

The Hardware Key Guide

How to Lock Down Your Accounts, Phone, and Privacy, Step by Step, with No Technical Background

By Lawrence Winnerman

October 2026

Prices, products, and menu names were checked against each company's own help pages on October 22, 2026. Menus change; if a screen looks different from what is described here, search that company's help center for "security key" and follow its current steps.

Contents

The Bottom Line

Part 1: Why This Works

Part 2: What to Buy

Part 3: Before You Start: The No-Lockout Rules

Part 4: Choose and Set Up a Password Manager

Part 5: Lock Down Your Main Email and Cloud Account

Part 6: Facebook and Instagram

Part 7: Banks and Money Apps

Part 8: Lock Your Phone Number

Part 9: Lock Down Your Phone and Computer

Part 10: AI-Scam Defenses

Part 11: Private Messaging with Signal

Part 12: Doxxing Cleanup

Part 13: High-Risk-Day Checklist

Part 14: If Something Goes Wrong

The One-Page Checklist

Sources

The Bottom Line

Buy two small hardware security keys, about \$60 for the pair, and register both of them on every account that matters. A key is a physical object that proves it is really you when you sign in. It cannot be phished, guessed, or talked out of you by a scammer with a cloned voice, because it checks the real address of the website before it answers. A fake login page gets nothing.

Keys protect your sign-ins. They do not protect what is already on your phone, what sits in your cloud backups, or what is posted about you on the internet. So this guide pairs the keys with a short list of other steps: a password manager, a locked-down phone and computer, defenses against AI voice and video scams, a cleanup of your personal information online, private messaging, and a checklist for days when you might face police or border agents.

You can do all of it alone at home. Plan on three sittings of about an hour each:

- **Sitting one:** buy keys, set up a password manager, and lock down your main email account (Parts 2 through 5).
- **Sitting two:** add your keys to your other accounts, your social media, and your bank, and lock your phone number with your carrier (Parts 6 through 8).
- **Sitting three:** lock down your phone and computer, and work through the four extra sections (Parts 9 through 13).

The One Rule That Matters Most

Never register just one key. If you lose a lone key, you can be locked out of your own account for days or for good. Every time you add a key to an account, add both keys before you close the page.

Part 1: Why This Works

What a Security Key Is

A security key is a small device about the size of a house key. It plugs into the charging port of your phone or computer, or you tap it against the back of your phone. When you sign in, the website asks the key to prove who you are, and the key answers only if the website is the real one.

That last part is why keys beat every other kind of sign-in protection. A text-message code can be stolen by a scammer who talks your phone company into moving your number to their phone. A

code from an app can be typed into a fake website by mistake. A key cannot be tricked either way, because there is nothing for you to type and nothing for anyone to read over the phone.

Passkeys and Security Keys

You will see the words **passkey** and **security key** used almost interchangeably. A passkey is a sign-in that replaces your password with something you have and something you are or know. It can live inside your phone, inside your password manager, or on a hardware key. When this guide says to add your key, some sites will call it a passkey. That is fine. If a site asks where to save the passkey, choose the security key.

What Keys Do Not Protect

- **What is already on your devices.** If someone gets your unlocked phone, a key does not help. Part 9 covers that.
- **What is stored in the cloud.** A company can be ordered to hand over data it can read. Apple’s Advanced Data Protection (Part 5) and Signal (Part 11) keep more of your data where even the company cannot read it.
- **What is already public.** Data brokers sell home addresses and phone numbers. Part 12 shows how to get yours removed.
- **You, if you are talked into sending money.** Part 10 covers AI voice and video scams.

Part 2: What to Buy

The Recommended Key

Buy two of the **Security Key C NFC by Yubico**, which costs about \$29 each from [Yubico’s store](#). It plugs into a USB-C port and also works by tapping it against the back of a phone. It holds up to a hundred sign-ins, more than most people will ever need.

Your Device	What Works
iPhone 15 or later	Plug it into the charging port, or tap it on the back of the phone.
iPhone 7 through iPhone 14	Tap it on the back of the phone. (These phones have a Lightning port, so the key will not plug in.)
Android phone	Plug it into the charging port, or tap it on the back of the phone.
Mac	Plug it into any USB-C port.
Windows PC with USB-C	Plug it in.

Your Device	What Works
Older Windows PC with only rectangular USB-A ports	Buy the USB-A version instead, the Security Key NFC by Yubico (also about \$29), or buy a small USB-C-to-USB-A adapter.

