

Cyber Safety



The Web is a powerful tool that is often essential for getting along in today's society. Remember to stop and think before sharing personal information. This handout offers tips for staying safe online. For more information, visit stophinkconnect.org.

Emails

Links in emails may lead to harmful viruses and malware. Use your best judgement before clicking on a link in an email. Even if the message is from someone you know, it could contain a malicious link or attachment. Some scams use a person's contact list to spread a

bad link, knowing the recipient will be more likely to click on a link if it is sent from someone they trust. If you are unsure about a link or attachment, do not click on it. An email apparently from a trusted source that contains a bad link or attachment is known as a phishing email.

Banks and creditors are not going to ask you to email in your social security number or other sensitive information. If you receive an email asking for this kind of information, it is probably a scam even if it looks like it came from your bank. You can always open a new window and sign into your bank account, or call your bank to update information. If there is a link in an email like this to sign into your account, you do not need to click on it. Open a new window and type in your bank's address to safely get to their site. Watch out for emails that claim you won a prize, or that ask you to deposit a check. These are common scams.



Websites

Anyone can make a website, so think critically while you browse the Web and do not believe everything you read. Look for an About section on a website to learn more about who is behind the content you are reading. Know the components of a URL:

<https://www.staysafeonline.org/>

Notice that this Web address begins with <https://>. The S stands for secure. This means there is more encryption on this site than on one that starts with <http://>. Look for <https://> when you are buying something online. The .org part of the address is called a domain extension. Non-profit organizations often use .org, but this is not always the case. Educational institutions use .edu and government entities use .gov. Knowing that a site is run by a government entity or school is an indicator that you are getting good information. Include site:.gov (no spaces) in a Google search to limit results to government sites. For example, try searching: health site:.gov.

The Web continues to get more and more social. Limit the amount of personal information you share online. Think twice before posting something. Once it is out there, it can remain public forever.



Elmwood Park

PUBLIC LIBRARY

explore. connect. create.

Passwords

Make your passwords strong by using combinations of uppercase letters, lowercase letters, numbers, and special characters. Long passwords that do not use any dictionary words are harder to crack. Avoid using easy to guess passwords and avoid re-using passwords for multiple accounts. Keep a physical list of your passwords to help yourself remember, rather than a "passwords" file on your computer or device.



To avoid using dictionary words, try taking the first letter of each word in a phrase. For example, you could take the phrase "It sure is a nice day for a bike ride" to make the password Isiandfabr. Add numbers and special characters and you have a strong password. Change your passwords regularly. If you have any reason to suspect someone has gained access to your account, immediately change your passwords. Even under normal circumstances, it is a good practice to change your passwords on a regular basis.

Sign out of everything when you are finished using a public computer. You may find it convenient to remain signed in on your personal devices. When using a public computer, you should always log out of everything and log off the computer when you are done. Close or deactivate accounts that you do not use anymore. If you are sure you will not use the account again, cancel the account rather than letting an inactive account hang there.

Shopping

Online shopping is very common and convenient. Be smart about where you are shopping and where you are entering sensitive information. If you are unfamiliar with a seller, look at reviews from other buyers before buying. If something sounds too good to be true, it might be a scam or there might be a catch. Look for the https:// in the URL before you enter your credit card information. A site using the https:// protocol offers a more secure transaction. Avoid saving your credit card information on websites.

Calculate your risk

Complete this short quiz about your habits online to calculate your online identity risk:

<http://www.emc.com/microsites/fraudgame/flash.htm>

Online privacy

If you want to keep your browsing history private, consider these tools for extra protection.

Adblock Plus

Blocks banner ads, pop-ups, tracking, malware, and more. This extension does not block every single ad, only intrusive materials. Learn more and install for all the major browsers here: <https://adblockplus.org/>

DuckDuckGo

Search the Web without being tracked by the search engine and without having your search history saved. Learn more and start searching here: <https://duckduckgo.com/>





Ghostery

Block trackers on websites by using Ghostery, which is available for all the major browsers and has its own mobile browsers for Apple and Android. Learn more here:

<https://www.ghostery.com/>

HTTPS://Everywhere

This browser extension for Chrome, Firefox, and Opera encrypts your activities whenever possible. Learn more and install this extension here: <https://www.eff.org/https-everywhere>

Internet Noise

When you click "Make some noise" on this site, your browser will open new tabs and perform random searches on the Web until you close it or tell it to stop. The idea is to render your browsing history useless to advertisers. This does nothing to encrypt your activities. Try it out here: https://slifty.github.io/internet_noise/index.html

Privacy Badger

This browser extension for Chrome, Firefox, and Opera blocks advertisers when they try to track you across multiple sites. Learn more and install this extension here:

<https://www.eff.org/privacybadger>

Tor browser

Tor lets you browse the Web just like Firefox, Internet Explorer, or Chrome. The difference is that Tor routes your traffic through a series of relays so the sites you visit do not learn your actual physical location. This does result in a slower browsing experience. Learn more about Tor and download it through their website:

<https://www.torproject.org/projects/torbrowser.html.en>

Questions? Contact Adult Services at askref@elmwoodparklibrary.org or 708-395-1217.