October is Cyber Security Awareness Month. Here is a list of basic things you can do to significantly increase your cyber resilience:

1) **Enable multi-factor or two-factor authentication** where possible when accessing external resources

2) **Use a modern anti-virus and malware detection system**. (i.e., https://www.malwarebytes.com)

3) **Create passphrases** with special characters and numbers instead of using passwords (i.e., "Th1sistopsecretstu44!") **do not use this passphrase, create one unique to you**

4) **Use a password manager** (i.e., https://LastPass.com)

5) **Regularly backup your data** on your phone and on your computer

6) **Update your software often**

7) **Never click on a link if you are not <u>100%</u> sure of its origin,** including links in text/SMS messages

8) **Avoid using public WiFi**; use mobile data from a cell phone as a hotspot for other devices (such as a laptop)

This online tool let users know if their password(s) has been leaked; it will also tell them exactly which password it was: **https://haveibeenpwned.com/**

This is a valuable resource to help mitigate the negative effects of password recycling: **https://www.avast.com/hackcheck/#pc**

CISA has some great guidance as well: **https://www.cisa.gov/uscert/ncas/tips**

The Government of Canada website has some great resources: **https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2020/10/cyber-security-awareness-month.html**

Cyber criminals are smart and creative; **when in doubt, check it out!** Don't be afraid to call someone who has e-mailed you something that looks suspicious and confirm that the e-mail they sent and/or a link that they shared is legitimate.