



**The CENTCOM Family Readiness Program is pleased to sponsor**

## ***Family Cyber Security and Social Media Awareness Briefing***

***Presented by the CENTCOM Cyber Security Division and CENTCOM Information Operations Division***

***The briefing is open to ALL CENTCOM members and their families***

Cyber threats are real and constant; any CENTCOM teammate or family member could be targeted. This is why we all should maintain a heightened sense of vigilance whether dealing with work or home computer usage, specifically as it relates to Social Media. Our team of experts will be on hand to provide answers to your questions pertaining to Cyber Awareness and Security.

**CENTCOM Welcome Guide: <https://www6.centcom.mil/welcomeguide>**

\*Use of these Family Cyber Security Awareness Brief images and source locations does not reflect official endorsement. Reproduction for private use or gain is subject to original copyright restrictions.



# ***Family Cyber Security Awareness Brief***

***UNCLASSIFIED***

***June 21, 2016***

**CCJ6-CC**

\*Use of these Family Cyber Security Awareness Brief images and source locations does not reflect official endorsement.  
Reproduction for private use or gain is subject to original copyright restrictions.



UNCLASSIFIED

# Cyber Awareness



**Due to the growth of internet enabled devices and online social media, Cybersecurity must become an integral part of daily routine.**

**The 1<sup>st</sup> step to protecting yourself is knowing the risks you take online and how to navigate it with caution.**

UNCLASSIFIED



UNCLASSIFIED

# Interchangeable Technology



1

## Home Computers and Smart Phones

UNCLASSIFIED



UNCLASSIFIED

# Smart Phone – Smart Home – Smart Life



2

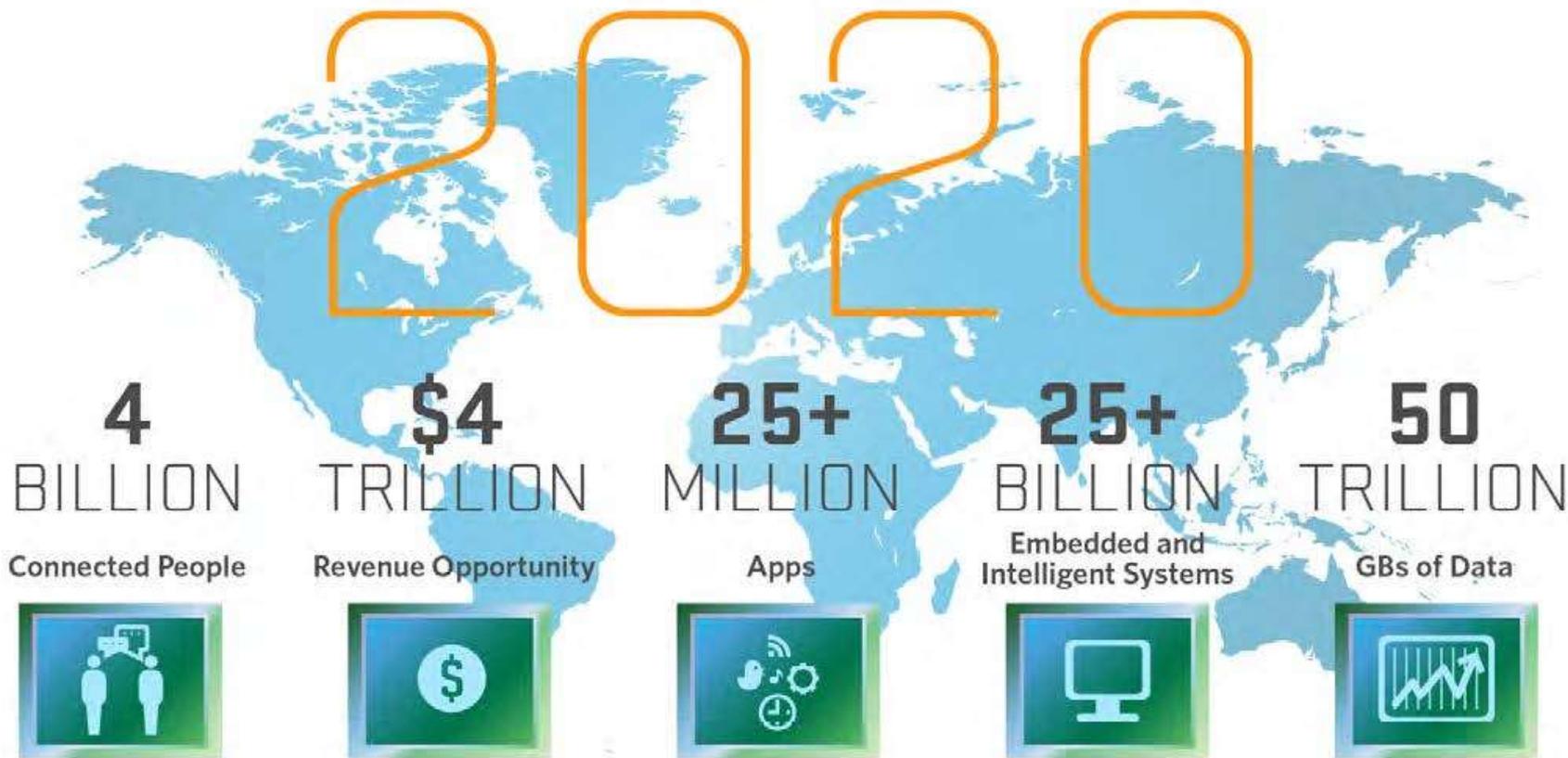
UNCLASSIFIED

5



UNCLASSIFIED

# “Internet of Things”



Source: Mario Morales, IDC

UNCLASSIFIED

# Internet Security Concerns



90%

of devices collect at least one piece of personal information about you

80%

of devices do not require passwords of a sufficient complexity and length

70%

of devices allow an attacker to discover user account through account enumeration

70%

of devices expose your personal data over unencrypted channels

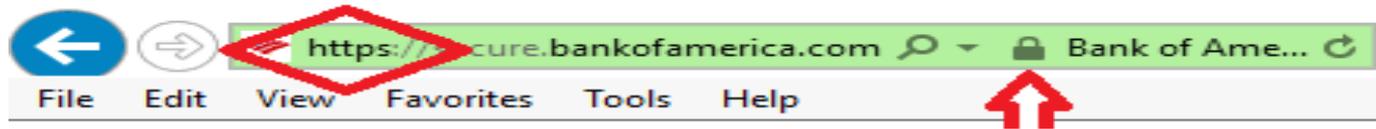
60%

of devices with user interfaces are vulnerable persistent cross site scripting and weak credentials



# Protect Your *Digital Self*

- **Online Accounts (Email, Banking, Shopping, etc.)**
  - Use different passwords for different accounts
  - Reminder: Some forms of web browsing are more secure than others; use 'HTTPS' when available and ensure your financial institutions encrypt



LOOK FOR THE CLOSED LOCK

- **Identity Theft**
  - If you regularly shop online be sure to use a real credit card and not a debit card; using the “BANKS” money where you are protected from fraudulent charges is better than exposing your own bank accounts
  - Never store credit card information on a web site



# Email Safety

# READ METHOD

1

Att: Dear Friend Spam x

**MR PETER BEN** <maria@nandos.com>  
to

**Be** from: **MR PETER BEN** <maria@nandos.com>  
reply-to: absabnk@sina.cn

De to:  
I a date: Wed, May 18, 2016  
ha ha  
ch ch  
be be  
My encryption: Standard (TLS) [Learn more](#)

I know this mail might meet you in utmo

Before his death he left the sum of 22M included any next of Kin on this Account

Therefore i require your partnership to stand as his next of KIN, please do not let this pass you bye .No risk is being taken ,this happens in the banking industry everyday, am completely incharge and have everything all worked out.

If you agree, please get back to me to enable me furnish you with more details as to the way forward on how this life changing opportunity can be achieved, I will also want you to provide me with the below information to enable us enter into the official stage of this transaction and to enable me prepare all legal paper works in your name with a view of moving the funds out of South Africa in your name .

COMPLETE FULL NAMES:  
CURRENT MAILING:  
RESIDENTIAL ADDRESS:  
DIRECT TELEPHONE NUMBER:  
FAX NUMBER :

Att: Dear Friend Spam x

**MR PETER BEN** <maria@nandos.com>  
to

**Be** from: **MR PETER BEN** <maria@nandos.com>  
reply-to: absabnk@sina.cn

De to:  
I a date: Wed, May 18, 2016 at 6:25 PM  
ha ha  
ch ch  
be be  
My encryption: Standard (TLS) [Learn more](#)

the only way presently at my disposal to communicate with you until we can n and read this mail comprehensively and you will know that this is a sincere life Africa, untill his death he was the CEO of the Porsche tuning company that

capable / reliable to champion this business opportunity.

