COMMUNITY WORKSHOP SERIES

DIGITAL LITERACY FOR ALL LEARNERS

A PARTNERSHIP WITH UNC SILS AND LOCAL LIBRARIES

CWS.WEB.UNC.EDU

Internet Security & Privacy

To complete feedback forms, and to view our full schedule, handouts, and additional tutorials, visit our website:
cws.web.unc.edu

Password Security

We use passwords for a wide variety of interfaces throughout our lives, such as email accounts, computers, web applications, bank accounts, etc. Are your passwords secure? Try testing them here:
https://howsecureismypassword.net/

Saving Passwords

After you've got a secure password, don't just leave it on a sticky note in a drawer. Try one of these password managers:
https://www.dashlane.com/
https://www.lastpass.com/
http://keepass.info/download.html
https://www.keepassx.org/downloads
https://www.pwsafe.org/index.shtml

Virus Software

If you don't already have virus protection on your computer, you need to install it immediately. There are many options.

For a comparison of a few different products:
https://www.pcmag.com/article2/0,2817,2372364,00.asp

If you're looking for free virus protection software, here are two options:
Avast (https://www.avast.com/)
AVG (https://www.avg.com)

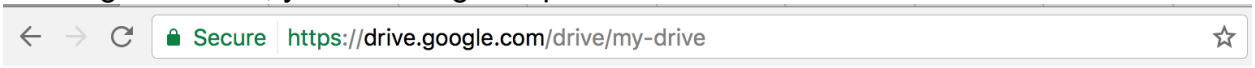
SSL Certificates

An SSL Certificate provides secure and encrypted communication between your web browser and the web server. The certificate is obtained for the domain, providing the owners with a cryptographic key. Any data (credit card numbers, addresses, social security number, etc.) submitted over a website with an SSL certificate will be an encrypted transmission to protect your data and information.

It's always good to visit websites with SSL certificates because you know that they are who they say they are; however, it's exceptionally important when submitting sensitive data.

So, how do you know when you're on a website that has an SSL certificate?

1. The web address will include https:// instead of http:// so look for the "s"
2. In Google Chrome, you'll see a green padlock to the left of the URL



If you're using Google Chrome, you can also add an extension called HTTPS Everywhere that will automatically switch websites to https wherever possible.

https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en

Ad Blockers

Even after you've checked for an SSL certificate and downloaded virus protection software, you might still encounter issues with popups and advertisements that redirect you to new sites. These are prime locations for you to encounter viruses. Here are a few options for browser extensions that will block ads and popups to protect your computer.

uBlock Origin (https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/) Firefox
Privacy Badger (https://www.eff.org/privacybadger) Chrome, Opera, Firefox
AdBlock (https://getadblock.com/) Chrome, Firefox, IE, Opera, Safari
Popup Blocker Pro (http://popup-blocker.org/) Chrome

Keep in mind that some websites might require you to disable your ad or popup blocker in order to view their content because they receive revenue through ad services.

Privacy & Search Engines

Most search engines are using data from your searches and constantly attempting to nudge you towards certain possibilities, primarily towards sites that provide the browser with money. They often know more about us than we realize.

If you're concerned about your privacy when using search engines, try DuckDuckGo, which doesn't track you. https://duckduckgo.com/

Alternatively, you can use a browser extension that will run additional searches in the background to confusing any algorithms or other analytical mechanisms.

TrackMeNot (https://cs.nyu.edu/trackmenot/)

Backing up Data

We can backup data to a "physical" location or we can use a cloud server. An easy way is to back up files to a thumb drive or hard drive. Just copy the files over the same way that you would with any other device.

To backup files to the cloud, you'll need an account with a cloud server, here are some examples.
https://drive.google.com
https://www.box.com/
https://www.dropbox.com

You can also use a backup program that will automate your back up. Two options that are already included on your computer, included Time Machine for Mac OSX or File History on Windows.

For step-by-step instructions on backing up files: http://www.wikihow.com/Back-Up-Data

Encrypting Your Data

Some of the files on your computer might contain sensitive information. You can protect these files with a password by encrypting them. You can also encrypt your entire hard drive.

Windows and Mac OSX both have innate programs to encrypt your hard drive. You just need to activate them. In Windows (Vista or later), you can use BitLocker. In Mac OSX, you can use FileVault.

Turning on BitLocker: https://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx#BKMK_S3
Turning on FileVault: https://support.apple.com/en-us/HT204837

Other Encryption Software:
Vera Crypt https://www.veracrypt.fr/en/Home.html

Privacy and Protection for Your Cell Phone

A few things to remember:

- Your cell phone doesn't have anti-virus software, so you should always avoid sending sensitive information using your cell phone
- If you're connected to an unsecured network (you didn't put in a password to connect), the data and information that you share over the network is not secure

Try using Signal for end-to-end encryption of your text messages and calls.
https://whispersystems.org/