

Family Cyber-Hygiene

4

Simple rules we can follow every day - and help each other follow without blame.

OUR HOUSE RULE: Urgency never outranks verification.

1 Use a password manager

- Give every account its own long, unique password.
- Let the manager create, save, and fill passwords.
- Never reuse the passwords for email, banking, or the password manager.

DO TODAY: Protect the password manager with two-factor authentication.

2 Turn on 2FA

- Start with email, banking, payment apps, and social media.
- Prefer a passkey, security key, or authenticator app. A text code is still better than none.
- Never approve a sign-in you did not start.

DO TODAY: Secure email first - it can reset many other accounts.

3 Hang up. Call back.

- Do not give a caller, text, or email your password, security code, or money.
- End the contact. Call the number on the back of your card or use the official app or site.
- Caller ID can be faked. Pressure is a warning sign.

FAMILY PROMISE: Asking for a second opinion is always the right move.

4 Back up what matters

- Back up photos and important documents automatically.
- Keep another copy separate - for example, cloud storage plus an external drive.
- Once a month, open a backed-up file to prove recovery works.

DO TODAY: Turn on automatic backup for every phone and computer.

IF SOMETHING FEELS WRONG

STOP

Do not click, pay, share a code, or install anything.

VERIFY

Contact the person or company through a trusted channel.

TELL

Ask the family. Fast reporting helps limit damage.

Choose One Home for Passwords

2

Keep the family setup simple: one trusted manager, one browser path, and no loose password files.

ALL APPLE

Use Apple Passwords

It is built in with no separate subscription, syncs through iCloud Keychain, and supports shared groups for family logins. Use Safari for the cleanest fit.

WINDOWS OR ANDROID TOO

Use 1Password

Choose 1Password for anyone who also uses Windows or Android. It keeps the same vault available across Apple and non-Apple devices.

HOUSE RULE: Each person uses one password manager - not two managers competing to save the same login.

Make Safari the easy path

On an all-Apple setup, Safari works directly with Apple Passwords for saved logins, passkeys, and verification codes.

Simple choice

Use Safari day to day. Keep Chrome only when a site or work task truly requires it.

If Chrome stays, turn its saving off

Chrome > Settings > Passwords and autofill > Google Password Manager > Settings

- Turn off **Offer to save passwords and passkeys**.
- Turn off **Sign in automatically**.

Chrome > Settings > Autofill and passwords > Payment methods

Turn off **Save and fill payment methods**.

MOVE SAVED PASSWORDS FROM CHROME

1. Export

In Chrome, open Google Password Manager > Settings > Export passwords, then download the CSV file.

2. Import

On the Mac, open Passwords. Choose File > Import Passwords and select the CSV.

3. Check

Open several important logins and confirm they arrived before removing anything from Chrome.

4. Delete

Delete the CSV, then empty the Trash. Do not email it, text it, or save it in cloud storage.

IMPORTANT: A password CSV is plain text. Anyone who opens it can read the passwords. Create it only for the move, and destroy it as soon as the verified import is complete.

Freeze Credit at All Three

3

A freeze helps stop someone from opening new credit in your name. Do it separately at Equifax, Experian, and TransUnion.

FREE TO PLACE OR LIFT. NO CREDIT-SCORE DAMAGE. TEMPORARILY LIFT IT WHEN YOU APPLY.

Free

There is no charge to place, temporarily lift, or remove a credit freeze.

Score-safe

A credit freeze does not lower or otherwise affect your credit score.

Flexible

When you apply for credit, lift the needed freeze for a limited time, then let it lock again.

1. Equifax

Place and manage an Equifax security freeze on the official Equifax page.

equifax.com/personal/credit-report-services/credit-freeze

2. Experian

Use Experian's official freeze guidance and freeze center.

experian.com - search "security freeze"

3. TransUnion

Use TransUnion's official freeze support center to place or manage the freeze.

transunion.com/credit-freeze

THE FAMILY ROUTINE

1. Freeze all three

A freeze at one bureau does not freeze the other two. Finish all three for each family member.

2. Save access safely

Keep each bureau login in the password manager. Do not store Social Security numbers in notes or email.

3. Lift only when needed

Ask the lender which bureau it will check. Lift only that freeze for the needed dates, then confirm it is frozen again.