, and all attempt to communicate with his Family was to no avail, and he never



UNCLASSIFIED

# Computer & Cell Phones



## Computer

- Create a basic account for each user
- Manage the local administrator role and functions separately



## Cell Phone

- A locked (password-protected) cell phone is a happy cell phone
- Emergency calls can still be made in most cases

2/3

UNCLASSIFIED



UNCLASSIFIED

# Anti-Virus for Your Devices

The screenshot shows the DISA MIL website. The header includes the DISA logo and the text "DEFENSE INFORMATION SYSTEMS AGENCY The IT Combat Support Agency". A search bar is located in the top right. The navigation menu includes: About, Computing, Cybersecurity, Enterprise Services, Network Services, Mission Support, and Initiatives. The breadcrumb trail is: Cybersecurity > Network Defense > Anti-Virus/Anti-Spyware Solutions > Home Use. The main content area features a large blue banner with the "AV ANTIVIRUS" logo and the text "HOME USE". Below the banner, the text reads: "Active duty military and civilian employees are encouraged to take part in the AV/AS Home Use program. Contractors are excluded from using the software at home or on any other system not belonging to the DOD. Information regarding the program is available here:". A purple button labeled "AV Portal" is visible in the left sidebar. The page number "4" is in the bottom right corner.

1

2

UNCLASSIFIED



# Data Backup



1



2

**Your computer has been locked!**

Your computer has been locked due to suspicion of illegal content downloading and distribution. Suspicious digital content (418 MB of video files) was automatically classified as child pornographic material. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2257 - Sexual Exploitation of Children (Production of child pornography)  
 18 U.S.C. § 2252 - Certain activities relating to material involving the sexual exploitation of minors (Production, distribution and receipt of child pornography)  
 18 U.S.C. § 2252a - Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

**Technical details:**  
 Involved IP address: [REDACTED]  
 Involved host name: [REDACTED]  
 Source or intermediary sites: <http://pwnedbox.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unlock your account in an unauthorized way.

Your case can be classified as occasional/unintentional, according to the 17 (f) 3, Code(1) § 342. Thus it may be closed without prosecution. Your computer will be unlocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$200.

Pyromaster lock on 05/01/2013 5:20 p.m. EST

**HOW TO UNLOCK YOUR COMPUTER:**

- Take your cash to one of the retail locations
- Get a MoneyPak and purchase it with cash at the register
- Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

1 2 3  
 4 5 6  
 7 8 9  
 Delete 0 Enter

4



3



# Ransomware



- A type of malware that prevents you from using your computer until you pay a certain amount of money
- It's extortion; putting all the data on your computer at risk until you pay

- NEVER pay the ransom, no matter how small it is
- You won't be dealing with "ethical hackers"
- The attacker(s) will only continue to siphon money from you

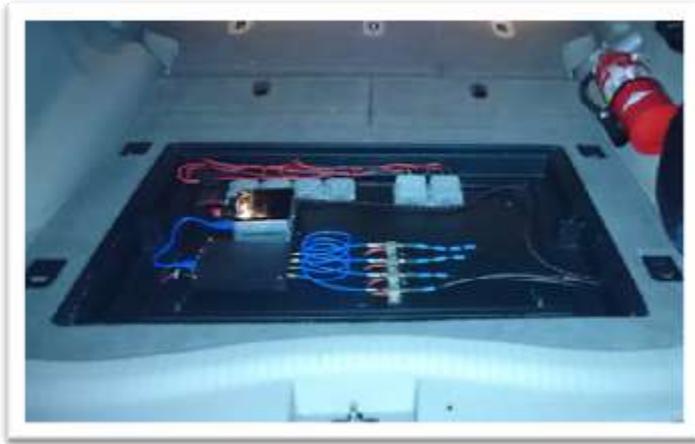


**Protect yourself through routine backups and good computer security habits**



UNCLASSIFIED

# WIFI – Safe and Secure



1



2



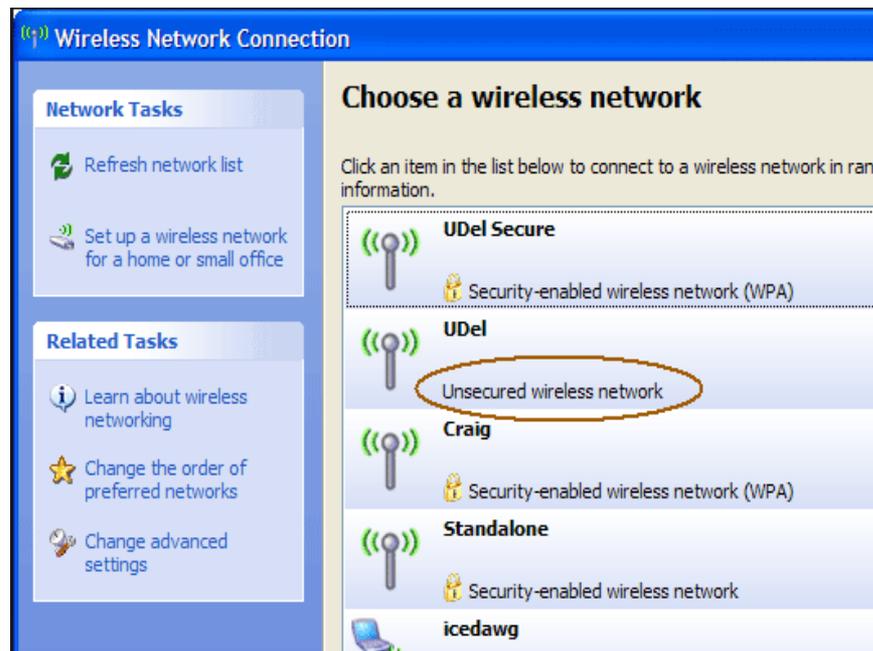
3

UNCLASSIFIED



# WiFi Safety

- Understand how to identify the network you're using
- Limit access to your Personal Wireless Network(s)
  - Use encryption
  - Don't broadcast your SSID
  - Secure your router (change router ID and password)
- Sometimes it's necessary to use public "free" access to the internet (airports, emergencies)
  - Make sure you are using the official network (ASK at an information desk)
  - Assume anything done on free networks are exposed (NO BANK APP!)
  - Mark the Wi-Fi connection as a public network



**Remember "Free WiFi" means "Security Free"**





UNCLASSIFIED

# Social Engineering Attacks

- **Impersonation – The act of pretending to be somebody else**
  - Attacker impersonates someone of authority, causing the victim to feel as if he/she must comply
  - Attacker impersonates someone who requires help (e.g., end user who requires assistance from a network administrator)
- **Phishing – Attacker casts out a broad net of emails that appear to be from a trusted source**
  - E.g., a well know bank or Google requesting users to click on a hyperlink
  - The hyperlink then connects to a malicious website and when the user inputs his/her login and password, which the attacker then steals
  - Usually employs authority and need for urgency to get the victim to respond
- **Typically Targets**
  - Financials
  - Personal Computer Access
  - Social Security Number



**Don't trust random communications  
or requests for information**

UNCLASSIFIED



# Social Engineering Take Aways

- **Working at United States Central Command (USCENTCOM) makes your family a target**
  - Don't advertise where your family members work
  - Don't use commercial email for work related communication
  - Don't post work schedules, contact or recall information, or base maps
  - Don't put USCENTCOM "identifiable" photos on social media sites
  - **Report suspicious communication related to USCENTCOM to the USCENTCOM Help Desk at 529-HELP**
- **Personal Safety – If you think you're a victim:**
  - **Contact companies, including banks, where you have accounts**
    - Inform the companies someone may be using your identity and find out if there are any unauthorized transactions
    - Close accounts so that future charges are denied. In addition to calling the company, send a letter so there is a record of the problem.
  - **Contact the main credit reporting companies (Equifax, Experian, TransUnion)**
    - Check your credit report to see if there has been unexpected or unauthorized activity
    - Have a fraud alerts placed on your credit reports to prevent new accounts being opened without verification
  - **File a report**
    - File a report with the local police so there is an official record of the incident
    - You can also file a complaint with the Federal Trade Commission.
  - **Consider other information that may be at risk**



