Tech Smarts:

Below are some recommendations from the Federal Trade Commision (FTC) on best practices for keeping your (and your child's) personal information secure.

Keeping Your Personal Information Secure Online

Know who you share your information with. Store and dispose of your personal information securely.

Be Alert to Impersonators

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Safely Dispose of Personal Information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Encrypt Your Data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Keep Passwords Private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

Don't Overshare on Social Networking Sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Keeping Your Devices Secure

Use Security Software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Avoid Phishing Emails

Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Lock Up Your Laptop

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Read Privacy Policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

Another good resource is commonsensemedia.org. Here you will find articles and videos on a wide variety of topics with practical tips and guides illustrating ways to make the digital world safer for your loved ones.

Here is a link to a step by step tutorial on their site covering how to set up the security features on your child's iPhone:

https://www.commonsensemedia.org/blog/step-by-step-tips-to-set-up-your-kids-iphone