Other Good Choices

- **Google Titan Security Key** (from about \$30 at the [Google Store](#)). Comes in USB-C and USB-A versions, both with tap. A fine alternative.
- **YubiKey 5C NFC** (about \$58). Does everything the basic key does, plus advanced features this guide does not use. Buy it only if a technical friend tells you that you need it.

Where to Buy Safely

Buy from the maker's own store or a well-known retailer that sells the product directly. Avoid third-party sellers on marketplace sites, where used or tampered keys sometimes turn up. A key is cheap; a fake one is expensive.

When the Keys Arrive

1. Mark one key **Main** and the other **Spare**. A dot of nail polish, a colored key ring, or a small sticker on the flat end all work.
2. Put the main key on your keychain.
3. Keep the spare loose for now. You will need both keys in hand for every account you set up. When you finish, the spare goes into a hiding place at home (see Part 3).

Part 3: Before You Start: The No-Lockout Rules

Security keys are so strong that the main risk is locking yourself out. These five rules prevent that.

1. **Two keys, every account, every time.** Add both keys before you leave each account's settings page.
2. **Print every set of backup codes.** Most accounts give you a list of one-time codes for emergencies. Print them, or write them by hand, and label each sheet with the account name.

3. **Keep the spare and the codes together, hidden at home.** Use an envelope in a drawer, a fireproof box, or the back of a bookshelf. Somewhere you will remember and a burglar would not look first. Do not keep the spare on the same keychain as the main key.
4. **Keep one other way in until both keys work.** Do not delete your phone number or other sign-in methods until you have signed in successfully with each key.
5. **Remember your key PIN.** Your key will ask you to choose a PIN, a short code of at least four characters, the first time you use it. Choose at least six digits and use the same PIN on both keys. Eight wrong tries in a row lock the key for good, and resetting it erases every account on it.

Setting the Key's PIN

On a Mac, iPhone, or Android phone, the first website you add the key to will ask you to create a PIN. Just follow the prompt.

On Windows, you can also set it ahead of time: open **Settings**, click **Accounts**, click **Sign-in options**, click **Security Key**, and click **Manage**. Insert the key and follow the steps.

Your Recovery Envelope

By the end of this guide, the envelope with your spare key should hold:

- ☐ The spare key
- ☐ Your password manager's master password, written down, plus its recovery code or Emergency Kit (Part 4)
- ☐ Google backup codes (Part 5)
- ☐ Microsoft recovery code (Part 5)
- ☐ Facebook and Instagram backup codes (Part 6)
- ☐ Any bank or other backup codes (Part 7)
- ☐ Your phone carrier's account PIN (Part 8)
- ☐ Your computer's encryption recovery key (Part 9)

Part 4: Choose and Set Up a Password Manager

A password manager remembers a different, strong password for every site so you never have to. You remember one master password; it remembers the rest and fills them in for you. It also warns you when a site is fake, because it will not fill in your password on a look-alike address.

Pick One

Option	Cost	Works On	Pick This If...
Bitwarden	Free; Premium is about \$20 a year	iPhone, Android, Windows, Mac, every major browser	You want a free option that works everywhere and accepts your security keys at no cost.
1Password	About \$48 a year (first year often about \$36); fourteen-day free trial	iPhone, Android, Windows, Mac, every major browser	You want the most polished, easiest-to-use app and do not mind paying.
Apple Passwords	Free	iPhone, iPad, Mac; Windows through iCloud for Windows; not Android	Everything you own is Apple (or Apple plus a Windows PC).
Google Password Manager	Free	Android; Chrome on any computer; iPhone through Chrome	You use an Android phone and the Chrome browser.

If you are unsure, start with Bitwarden. It is free, it works on every device in your life, and it is the easiest of the four to protect directly with your keys. The built-in Apple and Google options are protected by your keys indirectly, once you add the keys to your Apple or Google account in Part 5.

Make a Strong Master Password

Your master password should be a passphrase: five or six random, unrelated words, such as **lantern-velvet-tractor-oyster-maple**. It is easy to remember and almost impossible to guess. Do not use a song lyric, a quote, or anything about you. Write it on paper and put it in your recovery envelope.

Bitwarden: Add Your Keys

1. On a computer, go to vault.bitwarden.com and create an account with your passphrase. Install the Bitwarden app on your phone and the Bitwarden extension in your browser.
2. In the web vault, click **Settings**, then **Security**, then **Two-step login**.

3. Next to **Passkey**, click **Manage**. Enter your master password.
4. Type a name, such as **Main key**. Insert the main key and click **Read Key**. Touch the key when it blinks. Click **Save**.
5. Repeat with the spare key, named **Spare key**. Then click **Close**.
6. Back on the **Two-step login** page, click **View recovery code**. Print or write down the code and put it in your recovery envelope.

