Tech Coach Corner — General Rules for Mobile Security

By LTCL Librarian Karen Scott

With mobile devices like phones and tablets becoming more complex, you might consider them tiny computers. Well, you're not wrong. These tiny computers should be used with security in mind just like you would on a personal computer. Whether on a personal computer or mobile device there are general rules you can follow to keep yourself and your information safe.

Use your head and your gut for judgement

If something looks suspicious it probably is. This might be hard to embrace if you didn't grow up with technology and the internet like I did, but there are signs that can tell you something isn't right. For example, misspelled words, email addresses not matching the name of the sender, password resets you didn't ask for, and attempts to gain sensitive information are big red flags. You can read the tech coach column on phishing for more information about these clues.

Use strong passwords

Strong passwords use uppercase and lowercase letters, numbers, and special characters. The more complex the password, the better! If you want to take it a step further, pass-*phrases* are even more secure, when used with numbers and special characters. For example, "iced tea is great for summer" becomes ic3dT!sgr84$umm3R. It is best to avoid consecutive letters like "qwerty" or "bbbbb." Lastly, you can make the password on your mobile device more secure by enabling the 6-digit or alphanumeric passcode on your iPhone and using the alphanumeric password on your Android device rather than the default swipe-shape. It is also smart to use a different password for each account and change your passwords periodically.

Enable two-factor authentication

Two-factor authentication allows you to receive a code as a text, phone call, or email when logging into a website or service. You use this code to verify that you are the person logging into your account. This is useful to prevent anyone who isn't yourself from logging into your email account, bank account, or any other website that you want to keep secure. Read more about two-factor authentication here.

Keep your devices and applications updated

Updates for devices and applications sometimes have security patches and upgrades that are crucial for the safety of your device. Major security fixes will be force-installed, meaning you won't have the option of skipping it. Companies also stop servicing older versions of software and hardware, so, if your device or app is out of date there is a chance it will stop working all together. For example, the video conferencing company Zoom introduced a new update policy that states, “Customers will be required to update their Zoom software to ensure it is no more than nine months behind the current version, at any given time” and will disallow users running older versions from using the app.

Don’t submit sensitive information over insecure/unknown networks

Public networks aren’t secure. This means if you log into an unencrypted website your information may be visible to others. You might not be concerned about one website, but this vulnerability could make *all* of your information up for grabs—especially if you use the same username and password on multiple sites. Scammers could also use your info to try to scam others on your contact list or even steal your identity. To stay secure and private, you can use a VPN app or just use your cellular data if possible.

Navigating the web safely can be a daunting task, so don’t be afraid to reach out if you have any questions!

Tech Coach Assistance

Tech Coaches are now providing remote Tech Coaching. Simply send an email to techcoach@laketravislibrary.org and one of our coaches will respond to assist you with any questions or challenges you may have.