A Brief Guide to Internet Safety

1. **Avoid viruses.** A virus can harm your computer or access information on your computer's hard drive. Use virus protection software and do not download E-mail attachments from somebody you do not know, or download programs from websites that you do not trust.

2. **Avoid pop-ups.** Pop-ups are ads that may appear outside of your browser window when you visit some websites. They may contain buttons, links, flashing lights, animation, or sounds. Avoid clicking on pop-ups. Use the "F6" key to close any pop-up windows.

3. **Block cookies.** Some websites store your information using "cookies." Cookies store your data and may recall your data whenever you visit a website. You have the option of adjusting your security settings to block cookies, but some websites do require cookies to function.

4. **Use secure web pages.** If you are providing sensitive information, such as credit card information or personal information, be sure that the form you are using is secure. Only enter information into websites that you trust.

5. **Use secure passwords.** Choose a password that is at least 6 characters long and includes both numbers and letters (capital letters and lowercase letters). Never choose an obvious word or phrase such as your name, the name of the website, your username, or "password." An example of a good password would be "imGR4ud." In order to protect your password, change it frequently.

6. **Beware of phishing.** If you receive an E-mail from somebody you do not know, use caution when responding. Be sure the E-mail is legitimate, and do not give out any personal information. If you are not sure about an E-mail, ask for assistance. Check the URLs of any links provided to be sure they are legitimate. If you believe the E-mail is not legitimate, do not respond.

7. **Avoid scams.** If an offer seems too good to be true, it probably is. Use the same caution when interacting with strangers on the Internet as you would interacting with strangers on the street. Avoid the check-cashing scams, false offers of employment, or untrustworthy requests for personal information that are commonly found on websites such as Craigslist.

8. **Avoid using debit cards.** If you have a credit card, do not use your debit card when shopping online. It is more difficult to recover these funds in case of theft. Only enter your debit or credit card information on a secure website.

9. **Protect your personal information.** When you receive a request for personal information, be cautious about sharing it. Never transmit your social security number on the Internet, and be cautious when sharing information such as your full name, birthdate, address, or phone number. Only enter your credit card information on a secure website.

10. **Understand your privacy.** Information transmitted on the Internet should not be considered private. Use caution when publishing any personal information or pictures on social networking sites, websites, or blogs, because this information may be visible to others, including a family member, a coworker, an employer, or a total stranger. Once information is online it may be difficult to remove.

For more information, check out these links:

A webinar Internet safety hosted by CTN's Executive Director, Kami Griffiths: http://bit.ly/onlinesecuritywebinar

An online curriculum on Internet safety with great information on recognizing phishing scams and protecting your identity: http://bit.ly/Internetsafety