# Internet Safety

staying safe online

**Why consider Internet safety?**

- Protect yourself.
- Protect the equipment you are using.
- Remain safe online to maintain privacy, prevent identity theft, and avoid viruses.

**Privacy**

- What information about you is already available online?
  - Go to google.com and search for your name. Look at the results.
  - Go to images.google.com and search for your name. Look at the pictures in the results.
  - Log in to the Reference USA database available through the Salina Library. Use the U.S. Consumers/Lifestyles search to see what information is available about you.
- When considering privacy, ask yourself two questions:
  - What information do I want to share?
    - Am I willing to share my address, phone number, or age?
    - Do I want to share my interests and affiliations?
    - Do I want to share photos of myself?
  - With whom am I willing to share this information?
    - Is there information to which I only want my friends and family to have access?
    - Is there information to which I want anyone in the world to have access?
- Carefully consider what information you share over social networking sites.
  - Social networking sites include Facebook and Twitter.
  - The goal of social networking sites is to facilitate the sharing of information, not to facilitate the protection of information.
  - Check all of the sharing and access settings for these sites on a regular basis.

**Passwords**

- Create strong passwords.
  - Use letters, numbers, and symbols (where permitted) in each password.
  - Each password should be at least eight characters long. In general, the longer the password the better.
  - Consider using a sentence as a password.
  - Random passwords are best.
- When creating a password, do not use:
  - personal information such as your birthday or maiden name
  - information easy to find such as your favorite color or your address
- When creating a password, try to avoid using:
  - real words (in any language)
  - sequences of letters or numbers

- Use a trusted password checker to test the strength of your passwords.
- Use a different password for each website. This is especially important for banking and credit card websites.
- Change each of your passwords periodically.
- If you need help remembering your passwords, it is okay to write them down.
    - If possible, write down password hints instead of the actual passwords.
    - Keep the paper on which you write down the passwords secure.
- Do not create a file on your computer containing all of your passwords.
- Public computers should be treated differently than private computers.
    - Remember where you are.
    - Public computers aren't as safe as private computers.
- Consider who has access to a computer when deciding how to treat passwords.
    - Having the browser remember your passwords is okay on a computer to which only you have access if you are not worried about it getting hacked or stolen, but this should never be done on a public computer.
    - Closing the window in which a website was loaded which you signed into is often not enough to log you out of that website. Always log out before closing the window.
    - Be aware of options that are often automatically selected which allow you to "stay logged in" or ask the computer to "remember me." These options should not be used on public computers.

**Security**

- E-mail is not a secure form of communication.
    - Never send credit card numbers or your social security number to anyone in an e-mail.
    - Be aware of the difference between the "reply" and "reply all" options. Often people send personal information to large groups of people by choosing the wrong option.
- Never give out your password to anyone via e-mail or over the phone. Companies do not need this and typically do not ask people for this information.
- Only give information to a website if you know and trust the site. Look for the lock icon or "https" at the beginning of the address to indicate the site is secure.
    - The sign in page of Amazon.com is a secure website.
    - Most banking websites are secure.

**Viruses**

- A virus refers to code written to interfere with the use of the computer.
    - Viruses spread to programs and other computers.
    - Note: a viral video refers to a popular video. This is not a virus.
- What do viruses do?
    - Some viruses delete data from the infected computer.
    - Other viruses corrupt or change the data on the infected computer.
    - Some of the worst viruses crash the infected computer completely.

- How do you get a virus?
    - A virus is usually acquired by downloading a file containing the virus onto the computer.
    - This often happens when opening an e-mail attachment.
- Be aware of the following:
    - E-mails may appear to have been sent by a friend or someone in your contact list but actually originate elsewhere.
    - Some viruses can send themselves via a person's e-mail from an infected computer.
- How do you know you have a virus?
    - If files suddenly disappear or are corrupted, this may be a sign that you have a virus.
    - Some viruses are not noticeable to the average user.
- What should you do to prevent getting a virus or to get rid of a virus?
    - Download, update, and routinely run antivirus software. Many quality options are available for free.
    - If you get a virus you cannot seem to get rid of using antivirus software, expert computer service may be required.

**Phishing**

- A phishing e-mail is an e-mail that asks for personal information or money or which contains a link to reset or enter a password.
- The goal of these e-mails is to acquire personal information or passwords which can subsequently be used in identity theft or to acquire money.
- Beware of any e-mail:
    - asking for money or bank account information
    - from a site you didn't subscribe to
    - with misspellings or misuse of words obvious of a non-native speaker
- Note: banks and most reputable companies do not contact customers via e-mail asking them to reset a password via an included link.
- If you receive an e-mail suggesting you reset your password and you want to be safe and reset the password:
    - Open a new tab or browser window.
    - Type in the Web address you know to be accurate for that company.
- Web sites can be spoofed. This means that people can create sites that are not affiliated with a particular company but which look close to or identical to the company's actual Web site.
- One way to detect a phishing e-mail is to look at the URL a link within the e-mail actually directs you to. The URL usually appears in the bottom left of the screen when you point at the link with the mouse.

**Tips**

- Think before you give out information online.
- Always ask yourself two questions:
    - What information do I want to share?
    - With whom am I willing to share this information?
- Create strong passwords and change them often.
- Avoid viruses and know what to do when you get one.

Jennifer Ranger, Digital Services Librarian