TILLMANHARTLEY

Protecting Your Wealth Online

A Cybersecurity Guide for Tillman Hartley Clients

Ten practical steps to protect your brokerage, bank and personal accounts, plus custodian-specific guidance for Charles Schwab and Fidelity.

November 2026

Educational material. Not individualized advice.

Why this guide matters

Ten habits close the doors criminals use most often to reach financial accounts. Many take just a few minutes, such as turning on account alerts or choosing a family code word, and you can work through the rest at your own pace. Families with significant assets are targeted more deliberately than most: fraudsters research public records, social media and news coverage to make their requests look legitimate.

The good news is that the most common attacks rely on a handful of weaknesses: reused passwords, text-message codes, unverified payment requests and an unlocked phone number. Each section below explains one protection in plain terms and lists the steps to take.

We recommend working through the Quick Checklist at the end with a family member and calling us anytime a request involving your accounts feels unusual. We will never be offended that you double-checked.

1. Use a password manager and a unique password for every account

> **Before you start:** read sections 1 and 2 together. As you update each account, check whether it offers a passkey (explained in section 2). Where one is available, set it up at the same time. You will still keep a strong, unique password for that account in your password manager as a backup, so nothing you do in this step is wasted.

When one website is breached, criminals try the stolen password on banks, brokerages and email. A unique password for each account stops one breach from becoming many. A reputable password manager creates and remembers long, random passwords so you don't have to; the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the federal government's cybersecurity agency, recommends exactly this approach.

> **What is a password manager?** An app that securely stores all your passwords behind one master passphrase. It works on your phone and computer, fills in logins for you, and can create a new random password whenever you need one.

- Choose a well-established password manager. Three widely used options are **1Password** (1password.com), **Bitwarden** (bitwarden.com) and **Dashlane** (dashlane.com). All three work across Apple, Windows and Android devices, support passkeys and offer family plans.
- Protect the password manager itself with a long passphrase (four or more unrelated words) plus multi-factor authentication, the second login step described in section 2.
- Start with your most important accounts: primary email, banks, brokerages, retirement accounts and your phone carrier.
- Never reuse your email password anywhere else. Whoever controls your email can reset nearly every other password.
- Set up the password manager's emergency access or legacy feature so your surviving spouse, heirs, or trustee can reach it if needed.

2. Turn on strong multi-factor authentication everywhere it is offered

Multi-factor authentication (MFA) means a password alone is not enough to get in: you also confirm a login with something you have, such as your phone, or something you are, such as your fingerprint. Not all methods are equal. Codes sent by text message can be intercepted through a SIM swap, while passkeys and physical security keys cannot be phished. CISA calls this phishing-resistant MFA the gold standard and urges high-value targets to adopt it.

> **What is phishing?** A fake email, text or website designed to trick you into entering your password or a security code. Section 6 covers how to spot it.
>
> **What is a SIM swap?** The SIM is the chip (or digital profile) that connects your phone to your phone number. In a SIM swap, a criminal convinces your mobile carrier to move your number to a phone they control, so your text-message codes and calls go to them. A related scam, a "port-out," moves your number to a different carrier. Section 5 explains how to block both.
>
> **What is a passkey?** A modern replacement for a password. You log in with your fingerprint, face or phone's screen-lock PIN, and the passkey only works on the real website it was created for, so a fake site can't capture it. Many banks, brokerages and email providers now offer passkeys, usually under security or login settings.

From strongest to weakest:

1. **Passkeys or a physical security key.** A security key is a small device that plugs into your computer's USB port or taps your phone. Widely used options include **YubiKey** (yubico.com) and the **Google Titan Security Key** (store.google.com). Use these wherever your bank, brokerage or email provider supports them. Register two keys and store the spare somewhere safe.
2. **An authenticator app** on your phone that shows a rotating six-digit code. Widely used options include **Google Authenticator**, **Microsoft Authenticator** and the built-in code feature in 1Password or Bitwarden.
3. **Text-message or voice codes.** Better than nothing but replace them when a stronger option exists.

Never share an MFA code with anyone who calls, texts or emails you, including someone claiming to be from your bank or from our firm. Legitimate institutions do not ask for these codes.

