



# Cyber Security and Computer Safety

UT Wing  
Civil Air Patrol

# Objective

- Identify network and cyber vulnerabilities and mitigations
  - Social Media/Metadata/Exfil data
  - MITM Attacks
  - Malware
  - Social Engineering

# Social Media

- Do you know how much information an individual can collect about you?
  - You are probably already sharing more data than you think
  - Tagged pictures can show famous landmarks helping to identify hometown
  - You might already be sharing hometown, job, school with everyone

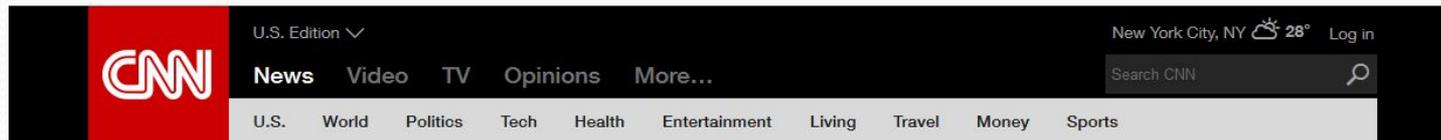
# Info Gleaned from Facebook

- Job listed
- School listed
- Residence listed
- Family info listed
- Hometown listed
- What can someone do with that info?



# Modern Concern for Members

- Bad guys are looking for Military members and their families, be aware of how to post pictures.



## Military families spooked



After ISIS threat, relatives rethink online lives

18 min

### The Latest

Astronauts scramble after alarm 1 hr

Kids die as mom gets hair done 19 min

Searchers find AirAsia fuselage 1 hr

Arrested teen helps save cop 4 hr

Jon Stewart rips Obama, Holder

Videos show Paris assault

37 babies saved in bust 1 hr

Razzies' picks for 2014's worst 1 hr

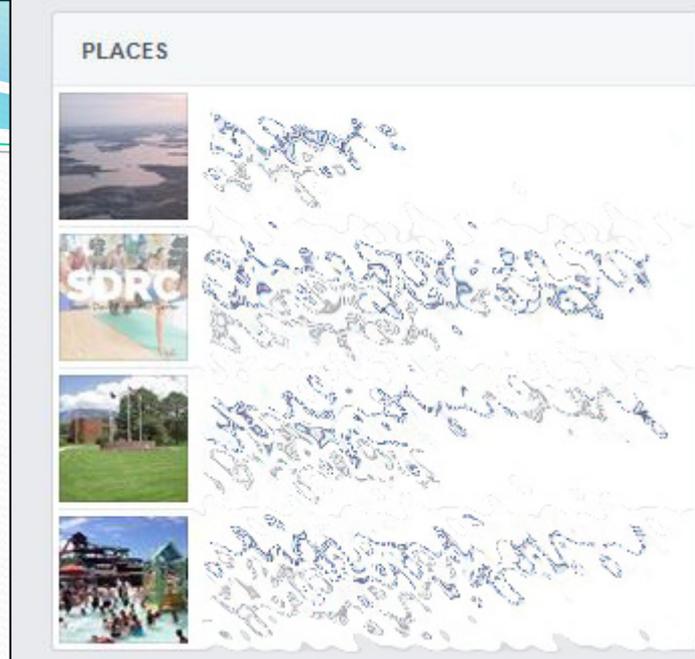
Helpful LeBron shoves own coach

# Metadata

- Data on data
- Can have GPS coordinates imbedded in the image:

Remember: It is easy to do a reverse lookup of someone's name online to find an address if I can already narrow the search down to a City or State

34 pictures in SLC, UT. Hmmm, probably lives there...



