# Android Club - Security Discussion - Feb. 20/17

**Knowledge is security**. There are no "magic programs or services" that will protect you from every threat. Be vigilant when online! You received a gift, an invitation or are asked to perform a specific action to your computer. Have the good reflex to ask why ..or ..do I know the person who's asking me this? Don't be afraid to decline or ask more information. Browse the web with care and try to resist your curiosity .. don't fall for clickbait.(links designed to catch your interest)

**Password protect your devices** - especially mobile devices such as phones and tablets.
Use a strong, unique password for every website. Installing a password manager can help you with this. LastPass - https://www.lastpass.com/

**Keep programs**(apps) and your operating system **up to date**.

**Antivirus software** - use them..but don't let them give you false sense of security. Run regular scans with your anti-virus program. Layered security is important. Run on demand anti-malware software alongside your traditional anti-virus solution.
AdWcleaner is an easy to use and free anti-malware program.
https://toolslib.net/downloads/viewdownload/1-adwcleaner/

**Use email wisely.** Email is a great way to keep in touch with friends and family, and as a tool to conduct business. Even if you have good security software on your PC, however, your friends and family might not have the same protection. Be careful about what information you submit via email. Never send your credit-card information, Social Security number, or other private information via email.
Phishing - Never click links in emails or texts that seem to come from your bank, the CRA, Paypal or any other institution. If you think the message might be valid, log into your account directly, without using the supplied link.

**Downloads** - If you must download the latest movie, song or game, think twice about where you are downloading it from. Is the site well-known? Have any of your friends used the site without incident or unexpected surprises? Is it actually the site you think it is rather than a clone? Check your browser for a padlock or a URL beginning with https:// for some certainty and don't ever visit a download link sent you via email.

**VPN** - Be cautious when using public wi-fi. ie., cafes, ferries, airports, schools, libraries etc. It is recommended to use a VPN(Virtual Private Network) when connecting to the Internet on a public wi-fi network....especially if doing anything sensitive such as banking.

Witopia is one such paid and respected VPN service -  https://www.witopia.com/

Opera web browser now comes with VPN "built-in" and is free - http://www.opera.com/blogs/desktop/2016/04/free-vpn-integrated-opera-for-windows-mac/

Opera VPN for Android - https://play.google.com/store/apps/details?id=com.opera.vpn&hl=en

**Shop safely.** If you plan to order from an online store, be sure that the Web site uses secure technology. When you are at the checkout screen, verify that the Web address begins with *https.* Also, check to see if a tiny locked padlock symbol appears somewhere on the web browser screen at checkout, or that there is a statement on the checkout screen stating that the pages are secure with a security technology.

**<u>Don’t forget to keep back ups!!!</u>** Backups in their most basic form are simply copies of files. Any important files should be backed up..either to a removable device such as a portable drive or USB stick...or online in the "cloud".

**Android devices - Remotely ring, lock, or erase** a lost Android device. This can be activated in your Device Manager Settings. GPS must be turned on.
Important: Android Device Manager won't work for devices that are turned off, or that don't have a Wi-Fi connection or mobile data connection with an active SIM card.

https://support.google.com/accounts/answer/6160500?hl=en