Defend your Online Privacy

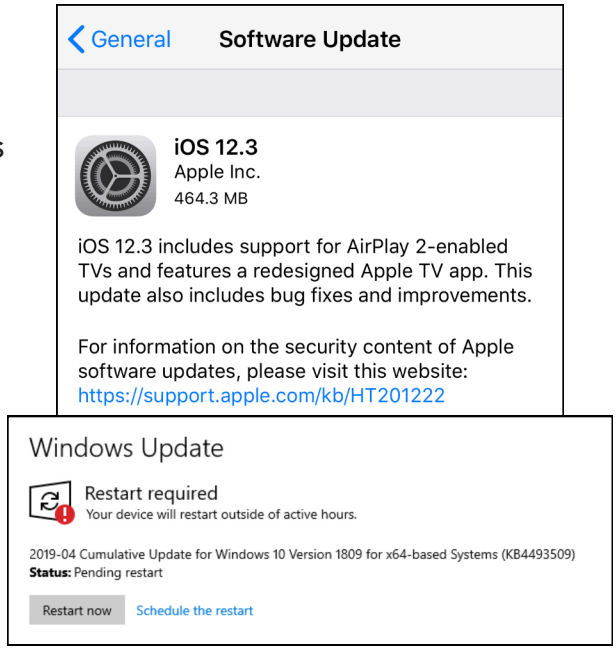
Tips and tools to increase your safety online

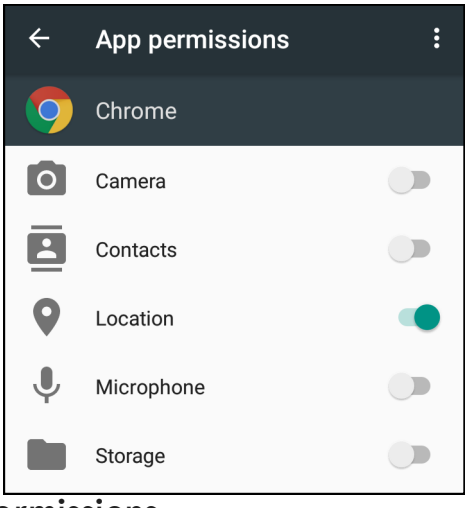
Delaware County District Library

This handout is designed to give you an overview of some tools and techniques you can use to better help yourself defend against the dangers of online life. Nothing on this list is 100% fool proof. But the more of these you use, the less enticing of a target you will become and can lower the damage done to you if you do become a target.

Software and Device Updates:

Keep you devices, antivirus, and apps up to date. These fix problems with the app that can leave you vulnerable to attack. These updates often bring with them new and helpful tools in addition to the fixes for older problems.



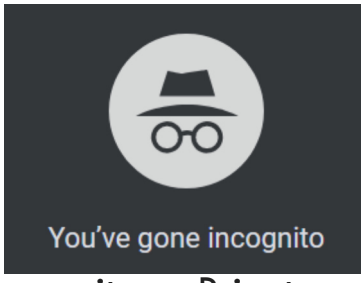


Permissions:

Apps need your permission to use certain features of your device. Carefully consider what you grant permission to. Does that mobile game need your location? Does that calendar app need to access your camera? There could be good reasons for these, but sometimes apps ask for more than they really need to function.

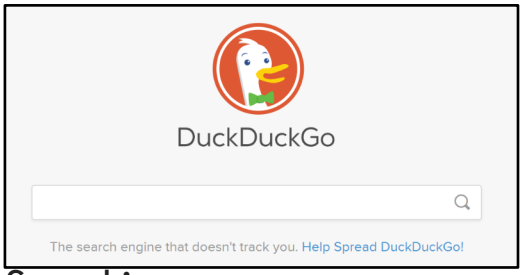
HTTPS:

When searching the web, always check that you're sending vital information over the internet only on a secure, encrypted page. Check the URL of the webpage your on. You should see either a lock or https:// at the start of the URL. This indicates your connection is encrypted and you're information is being sent securely to the website you're using.



