# Family Safety in the Age of Technology & AI

Practical Tips to Protect Your Family, Your Identity, and Your Assets

Technology has made our lives easier — but it has also created new risks. From password theft and phone scams to AI-generated impersonation, families face threats that didn't exist a decade ago. This guide provides simple, actionable steps you can take today to protect yourself and your loved ones.

## 1. Passwords & Account Security

Strong, unique passwords are your first line of defense.

### Create strong passwords:

- Use at least 12 characters — longer is better
- Mix uppercase, lowercase, numbers, and symbols
- Never reuse the same password across multiple sites
- Consider a passphrase: a random string of 4–5 words (e.g., *correct-horse-battery-staple*)

### Use a password manager:

A password manager (such as 1Password, Bitwarden, or Apple Passwords) generates and stores unique passwords for every account. You only need to remember one master password.

### Enable two-factor authentication (2FA):

- Turn on 2FA for email, banking, and social media
- Use an authenticator app (Google Authenticator, Microsoft Authenticator) instead of text messages when possible — SMS can be intercepted

> **Tip:** If you only secure one account, make it your email. A compromised email lets attackers reset passwords on every other account.

## 2. Device Settings: iPhone & Android

### iPhone (iOS):

- Enable **Face ID / Touch ID** and use a 6-digit (or longer) passcode
- **Find My iPhone:** Settings → [your name] → Find My → turn on
- **Automatic updates:** Settings → General → Software Update → Automatic Updates ON
- **Lock screen previews:** Settings → Notifications → Show Previews → "When Unlocked"
- **Stolen Device Protection:** Settings → Face ID & Passcode → Stolen Device Protection → turn on

- **Screen Time for kids:** Settings → Screen Time → set content restrictions, app limits, and downtime

### Android:

- Use **fingerprint or face unlock** plus a strong PIN (avoid pattern locks)
- **Find My Device:** Settings → Security → Find My Device → ON
- **Automatic updates:** Settings → System → System Update → check regularly
- **Lock screen:** Settings → Display → Lock Screen → hide sensitive notifications
- **Google Family Link:** Set up parental controls for children's devices

> **Tip:** Review app permissions regularly. An app that requests access to your contacts, microphone, or location may not need it. Revoke permissions you're not comfortable with.

## 3. Safeguarding Important Documents

Protecting your physical documents is just as important as protecting your digital accounts.

### What to secure:

- Wills, trusts, and powers of attorney
- Deeds, titles, and mortgage documents
- Birth certificates, Social Security cards, passports
- Insurance policies (life, homeowner's, auto)
- Financial account information and beneficiary designations
- Digital account credentials (password manager master password, recovery codes)

### How to store them:

- **Fireproof document bag or safe:** Inexpensive bags ($20–$40) protect against fire and water damage. Keep in a known, accessible location in your home.
- **Safe deposit box:** Good for originals, but note: they are *not* accessible immediately after death in PA — the Register of Wills may need to be involved
- **Your attorney's office:** We store original wills and estate documents in our fireproof vault at no charge

> **Tip:** Make sure at least two trusted people know where your documents are stored and how to access them. A fireproof safe is useless if no one knows the combination.

## 4. Family Safe Words & Verification

AI can now clone a voice from just a few seconds of audio. Scammers use this technology to impersonate family members on the phone. A **family safe word** is a simple but powerful defense.

### How it works:

- Choose a word or phrase that only your family knows — something that would never come up in normal conversation
- If someone calls claiming to be a family member in distress, ask for the safe word before taking any action

- Change the safe word periodically, especially if you suspect it may have been compromised
- Never share the safe word digitally — tell family members in person

**Tip: Teach children and elderly family members the safe word system. These are the groups most frequently targeted by impersonation scams.**