# Takeaway - Best Practices

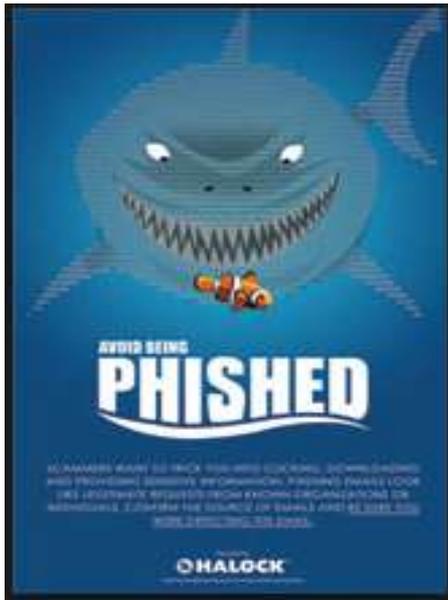
- **Personal accounts & devices (Google, Banking, Facebook, etc.)**
  - Use different passwords for different accounts (i.e. banking, email, etc.)
  - Avoid “Geotagging” photos you post online
  - Password protect your computers, smart phones and tablets
  - Check security before exposing credit card info... “Look for the lock”
  - Regularly update ALL of your computers software security
  - Never store credit card information online
- **Home Computer & Internet**
  - Install and update your anti-virus and anti malware software
  - MacOS is not immune to malware or a virus. Install appropriate software.
  - DISA provided software: <http://www.disa.mil/cybersecurity/network-defense/antivirus/home-use>
  - READ your Emails: Relevant – Expected – Addressed Properly – DOES IT MAKE SENSE
  - Back up your files now and often to protect yourself from ransomware and data loss



# Takeaway - Best Practices

- **WIFI (Home and Public)**

- “Free Internet” means “Security Free”-- assume anything done freely is free to everyone
- Use your Cellular data plan to create a “wifi hot spot” if possible (making your own Trusted Internet Connection)
- Always verify you are using the “official” network, even if it means asking
- Avoid using public networks for things like banking or shopping



**Being “Security Aware” is more important than ever.**

**The more knowledge and information you have the better you can protect *yourself* and *your family*.**



UNCLASSIFIED

# Cyber Security Aware



## Questions?

UNCLASSIFIED



Search OnGuardOnline.gov 🔍 **Español** 🗣️

## OnGuardOnline.gov

STOP | THINK | CONNECT™

[Avoid Scams](#) | [Secure Your Computer](#) | [Protect Kids Online](#) | [Be Smart Online](#) | [Video and Media](#) | [Onguard Online Blog](#)

---

**Blog**

### Official-sounding calls about an email hack

April 6, 2016  
by Andrew Johnson  
Division of Consumer and Business Education, FTC

There's a new twist on tech-support scams — you know, the one where crooks try to get access to your computer or sensitive information by offering to "fix" a computer problem that doesn't actually exist. Lately, we've heard reports that people... [Read More](#)

**Just for You...**

- ▶ Educators
- ▶ Parents
- ▶ Techies
- ▶ Small Business
- ▶ Military
- ▶ Kids



---

**Avoid Scams**



- ▶ Hacked Email
- ▶ Tech Support Scams

[View more articles](#)

**Protect Kids Online**



- ▶ Kids, Parents, and Video Games
- ▶ Kids and Mobile Phones

[View more articles](#)

**Stay Connected**

-  [Get Email Updates](#)
-  [Blog Feed](#)
-  [Facebook](#)
-  [YouTube](#)

---

**Be Smart Online**



- ▶ Understanding Mobile Apps
- ▶ Tips for Using Public Wi-Fi Networks

[View more articles](#)

**Secure Your Computer**



- ▶ Securing Your Wireless Network
- ▶ Malware

[View more articles](#)

**Partner of the Day**



Office of Justice Programs

Since 1984, the Office of Justice Programs has provided federal leadership in developing the nation's capacity to prevent and control crime,... [Read more](#)

[Learn about our Partners](#)



# ***USCENTCOM***

## ***OPSEC and Social Network Briefing***

**Mr. Felice Procaccio**  
**CCJ3-IO Security Manager**

\*Use of these Family Cyber Security Awareness Brief images and source locations does not reflect official endorsement.  
Reproduction for private use or gain is subject to original copyright restrictions.



# Agenda

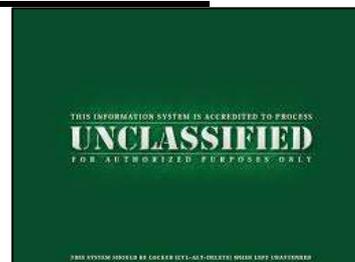
- **Definitions**
- **Social Networking Sites (SNS)**
- **Facebook**
- **Internet and Security**
- **Questions**





# Definitions

- **OPSEC or Operations Security**
  - OPSEC is a methodology that denies critical information to the adversary.
- **Critical Information**
  - Information we must protect to guarantee security and success
  - It is what the adversary needs to breach our security prevent our success
  - This can be classified or unclassified





# Definitions – Critical Information

- **Unclassified Information is critical information when you look at the statistics**
  - 90% of all intelligence collected is unclassified through Open Source Intelligence (OSINT)
  - Small bits of information can be put together to give the big picture.
  - The adversary just needs pieces of information to make a complete picture.
  - Bottom Line:
    - **Unclassified does not mean unimportant.**





# Big Open Source..... Social Networking Sites (SNS)

- **Social Networking Sites (SNS)**

- Allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries over social media
- Social Media is a **NEUTRAL** conduit
- **Factoid:** The safe use of social media is fundamentally a behavioral issue, not a technology issue.

Guidelines for Secure Use of Social Media by Federal Departments and Agencies Federal CIO Council

- Important for you to understand that information you put on Social Media is Open Source, unclassified and can be **CRITICAL** if it falls into the wrong hands

- **What did we say about critical information?**

- Information we must protect to guarantee security and success
- It is what the adversary needs to breach our security prevent our success





# SNS – Were do we Put Our Info??





# SNS – Explained

- **Social Media or SNS Explained**

- Twitter
  - *"I'm eating a donut"*
- Facebook
  - *"I Like donuts"*
- FourSquare
  - *"This is where I eat donuts"*
- Instagram
  - *"Here's a vintage pic of a donut"*
- YouTube
  - *"Watch me eat an entire box of donuts"*
- LinkedIn
  - *"My core strength is my donut eating skill"*
- Pinterest
  - *"Here's my fave donut recipe!"*
- LastFM
  - *"Listening to "Donuts"*
- Google+
  - *"I work for Google and I eat donuts."*
- SharePoint
  - *"I made the donut, now you frost it."*





