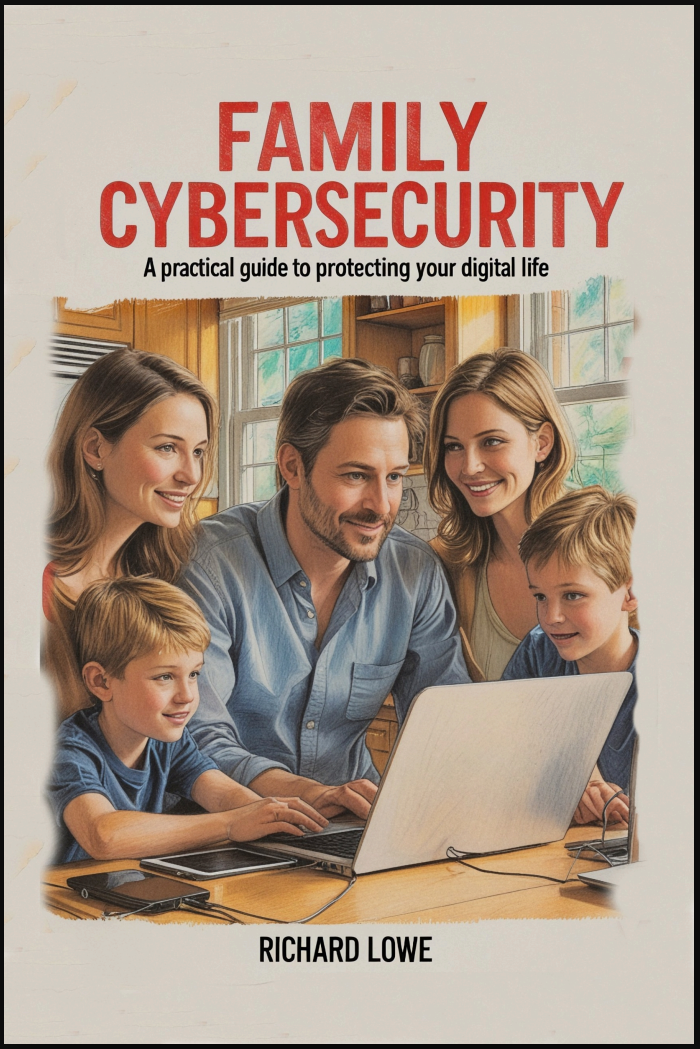
A FREE COMPANION TO FAMILY CYBERSECURITY

The Family Security Binder

Your household's devices, accounts, backups and emergency plan, written down in one place and kept current a few minutes a month.



RICHARD LOWE

How to Use This Binder

Print it, fill it in with a pencil, and keep it with your important papers.

Family Cybersecurity covers every device in your home, from the router to the refrigerator. This binder is where your family's own answers go: what you own, who uses it, how it is protected, and what to do on the bad day. Paper matters here. When a computer is infected or a phone is stolen, the plan has to live somewhere the criminals can't reach.

It has five parts:

1. **Devices and the network**: everything that connects, and the router that guards it.
2. **The account tracker**: passwords and two-factor authentication.
3. **Backups and upkeep**: the 3-2-1 rule, a restore log and the maintenance calendar.
4. **Children and older relatives**: settings by age and a simple support plan.
5. **The bad day page**: what to do when something goes wrong.

Don't try to finish it in one sitting. The book's advice is to choose three improvements that cover your family's biggest risks, do them well, and then move on to the next three.

> *Security that depends on perfect behavior from every family member will fail. Build systems that work even when people make mistakes.*

Three Rules for Everyone in the House

1. **A stranger who knows your name is still a stranger.** Criminals buy names, addresses and even computer models from data brokers. Knowing your details proves nothing.

2. **Nobody who contacted you first gets money, a password, a code or remote access.** Hang up and call the number on your card, your bill or the company's real website.

3. **Nobody loses a device for reporting a problem.** A child who is afraid of punishment hides the strange message. A child who isn't tells you the same day.

> *Security that's too hard to use gets ignored. The best protection is the kind that works automatically in the background while you live your life.*

Part 1: Devices and the Network

Walk through every room and count what connects. Most families find far more than they expected.