1Password: Add Your Keys

1. Sign up at 1password.com and install the 1Password app on your phone and computer.
2. During signup, 1Password gives you an **Emergency Kit**, a PDF with your Secret Key. Print it, write your master password in the blank space, and put it in your recovery envelope. (Lost it? Sign in at 1Password.com, click your name, click **Manage Account**, and click **Save Emergency Kit**.)
3. On a computer, sign in at 1Password.com. Click your name in the top-right corner and choose **Manage Account**.
4. Click **More Actions**, then **Manage Two-Factor Authentication**, then **Add a Security Key**.
5. Name the key. If 1Password offers to save a passkey instead, click the security key icon. Insert the key and touch it. Click **Done** when you see the success message.
6. Repeat for the spare key.

Apple Passwords or Google Password Manager

There is nothing extra to set up. These are protected by your Apple or Google account, which you will lock with your keys in the next part. On an iPhone, open the **Passwords** app. On Android, the password manager is built into your phone and Chrome.

Then Put It to Work

1. Start with your most important account: your main email. Use the password manager's generator to make a new, random password, and change your email password to it.
2. Do the same for your bank, your Apple, Google, or Microsoft account, and your social media.
3. Over the next few weeks, every time you sign in somewhere, let the manager save or replace that password. You do not need to fix everything in one day.

An Authenticator App for Sites That Don't Take Keys

Some sites, including many banks, do not accept security keys yet. For those, the next-best protection is an authenticator app, which shows a six-digit code that changes every thirty seconds. Google Authenticator and Microsoft Authenticator are free. 1Password can store these codes for you; Bitwarden stores them in Premium, or you can use the free Bitwarden Authenticator app. Avoid text-message codes wherever you have a choice.

Part 5: Lock Down Your Main Email and Cloud Account

Your main email account is the master key to your whole online life, because every other site sends its password resets there. Lock it down first. Most people have one of these three; do whichever applies to you, or all of them if you use more than one.

Google (Gmail, Android, YouTube)

Do this on a computer in the Chrome browser if you can. It is the smoothest path.

First, Turn On 2-Step Verification and Print Your Backup Codes

1. Go to myaccount.google.com and sign in.
2. Click **Security & sign-in** on the left.
3. Under **How you sign in to Google**, click **2-Step Verification** and follow the steps to turn it on. Google will ask for your phone number. That is fine for now.
4. On the same 2-Step Verification page, click **Backup codes**, then **Get backup codes**. You will get ten codes, each usable once. Print them and put them in your recovery envelope.

Then Add Both Keys

1. Go back to **Security & sign-in** and click **Passkeys and security keys**.
2. Click **Create a passkey**.
3. When your computer offers to save the passkey, choose the option for a security key. It may say **Use another device**, **USB security key**, or something similar.
4. Insert the main key. Create a PIN if asked, then touch the key.
5. Click **Create a passkey** again and repeat with the spare key.

6. Sign out, then sign back in with each key to make sure both work. Google says a new key can take up to seven days to appear as an option at sign-in on some devices, so if it does not show up right away, wait and try again.

Optional: Google's Advanced Protection Program

Google offers a free, stricter mode called the [Advanced Protection Program](#). It requires a key or passkey at every sign-in, checks downloads more strictly, and makes account recovery deliberately slow (it can take a few days) so an attacker cannot talk their way in.

Who should turn it on: anyone who is a likely target, such as journalists, activists, organizers, public figures, people facing harassment, and people in a legal fight. **The trade-off:** you can no longer use printed backup codes, so losing both keys means waiting days to get back in. If you turn it on, keep your spare key somewhere very safe.

Android phones running Android 16 also have a matching phone setting. Open **Settings**, tap **Security & privacy**, tap **Other settings**, tap **Advanced Protection**, and turn on **Device protection**. It blocks apps from outside the Play Store and turns on Google's strongest theft and scam protections.

Apple Account (iPhone, iPad, Mac, iCloud)

Apple's security-key feature is strong and a little unforgiving, so read the requirements before you start.

Before You Begin

- You need **both keys**. Apple will not let you add just one.
- Every Apple device you are signed into must be updated: iPhone and iPad to iOS 16.3 or later, Mac to macOS Ventura 13.2 or later. If you use iCloud on a Windows PC, it needs iCloud for Windows 15 or later.
- Any Apple device you have not used in more than ninety days will be signed out. Old devices that cannot be updated will not be able to sign back in.
- This does not work for children's accounts or for work-managed Apple Accounts.

