

Family Cybersecurity Checklist

Simple steps to protect accounts, money, devices, and the people you trust.

PROTECT WHAT MATTERS

Cybersecurity is not just an IT issue. It is part of protecting your money, your identity, your family, and the plans you have made for the future.

YOUR ACCOUNTS

- Use a different password for each important account.
- Consider a reputable password manager.
- Turn on two-factor authentication for email, banking, and financial accounts.
- Review account recovery information and keep it current.
- Close old accounts you no longer use.

YOUR MONEY

- Turn on transaction and login alerts when available.
- Review bank and credit-card statements regularly.
- Never move money because an unexpected caller says your funds are in danger.
- Never give an unsolicited caller remote access to your computer or phone.
- Treat gift cards, cryptocurrency, wire transfers, and unusual payment requests as warning signs.

YOUR DEVICES

- Keep phones, tablets, and computers updated.
- Use a passcode, PIN, fingerprint, or other device lock.
- Do not click unexpected links or open unexpected attachments.
- Avoid entering personal or financial information after following an unexpected link.
- Back up important photos and documents.

YOUR FAMILY PLAN

- Choose someone you trust who can help verify suspicious requests.
- Decide how family members should contact you if they receive a message claiming to be from you.
- Keep important Estate Planning and financial information organized.
- Review your Powers of Attorney and other planning documents as circumstances change.

THE GOLDEN RULE

If someone creates a crisis and demands immediate action, slow down. Hang up, close the message, and verify the situation independently.

Educational resource. For general information only. This handout is not legal, financial, or cybersecurity advice.