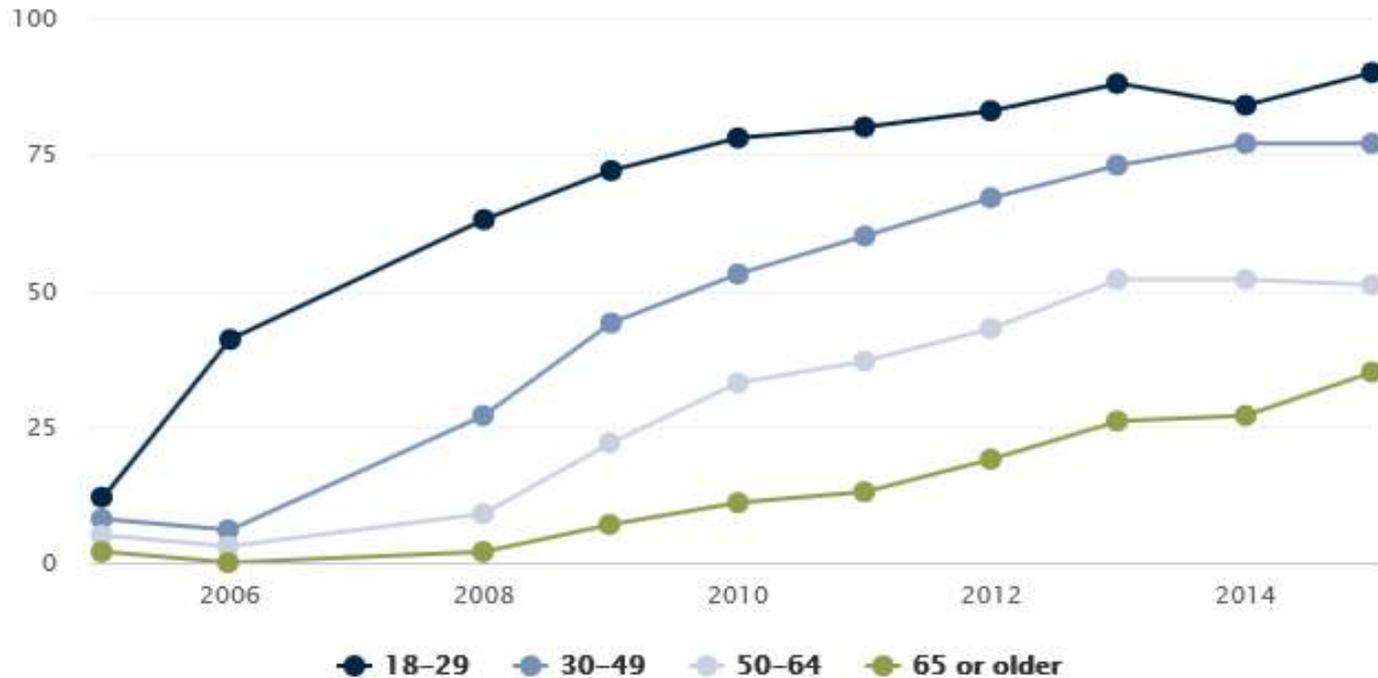
# SNS – Socializing is Rising

- **According to the PEW Research Center age is strongly correlated with social media usage:**
  - Those ages 18 to 29 have always been the most likely users of social media by a considerable margin.
  - Today, 90% of young adults use social media, compared with 12% in 2005, a 78-percentage point increase.
  - At the same time, there has been a 69 point bump among those ages 30-49, from 8% in 2005 to 77% today.
  - While usage among young adults started to leveled off as early as 2010, since then there has been a surge in user-ship among those 65 and older. In 2005, 2% of seniors used social media, compared with 35% today.



# SNS – Socializing is Rising (cont.)

Among all American adults, % who use social networking sites, by age



Source: Pew Research Center surveys, 2005-2006, 2008-2015.  
No data are available for 2007.



# *SNS – Let's Take a Look at the Web*





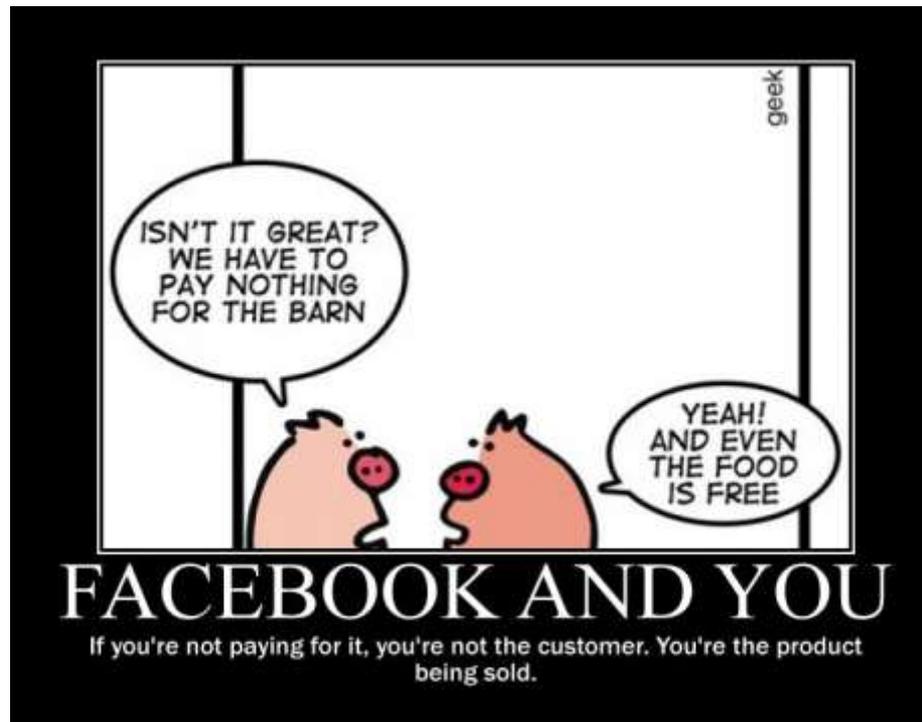
# *SNS – Let's Take a Look at the Web*





# SNS – Let's Take a Look at the Web

**QUESTION: What are some of the most popular shopping sites on the web today?**





# Fun Facebook Facts

- Every second there are 20,000 people on Facebook.
- 79% of all users are accessing Facebook from their mobile.
- There are 745 million daily mobile users
- Facebook is adding 7,246 people every 15 minutes
- Every 15 minutes there are over 49 million posts.
- There are 500,000 Facebook “likes” every minute
- Photo uploads are 350 million per day
- 66% of all millennials (15-34 year olds) use Facebook

## What's advertised



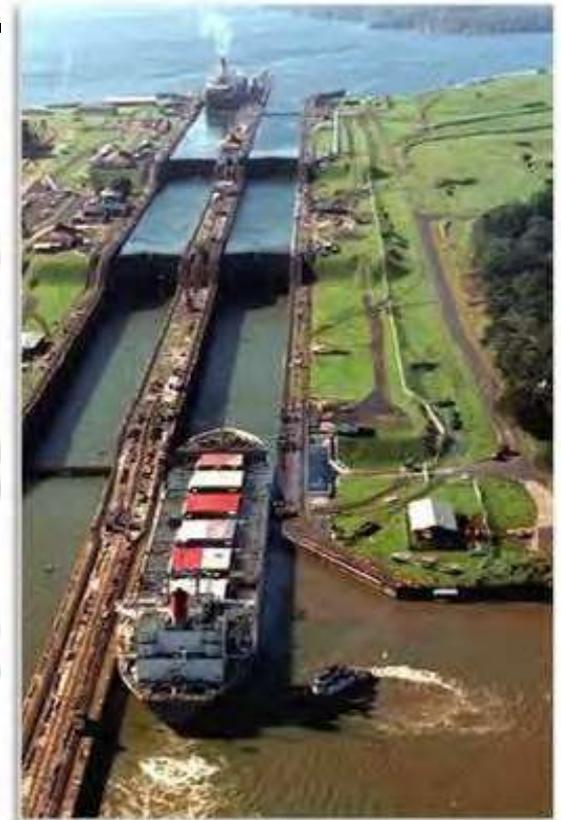
## What's happening





# *How Much of You is on Facebook?*

- **The moment you post online or communicate online, you created a path from them to you.**
  - Names and photos of you, your family
  - Birthdates
  - Maiden names
  - Job titles and work locations
  - Travel itineraries and vacation pics
  - Facebook check in
  - Banking information
  - Hobbies, likes, dislikes, etc.
- ***“Not me! I have a secure router and password protect my stuff!!”***