3. Verify every request to move money by calling a number you already know

This single habit prevents the costliest losses. Typical scenarios include a title company emailing "updated" wiring instructions before a closing, a family member texting from a "new number" asking for urgent help, or an email that appears to come from your advisor requesting a transfer.

- Before any wire, ACH transfer (an electronic bank-to-bank payment) or change to payment instructions, call the requester at a number you already have on file. Never use the phone number or link in the message itself.
- Treat urgency, secrecy and changed bank details as red flags, even when the request looks perfectly legitimate.
- Ask us about adding verbal confirmation requirements to your accounts. Our team will always confirm new money movement requests with you directly.
- Agree with family members, your CPA (certified public accountant) and your attorney that no one will ever request funds by email or text alone.

4. Freeze your credit and get an IRS Identity Protection PIN

A credit freeze stops anyone from opening new loans or credit cards in your name, and it costs nothing. Under federal law in effect since September 2018, freezes are free to place and lift at the three major nationwide credit bureaus, and parents can freeze the files of children under 16, according to the Federal Trade Commission (FTC), the federal consumer protection agency. Online and phone freeze requests must be honored within one business day, and online or phone requests to lift a freeze within one hour.

- Place a freeze at the three major credit bureaus: **Equifax** (equifax.com/personal/credit-report-services), **Experian** (experian.com/freeze) and **TransUnion** (transunion.com/credit-freeze). A freeze at only one bureau leaves the other two open.
- Freeze your children's files too. A child's clean Social Security number (SSN) is a favorite target because the theft can go unnoticed for years.
- Store each bureau's PIN (personal identification number) or login in your password manager so you can lift the freeze quickly when you apply for credit.

An IRS Identity Protection PIN (IP PIN) is a six-digit number that blocks anyone else from filing a tax return with your Social Security number. Anyone with an SSN or an ITIN (Individual Taxpayer Identification Number, which the IRS issues to taxpayers who aren't eligible for an SSN) can request one for free (IRS Tax Tip 2026-56).

- Request it through your IRS Online Account at IRS.gov/GetAnIPPIN. Each spouse and dependent needs a separate PIN.
- A new PIN is issued every January. The online tool is generally available mid-January through mid-November, so plan around that window.
- The IRS will never call, text or email you to ask for your IP PIN. Share it only with your tax preparer when filing.

This section is general information, not tax advice. Please consult your own tax professional about your situation.

5. Lock down your mobile phone and carrier account

Your phone number is a master key: many banks send reset codes to it. In a SIM swap, a criminal convinces your carrier to move your number to their device, then intercepts those codes. Federal Communications Commission rules adopted in 2023 require carriers to authenticate customers securely before a SIM change or number transfer and to notify

customers when one is requested. Your own settings add a second layer. (See "What is a SIM swap?" in section 2.)

- Call your carrier or open its app and turn on its account lock, number lock or port-out protection feature (a setting that blocks your number from being moved to another carrier), and set a unique account PIN that is not your birthday or the last digits of your SSN.
- If your phone suddenly loses service for no clear reason, call your carrier from another phone immediately. It can be the first sign of a SIM swap.
- Set a strong passcode (six digits or more) and enable automatic screen lock, Find My (Apple) or Find My Device (Android), and remote wipe, which lets you erase a lost phone from another device.
- Install apps only from the official app store and keep your phone's operating system updated.

6. Learn to spot phishing, fake calls and AI voice clones

Most account takeovers start with a message designed to make you act before you think. Phishing (email), smishing (text) and vishing (phone calls) now often use AI to sound fluent, personal and urgent, and a few seconds of audio from social media can be enough to clone a voice.

Common warning signs:

- Pressure to act immediately, keep the request secret, or avoid telling your advisor or family.
- Requests for codes, passwords, gift cards, cryptocurrency or a wire to a "safe account."
- A caller who claims to be from your bank's fraud department, the IRS, law enforcement or tech support and asks you to move money or install software.
- Links or attachments you weren't expecting, even from a familiar name.

What to do:

- Hang up or close the message, then contact the organization using the number on your statement or the back of your card.
- Choose a family code word that only your household knows. If a "grandchild" or spouse calls in a crisis, ask for it before doing anything.
- **Never let someone you don't know take remote control of your computer.**

7. Turn on account alerts, review statements and name a trusted contact

The faster unusual activity is spotted, the more likely money can be stopped or recovered. Alerts cost nothing and put you, not the criminal, first in line to know.