Add Your Keys on iPhone

1. Open the **Settings** app and tap your name at the top.
2. Tap **Sign-In & Security**, then **Two-Factor Authentication**.
3. Tap **Security Keys**, then **Add Security Keys**, and follow the prompts. Tap or plug in the main key when asked, then the spare.

4. Apple will show you the devices that are signed in to your account. Keep the ones you use and sign out of any you do not recognize.

On a Mac, the path is the same: open the **Apple menu**, choose **System Settings**, click your name, click **Sign-In & Security**, click **Two-Factor Authentication**, and click **Set Up** next to **Security Keys**.

Add a Recovery Contact

A recovery contact is a trusted person with an Apple device who can give you a code if you are ever locked out. They cannot see anything in your account. This is a natural job for a friend who is doing this guide with you.

1. Open **Settings**, tap your name, and tap **Sign-In & Security**.
2. Tap **Recovery Contacts**, then **Add Recovery Contact**.
3. Choose a suggested person or tap **Choose Someone Else**. They will get an invitation in Messages to accept.

Skip Apple's "Recovery Key" Unless You Are Sure

Apple also offers a twenty-eight-character Recovery Key. Turning it on removes Apple's normal account-recovery process, and losing it can lock you out permanently. A recovery contact gives you most of the protection with much less risk.

Turn On Advanced Data Protection

Normally, Apple can read much of what is in your iCloud, including backups, photos, and notes, and could be required to hand it over. Advanced Data Protection encrypts most of that data so that only your devices can read it.

1. Make sure you have a recovery contact (above).
2. Open **Settings**, tap your name, and tap **iCloud**.
3. Tap **Advanced Data Protection**, then **Turn on Advanced Data Protection**, and follow the prompts.

Once it is on, you cannot see your iCloud data at iCloud.com in a web browser unless you turn that access back on. That is the point. (Apple no longer offers this feature to new users in the United Kingdom.)

Microsoft Account (Outlook, Hotmail, Windows, Xbox)

Add Both Keys

1. On a computer, go to account.microsoft.com and sign in.
2. Click **Security** at the top, then **More security options**.
3. Click **Add a new way to sign in or verify**, then **Use a security key**.
4. Choose **USB** or **NFC**, create or enter your key's PIN, and touch the key. Give it a name, such as **Main key**.
5. Repeat for the spare key.

Next time you sign in, choose **Use Windows Hello or security key instead**.

Print Your Recovery Code

1. On the same **More security options** page, find the **Recovery code** section.
2. Click **Generate a new code**. Print it or write it down, and put it in your recovery envelope. Do not save it on the same computer you sign in with.

Part 6: Facebook and Instagram

Meta runs both through one settings area called **Accounts Center**. Facebook accepts security keys. Instagram has been offering them to some accounts; if you do not see the option on Instagram, use an authenticator app instead.

Facebook: Add Your Keys

1. On a computer, go to facebook.com. Click your profile picture in the top-right corner, then **Settings & privacy**, then **Settings**.
2. Click **See more in Accounts Center**, then **Password and security**, then **Two-factor authentication**.
3. Choose your Facebook account and re-enter your password if asked.
4. If Facebook asks you to set up another method first, choose **Authentication app** and follow the steps, then come back.
5. Click **Security key**, then **Add** or **Register security key**. Insert the main key, enter its PIN, and touch it. Click **Done**.
6. Repeat for the spare key.

On an iPhone (iOS 17.4 or later), you can also do this in the Facebook app by tapping the key against the phone. The menu path is the same, starting from **Menu**, then **Settings**.

Instagram

1. In the Instagram app, tap your profile picture, then the menu (three lines) in the top-right corner.
2. Tap **Accounts Center**, then **Password and security**, then **Two-factor authentication**, and choose your Instagram account.
3. If you see **Security key**, add both keys as above. If you do not, choose **Authentication app** and follow the steps.

Print Your Backup Codes for Both

1. In **Accounts Center**, go to **Password and security**, then **Two-factor authentication**, and choose the account.
2. Tap **Additional methods**, then **Backup codes**. Print or write them down and add them to your recovery envelope.
3. Do this once for Facebook and once for Instagram.

While You Are in Accounts Center

Under **Password and security**, turn on **Login alerts** so you hear about any new sign-in, and check **Where you're logged in** for devices you do not recognize. Remove any you do not know.

