams-safety/computer_protect)





# ***Operation Security for USCENTCOM Family Members***



## Sources

**Bing archived cyber crime** – archived stock photos

**Creative Commons**-<http://creativecommons.org/> Except as otherwise noted, the content of this page is licensed under the Creative Commons Attribution 3.0

**Slide share Portal**-[https://vela.stratcom.mil/sites/cyber\\_gateway/default.aspx](https://vela.stratcom.mil/sites/cyber_gateway/default.aspx)

**Jeffrey's EXIF Viewer:**

[Http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=http%3A%2F%2Fregex.info%2Fexif.cgi&ei=g9bkVJeVFIOLNqi2hKAE&usg=AFQjCNENO9\\_6UzvwlrY7qcAGyJNyl0MtJg&bvm=bv.85970519,d.eXY](Http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=http%3A%2F%2Fregex.info%2Fexif.cgi&ei=g9bkVJeVFIOLNqi2hKAE&usg=AFQjCNENO9_6UzvwlrY7qcAGyJNyl0MtJg&bvm=bv.85970519,d.eXY)

**Kate Murphy**, “Web Photos That Reveal Secrets, Like Where You Live”, *The New York Times* Aug 11, 2010, [http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?\\_r=0](http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0)

**David Lazurus**, Consumer confidential, *Los Angeles Times*, April 16, 2012 , <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.latimes.com%2Fbusiness%2Fla-fi-lazarus-sg-storygallery.html&ei=U9jkVNPBNZH7gwSk5IAo&usg=AFQjCNFNKOXvC-x4JpOrTyuCdg8QxgZ5kA&bvm=bv.85970519,d.eXY>

**Internet Archive:** <https://www.archive.org>

**Wayback Machine:** <https://waybackmachine.org/>



# *Team Effort*

Your loved one has the training, leadership and equipment needed to perform the mission and come back home to you.

But did you know that you're half of the team?





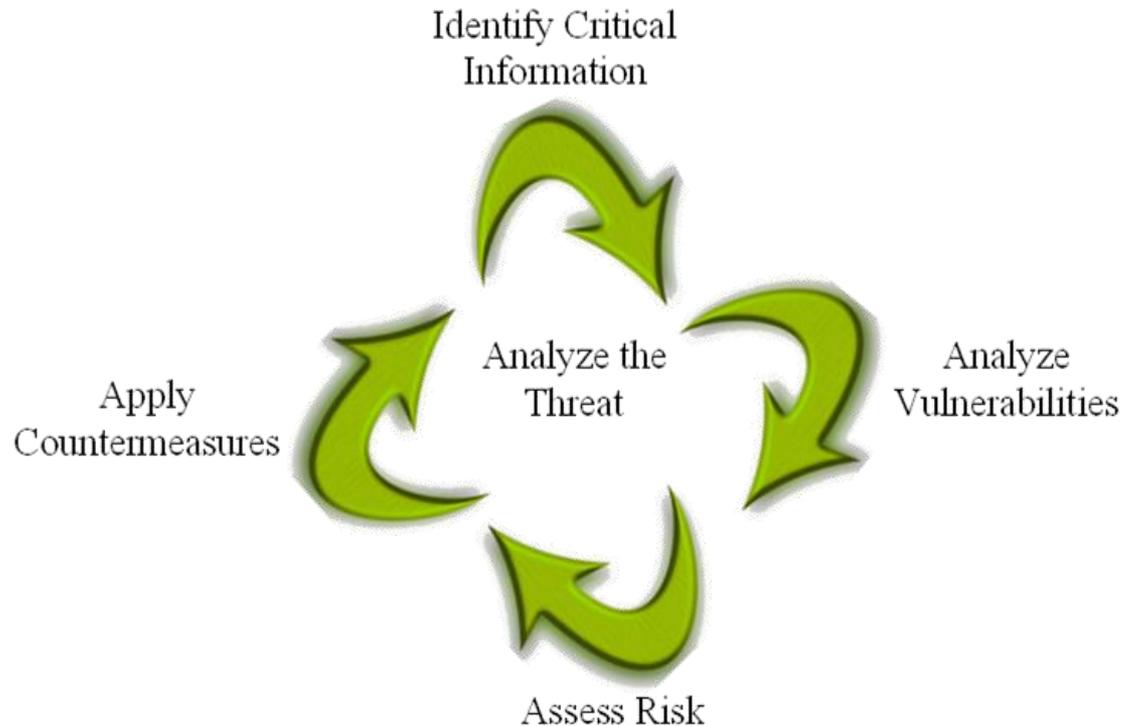
# *Agenda*

- **OPSEC Defined**
- **Information Environment**
- **Critical Information**
- **Vulnerabilities**
- **Hard Target example**
- **USCENTCOM Member and family Best Practices;  
DO's and DON'Ts**



# Operations Security (OPSEC)

OPSEC is a process that identifies critical information, outlines potential threats and risks and develops counter measures to safeguard critical information





## ***OPSEC Defined***

- **OPSEC is a process:**
  - **Analyze friendly actions**
    - That can be observed by adversary intelligence systems
    - That could be interpreted to be useful to an adversary
  - **Execute selected measures to eliminate or reduce adversary or criminal exploitation of friendly critical information**

Joint Publication 3-13 *Operations Security* Jun 2012



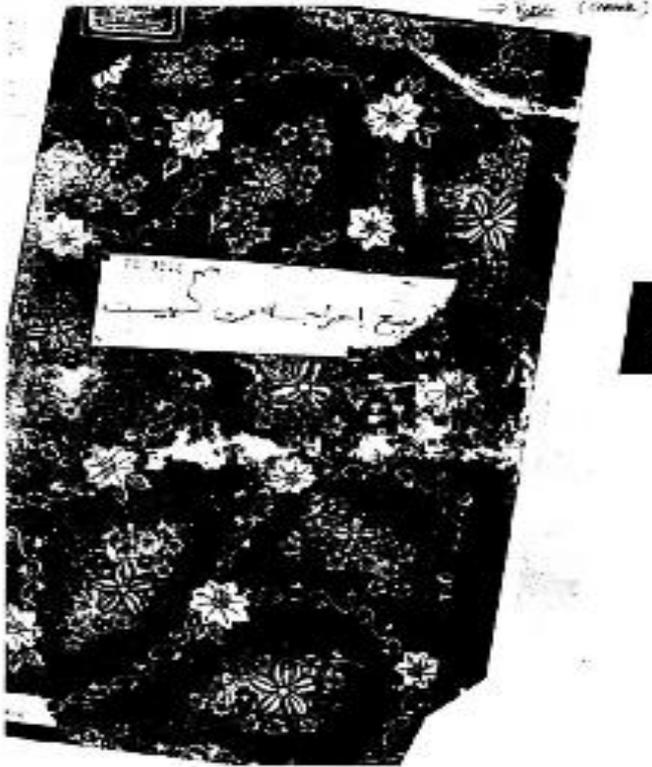
# “But it’s not classified...”

- Unclassified does **NOT** mean unimportant
- 90% of all intelligence collected is unclassified
  - Open Source Intelligence (OSINT)
  - THE INTERNET
- Anything we freely provide will be exploited
- Technical security only as good as the next *smart adversary or criminal*





# Adversary's Point of View



This manual was captured in a home raid in Iraq, and is only one of countless copies. According to this manual, 80% of military intelligence can be collected from legal sources, including websites, blogs, newspapers and online.

UNCLASSIFIED//FOUO

EXHIBIT  
1677-1  
320

IT IS FORBIDDEN TO REMOVE THIS FROM THE HIDE

Handwritten notes in Arabic script, including the name 'Said al-Mutairi' and other illegible text.



