THE FULL GUIDE



PLAIN ANSWERS · NO SCARE TACTICS

The Complete Proton Setup Guide.

Move your email, passwords, files and calendar to one encrypted account, then lock it down properly. App by app, setting by setting, including what the free plan can and can't do.

ACCOUNT · MAIL · PASS · AUTHENTICATOR · VPN · DRIVE · CALENDAR · WALLET · 30-DAY PLAN

BY ADAPTED.AI · CHECKED AGAINST PROTON'S DOCS, NOV 2026

START HERE

Set it up once. Set it up right.

Most people sign up, send a test email and stop there. That leaves the parts that actually protect you untouched: recovery, 2FA, app locks, autofill and aliases. This guide covers those too.

Read this first 02

Part 1: Your account 06

Part 2: Proton Mail 09

Part 3: Proton Pass 13

Part 4: Proton Authenticator 17

Part 5: Proton VPN 18

Part 6: Proton Drive 20

Part 7: Calendar 22

Part 8: Wallet 23

Your 30-day plan 24

If something goes wrong 25

Pick your pace

TIME	DO THIS	YOU END UP WITH
1 hour	Parts 1 and 3, plus phone apps	A locked-down account and a password manager
1 weekend	Add Parts 2, 4 and 5	Your inbox moved and your connection covered
30 days	Follow the plan on page 24	Old accounts updated and Google optional

OUR REFERRAL LINK

Our Proton links are referral links. If you're new to Proton and subscribe to an eligible paid plan, you and Adapted.ai can each receive $20 in Proton credit, subject to Proton's terms. The free plan costs nothing. We use Proton ourselves, and Proton didn't sponsor or review this guide.

Proton changes features, limits and menu names over time. Everything here was checked against Proton's public documentation in November 2026. Sources are on the last page.

THE MAP

What you get for free.

TOOL	USE IT FOR	FREE PLAN	MAIN REASON TO PAY
Mail	Encrypted email	1 address, up to 1 GB, 150 messages a day, 3 folders, 3 labels, 1 filter	More storage, addresses and filters, custom domains
Pass	Passwords and aliases	Unlimited logins, notes and devices, 2 vaults, 10 aliases, weak and reused password alerts	Built-in 2FA, dark web monitoring, unlimited aliases, Sentinel
Authenticator	2FA codes	Free. No account required; sign in only to sync	Nothing
VPN	Protecting your connection	1 device, 10 countries, no ads, unlimited bandwidth, kill switch	10 devices, all countries, NetShield, Secure Core, streaming
Drive	Encrypted files and photos	Up to 5 GB, Docs and Sheets, password-protected links	More storage, version history
Calendar	Private schedule	3 personal calendars	Up to 25 calendars
Wallet	Self-custody Bitcoin	3 wallets, 3 accounts each	More wallets, Sentinel
Lumo and Meet	Private AI, video calls	Limited Lumo use; Meet calls up to 60 minutes	More usage and features

The 1 GB and 5 GB limits include boosts you unlock by finishing Proton's get-started steps. Without them, you start at 500 MB in Mail and 2 GB in Drive.

What Proton protects, and what it doesn’t

HELPS WITH

- Your email provider reading your stored mail
- Reused and weak passwords
- Your real address leaking through sign-ups
- Your network seeing your browsing
- Files sitting unencrypted in the cloud

WON'T FIX

- You typing a password into a scam site
- Malware already on your device
- Someone with your unlocked phone
- Email you send to a non-Proton inbox being readable there
- Losing your recovery details

THE HONEST VERSION

Privacy tools reduce exposure. They don't replace your judgment. Keep your devices updated, be suspicious of urgency, and treat every unexpected login request as a scam until you've checked.

THE RULE

Apps first. Browser second.

Wherever Proton offers a dedicated app that fits the job, use it. Keep the browser for what actually needs it.

Why we start with the app

Your browser runs code from every site and extension you use. A malicious or hijacked extension can capture passwords, read what's on a page and steal session cookies, which can let someone act as you, sometimes even with 2FA on. A dedicated app isn't exposed to your extensions or to the sites you have open in other tabs.