Part 7: Banks and Money Apps

Banks are behind on security keys. A few accept them, more accept passkeys, and many still rely on text messages. The plan is to use the strongest option each one offers, then add a few safety nets that work everywhere.

What Major Institutions Offer

As of October 2026, this is what we could confirm. Banks change these settings often, so check your own bank's security page.

Institution	Security Key	Passkey	Notes
Bank of America	Yes	No	Key works on a computer; the mobile app still uses text codes.
Vanguard	Yes	Yes	Not usable in the mobile app or mobile website.
PayPal	Yes	Yes	Website only; turn on another method first.
Coinbase	Yes	Reported	Under security settings.
Fidelity	Through a passkey	Yes	Lets you save the passkey on a hardware key.
Wells Fargo	No	Yes	App and website.
Capital One	No	Yes	Website.
U.S. Bank	No	Yes	Website only, still rolling out.
Chase	No	Partial	Rolling out to some customers.
Robinhood	No	iPhone only	
Charles Schwab	No	Not confirmed	Use Schwab app approval.
Citi, Venmo, Cash App	No	No	Text or app codes only.

The General Method for Any Bank

1. Sign in on the bank's website on a computer and find the security settings. They are usually under **Profile**, **Security Center**, or **Security & Privacy**.
2. Look for **security key** first. If it is there, add both keys.
3. If not, look for **passkey**. If the bank lets you choose where to save it, choose your security key. Otherwise, save it to your phone or password manager.
4. If neither is offered, use the bank's own app approval or an authenticator app instead of text messages, if the bank allows it.
5. Print any backup codes and add them to your recovery envelope.

Example: Bank of America

1. On a computer, sign in at bankofamerica.com and open the **Security Center**.
2. Click **Set up Two-Factor Authentication**.
3. Under **Additional Security Features**, click **Review**, then **Add a security key**, and follow the prompts for each key.

Bank of America's own instructions are on its [USB security key page](#).

Safety Nets That Work at Every Bank

- **Turn on alerts** in each banking app for every transaction, login, and change to your contact information.
- **Freeze your credit** at all three credit bureaus, [Equifax](#), [Experian](#), and [TransUnion](#). It is free, it stops anyone from opening new credit in your name, and you can lift it for a day when you need to apply for something.
- **Never pay anyone who contacts you first** with a gift card, wire transfer, cryptocurrency, a crypto ATM, or a payment app such as Zelle or Venmo. Those payments are almost impossible to reverse. See Part 10.

Part 8: Lock Your Phone Number

Most banks still send codes by text, and scammers know it. In a SIM swap, a criminal convinces your phone company to move your number to their phone, then receives your codes. Every major carrier now offers a free lock that blocks this. Turn it on.

Verizon

1. Open the **My Verizon** app and tap the **Me** tab.
2. Tap **Edit profile and settings**, then **Security**.
3. Turn on **SIM Protection** (tap **Confirm**) and **Number Lock** for each line.

AT&T

1. Open the **myAT&T** app on a phone that is on your account.
2. Tap the person icon, then **Wireless account lock**, and swipe to lock.

T-Mobile

1. On the T-Mobile website, sign in and go to **My account**, then **Profile**, then **Privacy and Notification**. Turn on **SIM Protection** for each line.
2. Also add **Port Out Protection**, which stops anyone from moving your number to another carrier. In the **T-Life** app it is under **Manage**, then **Manage add-ons**. If you cannot find it, call 611 from your T-Mobile phone and ask for it by name.

Whatever your carrier, also set an **account PIN** in the same security settings, and add it to your recovery envelope.

Part 9: Lock Down Your Phone and Computer

Keys protect your accounts online. These steps protect the devices themselves if they are lost, stolen, or taken.

Every Device

- **Use a strong passcode.** At least six digits on a phone; longer, or letters and numbers, is better. Never use a birthday or 123456.
- **Turn on automatic updates.** Most break-ins use flaws that an update has already fixed.

iPhone

1. **Stolen Device Protection.** Open **Settings**, tap **Face ID & Passcode**, enter your passcode, and turn on **Stolen Device Protection**. It may already be on. When you are away from home, a thief who saw your passcode still cannot use your saved passwords, erase the phone, or change your Apple Account password without your face or fingerprint, and some changes require a one-hour wait.
2. **Find My.** Open **Settings**, tap your name, tap **Find My**, and make sure **Find My iPhone** is on.
3. **Updates.** Open **Settings**, tap **General**, tap **Software Update**, then **Automatic Updates**, and turn everything on.