# *Internet Environment*

- **Nothing constrains Cyber Actors**
  - Very little legal consequence for most malicious activities
  - Hacker tools easily shared and leveraged
  - Security is secondary consideration in software/hardware development (richness of user experience primary driver)
- **Cyber crime laws having effect?**
  - Prosecution of four high-profile bot masters in 2009 and 2012

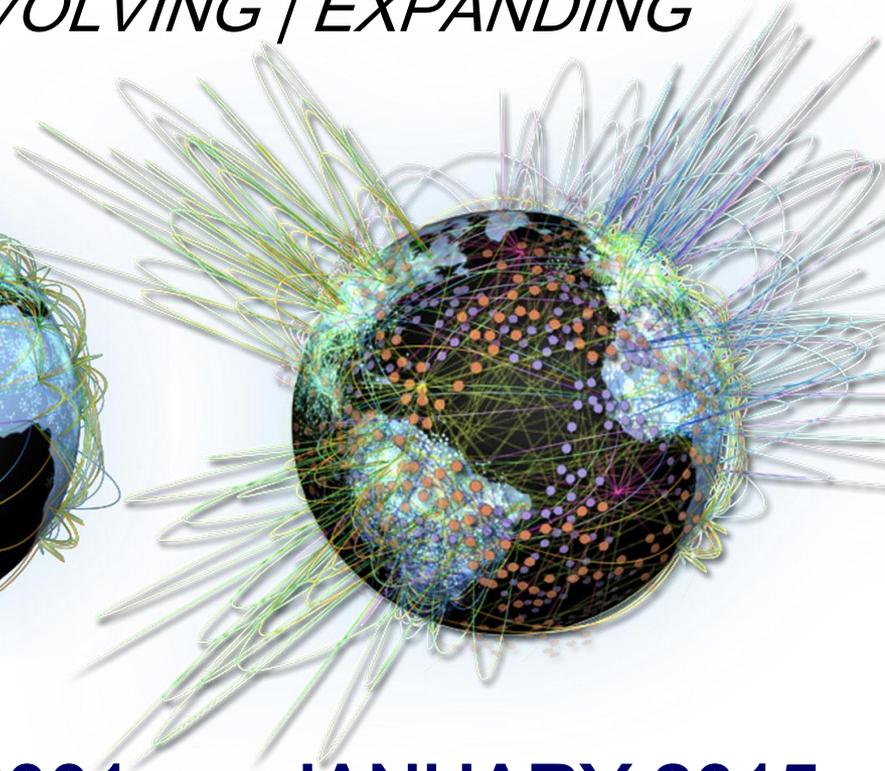
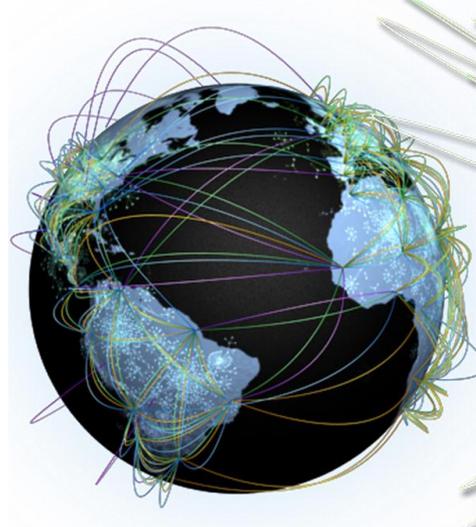


**As long as the information environment lacks sufficient restrictions, everyone is vulnerable**



# Cyberspace Never Stops...

*ACCELERATING / EVOLVING / EXPANDING*



**DECEMBER 1995**

16 million Internet users

**MARCH 2001**

458 million Internet users

**JANUARY 2015**

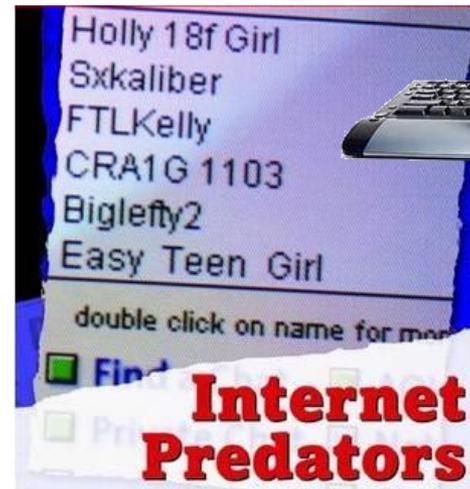
1.9 billion Internet users



## The Danger

Bad guys use it, too:

- Terrorist
- Hackers
- Thieves
- Stalkers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on...





## The Danger

Al-Qaeda communiqué December 2009:

“The affair with the U.S. Navy began several years ago, when the lions of Al-Qaeda struck the destroyer

Information on every U.S. Naval unit should be quietly gathered...what state they are from, their **family** situation, and where their **family** members live...  
 ...search for the easiest ways of striking these ships...

to western countries in general; searching all naval websites in order to gather as much information as possible, and translating it into Arabic; search for the easiest ways of striking these ships...

“M.... Do not underestimate the importance of any piece of information, as simple as it may seem....



# Data Aggregation

- Information collection from multiple sources
- Al Qaeda handbook: open and legal public sources accounts for 80% of all information collected
- Legal and illegal collection methods



# USCENTCOM Critical Information List

Critical information are items that identify specific facts about intentions, capabilities, and activities needed by adversaries to plan and target USCENTCOM and its missions, subordinates, or nodes.

**IT IS STRICTLY PROHIBITED TO DISCUSS THE FOLLOWING TYPES OF INFORMATION IN UNCLASSIFIED EMAILS OR PHONE CONVERSATIONS PER CCR 530-1 AND USCENTCOM POLICY LETTER 12.**

- CIL 1: Current and Future Operations
- CIL 2: Scope of Operations
- CIL 3: Intel, Recon and Surveillance information
- CIL 4: Schedule of Personnel Involved in Operations
- CIL 5: Communications Supporting Operations
- CIL 6: Admin Support to Operations
- CIL 7: Personnel Supporting Operations
- CIL 8: Logistical Support to Operations
- CIL 9: Items under investigation
- CIL 10: Command Directed Items of Interest not related to a specific CIL



# Family Critical Information

- Information **we must protect** to ensure success.
  - Information the **adversary needs** to prevent our success.
- 
- Names and photos of you, your family and co-workers
  - Usernames, passwords, network details
  - Job title, location, salary, clearances
  - Physical security and logistics
  - Position, mission capabilities and limitations
  - Operations & missions
  - Schedules and travel itineraries
  - Social security number, credit cards, banking information
  - Hobbies, likes, dislikes, etc.





## Potential Vulnerabilities

### Methods used to obtain Critical Information:

- Social Networking Sites
- Unprotected communications
- Sharing too much with strangers
- HUMINT Observations
- Technology
- Trash
- Media
- Email
- Web pages



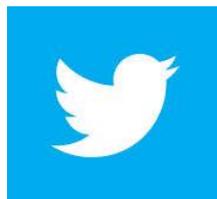
**Illegal methods are OK with adversaries!!!**



# Social Media

**Social Media allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries.**

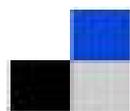
Google<sup>™</sup>  
Social



facebook

Blogger

TAGGED



del.icio.us



LinkedIn

YAHOO! You Tube

Broadcast Yourself

Blogger<sup>™</sup> web publishing service; Blogspot<sup>™</sup> web publishing service are registered trademarks of Google Inc.  
 Delicious (formerly del.icio.us) is sold Delicious to AVOS Systems in April 2011, relaunched in new beta" Sep 27 2012. AVOS sold the site to Science Inc in May 2014.  
 Facebook is a registered trademark of Facebook Inc. All rights reserved.  
 © 2012 Google Inc. All rights reserved. Google and the Google logo are registered trademarks of Google Inc.  
 LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks  
 Yahoo!, the Yahoo! logo, and the Yahoo! interface are trademarks or registered trademarks of Yahoo! Inc.  
 YouTube<sup>™</sup> video community and the YouTube logo are registered trademarks of Google Inc.  
 Flickr, and the Flickr logo<sup>™</sup>, are trademarks or registered trademarks of Yahoo! Inc. 2008 (filed in 2005)  
 TAGGED, Friend Search, and TAGGED © logo are 2015 are registered trademarks of Ifwe Inc.  
 The Twitter name, logo, Twitter T and Tweet are trademarks of Twitter, Inc.



## *Why use Social Media?*

### Personally

- Entertaining
- Maintain Relationships
- Network
- Centralized information

### Professionally

- Marketing/recruiting
- Public Relations
- Connect with customers
- Solicit ideas and feedback





# Social Media Vulnerability



- Policy Letter Number 51, USCENTCOM Policy for Internet-Based Capabilities approves SNS usage for official purposes only
- Social networks are a popular attack vector for Identity thieves, spammers and make an attractive target for spear phishing

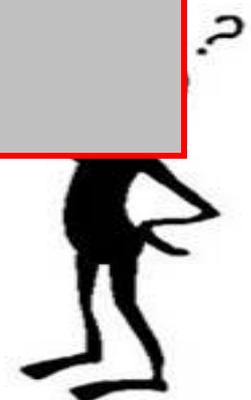
**USCENTCOM members and families must use social media sites responsibly during off duty time to avoid inadvertent disclosure of sensitive or personal information and elicitation by adversaries and criminals**



# Revised Statement of Rights & Responsibilities



- “
  - “
- Consent to Collection and Processing in the United States. By using Facebook, you consent to having your personal data transferred and processed .**
- Royalty-free
  - Worldwide license
- “We may collect information about you from other users.”
  - “Sometimes we share aggregated information with third parties.”





# Dangerous Applications

## **M** Allow Access?

Allowing Mafia Wars access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.



### Mafia Wars



Start a Mafia Family with your friends, do Crime Jobs for cash, buy Powerful Weapons, and Fight!!!

**Allow** or cancel

By proceeding, you are allowing Mafia Wars to access your information and you are agreeing to the Facebook Terms of Use in your use of Mafia Wars. By using Mafia Wars, you also agree to the Mafia Wars Terms of Service.