- In each bank, brokerage and credit card account, enable alerts for logins from new devices, password or contact-information changes, new payees, wires, ACH transfers and withdrawals above a threshold you choose.

- Review statements and online activity at least monthly. Look especially for small test transactions, which often come before larger theft.
- Check your free credit reports at AnnualCreditReport.com, the only federally authorized source.
- Name a **trusted contact person** on your brokerage accounts. This is an adult your firm may contact if it suspects fraud or exploitation or cannot reach you. A trusted contact cannot make transactions and is not a power of attorney.
- Make sure your custodian and our firm have your current phone number, email and mailing address, and tell us about travel plans that might trigger fraud alerts.

8. Keep your devices updated and protected

Outdated software and unprotected devices are among the easiest openings for cybercriminals, but a few simple habits can close them.

- Turn on automatic updates for your computer, phone, browser and apps. Most attacks exploit flaws that already have a fix available.
- Use reputable security software and sign out of financial websites when you finish. Options include **Microsoft Defender** (built into Windows), **Malwarebytes** (malwarebytes.com) and **Bitdefender** (bitdefender.com). Apple computers include built-in protection; keep macOS updated.
- Bookmark your financial sites and log in from the bookmark rather than through search results or email links, which can lead to convincing fakes.

9. Secure your home network and be careful on public Wi-Fi

Your home router is the front door to every device in the house, including smart cameras, thermostats and TVs that are rarely updated. A few settings close most of the gaps.

- Change the router's default administrator password and turn on WPA3 encryption (or WPA2 if WPA3 isn't available), the setting that scrambles your Wi-Fi traffic, with a strong Wi-Fi password.
- Turn on automatic firmware updates (the router's built-in software), and replace routers the manufacturer no longer supports.
- Put guests, visitors (including anyone who works in your home) and smart-home devices on a separate guest network so they can't reach the computers you use for banking.
- For larger or multiple residences, consider having a qualified information technology (IT) professional review the setup.
- Avoid logging into financial accounts on public or hotel Wi-Fi. Use your phone's cellular hotspot or a reputable VPN (virtual private network), an app that encrypts your internet connection, instead. Options include **Proton VPN** (protonvpn.com), **NordVPN** (nordvpn.com) and **Mullvad** (mullvad.net).

10. Limit your public footprint and protect your whole household

Criminals build convincing scams from details you and your family share publicly: travel dates, children's schools, a new home purchase, a business sale. Security also depends on everyone with access to your home and information.

- Set social media accounts to private, and post travel photos after you return rather than during the trip.
- Be cautious answering security questions with real facts that appear online. Use made-up answers and store them in your password manager.
- Consider a service that requests removal of your personal information from data broker and people-search websites. Widely used options include EasyOptOuts (easyoptouts.com), **DeleteMe** (joindeleteme.com), **Incogni** (incogni.com) and **Optery** (optery.com). Each repeats its removal requests over time, since listings tend to reappear.

> **What is a data broker?** A company that collects personal details such as your address, phone number, relatives and property records from public and commercial sources, then sells or publishes them. People-search websites let anyone look up this information, which scammers use to make their stories convincing.

- Create a private email address used only for banks, brokerages, your CPA, your attorney and our firm. Protect it with a passkey or security key.
- If practical, use one computer or tablet only for financial accounts, with no games, unfamiliar downloads or shared family use.
- Hold property in a trust or LLC (limited liability company) where appropriate to keep your name off public records. *Discuss legal structures with your attorney.*
- Talk with family members, including children and aging parents, about these scams. If anyone works in your home, such as a housekeeper, caregiver or contractor, set clear expectations for what they may share and how mail, deliveries and visitors are handled.
- Shred financial documents and consider a locked mailbox or a P.O. box for statements and checks.

Securing your Charles Schwab account

Schwab's security settings live in the **Security Center** (log in at schwab.com, then go to Profile and Security Settings). Setting up the items below takes about 20 minutes and puts every layer Schwab offers between a criminal and your account.