# Where's the Security?



**Internet Security  
is mostly mythical**

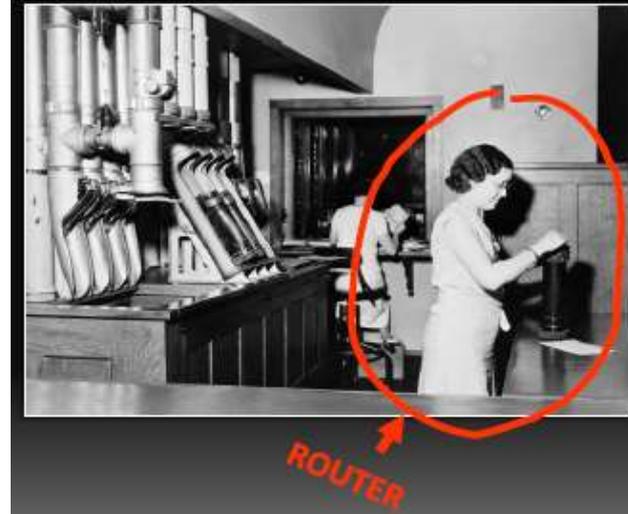


***Rule of thumb:***  
***The Internet and all things on it are  
NOT secure until and unless  
security is added***



# Where's my Stuff Go?

Home - secure



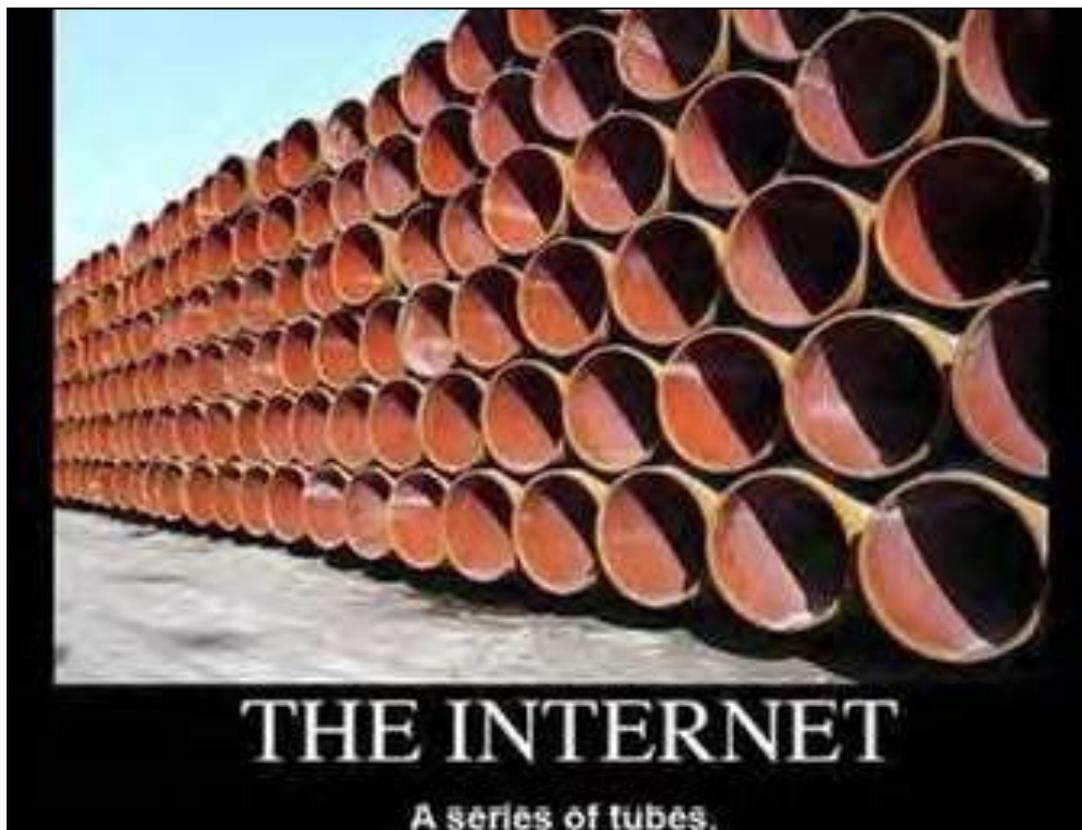
## Carrier and Connections



out of home  
not secure



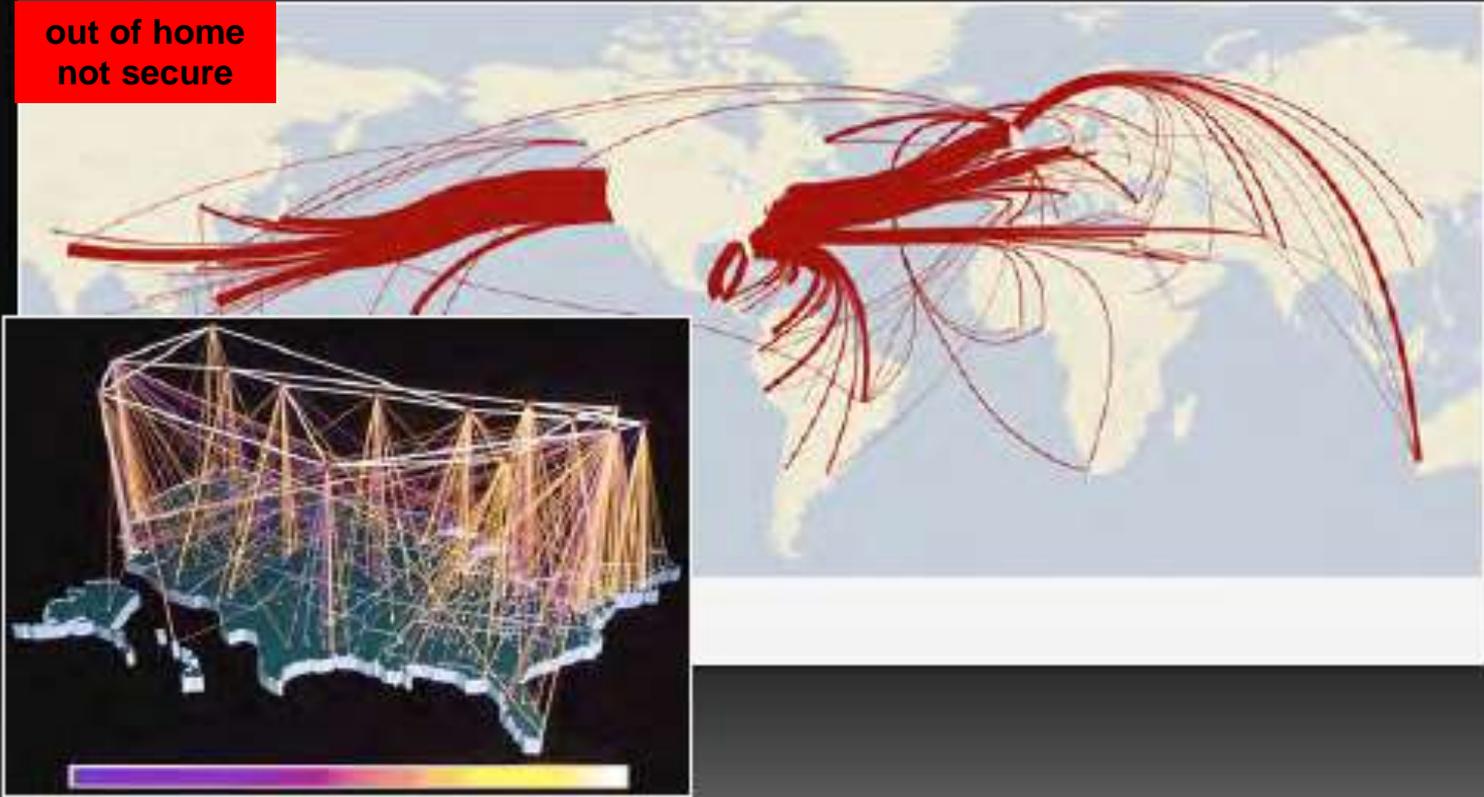
# Where's my Stuff Go (cont.)?





# Where's my Stuff Go (cont.)?

out of home  
not secure



**When you hit SEND.....your information is out there and vulnerable!**



# Internet Security Basics – Authentication

- Old friends....current friends
  - Re-evaluate who you consider a FRIEND!

“I haven't seen \_\_\_\_\_ in years!





# Internet Security Basics - Chat Rooms Dangers

**Disturbing.....watch were your kids go online!**

## CHAT ROOMS



**Hi. You sound real cute!!  
How old are you and what  
do you like doing after school?**



**I am 14 and a bit of a fitness  
fanatic, I often go power lifting  
after school.**

# Security Basics – Know the source!



General

how-to-spot-fake-website-phishing

Protocol: HyperText Transfer Protocol

Type: NET/BLOGS/HOW-TO-SPOT-FAKE-WEBSITE-

Address: **http://www.technospot.net/blogs/how-to-spot-fake-website-phishing/**

OK Cancel

Search

Advanced search

Sponsored link

Co Protect Your Brand, Fast Take Down

Some phishing scams use

This is where the link will take you.



Everything

Videos

News

More

Tampa, FL

Change location

Any time

Latest

All results

Related searches

More search tools

Not sure about the link destination?

- Open
- Open in New Tab
- Open in New Window
- Save Target As...
- Print Target
- Cut
- Copy
- Copy Shortcut
- Paste
- Add to Favorites...
- Properties**

Right click on the link and go to properties.