# Social Media “Add ons”

- Thousands of “applications”
  - Quizzes / games / gifts / etc.
  - Ingress vector for malicious code (viruses rampant)
  - User must agree to allow access before running





## Facebook “Features”

- **By default, FB profiles are completely open to everyone in the same region**
- **Privacy settings must explicitly be set**
- **Facebook “friends” are a two-way trust**
  - **Networks used to suggest more “friends”**
  - **This trust is easily exploited**
  - **FB often changes default page, photo and newsfeed setting without prior warning**





# *Social Engineering vulnerability*

**Social engineering is an effective method to stealing confidential data from organizations or individuals...**

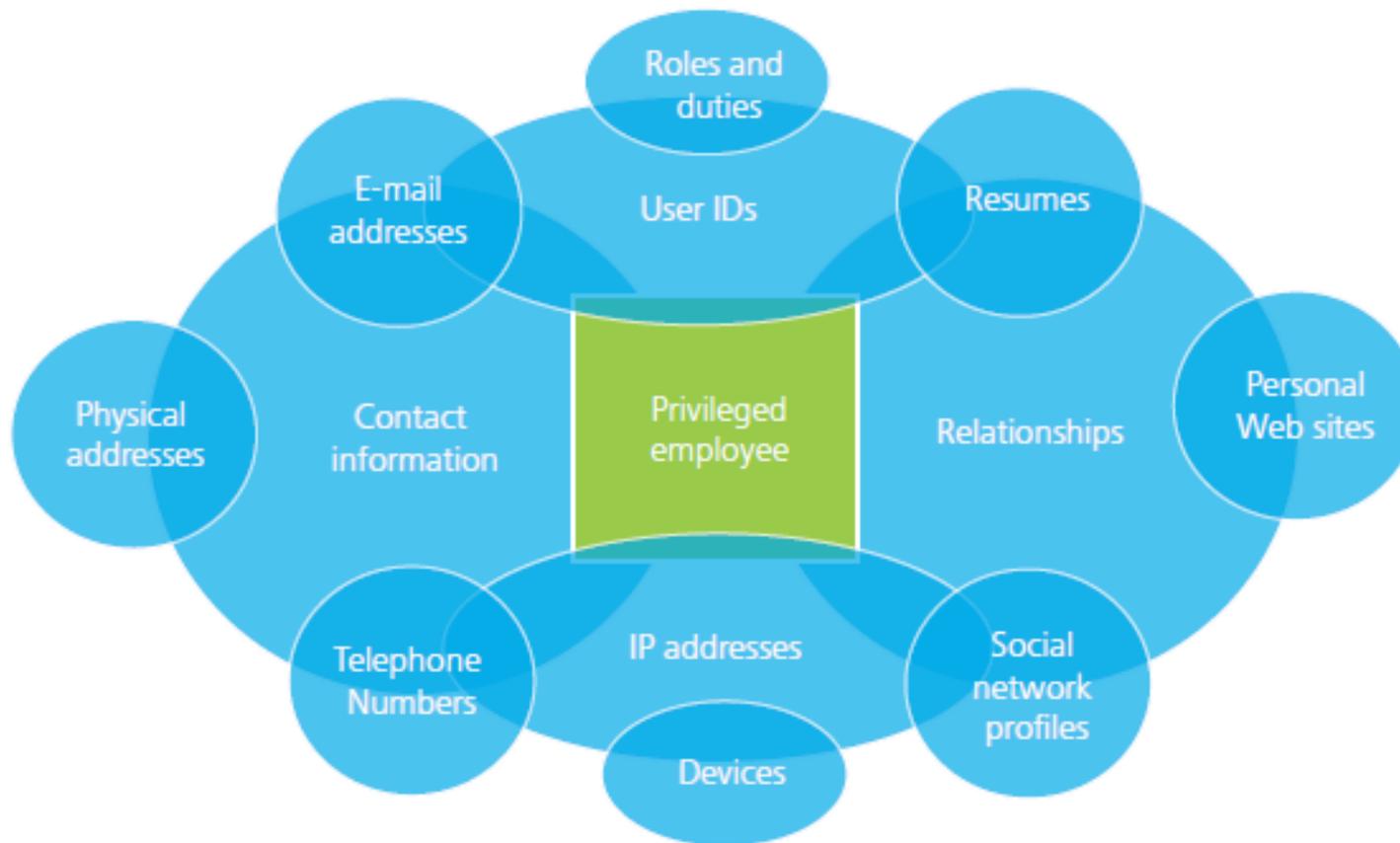
**In a recent test, 85% percent of individuals were duped using Social engineering.**

***“Most employees are utterly unaware that they are being manipulated,” says Colin Greenlees, security and counter-fraud consultant at Siemens.***





# Social Engineering Vectors





## *Military sites are vulnerable too*



**Four Fort Bragg soldiers had their paychecks stolen via the government “mypay” website by identity thieves who stole their logins and passwords**

**The soldiers noticed four days before their paycheck was scheduled to be paid that the funds would not be deposited in their regular accounts. They alerted Army finance immediately**

**However, even with four days’ warning, the funds couldn’t be recalled. Their pay was rerouted to the other bank, where it was captured on a bank-issued prepaid debit card and quickly withdrawn.**

**Even after a lengthy military investigation, the thieves were never caught**



## Persona Details

The Yahoo! logo in its classic red, 3D-style font.

The Google logo in its multi-colored, 3D-style font.

- Your persona is communicated to every web server (and every webmaster) of every web page that you visit.
- You should be explicitly aware of your persona before you visit any website.
- Your persona may also be transmitted via Java Applets such as Google's Urchin Tracking Module

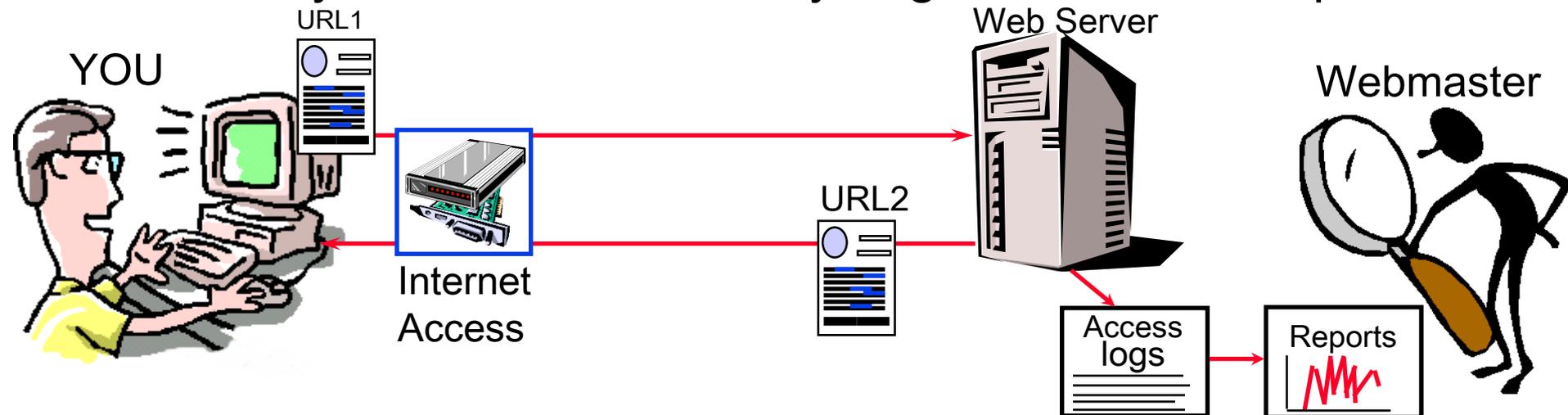


WIKIPEDIA  
The Free Encyclopedia **FI**ED



# Introduction to “Persona”

As you surf the Internet, you give-off a certain persona



- While viewing a web page (URL1), You click on a hyperlink to visit another web page (URL2)
- Your web browser sends “environment variables” to the web server.
- Webmaster’s use this information to determine information about you and your organization (**physical location, keyboard language, searches, Operating system, Software version, etc.**)



# Smart Phone vulnerabilities

➔ **Geo-tagging photos can lead to cyberstalkers finding you**



**I Can Stalk U**  
Raising awareness about inadvertent information sharing

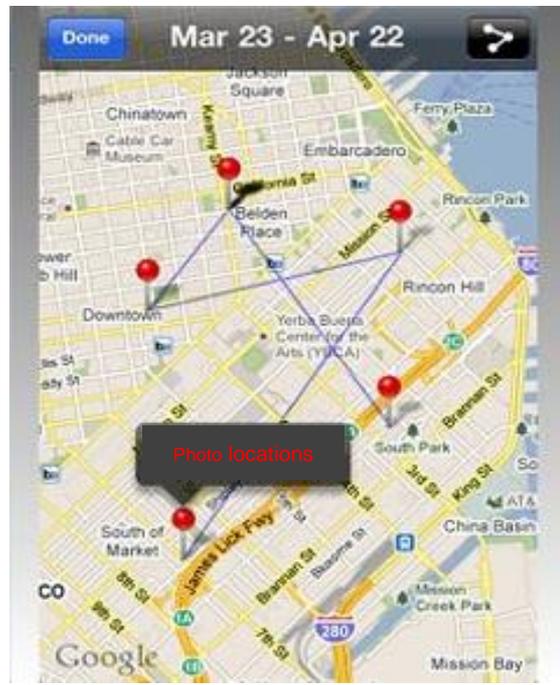


facebook

Places

**"Camera" Would Like to Use Your Current Location**  
Photos and videos will be tagged with the location where they were taken.