Android

1. **Theft protection.** Open **Settings**, tap **Google**, tap **All services**, and tap **Theft protection**. Turn on **Theft Detection Lock**, **Offline Device Lock**, and, if your phone offers it, **Identity Check**.
2. **Find Hub.** If your phone is ever lost, go to google.com/android/find to ring it, lock it with a message, or erase it.
3. **Updates.** Open **Settings**, tap **System**, then **Software updates** (the wording varies by phone maker), and install anything waiting.

Windows

1. Click **Start**, then **Settings**, then **Privacy & security**, then **Device encryption**, and make sure it is **On**. If you do not see **Device encryption**, click **Start**, type **BitLocker**, and open **Manage BitLocker** instead.
2. Encryption saves a recovery key to your Microsoft account. Go to aka.ms/myrecoverykey, sign in, and write the key down for your recovery envelope. Without it, a repair shop or a failed update can leave your files unreadable.

Mac

1. Open the **Apple menu**, choose **System Settings**, click **Privacy & Security**, and scroll to **FileVault**. Click **Turn On** if it is off.
2. When asked how to unlock the disk if you forget your password, choose to create a recovery key, write it down, and put it in your recovery envelope.

Part 10: AI-Scam Defenses

Scammers can now clone a voice from a few seconds of video, fake a live video call, and write flawless, personal emails. In its 2025 report, the FBI's Internet Crime Complaint Center logged more than 22,000 complaints involving AI and nearly \$900 million in losses in the first year it tracked them. The defenses are habits, not technology.

Set a Family Safe Word

The FBI's own advice is to "create a secret word or phrase with your family to verify their identity." Pick a word that never appears online, such as a childhood pet nobody posted about or a silly phrase, and share it only in person. If a loved one calls in a crisis asking for money, ask for the word.

Hang Up and Call Back

If a call, text, or video claims to be your bank, your boss, your grandchild, or the police, hang up and call back on a number you already know is real: the one on the back of your card, in your contacts, or on the official website. A real emergency survives a two-minute delay. A scam does not.

Know the Red Flags

- **Urgency and secrecy.** “Don’t tell anyone” and “You have to do this right now” are the scammer’s two favorite lines.
- **Unusual payment.** Gift cards, wire transfers, cryptocurrency, crypto ATMs, and payment apps. No real agency or bank asks for these.
- **Perfect writing.** Bad grammar used to be a warning sign. AI fixed that, so a polished message proves nothing.
- **Video that’s slightly off.** Odd hands, flickering around the face, shadows that do not match, or a lag between lips and words.

Shrink What Scammers Can Copy

- Set social media accounts to private and remove followers you do not know.
- Think twice about posting long videos of yourself or family members talking.
- Never read a sign-in code to anyone who calls you. No real company will ever ask for one. (Your security key makes this scam impossible for any account that uses it.)

If you are scammed, call your bank at once, then report it at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov) and ic3.gov.

Part 11: Private Messaging with Signal

Regular text messages can be read by phone companies and handed over on request. **Signal** is a free messaging app that encrypts every message and call so that only you and the person you are talking to can read them. Signal itself cannot read them either. Move your sensitive conversations there.

1. Install **Signal** from the App Store or Google Play and register with your phone number.
2. **Set a Registration Lock.** Tap your profile picture, tap **Settings**, tap **Account**, and turn on **Registration Lock**. This stops anyone who steals your phone number from taking over your Signal account. Write the PIN in your recovery envelope.
3. **Make a username.** Tap your profile picture, tap **Settings** (on iPhone), tap your profile, then tap next to the @ symbol and choose a username. Now you can share the username instead of your phone number.
4. **Hide your phone number.** Go to **Settings**, tap **Privacy**, then **Phone Number**. Set **Who can see my number** to **Nobody** first, then set **Who can find me by my number** to **Nobody**.

5. **Turn on disappearing messages.** Go to **Settings**, tap **Privacy**, tap **Default timer for new chats**, and choose a time, such as one week. New chats will clean themselves up.
6. **Turn on screen lock.** Under **Settings**, then **Privacy**, turn on **Screen Lock** so the app needs your face, fingerprint, or passcode to open.
7. **Check linked devices.** Tap your profile picture, tap **Settings** (on iPhone), then **Linked devices**. If you see a computer or tablet you do not recognize, unlink it.

Part 12: Doxxing Cleanup

Data-broker websites collect home addresses, phone numbers, relatives' names, and more, then sell them to anyone. Harassers use them to find people. You can ask them to delete you, either yourself for free or by paying a service to do it.

