

## Overview of Competency 2.02

- I. **Personal Online Internet Safety Guidelines**
  - A. **Online Disclosure of Personal Information**
    1. **Full name** – use androgynous nicknames and screen names instead of real names, which can quickly and easily be used by predators to steal personal information or locate a physical address of a potential victim
    2. **Home address** – generic or specific information can be used by predators to hone in on potential victims
    3. **Phone number** – a phone number can be used in a reverse search on the Internet to identify the addresses of potential victims
    4. **Social security number** – online disclosure of social security numbers is extremely hazardous and provides unwanted access to predators and hackers who steal financial, medical, and other personal information
    5. **Disclosure of passwords** to friends, relatives, and coworkers should be avoided. The greater the number of people with access to personal information, the greater the risk
    6. **Disclosure of the names of family members** is another trick used by predators and hackers to zero in on potential victims
    7. **Credit card information** should only be disclosed to trusted, verified, and secure sites
    8. **Photographs** are potential sources of risk because they can be used by predators to decipher the locations of potential victims. Photographs can also be edited to falsify information, such as to make fraudulent identification cards
  - B. **Social Networking and Online Chatting**
    1. **Behave properly when online**
      - a. Employers and college scouts are frequently turning to online social networking sites to assess the behavior of potential candidates
        - i. Inappropriate pictures of partying and illegal behavior may be viewed by future employers and can prove fatal to one's employability potential

## Overview of Competency 2.02

- ii. Your online reputation is valuable
      - b. Posting fraudulent and harmful information about someone on the Internet and especially on social networking sites can have disastrous effects
        - i. Fraudulent and malicious information posted on the Internet has resulted in many teen suicides across the country
        - ii. Act responsibly
    - 2. **Safety guidelines and precautions:**
      - a. Avoid yelling (keying in all caps) when chatting online. Keying in all caps symbolizes anger and should be noted as a possible warning sign. If yelled at, close the connection
      - b. Bullying – spreading malicious and false information.
        - i. In all cases, it is best to first ignore a bully
        - ii. If a situation escalates or a bully does not stop, the victim should contact school authorities and inform parents/guardians immediately
      - c. Explicit material – any material that is considered adult or explicit or that makes the user feel uncomfortable
      - d. Never meet someone in person that you have met online
  - C. **Financial safeguards**
    - 1. Do not open emails or respond to sites that promise you will get rich quick or anything else that seems too good to be true. These emails and sites are most often screens that spammers use to access personal and financial information which they then sell to other companies or use with malicious intent
    - 2. Do not give out credit information without parental permission and only when the site is certified as secure
      - a. The URL of a secure site begins with **https:** - the “s” indicates a secure site
      - b. An interactive lock is displayed on the site, usually in the bottom right or left-hand corner. Make sure the lock is interactive and read the contents of the link!
      - c. A seal is another indication of a site's safety. If there is a seal, inspect it and make sure it is authentic
- II. **Potential Computer Hazards**
  - A. **Virus** – a small piece of software that attaches to programs that are installed on a user's pc. Some viruses will automatically replicate themselves and spread to other computers. An email virus has the potential to automatically mail itself to dozens of people in the user's email address book
  - B. **Spam** – unwanted and unsolicited email advertisements or messages
  - C. **Spyware** – malicious software designed to take partial control of a computer's operations without the consent of the user.
    - 1. Some spyware intercepts and records passwords and credit card numbers
    - 2. Tracks a user's visits to different web sites to analyze their spending activity and forecast consumer behavior