**Don't Allow** OK

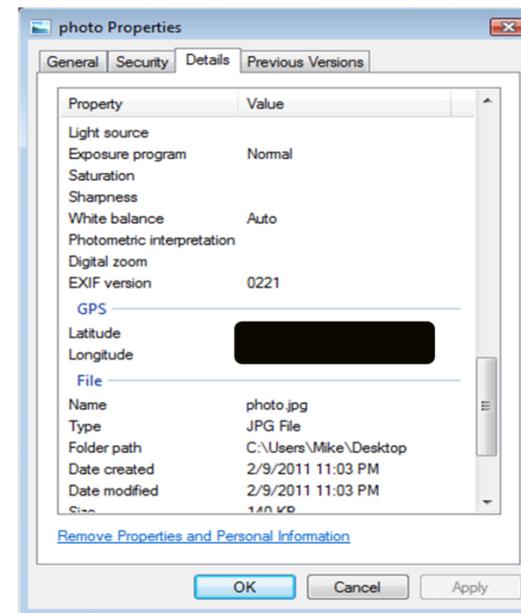




# Smart Phone -example

## Geotagging – Myth Busters

In August of 2010, Adam Savage, of “Myth Busters,” took a photo of his vehicle using his smartphone. He then posted the photo to his Twitter account including the phrase “off to work.” Since the photo was taken by his smartphone, the image contained metadata revealing the exact geographical location the photo was taken. So by simply taking and posting a photo, Savage revealed the exact location of his home, the vehicle he drives and the time he leaves for work.



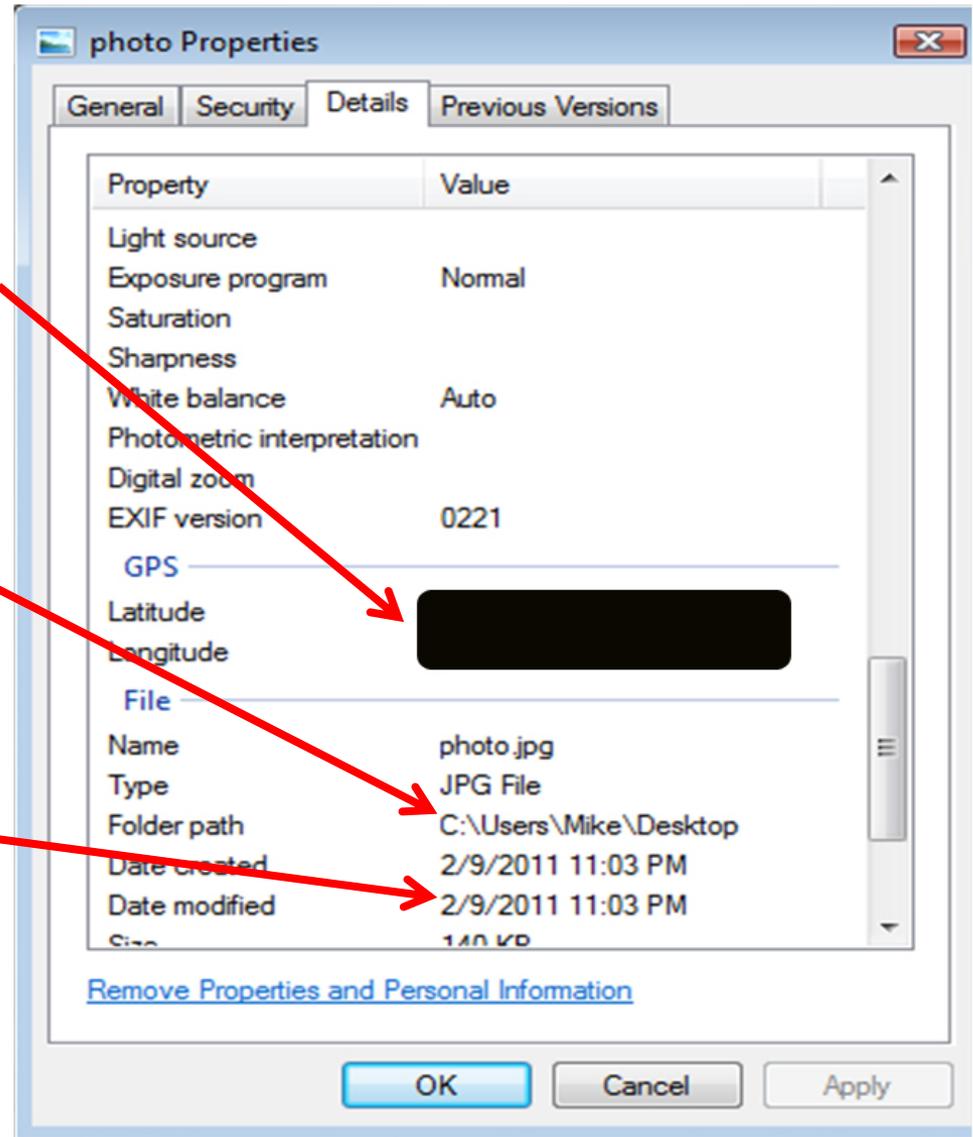


# Smart Phone Metadata

Exact **geographic location** of photo

Location of **picture** on your computer

Date photo taken





# EXIF Data in Photograph

Camera Type →

Date/Time photo taken →

Exact Geographic location  
Of Google earth GPS or  
LAT/LONG →

From Web  From File  Image URL:  [View Image At Url](#)

[CLEAR IMAGE]

**Jeffrey's EXIF Viewer**  
(help)

Drag this button to your button bar, then while on a page displaying an image, just click the button in the bar to view the image's EXIF data [EXIF](#)

You also might be interested in these Firefox extensions:  
Alan Raskin's [EXIF Viewer](#), which shows quite a bit of information, and Ted Markzark's [EXIF](#), which shows basic data only.

**Some of my other stuff**

- [My Blog](#) · ["Camera Stuff"](#) · ["Photo Tech"](#)
- [Desktop Backgrounds](#) · [Pretty Photos](#)

**Basic Image Information**

Description:	The main gate of the Heian Shrine, Kyoto Japan.
Creator:	<b>Jeffrey Friedl</b>
URL:	<a href="http://regex.info/blog/">http://regex.info/blog/</a>
Camera:	Nikon D200
Lens:	18-200 mm f/3.5-5.6 Shot at 18 mm
Exposure:	Auto exposure, Program AE, 1/320 sec, f/5.6, ISO 125
Flash:	none
User Comment:	Copyright Jeffrey Friedl
Date:	<b>January 29, 2006 11:31:12AM</b> (timezone not specified) (5 years, 1 month, 5 days, 13 hours, 34 minutes, 48 seconds ago, assuming image timezone of 9 hours ahead of GMT)
Location:	Map via encoded GPS coordinates at <a href="#">Google</a> , <a href="#">Yahoo</a> , <a href="#">WikiMapia</a> , <a href="#">OpenStreetMap</a> , <a href="#">Bing</a> (also see the <a href="#">Google Maps</a> pane below) Altitude: 51.1 m Timezone guess from <a href="#">earthtools.org</a> : 9 hours ahead of GMT
File:	<b>1,205 × 1,800 JPEG (2.2 megapixels)</b> 465,148 bytes (0.44 megabytes) Image compression: 93%
Color Encoding:	Embedded color profile: "sRGB"
Image URL:	<a href="http://regex.info/v_JEF1348.jpg">http://regex.info/v_JEF1348.jpg</a>

Extracted 256 × 171 14-kilobyte "Thumbnail Image" JPG  
Displayed here at 100% (1/16 the area of the original)



[Click image to isolate](#); [click this text to show histogram](#)

Main image displayed here at 25% width (1/16 the area of the original)



[Click image to isolate](#); [click this text to show histogram](#)

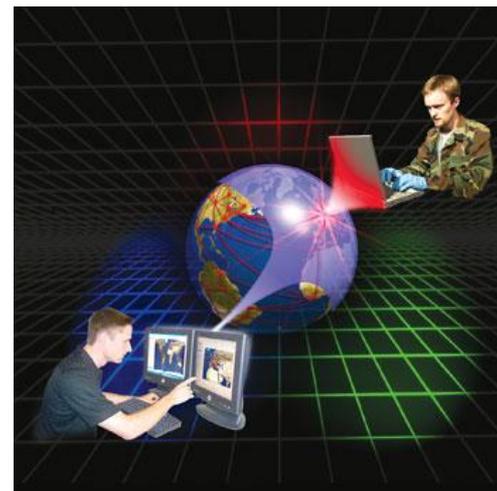
GPS-encoded location: 35° 0' 45" N, 135° 46' 37" E    Display area: 1.83 km × 440 m  
Map center: 35° 0' 45" N, 135° 46' 37" E    Distance between: 0 m    [Click on map to measure distance from GPS-encoded location](#)





## *Spear Phishing Email*

- **Phishing attacks are email based attacks customized to specific persons using data collected from public records.**
- **Emails sent often posing as someone else with a link or attachment that installs malware or a virus on the other person computer**
- **Accessing the link or attachment introduces viruses or malware to the entire network**





# Spear Phishing Example



- No specific bank
- Does not refer to a specific customer

- No date or amount of "transaction"

## Declined Direct Deposit payment

noreply@direct.nacha.org <jocking55@ablnc.att.com>

Mon, Nov 19, 2012 at 9:36 AM

Please be informed, that your latest Direct Deposit transaction (#001038638086) was rejected, because your business software package was out of date. Please use the link below to enter the secure section of our web site and see the details:

Details

Please apply to your financial institution to obtain the updated version of the software.

