Internet Safety Tips

7. Don't open email messages unless you know the sender. Delete suspicious email messages without opening them. Some indicators of suspicious email messages are:

    - You don't know the sender.
    - You did not subscribe to receive email messages from the sender.
    - The message has no subject.
    - The message has gross misspellings in the subject.

8. Don't click on any links or open any attachments in email messages unless you:

    - Know the sender, AND
    - Know where the link leads or what is in the attachment, AND
    - Know that the sender intentionally sent you the email message with the link/ attachment.

Internet Glossary of Terms

Internet – a global system of interconnected computers that consists of millions of private, public, education, business, commercial, and government networks. The World Wide Web (WWW) is part of the Internet.

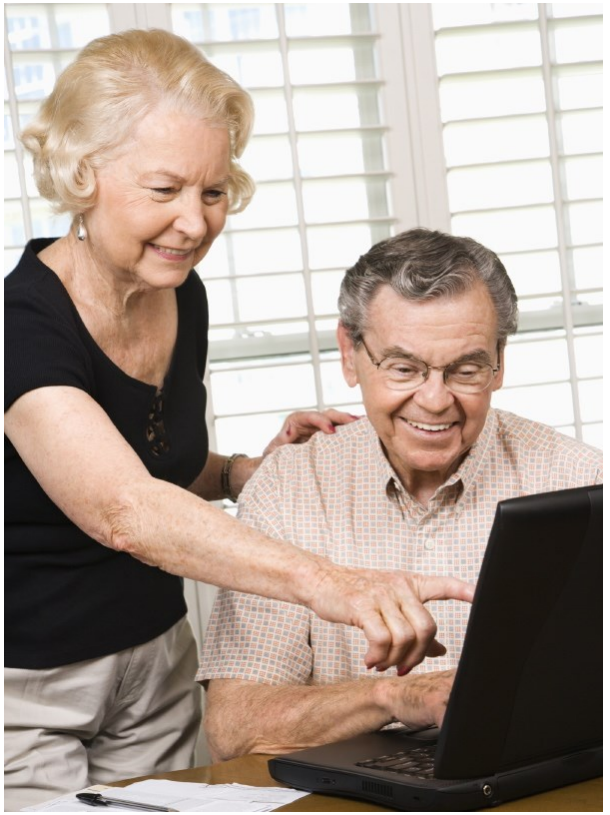
Browser – a software program used for viewing, navigating, and interacting with the Internet. Popular Web browsers include Mozilla Firefox, Google Chrome, Internet Explorer , and Safari.

Hyperlink – used to link one location on the Internet to another. When you click a hyperlink on a webpage, the Web browser will navigate to the website address embedded in that link. Some hyperlinks show the entire website address, like www.google.com, while other hyperlinks hide the full website address and have alternate text, like Google.

Download – transfer a copy of a file located on the Internet or attached to an email message onto your computer. Common download files include pictures, documents, music, and software.

Upload – transfer a copy of your file to a location on the Internet, or attach a file to an email message. Common upload files include pictures and documents (like resumes).

Internet Safety



Prosser Public Library

1 Tunxis Ave, Bloomfield, CT 06002

www.prosserlibrary.info

860-243-9721

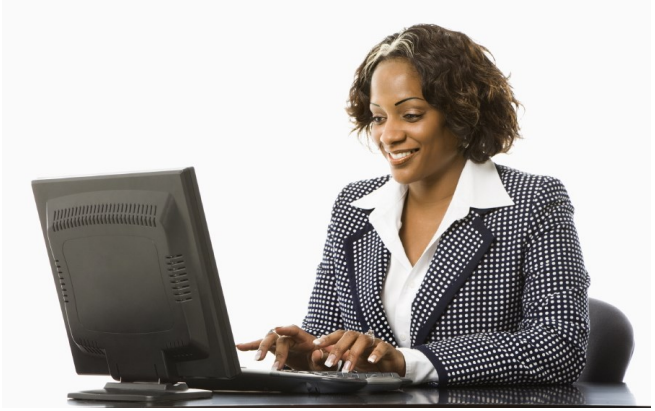
Internet Safety Tips

1. NOT everything on the Internet is true! There is a lot of *mis*information on the World Wide Web. Look for legitimate websites maintained by reputable sources. If you're not sure, ask a librarian!

2. Use caution when clicking on links or advertisements, as they may lead you to malicious or fraudulent websites. Many advertisements are designed to look like part of the website you are currently viewing and trust; however, the advertisements contain links to third party websites that may not be trustworthy. Don't click on pop-up advertisements. Look for an X in the top right corner to close the pop-up window.

   If you hover your mouse pointer over a link (or advertisement) without clicking on it, the website address embedded in the link will appear on the screen, either near the link itself or at the bottom of the browser window. Even if the text of the link looks legitimate (it may even look like a URL), the only way to know for sure where it leads is to hover your mouse over the link before clicking on it.

Internet Safety Tips



3. Keep the antivirus software on your computer up-to-date to help identify potential threats to your computer.

4. Never download files from a source you do not recognize or trust. Utilize well-known companies (like Adobe or Microsoft) when downloading free software, and be sure to download the file directly from the company's own site, not a third party site (pay attention to the domain name). Be aware of imposter sites and third party sites whose download files are not vetted. For reviews on antivirus and other software, visit www.pcmag.com or www.cnet.com, which are both reliable resources for computer information and software reviews.

Internet Safety Tips

5. Never submit your personal information online (address, phone number, credit card, etc.) unless you are sure that the website is legitimate and has a secure and encrypted connection. Look for HTTPS in the web address, which indicates a secure connection. Only make online purchases from trusted, well-known companies that have professional looking websites and obvious contact information.

6. Be wary of websites, advertisements, or email messages that offer a reward or prize in return for your personal information, or issue bogus warnings intended to alarm and trick you into revealing personal information. You can't win anything if you didn't purposefully enter a contest. If you have never heard of the company and/or have never associated yourself with the company in the past, then most likely it is a phishing scam or has other fraudulent intent.

7. Use strong passwords that include a combination of lower and upper case letters, numbers, special symbols (like !,@,#,$, or %), and are at least 8 characters long. It is good practice NOT to write down your passwords, and definitely never keep passwords near your computer or in another obvious spot. Do not divulge your password to anyone, in person or online. When entering a password online, look for HTTPS in the web address, which indicates a secure connection.