## 5. Recognizing Phone & Online Scams

Scammers are sophisticated. Knowing their playbook is the best defense. Here are the most common schemes targeting families in Western Pennsylvania:

| Scam Type | How It Works | How to Protect Yourself |
|---|---|---|
| **Grandparent / Jail Scam** | Caller claims to be a grandchild or relative who has been arrested and needs bail money immediately. Often says "don't tell Mom and Dad." | Hang up. Call the family member directly. Use your safe word. |
| **IRS / Tax Scam** | Caller claims you owe back taxes and threatens arrest or legal action unless you pay immediately by gift card or wire. | The IRS never calls demanding immediate payment. They communicate by mail. Hang up. |
| **Romance / Love Interest** | Someone builds a relationship online over weeks or months, then asks for money — often for a "medical emergency" or "travel to meet you." | Never send money to someone you haven't met in person. Reverse-image-search their photos. |
| **Tech Support Scam** | Pop-up warning or phone call claims your computer is infected. They ask for remote access or payment to "fix" it. | Microsoft, Apple, and Google will never call you. Close the pop-up. Don't call the number. |
| **AI Voice Clone** | AI replicates a family member's voice using social media clips. The "family member" calls asking for urgent financial help. | Use your family safe word. Call the person back on a known number. |
| **Phishing Email / Text** | A message appears to be from your bank, Amazon, or a government agency. It contains a link to a fake website designed to steal your login. | Never click links in unexpected messages. Go directly to the website by typing the URL. |
| **Deed / Title Fraud** | A criminal files a forged deed transferring ownership of your property, then takes out loans against it. | Sign up for your county's free title monitoring alerts (see Section 6 below). |

**The Universal Rule: Legitimate organizations will never pressure you to act immediately, pay by gift card, or keep a transaction secret from your family. If you feel rushed, it's a scam.**

## 6. Filtering Phone Calls

- **iPhone:** Settings → Phone → Silence Unknown Callers → ON. Known contacts and recent outgoing calls still ring through.
- **Android:** Phone app → Settings → Caller ID & Spam → Filter spam calls ON
- Register on the **National Do Not Call Registry:** donotcall.gov or call 1-888-382-1222
- If you answer and it's a robocall, **hang up immediately** — pressing any key may flag your number as active
- Consider call-blocking apps like Nomorobo, Hiya, or your carrier's free spam filter

## 7. Protecting Your Property Title

Deed fraud (also called title fraud or house stealing) occurs when a criminal files a forged deed with the county recorder to transfer ownership of your property. They then take out loans against it or attempt to sell it. Pennsylvania counties are increasingly offering free monitoring tools:

- **Westmoreland County:** The Recorder of Deeds offers free property fraud alerts — sign up at westmorelandcountypa.gov
- **Allegheny County:** Free property fraud alert system through the Recorder of Deeds
- If your county doesn't offer a program, check your county's Recorder of Deeds website periodically for any filings against your property
- **Title insurance** (obtained when you purchased your home) protects against covered title defects, but may not cover post-closing forgery — check your policy

> **Tip:** If you receive any notice about a deed, mortgage, or lien you didn't authorize, contact your attorney immediately. Early detection is critical.

## 8. Your Digital Legacy

Your estate plan should account for your digital life — not just your physical assets.

- Make a list of all digital accounts: email, banking, social media, cloud storage, cryptocurrency
- Store your password manager's master password and recovery information in your fireproof safe or with your attorney
- Designate a **digital executor** in your estate plan — someone authorized to manage or close your online accounts
- Set up **Legacy Contact** (Apple) or **Inactive Account Manager** (Google) to give a trusted person access if something happens to you
- Include digital asset instructions in your power of attorney — Pennsylvania law (20 Pa.C.S. § 5601) allows this

## Family Safety Checklist

- ■ Use a password manager and unique passwords for every account
- ■ Enable two-factor authentication on email and financial accounts
- ■ Set a 6-digit (or longer) passcode on all phones and tablets
- ■ Turn on Find My iPhone / Find My Device
- ■ Enable Stolen Device Protection (iPhone) or equivalent
- ■ Set up parental controls on children's devices
- ■ Store important documents in a fireproof bag or safe
- ■ Establish a family safe word for phone verification
- ■ Sign up for your county's free title/deed fraud alerts
- ■ Silence unknown callers on your phone
- ■ Register on the Do Not Call list (donotcall.gov)
- ■ Create a digital asset inventory for your estate plan
- ■ Designate a digital executor or Legacy Contact

■ Review and update your estate plan every 3–5 years

**Ament Law Group, P.C.**
3950 Wm Penn Highway, Suite 5 · Murrysville, PA 15668
(724) 733-3500 · ament.law

If you have questions about protecting your family, your property, or your estate plan, we're here to help. Call us or visit our website to schedule a consultation.