Sincerely yours

ACH Network Rules Department  
NACHA | The Electronic Payments Association

11558 Sunrise Valley Drive, Suite 994  
Herndon, VA 23370  
Phone: 703-424-1505 Fax: 703-521-8981

- Asks to "use the link"

- Wrong ZIP for Herndon, VA
- Address is "in" Dulles International Airport
- Phone number is a Verizon Wireless Cellphone



# *Spear Phishing Defense*

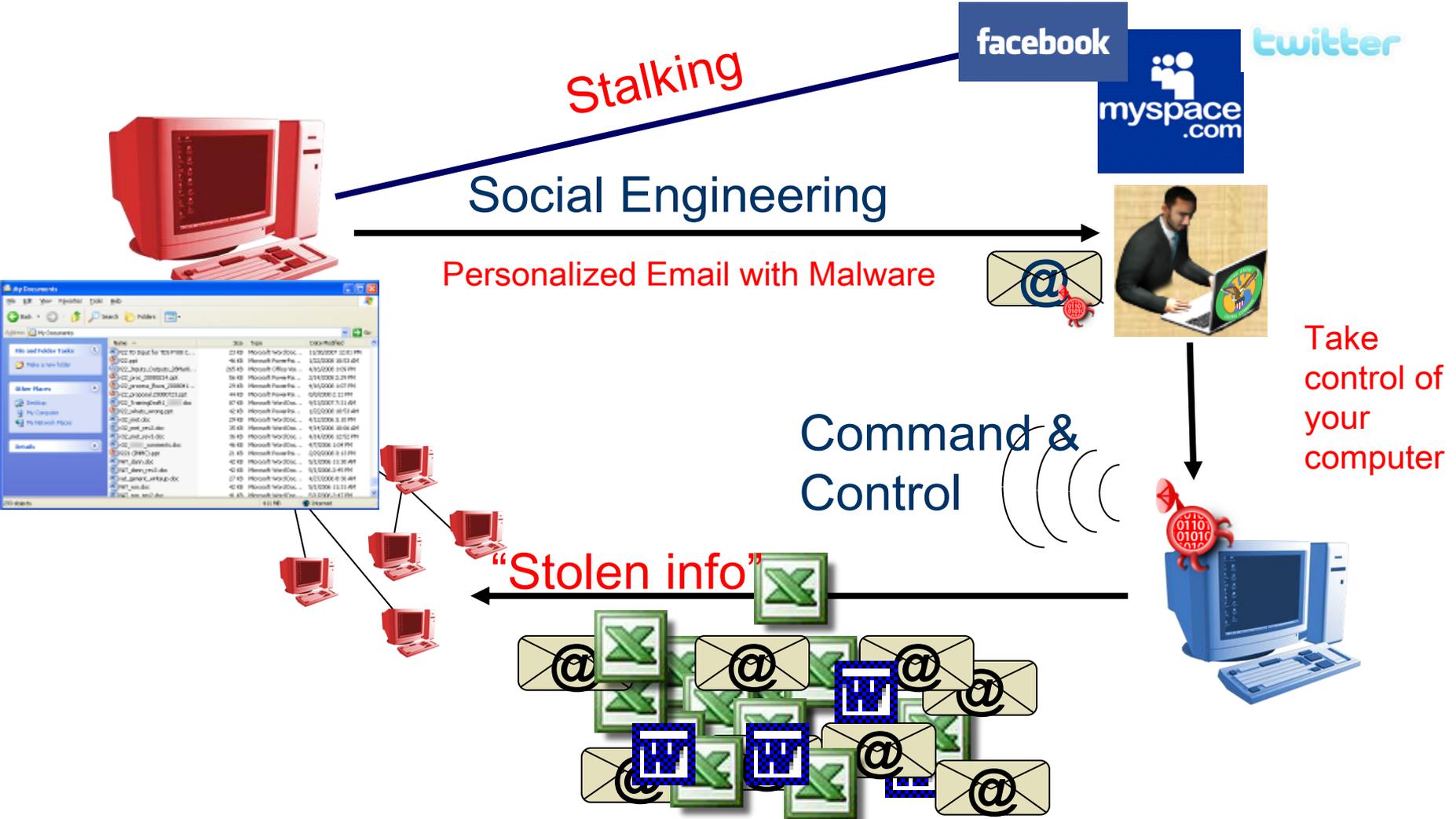
## Four tips to make sure you don't take the bait:

- ✓ **Be suspicious of email asking for confidential or financial information**
- ✓ **Don't be pressured into revealing information. Phishers often use scare tactics to pressure you into submitting confidential or personal data**
- ✓ **Even emails that appear to come from within your organization may be bogus, so never send sensitive data without confirming the legitimacy of the request**
- ✓ **When in doubt inform your USCENTCOM family member**





# Putting it all together - example



Personalized information (account credentials, emails, photos, etc)



# Protecting Yourself

Understand what information you are putting on the Web for targeting on social network sites





# Family Countermeasures

- Ensure all systems **anti** virus up to date
- Normalize security into **family** battle rhythm
- Google yourself
- Check your credit report
- Teach **teens** things to watch for Online
- Check children and teenagers net posts and photos





## *Hard Target Example*

**Can adversary use the internet to get targeting information?**

- **Military occupation info?**
- **Family?**
- **Where do they live?**
- **Where do the kids go to school?**
- **What's their routine?**





Washington DC: 5/26 7:03:44 AM    Dakar: 5/26 11:03:44 AM    London: 5/26 12:03:44 PM    Stuttgart: 5/26 1:03:44 PM    Baku: 5/26 4:03:44 PM    Vladivostok: 5/26 10:03:44 PM

- Home
  - Command Group
  - Command Staff
  - EUCOM A-Z
  - European Command
    - About USEUCOM
    - History
    - Mission
    - Posture
  - Exercises
  - Media Gallery
    - Photos
    - Video
  - Newcomers
  - News
    - Releases
    - Resources
  - Operations
  - Transcripts
  - Transformation
- 
- U.S. Forces, Europe
    - Army
    - Navy
    - Marine Corps
    - Air Force
    - Special Operations
- 
- NATO
    - SHAPE
- 
- Georgian Sustainment and Stability Operations Program
- 
- USEUCOM Portal

**Top Stories**

**Military planners discuss war on terror to wrap up conference**  
Release Date: 26 May 2005  
*By John Banusiewicz*  
*American Forces Press Service*

BUCHAREST, Romania — Military planners from more than 70 nations discussed the war on terror here May 25 to wrap up a two-day conference. Multilateral Planners Conference III kicked off May 24 with briefings and discussions of operations in Iraq and Afghanistan. In today's sessions, conferees...  
[\(Full Story\)](#)



Photo, read caption below

**U.S. Soldiers help Bosnia and Herzegovina Soldiers prepare for mission in Iraq**



Release Date: 25 May 2005  
*By Army Sgt. 1st Class Derrick Witherspoon*  
*7th Army Reserve Command Public Affairs Office*

MIHAIL KOGALNICEANU AIRFIELD, Romania — U.S. Air Force Airman 1st Class Ian Hoagland, right, talks with Romanian Air Force Pvt. Ciprian Bistieru about setting up a laser module that will be used for high-speed voice and data transmission here May 13. During exercise Combined Endeavor 2005, Airmen with the 1st Combat Communications Squadron from Ramstein Air Base, Germany, prepared communication equipment to test the interoperability of command, control, communications and computer systems among 1,200 servicemembers and civilians from more than 43 countries. The Airmen successfully completed more than 1,400 tests. (U.S. Air Force photo by Master Sgt. John Lasky)



**Headlines**

**Welcome**

# USS Carney big success in Black Sea engagements

Release Date: 19 May 2005

## USS Carney Public Affairs

USS CARNEY, Mediterranean Sea — Sailors from the guided-missile destroyer USS Carney (DDG 64) did their part to advance regional maritime security by completing a series of Black Sea engagement evolutions May 11.