REMEMBER: A credit freeze helps block new accounts. It does not stop fraud on an existing card or bank account, so keep watching statements and alerts.

Reboot. Update. Reconnect.

4

Give the family router five quiet minutes each week. Pick the same day so the routine becomes automatic.

ONCE A WEEK: Reboot the router, then check for a firmware update.

1 Reboot the router

1. Unplug the router's power cable.
2. Wait a full **30 seconds**.
3. Plug the power cable back in.
4. Give the router a few minutes to restart and reconnect.

TIP: Do this when nobody needs the internet for a call, class, or show.

2 Check for updates

1. Open the router manufacturer's official app or the router's admin page.
2. Sign in and look for **Firmware, Software Update, or Router Update**.
3. Install any available update. Let the router finish and restart.
4. Turn on automatic updates if the router offers them.

SAFER PATH: Use the saved official app or admin page - not a link from a surprise message.

REBOOT IS NOT RESET. Do not press the small recessed **Reset** button. A factory reset can erase the Wi-Fi name, password, and other settings.

Finish the check

Reconnect one phone or computer and open a website. If it does not connect, wait a few more minutes before unplugging anything again.

**THIS WEEK: [] REBOOTED []
UPDATED**

Payment Apps Need Rules Too

Venmo, Cash App, and Zelle move real money instantly. Treat them like cash - not like a bank.

TREAT PAYMENT APPS LIKE CASH: ONCE IT'S SENT, IT'S GONE.

1 Make it private

Transactions are public by default - anyone can see who you paid. Set past and all future payments to Private.

DO TODAY: Check the privacy setting on every payment app you use.

2 Keep it near zero

It is not a bank. Sweep your balance out to your real account. An empty app can't be drained.

DO TODAY: Transfer any balance out right now.

3 Know your payee

Check the handle twice - scammers use lookalikes (\$JohnSm1th vs \$JohnSmith). Confirm new payees by voice or text.

FAMILY PROMISE: No first-time payment without a double-check.

4 Lock it down

Face ID / PIN to open the app, plus two-factor on the account. Link a low-balance account or credit card - never your main bank.

DO TODAY: Turn on the app lock and check what's linked.

THREE SCAMS TO KNOW

"Accidental" payment

A stranger "accidentally" pays you and asks you to send it back. Don't - the original may be stolen. Let support reverse it.

Fake support

Nobody from the app will ever call you. Hang up on "Venmo support" calls. Use the app - or the number on the company's own site.

No recourse

Screenshot everything the day it happens: dates, amounts, dispute screens. If you dispute, the platform decides. Your records are your only leverage.

IF FRAUD HAPPENS - WHO TO CONTACT

FTC

[ReportFraud.ftc.gov](https://reportfraud.ftc.gov)

Report scams and fraud. The FTC doesn't resolve individual cases, but your report fuels investigations.

Missouri Attorney General

800-392-8222 - ago.mo.gov

Consumer Protection takes complaints, can mediate with the company, and investigates patterns of deception.

CFPB

consumerfinance.gov/complaint

For banks, lenders, and payment apps. Companies are required to respond to your complaint.

Shrink Your Data-Broker Footprint

Data brokers publish your address, phone, and relatives' names for anyone to see — including scammers. Here's how to get off their lists.

DATA BROKERS SELL YOUR ADDRESS, PHONE, AND RELATIVES' NAMES. SCAMMERS SHOP THERE.

Exposed

Data brokers publish your address, phone, age, and relatives' names on people-search sites anyone can view.

Scam fuel

Scammers shop these lists for phishing, impersonation, and identity-theft targets.

Removable

You can opt out site by site — or use a removal service to do it across hundreds at once.

THE FAMILY ROUTINE

1. Scan free

Run the free exposure scan at optery.com. It shows screenshot proof of exactly who's listing you.

2. Opt out

Opt out where you're listed, or use a removal plan — Core (~\$39/yr) automates removals across 380+ sites.

3. Recheck yearly

Brokers re-list. Removals need repeating, so check again every year.

HONEST NOTE: No removal service reaches every private backend broker — and to clean up your data, you hand your data to the service. Use a reputable one.

DO TODAY: Run the free scan at optery.com and see who's listing you.