Digital Security Handout

CONSISTENCY is critical to improving your digital security.

Personal Computer Safety

- Enable **Firewall** protection
- **Email** services
  - Gmail or Microsoft Outlook preferred over Yahoo!
  - Gmail's Two-Step Verification
    - Password
    - SMS with passcode
  - Hushmail
    - Provides integrated encryption
  - GnuPG (http://www.gnupg.org/)
    - Allows encryption/decryption of email
- **Encryption** of hard-drive
  - Uses mathematical algorithm to encrypt/decrypt files
  - Will generally require an additional password when accessing the hard-drive
  - Free open-source encryption services:
    - TrueCrypt (http://www.truecrypt.org/)
      - Windows and Mac
      - Can encrypt entire hard-drive, a portion of a disk, or a single file
    - FileVault 2 (http://support.apple.com/kb/HT4790/)
      - Mac
      - Entire hard-drive
- **Secure Deletion**
  - Placing file in the 'Trash' and emptying does NOT fully delete that file
  - Simply renders the file invisible to the user even though it remains until overwritten by another file
  - The best way to keep such 'deleted' files hidden is to make sure that they are overwritten immediately
    - Windows
      - Eraser (http://eraser.heidi.ie/download.php)
    - Mac OS X
      - On OS X 10.4 and above, files can be securely deleted by moving them ot the Trash, then selecting Finder > Secure Empty Trash
      - To ensure that previously deleted data cannot be recovered:
        - Open Disk Utility, choose Help > Disk Utility Help, and search for help on erasing free disk space
  - Overwriting the entire disk and installing a fresh operating system is the ONLY way to GUARANTEE that all records of a file have been securely erased
  - For more information on secure deletion, see the Electronic Frontier Foundation at https://ssd.eff.org/tech/deletion
- **Secure Back-Up**
  - Daily or weekly
- **Malware/Virus Detection**
  - *Prevention* is critical
  - Promptly install all software updates
  - Safe browsing/emailing
    - Be suspicious of unsolicited files or contact from unknown entities

        - NEVER open a link or file from an unknown source
        - Do not download or install software from banner advertisements or pop-ups
    - Download free software
        - Avast Free Antivirus:
            - http://download.cnet.com/Avast-Free-Antivirus/3000-2239_4-10019223.html?tag=main;pop
        - AVG AntiVirus Free 2014:
            - http://download.cnet.com/AVG-AntiVirus-Free-2014/3000-2239_4-10320142.html?tag=main;pop
        - Malwarebytes Anti-Malware:
            - http://download.cnet.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html?tag=main;pop
- **Passwords**
    - For stronger password security, use a lengthy passphrase that includes upper- and lower-case letters, one or more numerical digits and special characters
        - Opt for full passwords rather than four-digit passcodes
    - Do not use passwords that can be easily guessed such as names, birthdays, or words found in the dictionary.
    - Include non-alphabetic characters such as numbers and punctuation
    - Change the password frequently
    - Use different passwords for different assets
    - Never keep a password in the same physical location as the asset it protects
    - Use a password safe:
        - A password safe allows you to store your passwords on your computer in an encrypted virtual safe. You can access the safe – and your passwords – upon entering a master password.
        - http://keepass.info/
    - For devices such as the iPad, one can choose to have all the data on the device erased after 10 failed passcode attempts.
        - Settings > General > Passcode Lock options > Erase Data 'On'
- **Online Anonymity**
    - Makes your online traffic unable to be traced. Prevents others from learning your physical location or about your browsing habits. Allows you to circumvent any internet censors. Enables you to connect to an NGO's website while in a foreign country without signaling that they work with that organization.
    - Diverts your online traffic through a variety of locations so that your origin and destination remain unknown
        - Such diversion slows down browsing, so is best used sparingly
    - Tor: https://www.torproject.org/

Mobile Phones

- Mobile phones are one of the most vulnerable forms of communication.
- **Location Tracking**
    - Phones periodically communicate with transmission towers. The strength of the signal that is received is a measure of distance, so the network knows where each phone generally is.
    - Only way to ensure that they cannot be used to track one's location is to power off and remove the battery
- **Voice Calls**
    - Communications can be easily intercepted

    - Technology that allows for full encryption of voice calls is not yet widely available. Generally, it is the carrier that decides whether or not phone calls will be encrypted. Usually encryption or lack thereof is not indicated by the carrier.
        - Even if the carrier provides encryption, the protection would be lost if the carrier wanted to eavesdrop or if the carrier was ordered to do so by the government.
        - Also, most cell network cryptography has been broken, so encryption does not guarantee security.
- **SMS**
    - Very insecure method of communicating, so they should only be used for the most mundane of messages, if at all
- **Data storage**
    - Phones store…
        - Text message contents
        - Dates and times of calls
        - Location
    - Such data cannot be securely deleted as on a computer
    - One must manually delete files and hope that the file gets overwritten quickly

Further Resources

- Security in-a-box: Tools and Tactics for Your Digital Security
  Hands-On Guides to various digital security topics
  https://securityinabox.org/en/handsonguides
- Electronic Frontier Foundation
  Surveillance Self-Defense
  https://ssd.eff.org/
- Martus: A Global Human Rights Abuse Reporting System
  https://www.martus.org/index.shtml
- Huridocs – INGO helping human rights organizations use IT and documentation methods to maximize the impact of advocacy work
  http://www.huridocs.org/
- Information Security Coalition
  Online Security Advice
  https://www.informsec.net/online-security/