Official U.S. Navy file photo of USS Carney (DDG 64).

The engagements included port visits to Turkey and Ukraine, as well as training exercises with both countries' navies. All of the events supported the U.S. European Command's multifaceted, long-term theater security cooperation strategy, designed to enhance interoperability with countries throughout the region.

"The crew of USS Carney performed magnificently in a wide variety of tasks in the Black Sea," said Navy Cmdr [redacted] commanding officer. "From serving as ambassadors ashore in Turkey and Ukraine, to proudly demonstrating the U.S. Navy's professionalism at sea, these Sailors made a real difference in the Black Sea region."

Carney participated in the Turkish Marmaris International Maritime Festival and then proceeded to Sevastopol, Ukraine, to take part in celebrations marking the 60th anniversary of V-E Day. Both port visits included hosting Sailors from the respective navies aboard for training opportunities.

Carney wrapped up the Black Sea engagements by conducting exercises at sea with the Turkish navy, focusing on communications, navigation and seamanship — all leading to increased familiarity and interoperability between the navies.

The U.S. Navy conducts security cooperation efforts throughout the region, including the Gulf of Guinea, North Africa, Mediterranean Sea, Black Sea and North Atlantic.

"Theater security cooperation efforts are key to developing strategic regional partnerships that aid in the development of a comprehensive maritime theater picture," said Navy Vice Adm. Harry Ulrich, 6th Fleet's commander. "Regional security lies in mutual cooperation and

messenger [Go] [Links]

.S. Air with setting up voice base combat se, test the ions lbers rmen U.S. Air

the Commander, **nes L. Jones**, the United States mmand.

a unified mmand whose maintain ready duct the full military operations in concert with partners; to isatlantic security port to NATO; to onal stability; and i. interests in ca, and the Middle

M area of ity (AOR) covers million square ludes 91 countries s. Several other d territories are o be part of interest (AOI).



Pop-up blocked. To see this pop-up or additional options click here...

Submit Advanced

## Military

- Introduction
- Systems
- Facilities
- Agencies
- Industry
- Operations
- Countries
- Hot Documents
- News
- Reports
- Policy
- Budget
- Congress
- Links

## WMD

## Intelligence

## Homeland Security

## Space

## Public Eye

**VONAGE**  
The Broadband Phone Company



## DDG 64 Carney



The USS CARNEY (DDG-64) is the Navy's fourteenth Arleigh Burke Class Destroyer. Built at the Bath Iron Works in Bath, ME, she was launched to a clap of thunder and a flash of lightning. The ship was named after Admiral Robert B. Carney. The Carney was commissioned in Mayport, FL, where she is now homeported.

A newly developed ceramic membrane oil/water separator effluent polisher was installed aboard USS Carney (DDG 64) in April 1996. After seven months of successful operation, the unit was replaced with an upgraded version in November 1996. The polisher continues to operate and provide Carney with a bilgewater handling system

that complies with current discharge regulations and is anticipated to meet future global regulations well into the 21st Century.

The ceramic membrane polisher is designed to remove and concentrate emulsified oils and suspended materials from the effluent of the ship's gravity oil/water separator leaving a clean water stream which can be discharged overboard. Within the polisher, three membranes connected in series are powered by a 10 hp centrifugal pump to create a recirculation loop. Bilgewater is recirculated through each membrane at a sufficiently high velocity to reduce the amount of fouling that occurs on the membrane surface. As contaminants are concentrated within the membrane loop, clean water is forced through the walls of the porous ceramic membrane. Automatic releases of concentrate to an existing storage tank are used to control the concentration of oil and particulates that build up within the membrane loop. The unit is set up to create a hydraulic volume reduction of 100 to 1; that is, for every 100 gallons of oil/water separator effluent, the unit creates one gallon of concentrated waste and 99 gallons of clean water. The polisher is designed to match the flow rate of the 10 gal/min Navy oil pollution abatement 10NP oil/water separator. It uses a programmable logic controller to accomplish this task and to monitor critical process parameters, including loop pressure and temperature, processing flow rate, and effluent pressure. The polisher aboard USS Carney has produced an average effluent concentration of less than 5 mg/L oil.

Dark blue and gold, of the shield on the Coat of Arms, are the colors traditionally associated with the Navy and recall the sea and excellence. The gold cross suggests the Navy Cross, one of the

[Arleigh Burke Class](#)

## Tactical Assignments

- [George Washington Battle Group](#) [1998]
- [John F. Kennedy Battle Group](#) [2002]

## Operations

- [Southern Watch](#)
- [Enduring Freedom](#)

## Homeport

- [Mayport, FL](#)

## Official Homepage

- [DDG 64 Carney](#)

ARE YOU **HOT?**



COMMANDER [REDACTED]

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address http://www.zabasearch.com/query1\_zaba.php?sname=KRISTI+A+CHIARAVALLOTTI&state=all&ref=zaba&se=O&name\_style=1

All States

Purchase a Background Check today to be guaranteed unlimited access to ZabaSearch people search throughout 200

- 3 FREE RECORDS!

Click Name to Search Web	Born	Click Address for Satellite Photo	Telephone	Background Check	Search ZabaSearch
<input type="text"/>	Jul 1963	<a href="#">2147 CHALCEDONY ST SAN DIEGO CA</a>	<input type="text"/> 6755	<a href="#">Background Check</a>	<a href="#">ZabaSearch KRISTI A</a>
<input type="text"/>	Jul 1963	<input type="text"/> JACKSONVILLE FL	<input type="text"/> 3509	<a href="#">Background Check</a>	<a href="#">ZabaSearch KRISTI A</a>
<input type="text"/>	1963	<a href="#">SPRING MD</a>		<a href="#">Background Check</a>	<a href="#">ZabaSearch KRISTI A</a>

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address <http://www.mapquest.com/maps/map.adp>

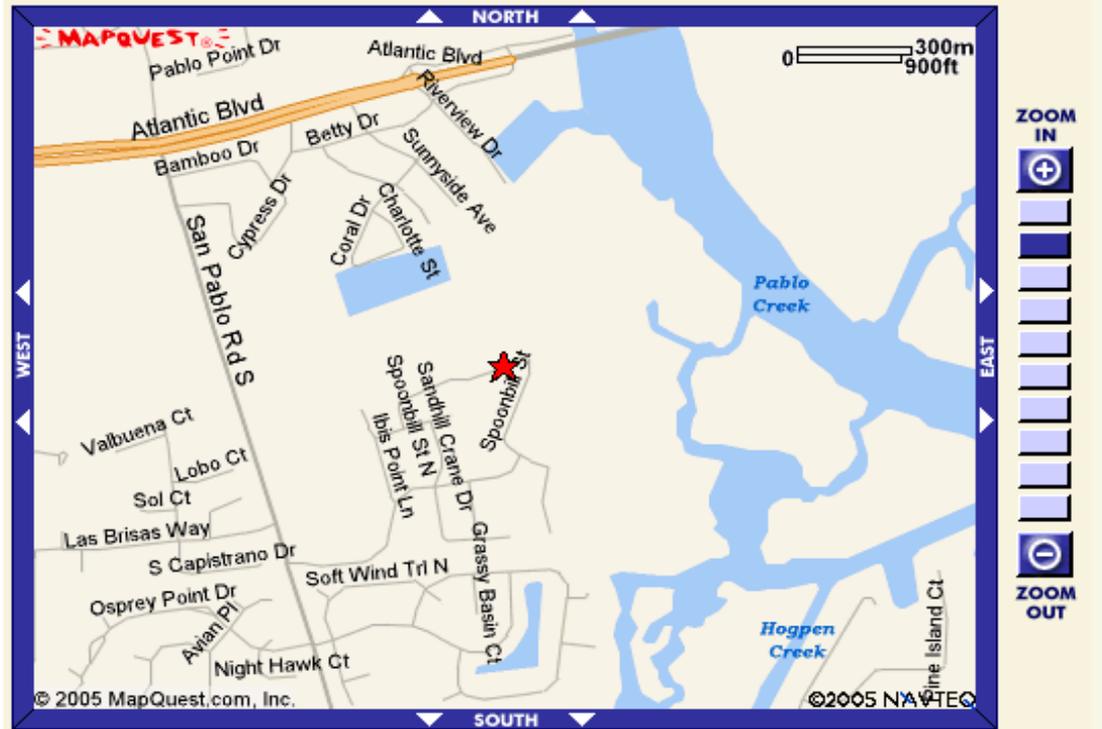
Maps [Print](#) [E-Mail](#) [Send to Phone](#) [PDR](#) [Reverse](#) [New Map](#) [Directions To](#) or [Directions From](#)

★ 13936 Spoonbill St N Jacksonville, FL 32224-1387, US - [Jacksonville Hotel Offers](#) - [Jacksonville Real Estate](#)

