Personal Online Safety

Checklist for keeping safe

I. Protect Your Computer:

A. Anti-Virus Software
Anti-virus software is a program installed on a computer to prevent the introduction of malicious software. It can also fmd it, remove it, and often repair infected files.
(FREE programs: AVG, Avast; also check with the local ISP)

- Install anti-virus software
- ***Immediately update it***
    - o Regularly update it thereafter
- • Review the settings carefully
    - o Make sure it is scans "real time"
    - oScan ALL FILES, not just program files
- • Run a scan regularly
    - o Every day is not too often

B. Firewalls
A firewall is a program that protects a network from unwelcome traffic by enforcing an access control policy between the local network and the Internet
(FREE programs: Windows Defender, Zone Alarm; also check with the local ISP)

- Install a software firewall
- Do your homework - make sure it is set up properly
- Firewalls CANNOT protect against
    - o Email attacks
    - o Internal attacks (such as a CD)

II. Protect Your Information:

A. Passwords
A strong password is one that has at least fifteen characters including letters, numbers, and other non-alphanumeric characters

- Don't use your username
- Don't make it anything guessable
- Don't store it where someone can see it or find it
- Use a "passphrase:" it looks random ... but it makes sense to you

Example: A&Bh3 fcnJ ,P ,&E.
(Ann and Bob have three fine children named Jason, Paul, and Elizabeth.)

Personal Online Safety

Checklist for keeping safe

B. Downloads

- Malicious software often hides in free downloads
- Trojan horses allow attackers to take over your computer, and operate it in secret
- Be cautious of email attachments
- 70 of spam contains malicious software

C. Web sites

• Be suspicious of websites that
  - o Are from a link in spam
  - o Are linked to ads that are tailored just for you
  - o Call you "customer" or "friend"
  - 0 Try to give you something * free *
  - oAsk for any personal information - for ANY reason

• Always read the address carefully
  - o "bankofamerica" vs. "bankofamerca"

• Set up your browser to warn you
  - o Internet Explorer, Firefox, and Safari all include tools for flagging suspect sites

D. Patches & Backups

• Install patches
  - o Patches usually are for improved security
  - o Check for updates regularly
  - o Turn on the "auto-update" feature

• Create backup files
  - o It takes only a few minutes
  - o Use a CD, a flash drive, or external hard drive
  - o Copy those files that you care about losing

E. Email

• Beware phishing scams!
  - o They pretend to be from a business you know
  - o They claim there is an account problem
  - o They insist you respond *immediately*
  - o They threaten your account privileges

- **Don't**
  - Read email from persons you don't know
  - "Opt out" of spam *(just delete it)*
  - Click on any links in unfamiliar email
  - Give out any personal information in emails
- **Do**
  - Scan any attachments for viruses before opening
  - Delete suspicious looking emails

F. Online shopping

- Use a credit card
  - Fair Credit Billing Act limits consumer liability
  - Electronic Fund Transfer Act limits consumer liability for debit cards, **with stipulations**
- Buy only from businesses you know
- Check the seller's reputation (Auctions)
- Always use a secure connection

III. Protect Yourself:

A. Social Networking

- Make your profile PRIVATE
- Limit the information you put into your profile
- Make sure you know your friends

B Posting Images

- Be cautious when posting an image on a public site - one that can be seen by all
- Know where you have pictures of your children and grandchildren
- Check the images that your friends have posted too

C. In-person Meetings

- Make your meeting in a place public - popular restaurant, public park, ball game
- Tell friends where you will be
- Take a friend with you, and ask them to stay for the entire meeting
- Once you are back home, evaluate the encounter

Personal Online Safety

Checklist for keeping safe

D. Identity Theft

- Get a free credit report annually
  - o **www.annualcreditreport.com**
- Review all bank and account statements
- Beware of sites that ask for personal information; make sure they need it
- Keep your anti-virus updated
- Use a shredder

E. Public Computers

- Don't save your logon information
  - o Always click "log out" on the site.
- Disable automatic login features
  - o Never check "Remember me" or "Keep me logged in."
- Don't leave the computer unattended
  - o Log out of all programs and close all windows.
- Erase your tracks
  - o Delete your temporary Internet files and your history.
  - oUse Google/Bing/Yahoo! if you need help with this.
- Watch for over-the-shoulder snoops
  - o They can watch as you enter sensitive information.
- Don't enter sensitive information into a public computer
  - o Sometimes all the steps we take to hide it are not enough.