1. **Turn on two-step verification, set to "Always at login."** Schwab lets you require a second step only on unrecognized devices or on every login. Choose "Always at login" for the strongest protection, then pick a method:

- **Schwab mobile app push notification** (a prompt that pops up on your phone asking you to approve the login). Download the app and log in at least once before selecting it.
- **Security token** using the free Symantec VIP Access app or a VIP hardware token, which generates a rotating code.
- **Text or voice code** only if neither option above works for you, since text messages are exposed to SIM swaps.

2. **Sign up for security alerts.** In the Security Center, turn on notifications so you know right away when activity occurs in your accounts, especially changes to your login ID, password, email, phone number, or address. Navigate to **Profile** and select the **Alerts** tab. At a minimum, we recommend turning on **Profile Information Changes, Portfolio Alerts, and Deposits and Transfers**. You can receive alerts as push notifications through the Schwab mobile app or as text messages.

3. **Enroll in Voice ID.** Schwab can confirm your identity when you call by having you say "At Schwab, my voice is my password," so representatives don't need to ask for personal details a fraudster might already know (schwab.com/VoiceID).

4. **Add a verbal password.** Schwab lets you add a verbal password to each account. Once set, it becomes the primary check before Schwab discusses the account or accepts phone instructions. Use a phrase unrelated to public information about you.

5. **Keep your contact information current and review trusted devices.** Check your profile at schwab.com/MyProfile so security notices reach you, and review the list of previously used devices for anything you don't recognize.

6. **Name a trusted contact** on each Schwab brokerage account (see section 7).

> **Good to know:** Schwab's Security Guarantee states it will cover losses in Schwab accounts due to unauthorized activity, but it requires you to keep your login information private and report problems quickly. Schwab does **not** cover losses that result from sharing your login with anyone, linking your account to a third-party budgeting or aggregation app (other than a Schwab partner), or letting someone remotely access your computer or phone. Schwab's fraud line is **877-862-6352** (+1-602-355-7300 from abroad).

If your accounts are held at Schwab through our firm, please call us if you run into trouble on any of these steps.

Securing your Fidelity account

Fidelity's options are under **Security Settings** after you log in (Accounts & Trade, then Security Settings). The single most powerful step is the money transfer lock, which stops electronic money from leaving your accounts even if someone gets your password.

1. Set up a passkey. Fidelity supports passkeys, which let you log in with your fingerprint, face or device PIN and only work on Fidelity's real website, so a fake site can't capture them. Passkeys can live on your phone, your computer, a password manager or a hardware security key.

2. Add a backup login method. Fidelity also lets you approve logins with a push notification in the Fidelity mobile app (with fingerprint or face login turned on) or connect a standard authenticator app such as Google Authenticator or Microsoft Authenticator. Set up at least one of these as a backup in case you lose the device that holds your passkey, and save any recovery codes somewhere safe.

3. Turn on the money transfer lock. This blocks electronic money movement out of your accounts. Keep it on, unlock it only when you need to move money, then lock it again. Ask us before turning it on for accounts with scheduled distributions or automatic transfers so nothing you rely on is interrupted.

4. Turn on security text alerts. Fidelity sends instant texts to your mobile number when certain transactions or profile updates occur. Keep your mobile number and email current so these reach you.

5. Enroll in voice biometrics (Fidelity MyVoice). Fidelity can create a voiceprint so it recognizes you when you call, without PINs or passwords. To enroll, call 800-FIDELITY, say "account access" when prompted and tell the representative you'd like to enroll.

6. Manage trusted devices carefully. "Remember this device" skips the extra login step on that device. Use it only on your own personal devices, never on shared or public computers, and review your trusted device list periodically.

7. Name a trusted contact on each Fidelity brokerage account (see section 7).

> **Good to know:** Fidelity's Customer Protection Guarantee states it will reimburse losses from unauthorized activity in covered accounts occurring through no fault of your own. To stay eligible, Fidelity asks you to review statements and alerts promptly (no later than 30 days after they are posted or delivered) and to report anything suspicious right away at **800-544-6666**. Activity is **not** covered if you share your login with anyone, authorize a third-party app or tool to access your account, grant remote access to your computer, or read back a security code on a call you didn't initiate. Forward suspicious emails to phishing@fidelity.com.