Start with the list of connected devices in your router's settings or app, then walk the house. Thermostats, door locks, cameras, washers, toys, fitness trackers and the car in the driveway all count.

DEVICE	WHO USES IT	MAIN OR GUEST NETWORK	DEFAULT PASSWORD CHANGED	LAST UPDATED	STILL GETS UPDATES?

The router and Wi-Fi

- [ ] Router administrator login changed to something new and strong (or, for an app-managed router, the app account has two-factor authentication)
- [ ] Firmware checked, automatic updates on, and the maker still supports this model
- [ ] Wi-Fi set to WPA3, or mixed WPA2/WPA3 if an older device needs it. Never WEP, WPA or TKIP
- [ ] Wi-Fi password at least 15 characters, or four or five unrelated words
- [ ] Network name reveals neither your family name nor your equipment; WPS turned off
- [ ] Guest network on, isolated, with its own password; alerts on for new devices

The devices

- [ ] Default password changed on every camera, doorbell and smart home hub
- [ ] Smart devices, consoles and streaming sticks on the guest network where they still work there
- [ ] Smart speakers: voice purchasing off, recordings set to delete themselves
- [ ] Smart TV: Automatic Content Recognition (whatever your brand calls it) and unused voice recognition off

Part 2: The Account Tracker

One stolen password opens every account that shares it. Two-factor authentication stops most break-ins even after a password is stolen.

Choose a password manager with a family plan and set it up on your own devices first. Then work down this table, most important accounts at the top. Email comes first because email resets everything else.

ACCOUNT	WHOSE	UNIQUE PASSWORD IN MANAGER	SECOND FACTOR (PASSKEY, KEY, APP, TEXT)	BACKUP CODES PRINTED AND FILED
Email				
Email				
Bank				
Credit card				
Password manager				
Cloud storage				
Apple, Google or Microsoft				
Social media				
Game console				
Router or camera app				
Internet company				

Strongest to weakest

When an account you rely on offers a passkey, take it. Otherwise the order is security key, authenticator app, text message. Any of them is far better than none.

- [ ] Ran the password manager's audit and replaced reused passwords, bank and email first
- [ ] Everyone knows: if you get an approval request you didn't start, deny it and change that password
- [ ] Everyone knows: no real company asks for a two-factor code by phone or email
- [ ] Authenticator apps move to the new phone before the old one is wiped

Part 3: Backups and Upkeep

Every storage device will fail. Real backups follow the 3-2-1 rule: three copies, on two kinds of media, with one copy away from the house.

A copy on the same drive, or a cloud folder that syncs a damaged file to every device, is a fake backup. Fill in where each copy lives. Skip what can be downloaded again.

WHAT	COPY 1 (THE DEVICE)	COPY 2	COPY 3 (AWAY FROM HOME)	LAST CHECKED
Family photos and videos				
Tax, financial and legal papers				
Medical, insurance and ID documents				
Work files				
Each phone (photos included)				

The restore log

A backup you have never restored from is a hope. Restore one file now, then every three months.

DATE	WHO	WHAT WAS RESTORED, FROM WHERE	WORKED?	PROBLEM FOUND

The maintenance calendar

One family in the book shared these jobs out and spent about two hours a month in total.

MONTHLY (FIRST WEEKEND) WHO: _____	FOUR TIMES A YEAR WHO: _____	ONCE A YEAR WHO: _____
Read the router's device list Install updates everywhere Check the password manager report Check statements and credit Check the date of the last backup	Full security scan on every device Updates on every smart device Review privacy settings Remove old accounts and app connections Check recovery phones and emails Restore one file and log it	Change passwords where there is a reason Review the Bad Day Page Check backup space against need Ask about personal cyber coverage Plan replacements for devices losing updates

Part 4: Children and Older Relatives

Restrictions that protect a seven-year-old will frustrate a fourteen-year-old. Loosen them as judgment grows.

