Security and You Presentation
By Jamie Leben
August 9, 2013

- Threat surfaces
  - Any information that leaves your computer un-encrypted is likely to be collected
  - Encryption: (http://en.wikipedia.org/wiki/Encryption) **encryption** is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. For our purposes "public key encryption" is what is typically used. Recipients create a "public key" which can be given to anyone, which a sender uses to encrypt the data, which is then only de-cryptable with the recipients "private key" which should only be usable and known by the recipient.
  - "Lockbox" analogy: The data is encrypted in such a way that it cannot be read by anyone without the key to decrypt the data. The key for decrypting the data is different from the key used to encrypt the data and is NOT shared with anyone.
  - Secure websites perform this task automatically with you browser. Non-secure websites and most email is NOT encrypted at all, or at some point in its travels.
  - Use "pre-Internet encryption" for private information—encrypt the information on your computer before it leaves your computer to travel across the Internet.
- Encrypting Thunderbird email
  - Menu > Add-ons > search "encryption"
  - Enigmail > install > restart Thunderbird
  - Menu > Open PGP
- Browser webmail encryption plug-in: http://www.mailvelope.com/
  - Allows you to encrypt webmail
- Browser add-ons that protect your privacy
  - Ghostery: http://www.ghostery.com
  - Abine: http://www.abine.com/
  - Privacy Fix: http://www.privacyfix.com
- Use unique, secure passwords for each website
  - https://lastpass.com/ generates and stores passwords for you
- VPN
  - A VPN (Virtual Private Network) is a way to encrypt all network traffic between your computer and a trusted exit point.
  - Useful for protecting information on an untrusted connection like a hotel or coffee shop
  - VPN and TOR: http://www.proxpn.com
  - LogMeIn: http://www.Logmein.com
  - GoToMyPC: http://www.gotomypc.com
- TOR
  - The Onion Router (https://www.torproject.org/)
  - Free VPN network routing software originally developed by the military that encrypts and masks network origin and destination points
  - Extra anonymity, but not as fast as a regular VPN
- Operating system choices (avoid spyware and keyloggers)
  - "Highly concerned": Use a bootable Linux disk (Ubuntu, Knoppix) with desired privacy

features. More maintenance, less chance of compromises
    - "Concerned": Linux on dual boot
    - "Moderately concerned": Linux or Mac
- Resources:
    - https://www.grc.com/securitynow.htm

Web browser search result changes

- Internet Explorer
    - Tools > Manage Add-Ons
    - (left pane) Search Providers
    - Find desired default search provider, right click it, left click "set as default"
    - (left pane) Toolbars and Extensions
    - Right-click unwanted toolbars and extensions, left click "disable"
    - "Close"
- Chrome
    - Tools (upper right Gear or horizontal bars menu) > Settings
    - Search (on the left)
    - Left-click desired default search engine to select it, left click the "default" box to the right
    - Delete any unwanted search providers
    - "Done"
    - Extensions (on the left)
    - Uncheck or delete any unwanted extensions
- Firefox