Step One: See What Is Out There

1. Search your full name plus your city on Google, then your phone number, then your home address.
2. Turn on Google's free **Results about you** tool. In the Google app, tap your profile picture and choose **Results about you**, or go to myactivity.google.com/results-about-you and click **Get started**. It watches Google Search for your phone number, home address, and email, alerts you, and lets you request removal. Note that it removes the result from Google, not the page itself.

Step Two: Opt Out of the Biggest Sites

Each site has a free removal page. Most ask you to find your listing first and confirm by email or phone. Plan on an afternoon for the list below.

Site	Opt-Out Page
Whitepages	whitepages.com/suppression_requests
Spokeo	spokeo.com/optout
BeenVerified	beenverified.com/app/optout/search
Intelius, TruthFinder, Instant Checkmate, US Search	suppression.peopleconnect.us
Radaris	radaris.com/control-privacy
MyLife	mylife.com/privacyrequest

Site	Opt-Out Page
FastPeopleSearch	fastpeoplesearch.com/optout
TruePeopleSearch	truepeoplesearch.com/removal
Nuwber	nuwber.com/removal/link

A volunteer-maintained list of many more brokers is kept at the [Big Ass Data Broker Opt-Out List](#).

Or Pay a Service to Do It

Removal services submit and resubmit requests to hundreds of brokers for you, since listings often reappear. Prices at the time of writing: [Optery](#) has a free scan and paid plans from about \$39 a year; [Incogni](#) is about \$96 a year; [DeleteMe](#) is about \$129 a year.

California Residents: Use DROP

If you live in California, the state's free [Delete Request and Opt-out Platform](#) sends one deletion request to more than 600 registered data brokers at once, and they must act on it. It is the best deal in the country, but it is only for California residents.

Step Three: Lock Down Your Profiles

- On every social account, set past and future posts to **Friends** or **Private**.
- Turn off the setting that lets people find you by email or phone number.
- Turn off location sharing and location tags on posts. Post vacation photos after you get home.
- Ask friends not to tag you or post your location without asking.
- Use a separate email address for shopping and newsletters, and keep your main address private.

Part 13: High-Risk-Day Checklist

Use this before a protest, a border crossing, or any day you might deal with police. It is general information for people in the United States, not legal advice. For your specific situation, read the [EFF's guide to attending a protest](#) and the [ACLU's Know Your Rights resources](#), or talk to a lawyer.

Why Passcode, Not Face or Fingerprint

In the United States, courts generally treat forcing you to reveal a passcode as forcing you to testify, which the Fifth Amendment protects against. Whether police can force your face or finger onto your phone is unsettled; federal appeals courts have disagreed. The EFF's advice is simple: on a high-risk day, turn off face and fingerprint unlock so the phone can only be opened with a passcode.

Before You Go

- ☐ Consider leaving your main phone at home, or bring a spare phone with little personal data on it.
- ☐ Update your phone and make sure your passcode is at least six digits.
- ☐ Turn off face and fingerprint unlock for the day.
- ☐ Move sensitive conversations to Signal with disappearing messages on.
- ☐ Write a lawyer's or trusted friend's phone number on paper, or on your arm in permanent marker, as the ACLU suggests.
- ☐ Carry your ID and only the cards you need.

If Things Get Tense: Lock the Phone in Seconds

- **iPhone:** press and hold the side button and either volume button for about two seconds, until the power-off screen appears, then tap **Cancel**. Your passcode is now required to unlock.
- **Android:** press and hold the power button and tap **Lockdown**. This hides notifications and turns off face and fingerprint unlock until you enter your PIN. (On Samsung phones, first turn the option on in **Settings**, then **Lock screen**, then **Secure lock settings**, then **Show Lockdown option**.)
- Airplane mode is not enough to stop location tracking. Turning the phone fully off is.

For People Who May Be Targeted

If you are an activist, journalist, or organizer and worry about sophisticated spyware, turn on iPhone **Lockdown Mode**: open **Settings**, tap **Privacy & Security**, tap **Lockdown Mode**, tap **Turn On Lockdown Mode**, then **Turn On & Restart**. It blocks most message attachments and link previews, some web features, FaceTime calls from people you have not called recently, and wired accessories while the phone is locked. It is meant for people at real

risk, and it makes the phone a bit less convenient. On Android, Google's Advanced Protection (Part 5) plays a similar role.