AN APP ISN'T A FORCE FIELD

If your computer or phone has malware, an app won't save you. Apps reduce your exposure to browser-based risks. Updates, device locks and care about what you install still matter.

TOOL	PHONE	COMPUTER	IN THE BROWSER
Mail	Mail app	Web app on the free plan, since the desktop app is a 14-day trial; desktop app on paid plans	For free-plan users on a computer; check the address every time
Pass	Pass app, with system autofill	Pass desktop app for managing your vault	Official extension only if you want autofill on a computer
Authenticator	Authenticator app	Desktop app if needed	Not needed
VPN	VPN app	VPN app	Skip the extension: the app covers your whole device
Drive	Drive app	Windows or macOS app	Web app for quick access
Calendar	Calendar app	Desktop app	Web app

THE EXTENSION TRADE-OFF

The Pass extension is fine to use, and it has one real upside: it suggests logins by the site you're on, which helps you spot a lookalike page. If you use it, keep it pinned, give it a PIN and auto-lock (page 16), and keep your other extensions to a minimum.

HARDEN YOUR BROWSER

If you use the browser, clean it up.

Five minutes here removes a lot of risk, whichever password manager you use.

1. **Audit your extensions.** Remove anything you don't recognize or no longer use. Fewer extensions means fewer chances for one to go bad.
2. **Check permissions.** "Read and change all your data on all websites" is a lot of trust. Pass needs it for autofill, but a coupon finder probably shouldn't have it.
3. **Install from official links only.** Start at proton.me/pass/download, not a search ad or a link in a message.
4. **Stop saving passwords in your browser.** After you import to Pass (page 14), delete them and turn off your browser's offer to save.
5. **Check the address before you sign in.** Proton's own sign-in lives at account.proton.me.
6. **Use a separate browser profile for banking and admin work.** Keep extensions out of it.
7. **Sign out of what you don't use.** Then review your Proton sessions (page 8).
8. **Keep your browser updated.** Turn on automatic updates and restart when it asks.

Think your browser's been compromised?

- Remove the suspicious extension and run a malware scan.
- From a device you trust, change the passwords for accounts you used in that browser, starting with email and banking.
- Sign out of all active sessions on those accounts. Changing a password alone may not end a stolen session.

OUR RECOMMENDED SETUP

On your phone, install the Mail, Pass, Authenticator, VPN and Drive apps. On your computer, install the Pass, VPN and Drive apps, and add the Pass extension only if you want autofill there.

PART 1 · ACCOUNT

Lock the front door.

Everything else sits behind this login, so do this part first.

Create the account

1. Go to pr.tn/ref/4AMJ01QS, or proton.me if you'd rather not use our link.
2. Start on Proton Free. You can upgrade later.
3. Choose your address carefully. It's the one you'll give your bank.
4. Create a long, unique password that you've never used. Four or five random words work well, and you need to be able to remember this one.
5. Keep that password in your head and on paper somewhere safe, not only inside Pass. Pass sits behind this login.

Then turn on 2FA, in this order

1. Install Proton Authenticator or another authenticator app on your phone.
2. Open Settings → All settings → Account and password, and add two-factor authentication.
3. Scan the QR code and enter the 6-digit code.
4. Save the recovery codes offline. They're how you get in if you lose your phone.

DON'T STORE THIS CODE IN PASS

Proton says never to use Proton Pass for your Proton Account's own 2FA. If you did, you could lock yourself out of your codes and your account at once. Use a separate authenticator app.

EXPERT MOVE

You can link multiple 2FA devices. Add a second phone or tablet, or a hardware security key (U2F or FIDO2, such as a YubiKey), so losing one device doesn't become an emergency. If you're high-risk or hold Bitcoin, a security key is worth buying.

PART 1 · RECOVERY

The step everyone skips.

Proton encrypts your data and can't reset your password for you. If you only reset your login, older data stays locked. Proton says to enable at least one password reset method and one data recovery method.

