FROM LEGACYGUARD · A SHORT PRACTICAL GUIDE

5 Things You Can Do Today to Improve Your Cybersecurity

By Bryan Kemler · California Trust and Legacy

A short, practical list. You can finish all five before dinner. None of them require buying software, hiring a consultant, or learning anything technical. They will not solve every problem, but they will close the easiest doors most attackers walk through.

1. Turn on two-factor authentication for your email — first

Your email account is the master key to every other account you have, because every other account uses email to reset its password. If an attacker takes your email, the rest follows. Today, in the next ten minutes, log in to your primary email provider — Gmail, iCloud, Outlook, whichever — and turn on two-factor authentication. Use an authenticator app rather than text messages if the option is offered. Then do the same for your spouse's email. Then for any adult child who might receive a "Mom needs help" message that looks like it's coming from you.

If you only do one of the five things on this list, do this one.

2. Pick up the phone and call your wealth manager and your CPA

Make this call today. Tell them — out loud, in your real voice — that from now on, any request to move money, change account information, or send sensitive documents must be confirmed by a phone call back to a number that the two of you have agreed on in advance. Not a number that came in the email. Not a number on a recent invoice. The number you have written down at home or saved in your phone *before* today's call.

This is the single most effective defense against AI-generated voice cloning and email spoofing attacks. It costs nothing. It takes one phone call per advisor. The advisor will appreciate the conversation; this is how they want to work.

3. Have the same conversation with your family

Pick a word. Any word — a quiet, unmemorable one is best — that nobody outside your family would guess and that you will remember in an emergency. This is your family's verification word. If anyone in your family ever receives a phone call that sounds like you in distress, asking for money or for sensitive information, the rule is simple: ask the question only the real you can answer. The

verification word is the answer.

Tell every adult in your family. Tell your teenagers. If you have college-age children living away from home, this is the conversation that matters most: voice-cloning attacks targeting parents through panicked-child phone calls are happening now.

4. Walk your house and find your important paper

You probably have, somewhere in your home, a folder or a drawer or a safe deposit box that contains the original of your trust, your deeds, your birth certificate, your passport, the list of accounts you've been meaning to update. Find it today. Make sure your spouse knows where it is. If the location is "I'd have to think about it for a minute," the location is wrong. Move it somewhere both of you would name in your sleep.

If you cannot remember whether you have such a folder at all, that is information too. Make a list this afternoon, on paper, of the accounts and documents you would need someone to be able to find on your behalf. You don't have to organize anything yet. Just write the list. The list is the start.

5. Look in your password manager — or, if you don't have one, decide tonight which one you'll set up this weekend

If you already use a password manager — 1Password, Bitwarden, Apple Passwords, Dashlane — open it today and look at how many of your accounts have password reuse warnings or weak-password warnings. Don't fix them all. Fix the five most important ones: your email, your bank, your brokerage, your healthcare portal, your phone carrier. Set them to long, unique, generated passwords.

If you do not yet use a password manager, the honest answer is that this is one place where setting it up takes a Saturday afternoon and is the single best long-term investment you can make in your family's digital safety. Pick one tonight. Block out a Saturday. The discomfort of switching is real and it ends.

What this list does not do

This list closes the easiest doors. It does not solve everything. It will not protect you from a determined, targeted attack, and it will not unwind damage already done. If you have specific reason to believe your family is currently being targeted — unexplained activity in your accounts, a wave of suspicious calls, a wealth manager who's reported anomalies — that is not a five-things-list situation. That is the situation you call us about, or call an incident-response firm about, today.

For families who want a more thorough hardening — the password manager rolled out across the household, hardware security keys configured, the heir access protocol documented, the verification protocol trained with your advisors — that is the LegacyGuard service.

If you'd like to do something more about this

LegacyGuard is a service of California Trust and Legacy. It is the structured response we built for our own clients — five components configured for your family, no custody of your credentials, no outcome guarantees, no monitoring subscriptions. Just the careful configuration and training of established practices, delivered for the families being targeted now.

To start a conversation: Schedule a 15-Minute Discovery Call at **californiatrustandlegacy.com/book-a-call** or read more at **californiatrustandlegacy.com/services/legacyguard**