Family Data Security Recommendations
http://www.networkpaladin.org/#!personal-safety/cv24

Quick Reminders for using Mobile devices more securely

- B**e aware of what one can do with metadata**
  - Includes GeoTagging, Photo Time, Device Type, Username...
  - View Metadata Online http://regex.info/exif.cgi
- **Remove Metadata from photos**
  - Jpg and PNG metadata striper http://www.steelbytes.com/?mid=30
  - BatchPurifier LITE http://www.digitalconfidence.com/downloads.html

Modern phones keep information, even after deletion:

Text messages	Contacts (Facebook/Phone/etc)
Location data, Website usage	Location mapping/fencing
Email (including check frequency)	Photos (Including Geolocation)
Any applications ever installed	

- This information can be stolen simply by visiting a malicious website
- Call details can easily be spoofed
- Family Locator services can be use maliciously
- Open or Public Wifi is not secure - 7 year old can see what your are doing goo.gl/zCMXGp

How Can You Protect Yourself?

- Turn off Location Services Unless Needed **(Apple: Settings > Privacy > Location Services)**
- Lock your device **mobile or portable with a six digit code**
- Turn off Wi-Fi and Bluetooth unless needed **You are tracked from Taco bell to Home depot**
- Be wary of unknown numbers, odd calls or texts – **you don't *have* to answer everything**
- Texts can be forwarded indefinitely – **assume everyone will be able to read your texts**
- Never reveal personal information (**mobile numbers, passwords, zip codes etc) online or to store clerks**
- Be aware of indicators of a hacked phone: terrible battery life, high battery temperatures, unusual coded messages, background noise, electrical interference on failure to receive texts/calls
- Keep in mind phone locations can be triangulated even if location services are disabled
- Install an antivirus program
- Don't root or jailbreak your phone
- Only use trusted application sources Never install an app from Email or TXT
- Verify all application permissions before installation, restrict permissions when possible/necessary
- Carefully choose **what is backed up to iCloud/Google**
- Use a password manager (e.g. LastPass) and unique passwords for all internet accounts
- Review social network privacy settings and privacy policies **Change Your Facebook Settings To "Friends Only"**
- Create personal and professional personas – **don't mix the two**
- **Sign Out Of Your Online Accounts When You're Finished Using Them**
- **Don't use social media to logon to other sites**
- Check your email accounts https://haveibeenpwned.com/

Recommended Applications

- "Find my phone" application
- Antivirus CM Security (Android)
  https://play.google.com/store/apps/details?id=com.cleanmaster.security
- FortiClient (Personal PC and Mac home computers)

Using "Free" Public Wi-Fi

- Use a VPN connection on personal device hotspot shield or others
- Pay attention to certificate warnings
- Use HTTPS (SSL) links when possible
- Use multi-factor authentication (Google Authenticator, for instance)
- When in doubt, use your data plan
- **25 Scariest Things You Didn't Know About Using Public Wi-Fi**
  https://www.youtube.com/watch?v=c_N_lkEweM0

Dealing With A Lost Phone

- Use a strong passcode (passwords are better)
- Require the passcode after the phone is locked
- Encrypt the phone
- Use phone location applications
- Notify the cell phone carrier

Parent Control software

On home Router : Open DNS family Shield : http://goo.gl/xfvNb1

On Mobile Devices: Mobicip Safe Browser With Parental Control http://www.mobicip.com/pricing

Social Media: Social Shield www.**socialshield**.com

Stealth mobile Device Tracking/ Filtering: http://goo.gl/qrmoUp

Put A Google Alert On Your Name

This is an incredibly easy way to stay on top of what's being said about you online. Go to: http://www.google.com/alerts and enter your name, and variations of your name, with quotation marks around it.

What the Internet knows about you - https://www.youtube.com/watch?v=eLcTF0YyK5Y