**Search Jacksonville, FL:**

MapQuest Search

**Find Nearby:** (e.g., Theaters)  or **Top Categories**



- Jacksonville Offers:**
- [Jacksonville Hotels](#)
  - [Jacksonville Flights](#)
  - [Florida Vacations](#)
  - [Jacksonville Schools](#)
  - [Florida Summer Camps](#)
  - [Jacksonville Insurance](#)
  - [Jobs in Jacksonville](#)
  - [Apartments in Jacksonville](#)
  - [Jacksonville New Cars](#)
  - [Florida Real Estate](#)
  - [Jacksonville Dining](#)
  - [Jacksonville Homes](#)

Get Directions To  Above Location

Search Jacksonville For

**Starting Address**

- [Airports](#)
- [Hotels](#)
- [Restaurants](#)
- [Post Offices](#)



# Home Reconnaissance

Google

Get directions My places

Map Traffic

Directions Search nearby Save to map more

Maps Labs - Help

Google Maps - ©2013 Google - Terms of Use - Privacy

200 ft 50 m

©2013 Google

Edit in Google Map Maker Report a problem



# County School Records

## PUBLIC SCHOOLS

## DCPS at a Glance

School Board  
Administration  
DCPS at a Glance  
Schools & Info  
Academic Excellence  
Community Involvement  
Parents  
Students  
Employees  
Employment Opportunities  
Media

### HOW TO ENROLL

Registration for kindergarten and first-grade students occurs during the months of May and August at any Duval County public elementary school.

Under Florida Law:

- A child must have successfully completed kindergarten in order to be eligible for first grade.
- Children may enter kindergarten if they will be five years old on or before September 1<sup>st</sup>.
- Children may enter first grade if they will be six years old on or before September 1<sup>st</sup>, and have successfully completed kindergarten.
- All children who will be six years old by February 1<sup>st</sup> must attend school.
- All children must attend school until they reach the age of 16.

This is Florida law and there are no exceptions.

### How do you register your child in Duval County Public Schools?

1. **Find out which school your child(ren) will attend.**

If you don't know where your child will attend school, call Pupil Assignment at [390-2144](tel:390-2144). They will tell you where your child(ren) will attend school based upon your home address.

2. **Visit the school your child(ren) will attend to register during school hours.**

You can check the school listing on our website for individual school hours. **Click here to go to the school listings.** After the last day of school, please call ahead before going to the school to verify school hours. **To find the last day of school, click here to see the District calendar.**

3. **Bring the following information with you:**

- Results of a Florida physical (school-entry health exam) performed within one year of the date of



# School Reconnaissance

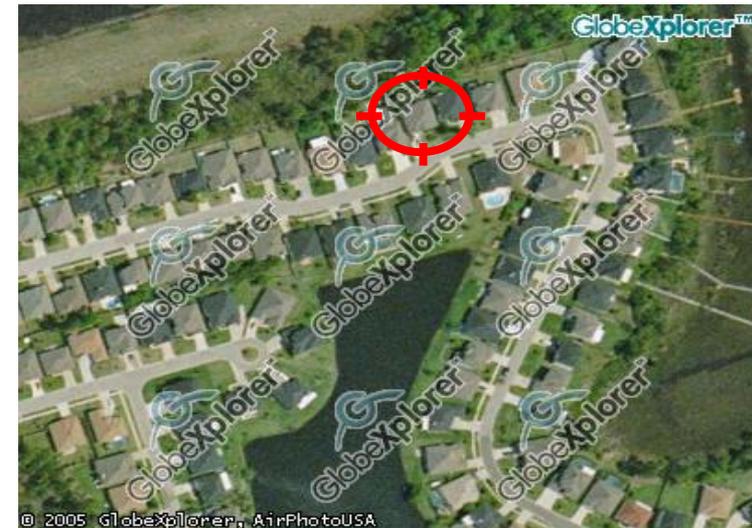
A screenshot of the Google Maps interface. The search bar at the top contains "Jacksonville, FL 32246". Below the search bar, there are buttons for "Get directions", "My places", and a print icon. A small thumbnail image shows a street view of a residential area. The main map area displays a street view of a yellow school bus parked on a street. A red target symbol is overlaid on the bus. The bus has "STOP" written on its side and "STUDENT TRANSPORTATION" on the back. The map interface includes a compass, a zoom in (+) and zoom out (-) button, and a small inset map in the bottom right corner showing the current location. The footer of the map shows "© 2013 Google" and "Image Date: April 2011".



# *Understand Vulnerabilities*

Adversaries can easily get targeting information

- ✓ Professional/work information
- ✓ Detailed family information
- ✓ Home address
- ✓ Schedule/routine
- ✓ Children school information





# *What can you do to protect your family?*

Learn and use the online Do's and Don'ts



## Remember Computer Security

**Do not be an easy target for computer crimes**

- **Hacking**
- **Theft**
- **Planted code**

**vs.**

- **Antivirus software**
- **Firewalls**
- **Strong Passwords**
- **Permission Settings**





## *Password Protect your wireless access*

**An adversary can gain access to your computer and sensitive internet files through your router. As well as install and run spyware and viruses that will be downloaded on all your wireless devices.**





# “Do’s”

## Watch Your Friends

**You didn’t post sensitive pictures of you and your kids, but your brother, wife, mother, or friend did.**



flickr - vles

**Verify Supposed “Real” Friends**

**Jimmy Smith from the high school swim team:**

**OR adversary?**



**They can get the data from:**

- **Yearbooks**
- **Other SNS’s**
- **Your posts/profile**



**VERIFY BEFORE ADDING!**



## Modify Your Search Profile

**Search profile: the data about you that is visible when someone is searching for “friends”**

**What might be publicly visible even if your profile isn’t:**

- **Name**
- **Photo**
- **List of networks and groups**
- **List of friends**
- **Age / Sex / Location**





# “Do’s”

## *Consider All the Players*

**Before posting data to an SNS, ask:**

- **Who owns the company?**
- **Who are their partners?**
- **Where are they hosted?**
- **Who has access to the data?**



**Some might be adversaries or affiliated**



## Use Reasonable Suspicion

**Social engineering and “conning” start with becoming a friend.**

**They:**

- Like what you like
- Hate what you hate
- Understand you



**Be especially cautious about dating sites**

***Verify all friend request***

## Social engineering and “conning” starts with a friend request



Adversaries can get the data from:

- Free people search engines
- Other SNS's
- Your posts/profile
- Your friends posts/profile

## Verify Requests Before Approving!



## Utilize all available privacy settings

Customize available settings to be as secure as possible

- “Everyone” may be accessed by anyone with access to the internet
- How many security settings are available on Facebook?

**Over 120**





# “Do’s”

## *Watch your friends settings*

**Sure your profile is secure, but what about your 115 friends profile settings?**

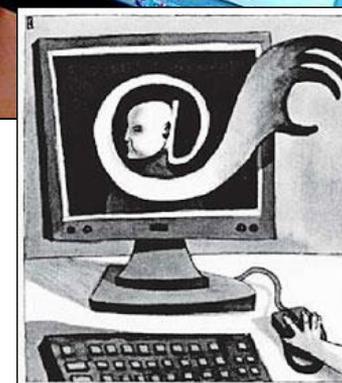


flickr - alexander...



## *Closely Monitor Your Children’s Use of the Internet*

- **Cyber-bullying**
- **Kidnapping**
- **“Sexting”**
- **Stalking**
- **Pedophiles**
  - **500,000+ registered sex Offenders in the USA**
  - **95,000 registered sex offenders profiles on Myspace**





# “Do’s”

*Verify links and files before executing*

**Would you follow a link in e-mail? Would you download and run an attachment? Then why do you do these things on SNS’s?**

- **Phishing scams**
- **Malicious coding**
- **Viruses**
- **Ransomware**

**Verify before executing!**





# Ransomware

- A type of malware restricting access to the computer system or smartphone that it infects
- Demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed
- Some forms **encrypt files** on the system's hard drive and destroy data files, photos if ransom not paid

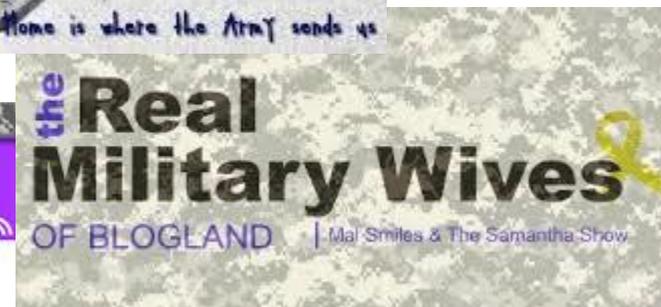
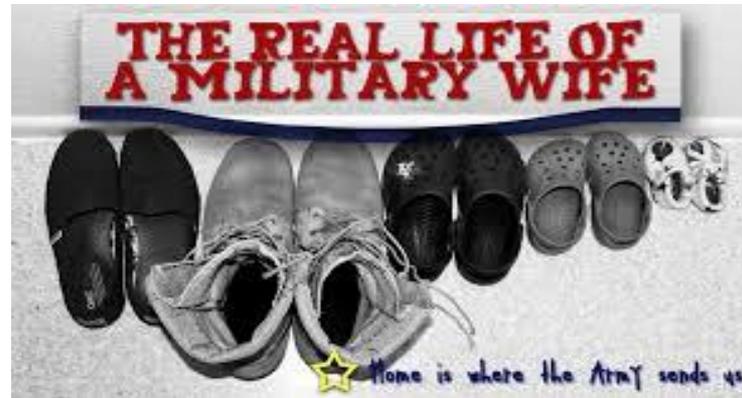




# “Do’s”

*use BLOGs with caution*

- Avoid details, don’t get personal
- Who is reading your blog?
- Lessons learned 101 for the adversary





## *Understand the risks associated with Geotagging*

- Location/GPS data attached to photos
- Feature in Smartphones and digital cameras
  - Lat/Long
  - Device details
- “Check-in” feature
  - Facebook Places
  - Google Latitude
  - Foursquare
  - Gowalla





## *Be an informed User of Social Media*

- **How much personal information do you broadcast?**
- **Are you very careful about what details you post?**
- **Do you understand data aggregation issues?**
- **Are you willing to find and learn all the security settings and keep up with them as they change?**



Are you willing to accept the risk?