METHOD	GETS YOU BACK IN	UNLOCKS OLD DATA	GOOD TO KNOW
Recovery phrase	Yes	Yes	12 words. The most convenient option in most cases.
Signed-in reset	Yes	Yes	Only works while signed in somewhere. Don't rely on it alone.
Recovery email	Yes	No	Pair it with a data recovery method.
Recovery phone	Yes	No	Pair it with a data recovery method.
Device data backup	No	Yes	Stored in your browser on a trusted device.
Recovery file	No	Yes	An encrypted file you download and keep safe.
Trusted contacts	No	Yes	Contacts you choose can verify your request.

Our setup for most people

1. **Recovery phrase:** write it on paper and keep it somewhere safe. A fire safe is ideal.
2. **Signed-in reset:** turn it on in Recovery settings, so a signed-in phone can rescue you.
3. **Recovery email:** add one you control that isn't your Proton address, and protect it with 2FA too.
4. **Trusted contact:** add someone you'd trust with an emergency.

TREAT THE PHRASE LIKE CASH

Anyone with your phrase may be able to reset your account. Don't photograph it, email it to yourself or store it in a notes app. Nobody from Proton will ask for it.

EXPERT MOVE

Some recovery methods only work once. If Proton shows you a notice that one is outdated, regenerate it right away in Recovery settings. Then test yourself: could you get back in if your phone fell in a lake today?

PART 1 · HARDENING

Check who's signed in.

Review your sessions

1. Go to account.proton.me → Settings → All settings → Security and privacy → Session management.
2. Check every device on the list.
3. Click **Revoke** on anything you don't recognize, or **Revoke all other sessions** if you're unsure.
4. If you find a stranger, change your password, then check your recovery methods and email forwarding.

Do this monthly. Sessions you don't end expire after 60 days of inactivity.

Proton Sentinel

Sentinel adds stricter checks for suspicious sign-ins, more sign-in visibility, and analysts who review escalated attempts around the clock. It's included with Pass Plus, Unlimited, Duo, Family and Visionary, so it isn't on the free plan. Turn it on in Security and privacy, then enable the Activity monitor and detailed events.

Two-password mode: skip it

You'll see this in settings. Proton calls it a legacy feature and generally doesn't recommend it. It says one-password mode is no less secure, and 2FA gives stronger protection that's easier to use.

Lock your devices

- Use a strong passcode and biometrics on your phone.
- Turn on automatic updates for your phone, computer and apps.
- On iPhone, add Face ID, Touch ID or a PIN lock inside the Proton Mail app, so an unlocked phone doesn't mean an open inbox.
- Turn on Find My or Find Hub, so you can lock or erase a lost device.

ONE ACCOUNT FOR EVERYTHING

Your Proton account signs you in to every app below. If you join through Pass or VPN using a Gmail address, you currently can't connect that Gmail account to Proton Mail, so create a real Proton address first.

PART 2 · PROTON MAIL

What's encrypted, exactly.

"Encrypted email" gets oversold. This is what actually happens, so you know what to trust and when to take an extra step.

SITUATION	IN TRANSIT	WHO CAN READ IT
Proton to Proton	End-to-end encrypted, automatically	Only you and the recipient
Proton to Gmail, Outlook etc.	TLS, when their server supports it	You and the recipient's provider
Password-protected email	End-to-end encrypted	Only someone with the password
Gmail, Outlook etc. to Proton	TLS, unless PGP is used	The sender's provider may keep a copy
Stored in your mailbox	Zero-access encrypted	Proton can't read the message content

THREE THINGS THAT AREN'T END-TO-END ENCRYPTED

Subject lines, sender addresses and recipient addresses are encrypted, but not end-to-end. Never put anything sensitive in a subject line. Use "Documents for Friday," not your client's name and diagnosis.

Send something sensitive to a non-Proton address

1. Write your email in Proton Mail.
2. Add a password using the Password-protected Emails option in the composer, with a hint if you like.
3. Send it. The recipient opens the message using the password.
4. Share the password another way, such as a phone call or text. Never in the same email.

EXPERT MOVE

Check the lock icon in the To field before you send. It shows how the message will be protected for that recipient, so you can add a password or rephrase before it's too late.

PART 2 · PROTON MAIL

Move your Gmail without losing a thing.

Easy Switch brings across your mail, contacts and calendar, and can keep your Gmail address working inside Proton while you move.

