THE FAMILY DIGITAL DEFENSE SHIELD

10 SIMPLE RULES TO KEEP YOUR FAMILY SAFE ONLINE

Immediate

Adopt these defenses now. These tactics cause the fastest, most costly harm.

- **1. The "Zero Trust" Click Rule (Phishing)**
  - ☐ Never click unexpected links or attachments, even if they look familiar.
    Action: If you get an “account issue” alert or a special deal at an online store, close the message and go directly to the company’s official site.
- **2. Verify the Voice (Deepfakes & AI)**
  - ☐ AI can fake voices and faces. Treat surprise emergency calls with caution.
    Action: Hang up and call the person back on their real number.
    Pro-Tip: Use a family-only emergency **“Code Word”** to confirm identity.
- **3. Silence the Unknown (Phone Scams)**
  - ☐ Caller ID can be spoofed.
    Action: Let unknown numbers go to voicemail. Legitimate callers will leave details.
- **4. Trust Your Gut & Tell Someone**
  - ☐ Scammers rely on fear, urgency, secrecy — and isolation. They want you to act fast without checking in with anyone.
    Action: If something feels off, pause. Put the device down and talk to a trusted family member before responding. Remember, scammers may impersonate real officials.

Near-term

Protect against account takeovers and impersonation. Critical for long-term safety.

- **5. One Account, One Password**
  - ☐ Reusing passwords means that a single breach can compromise several accounts.
    Action: Use a password manager to create and store strong, unique passwords. Remember only the master password. 1Password and Bitwarden are good options.

- **6. Double the Locks (Two-Factor Authentication)**
  - ☐ A password alone is not enough any longer.
    Action: Turn on 2FA (also called multi-factor authentication or MFA) for email, banking, social media, any account that offers it, so that stolen passwords can't be used.
- **7. Lock Down Social Media**
  - ☐ Information you post publicly can help scammers target you.
    Action: Set profiles to private. Don't accept requests from people you don't know, and never send money to online "relationships."

Foundational Habits

Strengthen everyday digital security and reduce exposure to opportunistic threats.

- **8. Update on Autopilot**
  - ☐ Old software is an easy entry point for attackers.
    Action: Enable automatic updates on all devices.
- **9. Avoid Public Wi-Fi When Possible**
  - ☐ Airport and café Wi-Fi are never secure.
    Action: Use cellular data for financial transactions. If you must use public Wi-Fi, turn on a VPN.
- **10. Stop Before You Open (Attachments)**
  - ☐ Malicious files spread infections quickly.
    Action: Delete suspicious files, especially those with .exe or double extensions. Verify unexpected attachments with the sender before opening them.

- **Bonus. Pick Your Family Code Word**
  - ☐ _____