

CWS

community workshop series

University of North Carolina at Chapel Hill Libraries
Carrboro Cybrary | Chapel Hill Public Library | Durham County Public Library

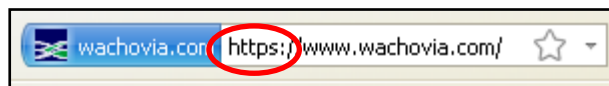
ONLINE SHOPPING AND PREVENTING IDENTITY THEFT

Things to do before you begin shopping online:

- Contact your bank and find out what their policies are regarding identity theft. Also, find out the policies for your credit cards.
- Consider installing anti-virus software on your computer. Antivirus software for one computer is typically less than \$50, depending on the brand and protection period (e.g., some antivirus software is only good for a year); it is also often possible to buy a software “bundle” so that you can install the program on more than one computer (typically more expensive than for one computer, but less expensive than buying software for each separately).
- The most popular brands of anti-virus software are Symantec/Norton and McAfee. You can buy anti-virus software anywhere computers are sold. Talk with a sales associate at a computer store in order to determine which program best suits your needs.
- Note that after you install an antivirus program on your computer, you will need to update it frequently (most programs will do this automatically), as computer viruses—just like real viruses—can change.
- Be aware of the variety of scams that appear on the Internet. As a general rule, if you get an offer from an unknown e-mail address (or even an email forwarded on from a friend!) that sounds too good to be true, it most likely is.

Things to pay attention to while shopping online:

- Shop on secure websites. When you log in with your account information, a secure website's address will begin with "**https://**" instead of "**http://**". This stands for a secure HTTP connection. If you are using the Windows operating system, a padlock should appear in the lower right-hand corner of the screen of your internet browser window. Many sites will also have some form of a verification symbol to show that company complies with the highest form of encryption and security.
- Always read a website's privacy policy before providing any information. If something doesn't sound right, don't give them your information! You wouldn't hand your credit card to just anyone on the street, so don't do it online. Making websites is easier than you think!
- Smaller websites often use PayPal, an external company that exclusively handles online purchases. Using PayPal is generally considered safe, but always read the privacy policy and beware of imposters!



- PayPal and other websites will *never* ask for your credit card number or other personal information by email, so never trust emails that request this information, even if it appears the email came from PayPal or Amazon.com. Also, don't click any of the links in the email if it requests this sort of information—it's probably a scam.
- Deal with businesses that are accredited by the Better Business Bureau. Businesses that are accredited by the BBB are committed to solving consumer complaints. These businesses assure a method of recourse if something goes wrong during your transaction.
- If you're not sure, stick to the websites of large companies you're already familiar with—they're more likely to have a secure website. For example, Target.com or Bestbuy.com. Other popular online shopping sites include Amazon.com (books, music, etc.), Zappos.com (shoes), Etsy.com (DIY apparel).

Other things you can do to protect your identity:

- If you have anti-virus software on your computer, be sure to periodically update it. This will keep newer viruses from infecting your computer.
- Do not open .exe files sent to you via e-mail if you do not trust the source. .Exe files can install malware on your computer that can be difficult to remove.
- Anti-virus software will sometimes remove links from e-mail messages if they have been flagged as malware (spam). If you occasionally get e-mails missing links, your anti-virus software is working!
- Do not forward chain e-mails. Chain e-mails often prey on sympathy, contain jokes, or vague threats (i.e. "someone will die of cancer if you do not forward this"). Computer programmers can collect e-mail addresses and information from these e-mails, so it is best to ignore them.
- Firefox is generally considered a more secure browser than Internet Explorer (though newer versions have improved security). Use a secure browser when making purchases online, and avoid storing passwords and personal information on your computer.

Helpful Links:

www.safeshopping.org – an information website maintained by the American Bar Association that has more information about how to stay safe while shopping online.

www.ftc.gov – the Federal Trade Commission has excellent information listed within the “Consumer Protection” tab, under “Consumer Information”

<http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams.htm> – a list of the top ten e-mail scans in 2009

<http://anonymizer.com/> – software that allows you to encrypt your computer and hide your IP address

www.annualcreditreport.com/ – a secure website that will allow you to see your credit report for free. NOTE: Not all of the services on this website are free—make sure you choose the FREE credit report. We suggest using this as opposed to the freecreditreport.com website.

View our full schedule, handouts, and additional tutorials on our website:

www.lib.unc.edu/cws