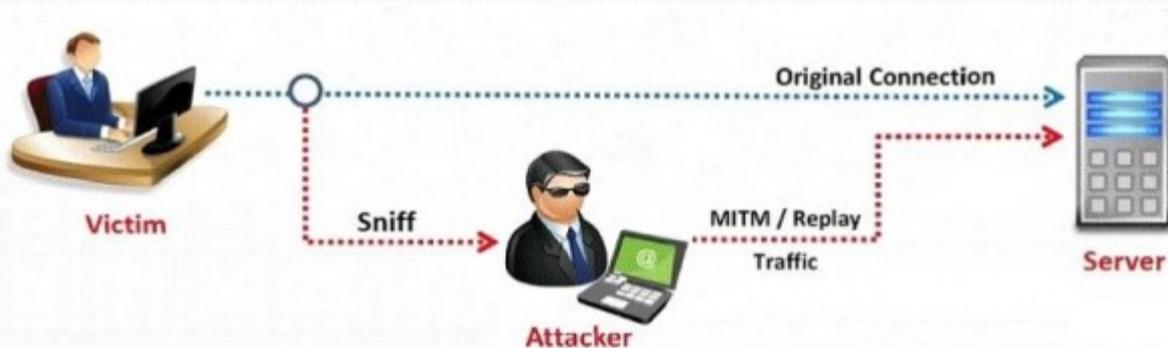
# Social Media

- Solution:
  - Lock down privacy settings to only share with friends
  - Be careful on how you affiliate yourself with different entities; if someone doesn't like that group you may become a target



# Man in the Middle Attacks: MITM

- A hacker can intercept data going from your computer to the router
- You do not have security on an unsecure network!
- Unsecure networks include Coffe Shops, Hotels, Airports
- Your passwords and usernames can be seen by a hacker, even if using HTTPS when on an unsecure network
- Always do online banking, and sensitive web use on a secure network that is trusted
- WEP encryption does not make your network very secure, may be time to upgrade to WPA2
- Disable WPS is on your router, this can be brute-forced and compromise your network



# Malware

- Hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs
- 30% of households in the U.S. are infected with Malware
- SLC ranks 5<sup>th</sup> in the U.S. for most computer infections
- A hacker can gain access to your computer to steal passwords, steal documents, use your webcam or microphone, or use your computer to attack another
- Most malware is installed by opening email attachments.

Northwestern European countries such as Norway, Switzerland, and Sweden all have the lowest amount of computers infected with malware.

The United States has the eleventh highest rate of infection with just over 30 percent of households being infected with malware.

The most common types of malware are viruses, Trojan Horses, and unwanted software. The most common computer virus of all time is the Conficker worm. This worm targets Windows operating system flaws and spreads across networks forming a botnet of auto-acting malware. Conficker, also known as "Downup", was first detected in late 2008 and spread to over 200 different countries making it the biggest, most widespread computer worm ever.

Last year, in the United States alone, malware cost us an estimated \$4.5 billion, and one million U.S. households lost money or had accounts misused due to malicious software.

With each passing day it's becoming more and more important that you have some sort of antivirus or [security program](#) on your computer. In addition to having software to protect your PC against threats, it's also vitally important that you make smart choices while browsing the web and opening emails.



## SLC ranks 5th in U.S. for most computer infections, study says

By Brianna Bodily

December 30th, 2014 @ 9:14am

This archived news story is available only for your personal, non-commercial use. Information in the story may be outdated or superseded by additional information. Reading or replaying the story in its archived form does not constitute a republication of the story.



# Malware Continued

- Phishing is done by either attaching a bad file that you have to open, and in SOME cases install
- Could be opened by having a URL link that takes you to a site that looks like the expected site but the URL name is wrong.
- Anti-virus use will NOT stop you from installing malware or a virus! The computer usually asks YOUR permission to install a piece of software that you have to agree to – unknowingly.
- NEVER download anything unless you know exactly what it is! Never go to a webpage unless you know exactly what it is!

# Social Engineering

- A hacker will have full access to your computer if they can have physical access
  - Never use a USB thumb drive, disc, or open an attachment from anyone you don't trust. Never download anything unless you know exactly what it is
  - If a bad person can have a few minutes alone with your computer, they can easily get full access
  - A bad person will try to trick you (socially engineer you) and get you to use a thumbdrive, disc, or file that is corrupted

