Best Practices for Cyber Security

Tips for Keeping You Safe

Computers & Laptops

- Keep all operating systems up to date
- Install one anti-virus program. Keep it updated, and run scans regularly*
- Install an anti-malware program. Keep it updated, and run scans regularly*
- Regularly check for updates to all current software programs. Uninstall programs that are out of date or no longer used.
- Keep your hardware up to date. Outdated computer hardware may not support the latest security upgrades and technologies. For example, an outdated network/Wi-Fi adapter may not provide the newest Wi-Fi standards thus preventing you from getting online.
- Lock your computer when stepping away from it, even momentarily. (On a Windows PC, press Crtl+Alt+Delete then Lock, or Windows Key+L)
- Scan external storage devices and backups for viruses and malware
- Never allow someone to use a computer while it is logged into your account. Have separate accounts for family members.

Passwords

- Use a strong password
- Never share your password
- Password protect all devices such as laptops, phones, etc.
- Use a unique password for every site online.
- Use a password keeper on your phone to keep up with them.
- Do not use common words, or information that can be commonly guessed. Do not reuse passwords.
- Only store your passwords in a secure location.
- Enable two-factor authentication on any account that provides this service.
- Do not use the option to 'Sign in with Facebook' or another social media account on websites.

Data

- Backup important data to the cloud, another computer, or an external hard drive. (Also, verify you can access your backup in case you need to restore them.)
- GNTC provides you with free cloud storage using OneDrive, where you can back up your data to.
- After you do a backup, purge your old files. Delete anything no longer needed.

Browsers

- Always keep your browser up to date
- Remove questionable extensions
- Make sure that you are using a secure website that starts with HTTP**S**.
- Hover over links to see exactly where they are sending you.

Emails

- Always use your GNTC email for all GNTC correspondence. Use a generic email for all social media, shopping, and general use.
- Do not click links in email unless you were expecting the email and know who it is from.
- Avoid opening suspicious emails
- Do not open unexpected attachments
- Misspelled words and poor grammar are warning signs to be wary of.

Wi-Fi

- Avoid using public Wi-Fi networks, or use a VPN when connected to one
- Always log off from public computers
- Ensure that your home Wi-Fi is password protected with a secure password.
- Adjust your Wi-Fi device settings so it does not automatically connect to nearby Wi-Fi networks

Social Media

- Limit the amount of personal information that you share on social media!

Mobile Phones

- Use a passcode for your phone.
- Keep the operating system on your phone up to date.
- Keep apps updated and delete and unused or rarely used apps.
- Be wary of apps that require access to information that is not relevant to the service
- Consider the amount of data that apps collect vs the benefits you receive in return.
- Turn off your Bluetooth when not in use.
- Put your phone number on the National Do Not Call Registry
- When transmitting sensitive data (personal information) using your cellphone data instead of Wi-Fi may be more secure

* Note: GNTC does not make recommendations for specific software for personal devices.

Take the time to Google and research additional ways for you to stay safe online.