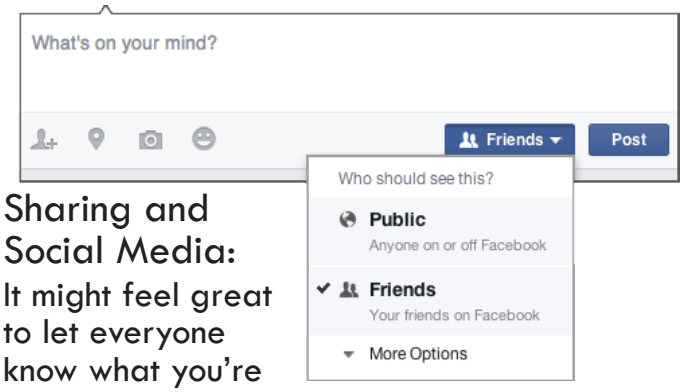
Incognito or Private Mode:

Using a private window or incognito mode will prevent the things you do on a public computer from being stored on that computer where the next person could find it. This does not make you invisible online, but merely prevents someone else from seeing what you were doing once you lave that computer.



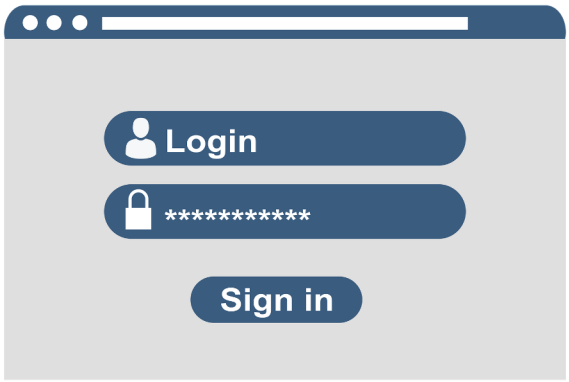
Searching:

Many search engines track your results and questions for advertising purposes. DuckDuckGo is a privacy focused search engine that won't track what you look for and won't sell that information.



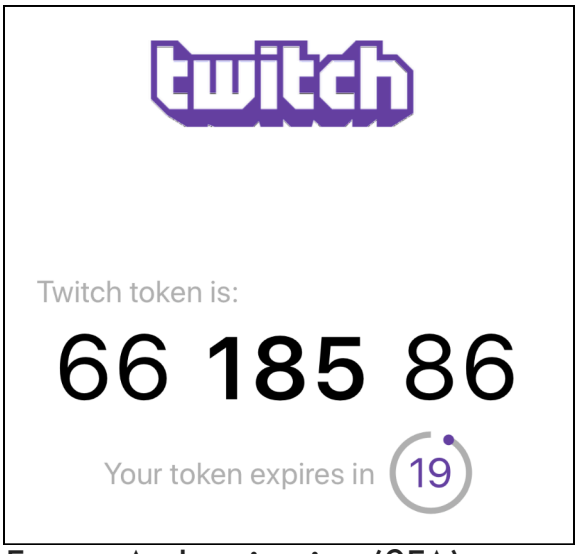
Sharing and Social Media:

It might feel great to let everyone know what you're up to, but consider what you're telling and to who. Are you broadcasting publicly to the entire internet that you're at the beach for a week? Are you sharing intimate information publicly or with just friends? Are your friends people you really know or is it a group of strangers you don't know.



Password managers:

Using a strong, unique password for every website becomes easier if you use a password manager. This tool, like Bitwarden, requires you to know just the one password to gain access to your secure vault of passwords. From there the tool will allow you to store and manage all your passwords, making them secure and strong so you don't have to keep track of hundreds of unique passwords on your own.



Two Factor Authentication (2FA):

An extra security step with logins can be to enable 2FA on your accounts. If enabled, the website will text you a secure code to verify you're really you when logging in. You can also use an authenticator app to provide you a constantly rotating code to use with your logins. This method relies on someone not just knowing your password, but also having your authenticating device on hand when logging in.

Phishing:

Phishing is a term used to describe any attempt to get information from you through deceptive methods where the attacker relies on your trust. It's a digital con game. Often they will reach out acting as either someone in particular that you know, or as a company you might expect to have business with and ask for verification of information. Whether it's login information, financial accounts, addresses and phone numbers, or some other kind of identifying information. Often these are done through email, but can be done through any kind of messaging system. They key things to look for are logos that don't look quite right, misspellings and poor grammar, poorly arranged emails, phone numbers that don't look right, and other things that feel generally off. They often rely on a false sense of urgency, so always be sure to take a moment to step back and gather yourself before responding.