AGES	SETTINGS FROM THE BOOK	CHILD AND DATE SET
5 to 8	Supervised account, maximum restrictions. No messaging, email, video calls or social media. Pre-approved apps only. No purchases. Short automatic logout.	
9 to 12	Limited communication with approval. Strong content filters. Each app download approved. Time limits for sleep and homework. Activity monitoring the child knows about.	
13 to 15	Messaging with known friends and family. Filters aimed at harmful material. Social media with privacy at maximum and friend lists you review. Spending approvals.	
16 to 18	Fewer restrictions, more privacy, open conversation. They manage their own cloud storage and settings. Teach password management, scams and digital footprints.	

- [ ] Parental controls set through Family Sharing (iPhone, iPad) or Family Link (Android)
- [ ] Bedtime and homework hours set at the router
- [ ] Each child has a child account on every console; voice chat limited to friends; purchase PIN set
- [ ] Family technology agreement written together (a conversation starter, not a legal document)

For a relative who struggles with technology

QUESTION	ANSWER
Accounts they use (sit with them and list every one)	
Password method they will actually keep using	
Automatic updates and backup turned on?	
Spam filtering and call blocking turned on?	
Who they call before letting anyone into the computer	

Content filtering helps seniors too, but a senior is an adult. Set it up with them and get their agreement. Never install it behind their back.

Part 5: The Bad Day Page

The first few minutes decide how much damage is done. Keep this page on paper where everyone can find it.

1. **Disconnect.** Unplug the network cable or turn off Wi-Fi on the affected device.
2. **Change passwords from a different, clean device.** Email first, then banking, then social media.
3. **Call the bank and card companies.** If identity details may be exposed, freeze your credit at Equifax, Experian and TransUnion. It's free.
4. **If there is a ransom demand, don't pay.** Report it, restore from your backup, and check NoMoreRansom.org for a free decryption tool before giving up on files.
5. **Write down what happened**: when you noticed, what you saw, what you have done.
6. **Tell the family** so everyone checks their own accounts and devices.

FRAUD LINE	PHONE NUMBER
Bank	
Credit card	
Credit card	
Person who helps us with technology	

Where to report

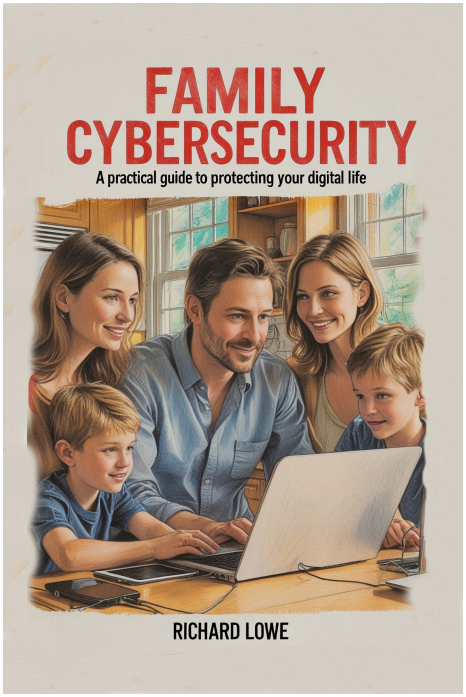
- **Anyone in danger:** 911.
- **Internet fraud and cybercrime, any amount:** the FBI at ic3.gov.
- **Scams:** the FTC at ReportFraud.ftc.gov. **Identity theft:** IdentityTheft.gov.
- **Crimes against children:** CyberTipline.org.
- **Credit reports:** free each week at AnnualCreditReport.com. A child should have no credit report at all.

☐ We have agreed on a family code word, and everyone asks for it before sending money to a caller who sounds like family

If you suspect a partner or an ex is watching your phone or computer, don't search for help or remove anything on that device. Use one they can't reach and call the National Domestic Violence Hotline at 1-800-799-7233 to make a plan first.

The Whole Story

This binder holds your answers. Family Cybersecurity explains the reasons behind every line: how criminals pick families, how to set up routers, computers, phones, TVs and consoles step by step, how to protect children at each age, and how to help relatives who find technology hard.



Family Cybersecurity:
A Practical Guide to Protecting Your Digital Life
Digital Self-Defense

Get the full book

thewritingking.com/library/family-cybersecurity/

More free books: free.coolauthor.com

Copyright © 2026 by Richard Lowe. You may print and share this workbook for personal, noncommercial use.