THE ULTIMATE GUIDE TO SECURING YOUR DEVICES & ACCOUNTS

KNOWLEDGEFLOW
CYBERSAFETY FOUNDATION

1 Device Security

- Make a list of all devices including: phones, laptops, tablets and other connected devices like security cameras, smart TVs, etc
- Ensure each device is configured with a custom, unique login password or PIN and a locking screen saver
- Be sure to enable automatic updates where possible

2 Account Access

- Avoid using a shared account and select an 'unguessable' password
- Ensure that you are the only one with access to each of your accounts
- Update any backup emails or contact info for your accounts. Remove any person you no longer want as your trusted contact
- In some cases, you may want to create new accounts. If so, remove any sensitive data from the original account.

3 Password Security

- Use a trustworthy password manager
- Passwords should be long and unique for each site and include a variety of numbers, characters, capitals, etc.
- Never store your passwords on shared devices or in your web browser
- Enable two-factor authentication or verification

4 App Settings

- Delete apps you don't recognize on your devices
- Review the permissions of each app, check access to:
  - location (ex; fitness tracker & weather app)
  - microphone and camera
  - notes, documents, photos, etc.
- Ensure that apps do not operate in the background and those that require connectivity request it every time

5 Back-Up

- Securely back up the data on your devices to make recovery from a crash or hack much easier
- Use an encrypted or password protected physical storage device (like a USB stick) which can be more secure than online storage if kept safe

6 Shared Devices & WiFi

- Remember to log out of your accounts if using a public device such as at work, school, or library
- Never save passwords to devices that are shared
- Be cautious using public WiFi when accessing sensitive accounts or entering personal information

7 Privacy Settings

- Ensure posts and accounts are set to 'private'
- Use a secondary account to check how your primary account 'looks' to the world and what the public can see
- Review all privacy settings on your phone and devices including online data storage and backups (like iCloud)
- Check the Find My settings (or others) to see if your location is shared with anyone

8 Check-In

- Regularly review your accounts and devices for suspicious activity and log-ins if technology permits
- Pay attention to new icons, installed apps and system tray icons that you do not recognize
- Use Virustotal to check on suspicious files and websites

9 Your Home Network

- Change the default name and password on your router
- Make a "Guest Network" on your router for your smart devices like speakers, thermostats, and alarms etc.
- Use such network separation to keep personal data away from less secure devices

10 Software

- Never disable built-in antivirus protection
- Consider supplementing with adblocking browser extensions and antikeylogger tools
- Run system updates & install security patches