Below is a copy of the presentation created by 4 Walls Media Group http://www.4wmg.com and presented at our April meeting.

If you would rather see an interactive web site click the link below. Use arrow keys to navigate around the web site.
http://www.4wmg.com/score/#/slide1

Internet Security

Presented April 8, 2015

Merrimack Valley SCORE

4Walls Media / www.4wmg.com

Topics

- What is Computer and Internet Security
- Who Should be Concerned
- Why Should I Care
- General Computer Security Tips
- Securing Mobile Devices and Social Networks
- Mobile Devices – Risks

- How are Location Sharing Technologies Used
    - Risks of Location Sharing Technologies
    - Examples of Location Sharing Technologies

What is Computer and Internet Security

- Computer Security
    - Protecting computers, information, and services from unauthorized access, change or destruction
    - Internet security extends this concept to systems that are connected to the Internet
        - Browsing the Internet
        - E-Commerce
        - Social Networks
        - Email

Who Should be Concerned

- Anyone who uses
    - Computers
    - Mobile Devices
    - The Internet
    - Email
    - Social Networks

Why Should I Care

- **Infections from viruses, spyware, or malware**
    - Virus - Program designed to infect your computer, replicate itself, and usually cause corruption or loss of data
    - Spyware - Malicious code that tracks your activity on the Internet, generally without your knowledge, and collects personal information
- **Phishing, Hoaxes, Malware, Scams, and Spam**
    - The most prevalent and persistent threats to your security come to you in your Inbox. They come by different names and may even appear legitimate and even supposedly from people you may know.

    - They all have this in common: they are designed to get you to click on an item like an attachment, link, or picture.
- **Malfunctioning Device**
    - Devices that do not work when needed or as expected
- **Privacy and personal security concerns**
    - Preventing private, personal, or sensitive information from being disclosed

Basic Approaches to Security

Use strong passwords whenever possible

- Do not use the same password for multiple purposes/services.
- Never disclose your passwords to anyone. If you need to disclose a password, change it to something temporary before giving it out, then make sure you change it back as soon as possible (or create a new one).

Updates: Use anti-virus and anti-spyware software

- Detect and remove viruses and spyware from your computer
- Must be kept up-to-date
- Install security patches
- Enable firewalls
- Be cautious about downloading free software or files from untrusted sites

Think before you click on links

- Do not automatically click on Internet links unless you absolutely trust them.
- Look at the actual address for the links in question. For instance, if the link indicates "Click Here", be sure to hover your mouse pointer over the link and investigate before you proceed.
- Often, links in emails will appear to point to a legitimate location, but the actual link may differ from what is shown. When in doubt, type in the address of the site you want to visit rather than clicking the link.

Security for Mobile Devices and Social Networks

- Mobile devices have become the devices of choice for communicating and connecting to the Internet
    - Smartphones
    - Tablets
    - Laptops
- Social Networks
    - Facebook
    - Twitter
    - Google+
    - Pinterest

Mobile Devices - Risks

- Mobile devices are easy to lose or steal
- Oftentimes carry large amounts of data
    - If stolen, an unsecured smartphone grants access to your private information, email correspondence, and any unsecured documents
- Often unprotected by password or pin/code
- Data may be "sniffed" during unprotected wireless communications (unencrypted WiFi)

How are Location Sharing Technologies Used

- Apps might provide you with information on nearby restaurants, notify you of traffic jams, or let your friends know where you are.
- Maps and/or real-time directions usually require GPS functionality to be turned on

Risks of Location Sharing Technologies

- Makes users "human homing beacons"
- Increases the chances of being stalked
- May reveal when you are home or away

Examples of Location Sharing Technologies

- GPS Geo-tagging of photos (location details embedded in photographs)
- Foursquare for custom-tailored dining and entertainment suggestions based on location

Security Guidelinies for Location Sharing Technologies

- Most apps offer privacy controls
- Defaults are usually too open
- Only enable GPS capabilities for features that you actually use, and disable them when they are not needed

Security Guidelines - Mobile Devices

- Enable auto-lock
- Enable password protection
- Keep the phone/tablet OS and apps up-to-date
- Enable 'Find My Device' and remote-wipe features where possible
- Avoid connecting to public wireless networks when transmitting sensitive information

Security Guidelines - Social Networks

- Before you post, ask the following:
  - Will this post/picture cause a problem for me?
  - Would I say this in front of my mother?
- Limit the number of people that see it:
  - Share public information with the public
  - Share inner thoughts and personal feelings with close friends
- Turn off "face recognition" in photos and videos
- Turn off geo-location for photos

Thank You!

Presented April 8, 2015 to Merrimack Valley SCORE by 4Walls Media

www.4wmg.com