At the Border

- U.S. border agents can search phones and laptops without a warrant. Most searches are manual; deeper forensic searches are supposed to require reasonable suspicion.
- Power your devices fully off before you reach the checkpoint, so they require your passcode to unlock.
- U.S. citizens cannot be refused entry for declining to unlock a device, but the device can be held. Green-card holders and visa holders face greater risk; talk to a lawyer before traveling if you are not a citizen.
- If a device is taken, ask for a receipt (Form 6051D).
- The [EFF's border guidance](#) has more detail.

At a protest or with police, the ACLU's guidance is that you never have to consent to a search of your belongings, and police may not demand to see or delete your photos or videos without a warrant.

Part 14: If Something Goes Wrong

You Lost One Key

1. Use the other key to sign in to each account and remove the lost key from its security settings. (This is why you named them.)
2. Order a replacement and add it to every account, so you have two again.

You Lost Both Keys

1. Get your recovery envelope.
2. Use your backup codes for Google, Microsoft, Facebook, Instagram, your password manager, and any bank.
3. For Apple, sign in on any device that is still signed in, or ask your recovery contact for a code.
4. Remove the lost keys from every account, buy two new keys, and add them.

You Got a Suspicious Sign-In Alert

1. Do not click anything in the alert. Open the app or type the website address yourself.
2. Check the account's list of signed-in devices and sign out any you do not recognize.
3. Change that account's password using your password manager.

You Think You Were Scammed

1. Call your bank or card company right away, using the number on the back of your card.
2. Change the passwords on any accounts you gave information about.
3. Freeze your credit if you have not already (Part 7).
4. Report it at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov) and ic3.gov. If your identity was stolen, go to IdentityTheft.gov for a recovery plan.

The One-Page Checklist

Sitting One

- ☐ Bought two security keys and labeled them Main and Spare
- ☐ Set up a password manager and wrote down the master password
- ☐ Added both keys to the password manager (or to the Apple or Google account that protects it)
- ☐ Added both keys to my main email account and printed its backup codes
- ☐ Changed my main email password to a new, random one

Sitting Two

- ☐ Added both keys to my Apple, Google, or Microsoft account (whichever I have not done)
- ☐ Apple only: added a recovery contact and turned on Advanced Data Protection
- ☐ Facebook and Instagram: keys or authenticator app, backup codes printed, login alerts on
- ☐ Banks: strongest option turned on, alerts on, credit frozen at all three bureaus
- ☐ Phone carrier: SIM lock and number lock on, account PIN set

Sitting Three

- ☐ Phone: strong passcode, theft protection, Find My or Find Hub, automatic updates
- ☐ Computer: encryption on and recovery key written down
- ☐ Family safe word chosen and shared in person
- ☐ Signal installed, registration lock on, number hidden, disappearing messages on
- ☐ Data-broker opt-outs done (or a removal service signed up), Results about you turned on, profiles set to private
- ☐ Read the high-risk-day checklist
- ☐ Spare key and recovery envelope hidden at home

Sources

- [Yubico Security Key C NFC](#) and [YubiKey 5C NFC](#)
- [Google Titan Security Key](#)
- [Google: Use a passkey or security key](#) and [backup codes](#)
- [Google Advanced Protection Program](#) and [Android Advanced Protection](#)
- [Apple: About Security Keys for Apple Account](#), [Recovery Contacts](#), [Recovery Key](#), [Advanced Data Protection](#), [Stolen Device Protection](#), and [Lockdown Mode](#)
- [Microsoft: Sign in with a security key](#) and [recovery code](#)
- [Bitwarden: FIDO2 two-step login](#) and [pricing](#)
- [1Password: Use a security key](#), [Emergency Kit](#), and [pricing](#)
- [Bank of America: USB security key](#), [Vanguard: Security keys](#), [Wells Fargo: Passkeys](#), [U.S. Bank: Passkeys](#), and the [2FA Directory](#)
- [Verizon: SIM Protection and Number Lock](#), [AT&T: Wireless Account Lock](#), and [T-Mobile: Online safety](#)
- [Microsoft: Device encryption in Windows](#), [Apple: FileVault](#), and [Google: Theft protection](#)
- [FBI public service announcement on AI-enabled fraud](#), [FBI 2025 Internet Crime Report](#), and [FTC on AI family-emergency scams](#)
- [Signal: Registration Lock](#), [usernames and phone number privacy](#), and [disappearing messages](#)
- [Google: Results about you](#), [California DROP](#), and the [Big Ass Data Broker Opt-Out List](#)
- [EFF: Attending a protest](#), [EFF: Protecting yourself on social networks](#), [EFF: Border searches](#), [ACLU: Protesters' rights](#), and the [Center for Democracy and Technology on compelled biometric unlocking](#)