

## **BASIC PROTECTION TIPS**

Never assume anything is safe online. If it looks too good to be true, it probably is! Never provide sensitive information on social media or via email. Be cautious of promises of money or rewards in ads and emails. Do not open attachments unless you are sure of the sender and purpose.

- Keep your computer and devices safe by installing and updating anti-virus and other programs.
- Think before you click on anything online or open email attachments to avoid malware.
- Back-up your pictures and documents.

### **ALWAYS STOP AND THINK**

**Think before you click on anything online, links, or open email attachments to avoid malware.**



#### **GET ANTIVIRUS AND KEEP IT UPDATED**

Antivirus is software to defend your computer and laptop against the bad stuff. New operating systems may actually come with antivirus already built-in and will even update for security- you'll simply need to restart to apply updates.

#### **APPLY SECURITY UPDATES:**

Security updates are a way for companies to patch up security holes hackers find in your software: antivirus, internet browser, operating system, device apps, and all other programs. Your software will prompt you to allow these updates. Simply follow the prompts or set the program to install updates automatically.

#### **BACK-UP YOUR DATA:**

Computers crash and phones and devices break and get lost. Simply use an external portable storage device or cloud services to back-up everything that is important to you. If you do stumble across something and make a mistake infecting your computer, you'll still have your important family photos and documents backed up externally.