If your accounts are held at Fidelity through our firm, please call us if you run into trouble on any of these steps.

If something goes wrong

Speed matters most: wires can sometimes be recalled if the bank is alerted within hours. Act quickly—you will not be judged; these schemes fool careful, intelligent people every day.

1. **Call your bank or custodian immediately** using the number on your statement or card, and ask them to stop or recall any transfer.
2. **Call us** at 352-335-9015. We will help coordinate with your custodian and place extra safeguards on your accounts.
3. **Change passwords** for your email and financial accounts from a clean device, and sign out all other sessions.
4. **Call your mobile carrier** if you've lost service or suspect a SIM swap.
5. **Report it** to the FBI at IC3.gov and to the FTC at IdentityTheft.gov, which also builds a personalized recovery plan.
6. **Freeze your credit** at all three bureaus if you haven't already.
7. **Keep records** of every message, call, transaction number and person you speak with.

Quick checklist

Tick these off as you go.

- ☐ Install a password manager and give every financial account a unique password
- ☐ Turn on passkeys, security keys or an authenticator app for email, banks and brokerages
- ☐ Agree with family and advisors to verify every money request by phone
- ☐ Freeze credit at Equifax, Experian and TransUnion, for yourself and your children
- ☐ Get an IRS IP PIN for each family member
- ☐ Add a port-out lock and PIN to your mobile carrier account
- ☐ Choose a family code word
- ☐ Schwab: two-step verification "Always at login," security alerts, Voice ID and a verbal password
- ☐ Fidelity: passkey plus a backup method, money transfer lock, security text alerts and MyVoice
- ☐ Turn on account alerts and name a trusted contact on brokerage accounts
- ☐ Set up a private email used only for finances; turn on automatic updates
- ☐ Change your router password and create a guest network
- ☐ Make social media private and review what's public about your family
- ☐ Save Tillman Hartley's number (352-335-9015) and your custodian's fraud line in your phone (Schwab 877-862-6352; Fidelity 800-544-6666)

Important information

This guide is educational material provided for general informational purposes. It is illustrative and is not individualized advice. It does not constitute tax, legal or accounting advice; please consult your own tax, legal or accounting professional regarding your specific situation. Following these recommendations reduces risk but cannot eliminate it, and no security measure can prevent every fraud. References to government agencies and regulations are for information only and do not imply endorsement of our firm. Products and services named in this guide are examples of widely used options, not endorsements; Tillman Hartley is not affiliated with and receives no compensation from any of them. Evaluate any service before use. Figures and regulatory details are current as of the date shown and may change.

Sources

- CISA, Implementing Phishing-Resistant MFA (fact sheet). https://cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- FBI Internet Crime Complaint Center, 2025 Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- ABA Banking Journal, "FBI: Cybercrime losses increased 26% in 2025," April 2026. https://bankingjournal.aba.com/2026/04/fbi-cybercrime-losses-increased-26-in-2025/
- FTC, Free credit freezes are here (2018). https://consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here
- IRS Tax Tip 2026-56, Identity Protection PINs (July 2026). https://www.irs.gov/newsroom/identity-protection-pins-help-taxpayers-guard-against-tax-related-identity-theft
- FCC, Protecting Consumers from SIM-Swap and Port-Out Fraud, Federal Register (Dec. 2023). https://regulations.justia.com/regulations/fedreg/2023/12/08/2023-26338.html
- FINRA, Senior Investors and Trusted Contact Persons (2026 Oversight Report). https://www.finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report/trusted-contact-persons
- Charles Schwab, SchwabSafe. https://www.schwab.com/schwabsafe
- Charles Schwab, Quick tips to better protect your account. https://www.schwab.com/legal/public-security-tips
- Charles Schwab, Security Guarantee. https://www.schwab.com/schwabsafe/security-guarantee
- Fidelity, Security overview. https://www.fidelity.com/security/overview
- Fidelity, Extra login security with multi-factor authentication. https://www.fidelity.com/security/extra-security-login
- Fidelity, MyVoice. https://www.fidelity.com/security/fidelity-myvoice/overview
- Fidelity, Customer Protection Guarantee. https://www.fidelity.com/security/customer-protection-guarantee