**How to spot a fake web site – Phishing**  
Nov 25, 2006 ... caption id=attachment\_2085 align=align  
Mobiles and Emails][[/caption] In computing, **phishing** is  
[www.technospot.net](#) > Home > Security - Cached - Similar

**Phishing Filter FAQ - Microsoft Corporation**  
From the warning, you can choose to report this site as :  
**phishing Website**. Follow the instructions on the ...  
<https://phishingfilter.microsoft.com/faq.aspx> - Cached -

[PDF] **Is it a phishing Web site? - IRS.gov**  
File Format: PDF/Adobe Acrobat - Quick View  
In Internet Explorer you can hide or show the. Address bar by right-clicking the toolbar, and then  
clearing or checking the check mark for the. Address bar. ...  
[www.irs.gov/pub/irs-utl/address\\_bar.pdf](http://www.irs.gov/pub/irs-utl/address_bar.pdf) - Similar

**Fraudwatch International - Anti-Phishing Specialists - Phishing ...**  
**Phishing** web sites utilize copied images, text and in some cases simply mirror the legitimate  
web site. This will contain the normal links on the web site ...  
[www.fraudwatchinternational.com](http://www.fraudwatchinternational.com) - Phishing - Cached - Similar



## Internet Security Basics - Stored Credentials



**“REMEMBER ME” / “STAY LOGGED ON”**

**Lesson learned.....always log out!!**



## Internet Security Basics - Hijacking

### Facebook hijacked by cyber criminals in scam to con 'friends' out of cash

By DAILY MAIL REPORTER

Last updated at 9:12 PM on 11th November 2008

[Comments \(4\)](#) [Add to My Stories](#)

Cyber criminals are targeting Facebook users and trying to con money by posing as friends in need.

They hijack the victim's account on the social networking site and then email their friends with a sob story asking for cash.

Computer experts have warned that those with a lot of Facebook friends could be especially at risk.



Hijack an account,  
send message to all  
people in contacts /  
friends list

Friends are more likely  
to believe messages  
from people they  
“know.”



## *Internet Security Basics - Passwords*

**Think of one of your passwords right now.....**

- **Most-used passwords:  
123456, password, 12345678, qwerty, abc123**

<b>Length</b>	<b>Lowercase</b>	<b>+1 Uppercase</b>	<b>+ Nos. &amp; Symbols</b>
6 Char	10 min	10 hours	18 days
7 Char	4 hours	23 days	4 years
8 Char	4 days	3 years	463 years
9 Char	4 months	178 years	44,530 years



# Internet Security Basics - Passwords

## 1. Armored Truck

ex. U2rDaHo7!



## 2. Standard

ex. [site][phrase]



## 3. Throwaway

ex. Hotdog





## *Internet Security Basics - Passwords (cont.)*

- **Make a rule and stick with it for every site**
  - Never utilize the same password for multiple sites
  - Create a 14 character minimum
  - One upper and lowercase letter, number and special character
  - Example: facebookK6x6=36



- **Bottom line**
  - Protect your passwords
  - Don't write them down
  - Don't save them on your computer, phone, email or any other electronic device



# Internet Security Basics - Don't do This

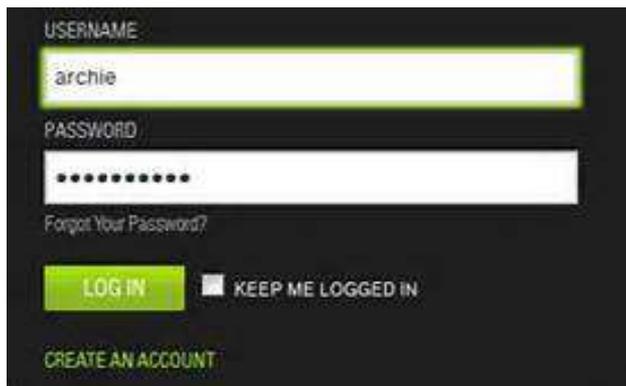
**Don't leave your camera exposed**

**Don't use free wireless for anything important**

**Don't leave your devices "open"**

**Don't stay "logged-in"**

**Don't give away "free" home internet**





## *Internet Security Basics - Wrap it up*

- **Protect you and your family**
  - Utilize privacy settings and educate yourself on how they work
  - Modify your profile – ensure you go through each setting and restrict access to sensitive information
  - Only establish and maintain connections with people you know and trust. Review your connections often.
  - Assume that **ANYONE** can see any information about your activities, personal life, or professional life that you post and share.
  - Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.



## *Internet Security Basics - Wrap it up*

- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Turn-off geo-tagging.
- Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.



**Assume the Internet is Forever**



# Questions





# ***USCENTCOM OPSEC and Social Network Briefing***

**Mr. Felice (Fel) Procaccio  
CCJ3-D-DA Program Security Officer**

*“Use of these OPSEC and Social Network Briefing images and source locations does not reflect official endorsement. Reproduction for private use or gain is subject to original copyright restrictions.”*



# Agenda

- **Definitions**
- **Social Networking Sites (SNS)**
- **Facebook**
- **Internet and Security**
- **Questions**





# Definitions

- **OPSEC or Operations Security**
  - OPSEC is a methodology that denies critical information to the adversary.
- **Critical Information**
  - Information we must protect to guarantee security and success
  - It is what the adversary needs to breach our security prevent our success
  - This can be classified or unclassified





# Definitions – Critical Information

- **Unclassified Information is critical information when you look at the statistics**
  - **90% of all intelligence collected is unclassified through Open Source Intelligence (OSINT)**
  - **Small bits of information can be put together to give the big picture.**
  - **The adversary just needs pieces of information to make a complete picture.**
  - **Bottom Line:**
    - **Unclassified does not mean unimportant.**





# Big Open Source..... Social Networking Sites (SNS)

- **Social Networking Sites (SNS)**

- Allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries over social media
- Social Media is a **NEUTRAL** conduit
- **Factoid:** The safe use of social media is fundamentally a behavioral issue, not a technology issue.

Guidelines for Secure Use of Social Media by Federal Departments and Agencies Federal CIO Council

- Important for you to understand that information you put on Social Media is Open Source, unclassified and can be **CRITICAL** if it falls into the wrong hands



- **What did we say about critical information?**

- Information we must protect to guarantee security and success
- It is what the adversary needs to breach our security prevent our success



# SNS – Were do we Put Our Info??





# SNS – Explained

- **Social Media or SNS Explained**

- Twitter
  - *"I'm eating a donut"*
- Facebook
  - *"I Like donuts"*
- FourSquare
  - *"This is where I eat donuts"*
- Instagram
  - *"Here's a vintage pic of a donut"*
- YouTube
  - *"Watch me eat an entire box of donuts"*
- LinkedIn
  - *"My core strength is my donut eating skill"*
- Pinterest
  - *"Here's my fave donut recipe!"*
- LastFM
  - *"Listening to "Donuts"*
- Google+
  - *"I work for Google and I eat donuts."*
- SharePoint
  - *"I made the donut, now you frost it."*