# “Do’s”

Assume the Internet is **FOREVER**

- There is no true delete on the Internet
- WWW means World Wide Web
- Every Picture
- Every Post
- Every Detail





# “Don’t”

## Discuss work Info or Media

- Assume the adversary will find and read comments and view photos and video
- Search engines make it easy. Poor security makes it possible.



Marines shared a link.  
7 hours ago

You voted, and this week's Top Corps Shot comes from Cpl. Alfred Lopez. Lopez was patrolling with 1st Light Armored Reconnaissance Battalion and 3rd Battalion, 3rd Marine Regiment. This was Lopez's first patrol through the canals, and the difficulty of traversing the terrain stood out to him. In fact, on the next patrol, he slipped and went under water, breaking his camera in the process. "I wanted to be able to share that experience with everyone who reads my stories," said Lopez. "It shows the viewer what kind of terrain and what kind of conditions these war fighters have to live through."



**Blood Is Thicker Than Water**  
[www.flickr.com](http://www.flickr.com)

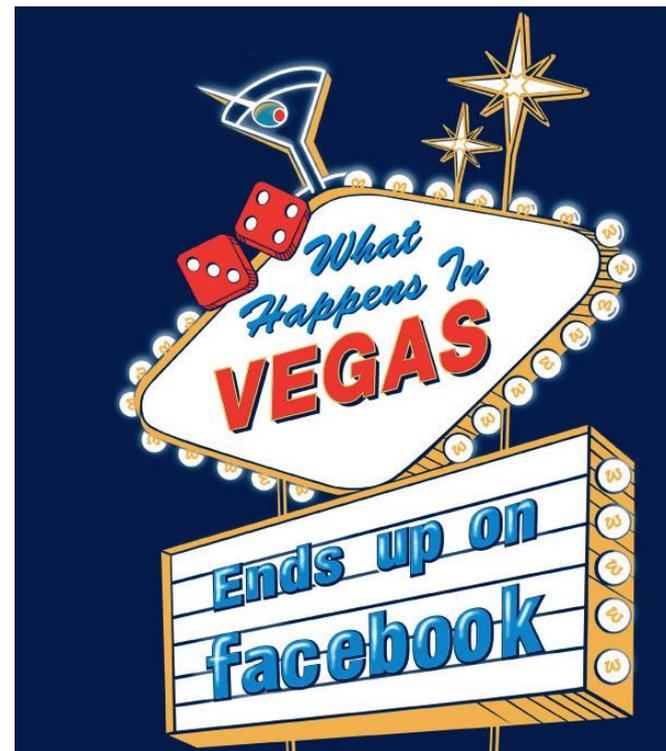
Lance Cpl. Brandon Mann, a dog handler with Alpha Company, 1st Light Armored Reconnaissance Battalion, and native of Arlington, Texas.



# “Don’t”

*Discuss sensitive details*

- Never post anything you would not tell directly to the enemy
- Never post private or personal information- no matter how secure you think your settings are
- Assume the information you share will be made public



Details make you vulnerable



# “Don’t”

## *Post Personal Information*

**Real friends already know your home address, phone number, etc. Don’t broadcast that to strangers.**



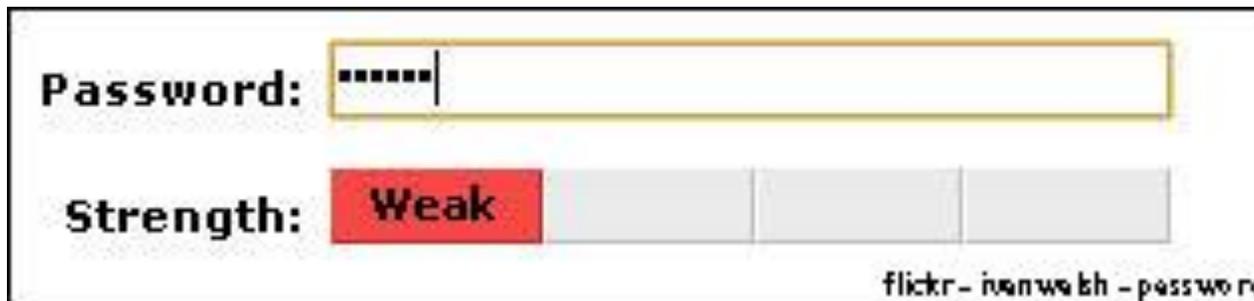


# “Don’t”

## Use the Same Passwords

To use only one password for everything is to hand your life to the first bad guy that works at any web service you register with

Password1 is not a strong password



flickr - ianwebb - password



# “Don’t”

## Give Away Passwords

Then Schmidt came to a page saying that "we'll find your friends and family who are already members and also automatically invite any nonmembers to join (it's free!)." **It instructed her to enter the password for her Yahoo e-mail account.**

"I thought I was just signing up to read my friend's message," Schmidt said. "At no time did I think I was authorizing them to access my online address book."

*David Lazerus  
Los Angeles Times  
April 16, 2012*





## Grant the same access to everyone

- Don’t treat all friends equally
- Control and customize individual access
- Do create groups
  - Reading clubs
  - Family
- Set permissions for everything
  - Your status
  - Photos
  - Postings

**About me**  
About Me refers to the About Me description in your profile

**Personal Info**  
Interests, Activities, Favorites

**Birthday**  
Birth date and Year

**Religious and Political Views**

**Family and Relationship**  
Family Members, Relationship Status, In

**Education and Work**  
Schools, Colleges and Workplaces

**Photos and Videos of Me**  
Photos and Videos you've been tagged i

**Photo Albums**

**Posts by Me**  
Default setting for Status Updates, Links

Only Friends ▼

Only Friends ▼

Only Friends ▼

Only Friends ▼

Only Me ▼

Only Friends ▼

Edit Settings

Only Friends ▼



# “Don’t”

## *Use Unsecured Logon at Public Hotspots*

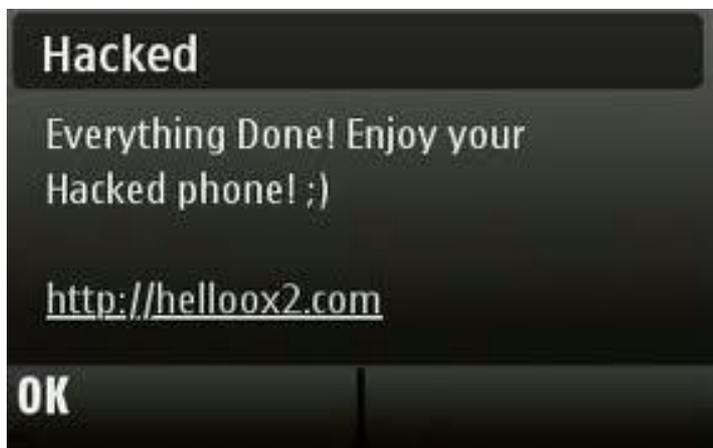
Most SNSs do **NOT** have a secure login capability.  
Remember that when using them





## Trust Add-On’s or Applications

- Plugins, Games, Applications
  - Third Party Software
  - Host privacy settings do not apply
  - Applications designed to collect data
  - Malicious code





## *Depend on social media security settings*

But it’s set to private ... right?

- Hackers
- Incorrect or incomplete settings
- Sale of data
- Upgrades/site changes
- “Risks inherent in sharing information”
- “USE AT YOUR OWN RISK. We do not guarantee that only authorized persons will view your information.”





## *Summary*

- **The Cyber threat to individual and your family is prevalent and ongoing**
- **Adversaries and criminals are becoming highly adaptive**
- **Be suspicious of email asking for confidential or financial information**
- **Mitigate family vulnerabilities with phones and social Media**
- **Use common sense!**