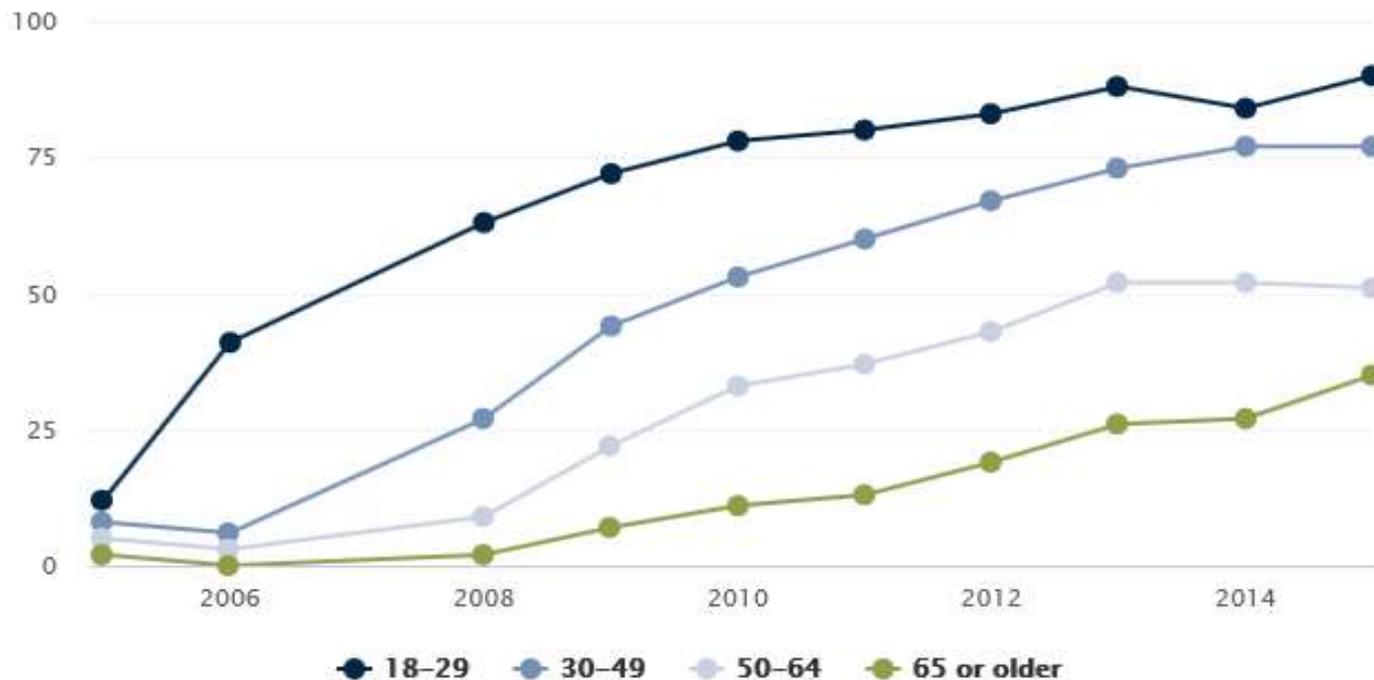
# SNS – Socializing is Rising

- **According to the PEW Research Center age is strongly correlated with social media usage:**
  - Those ages 18 to 29 have always been the most likely users of social media by a considerable margin.
  - Today, 90% of young adults use social media, compared with 12% in 2005, a 78-percentage point increase.
  - At the same time, there has been a 69 point bump among those ages 30-49, from 8% in 2005 to 77% today.
  - While usage among young adults started to leveled off as early as 2010, since then there has been a surge in user-ship among those 65 and older. In 2005, 2% of seniors used social media, compared with 35% today.



# SNS – Socializing is Rising (cont.)

Among all American adults, % who use social networking sites, by age



Source: Pew Research Center surveys, 2005-2006, 2008-2015.  
No data are available for 2007.



# *SNS – Let's Take a Look at the Web*





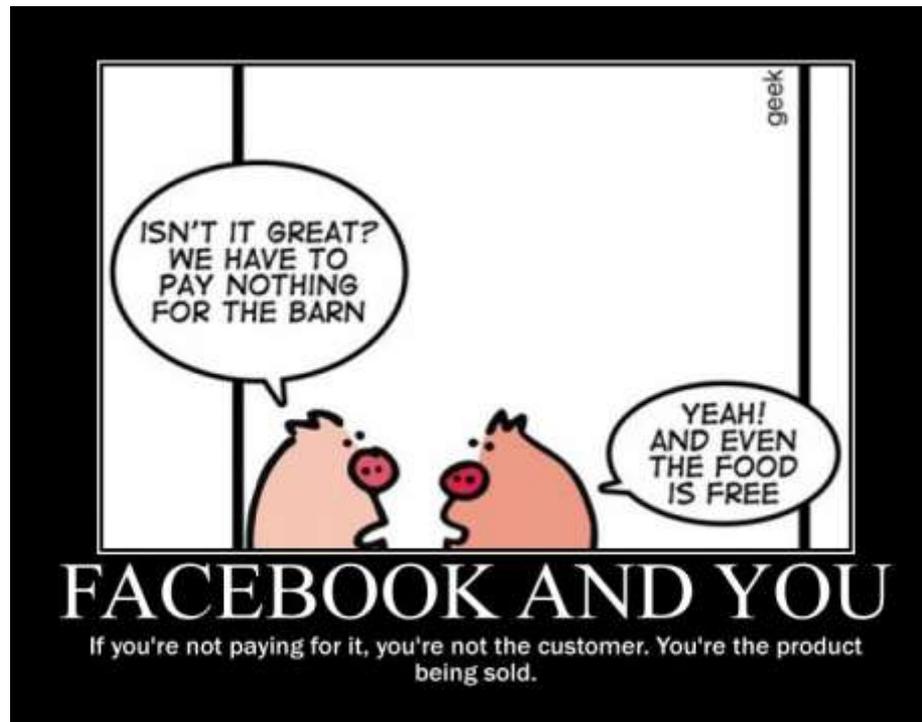
# *SNS – Let's Take a Look at the Web*





# SNS – Let's Take a Look at the Web

**QUESTION: What are some of the most popular shopping sites on the web today?**





# Fun Facebook Facts

- Every second there are 20,000 people on Facebook.
- 79% of all users are accessing Facebook from their mobile.
- There are 745 million daily mobile users
- Facebook is adding 7,246 people every 15 minutes
- Every 15 minutes there are over 49 million posts.
- There are 500,000 Facebook “likes” every minute
- Photo uploads are 350 million per day
- 66% of all millennials (15-34 year olds) use Facebook

## What's advertised



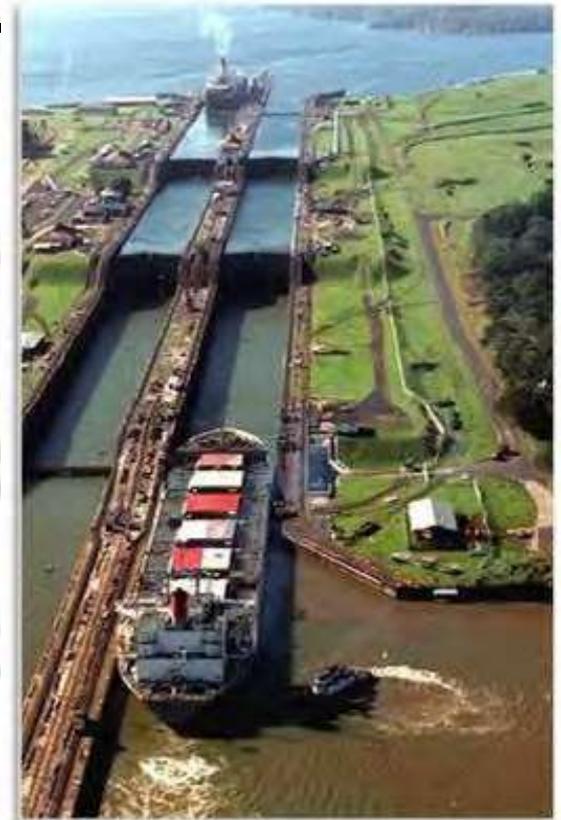
## What's happening





# *How Much of You is on Facebook?*

- **The moment you post online or communicate online, you created a path from them to you.**
  - Names and photos of you, your family
  - Birthdates
  - Maiden names
  - Job titles and work locations
  - Travel itineraries and vacation pics
  - Facebook check in
  - Banking information
  - Hobbies, likes, dislikes, etc.
- ***“Not me! I have a secure router and password protect my stuff!!”***





# Where's the Security?



**Internet Security  
is mostly mythical**

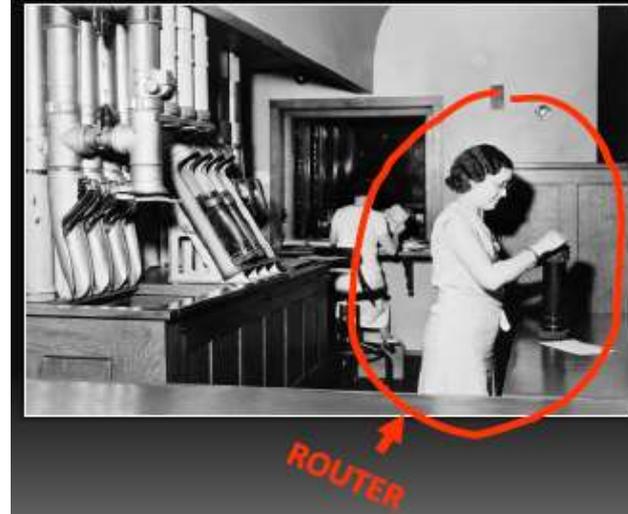


***Rule of thumb:***  
***The Internet and all things on it are  
NOT secure until and unless  
security is added***



# Where's my Stuff Go?

Home - secure



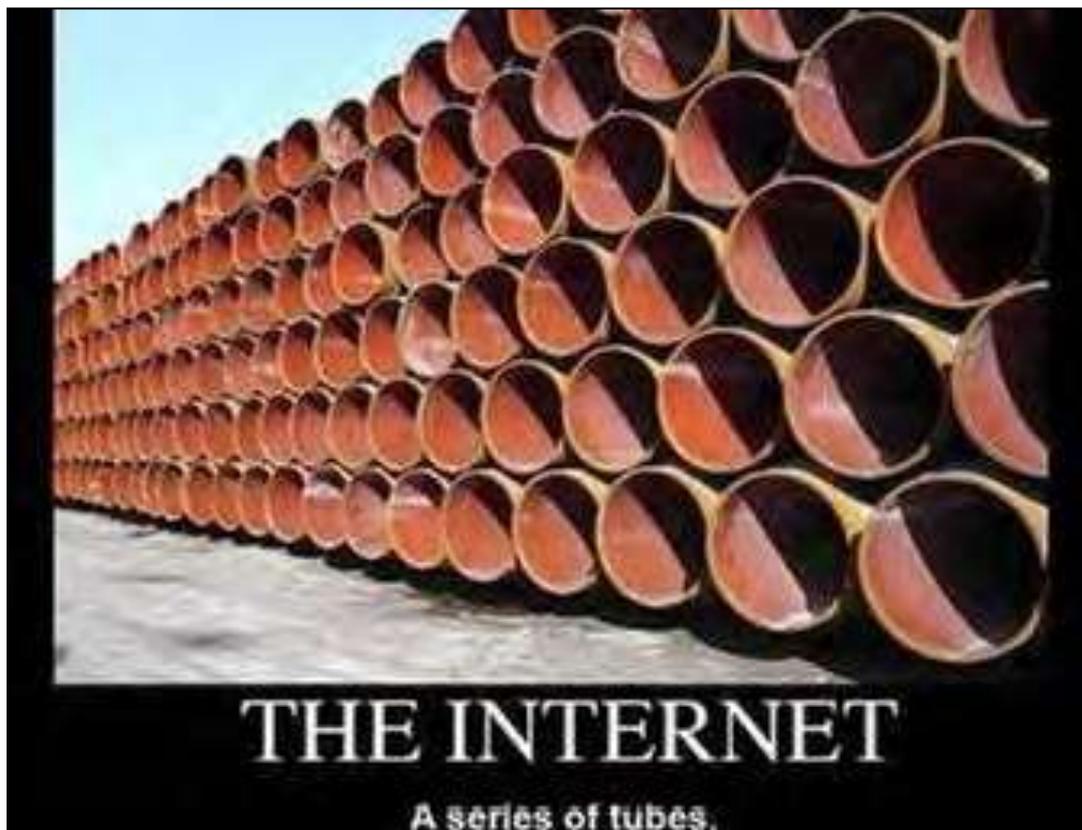
## Carrier and Connections



out of home  
not secure



# Where's my Stuff Go (cont.)?





# Where's my Stuff Go (cont.)?

out of home  
not secure



**When you hit SEND.....your information is out there and vulnerable!**



# Internet Security Basics – Authentication

- Old friends....current friends
  - Re-evaluate who you consider a FRIEND!

“I haven't seen \_\_\_\_\_ in years!





# Internet Security Basics - Chat Rooms Dangers

**Disturbing.....watch were your kids go online!**

## CHAT ROOMS



**Hi. You sound real cute!!  
How old are you and what  
do you like doing after school?**



**I am 14 and a bit of a fitness  
fanatic, I often go power lifting  
after school.**

# Security Basics – Know the source!



General

how-to-spot-fake-website-phishing

Protocol: HyperText Transfer Protocol

Type: NET/BLOGS/HOW-TO-SPOT-FAKE-WEBSITE-

Address: <http://www.technospot.net/blogs/how-to-spot-fake-website-phishing/>

OK Cancel

Search

Advanced search

Sponsored link

Co Protect Your Brand, Fast Take Down

Some phishing scams use

This is where the link will take you.

Sponsored links

Google [Website Optimizer](#)

Test ways to improve your site and boost conversions. Learn more.

[www.google.com/websiteoptimizer](http://www.google.com/websiteoptimizer)

See your ad here »



- Everything
- Videos
- News
- More

Tampa, FL

Any time

All results

Not sure about the link destination?

- Open
- Open in New Tab
- Open in New Window
- Save Target As...
- Print Target
- Cut
- Copy
- Copy Shortcut
- Paste
- Add to Favorites...
- Properties**

Right click on the link and go to properties.

[How to spot a fake web site – Phishing](#)

Nov 25, 2006 ... caption id=attachment\_2085 align=align

Mobiles and Emails][[/caption] In computing, **phishing** is

[www.technospot.net](#) > Home > Security - Cached - Similar

[Phishing Filter FAQ - Microsoft Corporation](#)

From the warning, you can choose to report this site as :

**phishing Website**. Follow the instructions on the ...

<https://phishingfilter.microsoft.com/faq.aspx> - Cached -

[PDF] [Is it a phishing Web site? - IRS.gov](#)

File Format: PDF/Adobe Acrobat - Quick View

In Internet Explorer you can hide or show the. Address bar by right-clicking the toolbar, and then clearing or checking the check mark for the. Address bar. ...

[www.irs.gov/pub/irs-utl/address\\_bar.pdf](http://www.irs.gov/pub/irs-utl/address_bar.pdf) - Similar

[Fraudwatch International - Anti-Phishing Specialists - Phishing ...](#)

**Phishing** web sites utilize copied images, text and in some cases simply mirror the legitimate web site. This will contain the normal links on the web site ...

[www.fraudwatchinternational.com](#) : ... Phishing - Cached - Similar



## Internet Security Basics - Stored Credentials



**“REMEMBER ME” / “STAY LOGGED ON”**

**Lesson learned.....always log out!!**



## Internet Security Basics - Hijacking

### Facebook hijacked by cyber criminals in scam to con 'friends' out of cash

By DAILY MAIL REPORTER

Last updated at 9:12 PM on 11th November 2008

[Comments \(4\)](#) [Add to My Stories](#)

Cyber criminals are targeting Facebook users and trying to con money by posing as friends in need.

They hijack the victim's account on the social networking site and then email their friends with a sob story asking for cash.

Computer experts have warned that those with a lot of Facebook friends could be especially at risk.



Hijack an account,  
send message to all  
people in contacts /  
friends list

Friends are more likely  
to believe messages  
from people they  
“know.”



## Internet Security Basics - Passwords

Think of one of your passwords right now.....

- **Most-used passwords:**

**123456, password, 12345678, qwerty, abc123**

<b>Length</b>	<b>Lowercase</b>	<b>+1 Uppercase</b>	<b>+ Nos. &amp; Symbols</b>
6 Char	10 min	10 hours	18 days
7 Char	4 hours	23 days	4 years
8 Char	4 days	3 years	463 years
9 Char	4 months	178 years	44,530 years



# Internet Security Basics - Passwords

## 1. Armored Truck

ex. U2rDaHo7!



## 2. Standard

ex. [site][phrase]



## 3. Throwaway

ex. Hotdog





## *Internet Security Basics - Passwords (cont.)*

- **Make a rule and stick with it for every site**
  - Never utilize the same password for multiple sites
  - Create a 14 character minimum
  - One upper and lowercase letter, number and special character
  - Example: facebookK6x6=36



- **Bottom line**
  - Protect your passwords
  - Don't write them down
  - Don't save them on your computer, phone, email or any other electronic device



# Internet Security Basics - Don't do This

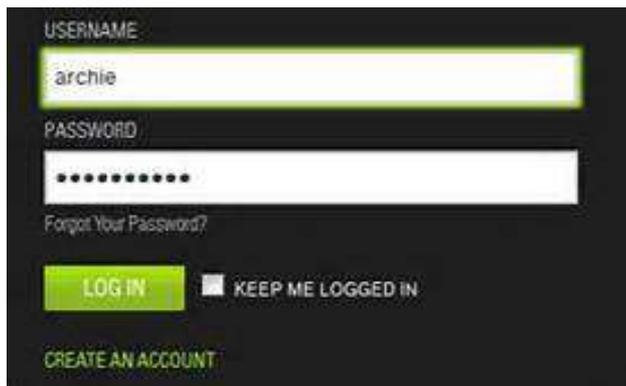
**Don't leave your camera exposed**

**Don't use free wireless for anything important**

**Don't leave your devices "open"**

**Don't stay "logged-in"**

**Don't give away "free" home internet**





## *Internet Security Basics - Wrap it up*

- **Protect you and your family**
  - Utilize privacy settings and educate yourself on how they work
  - Modify your profile – ensure you go through each setting and restrict access to sensitive information
  - Only establish and maintain connections with people you know and trust. Review your connections often.
  - Assume that **ANYONE** can see any information about your activities, personal life, or professional life that you post and share.
  - Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.



## *Internet Security Basics - Wrap it up*

- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Turn-off geo-tagging.
- Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.



**Assume the Internet is Forever**



# Questions