OPTION	BEST FOR	WHAT HAPPENS
Recommended setup	Most people	Imports recent mail, then connects Gmail so you can send and receive from it in Proton
Import only	One-time copy	Moves mail, contacts or calendar, with no ongoing connection
Connection only	A clean new inbox	Run the recommended setup, then Undo import, which keeps the connection

1. Open Proton Mail settings → **Import via Easy Switch** → Google.
2. Click **Connect to Gmail** and sign in.
3. Click **Select all** on Google's permissions, then Continue. Missing permissions cause errors later.
4. Wait for the first import. It brings in your most recent messages, up to 80% of your available storage.
5. To import more, choose **More import options**, where you can set a time range, label or specific folders.
6. Check your important folders and contacts.

ON THE FREE PLAN

You get up to 1 GB of Mail storage and can connect one Gmail account. If your Gmail is much bigger, import only the last 3, 6 or 12 months, then keep the rest in a Google Takeout archive.

KNOW WHAT STILL TOUCHES GOOGLE

While connected, messages you send from your Gmail address to non-Proton people go through Google's servers, and Google can read them. The connection is a bridge, not the destination. Google Workspace addresses use a different process.

EXPERT MOVE

Add a label such as "From Gmail" during import so you can always tell old mail from new. Running an import again won't create duplicates, because Easy Switch skips what it already brought in.

PART 2 · PROTON MAIL

Finish the move, for real.

Most people stall here, with two inboxes forever. Work through this order instead.

1. **Update your critical accounts first:** banking, government, healthcare, phone provider and anything linked to payments.
2. **Then update your daily accounts:** shopping, social, subscriptions and work tools. Generate a new password in Pass as you go.
3. **Watch what still arrives through Gmail.** Every time something lands, update that account.
4. **Use Newsletters view** to find subscriptions you forgot about, then unsubscribe or move them to an alias.
5. **Tell your people.** Add your new address to your signature and update your contacts.
6. **Download a full archive** with Google Takeout, then store it somewhere safe.
7. **Disconnect Gmail** under Settings → All settings → Import via Easy Switch, once nothing important arrives there. Forwarding stops at that point.
8. **Delete the Gmail account only if you're sure.** It may also hold your YouTube, Photos, Android and purchase history.

DON'T RUSH THE LAST STEP

Wait at least a few months, so annual renewals and rare logins have time to show up. Many people keep the old account, locked with 2FA and a long password.

CUSTOM DOMAIN?

If you own a domain, paid plans let you use it with Proton Mail. Then you're never tied to a provider's address again, which is the best long-term setup for a business.

PART 2 · PROTON MAIL

Tune your inbox.

Protection you should know about, and what to do when it fires.

FEATURE	WHAT IT DOES	YOUR MOVE
Link confirmation	Shows the full address before opening a link	Read the address before you continue
Tracker protection	Blocks spy pixels, hides your IP and strips known tracking from links in the web app	Check the shield icon to see what was blocked
PhishGuard	Flags possible spoofed Proton senders	Treat those warnings seriously
Password-protected email	End-to-end encryption to any inbox	Use it for tax forms, IDs and contracts
Post-quantum encryption	Prepares new messages for future threats	On all plans, including free
Hide-my-email aliases	Separate addresses that forward to you	Create them in Pass (page 15)

Spot the fake, even with protection on

- **Check the full sender address,** not just the display name.
- **Be suspicious of urgency.** "24 hours or your account closes" is a pressure tactic.
- **Don't sign in from an email link.** Open the app or type the address yourself.
- **A password manager is a phishing test.** If Pass doesn't offer your login on a page, stop and check the address.

ON THE FREE PLAN

You get 3 folders, 3 labels and 1 filter, so use them wisely. We'd use **Action**, **Receipts** and **Archive** as folders, and one filter for your noisiest sender.

USE THE PHONE APP

Install the app, sign in, and on iPhone turn on the app lock. On a computer, the desktop app is only a 14-day trial on the free plan, so use the web app afterwards, and bookmark mail.proton.me rather than searching for it.

AN HONEST TRADE-OFF

Proton describes enhanced tracking protection as a web app feature, so the web app has one real privacy edge. If you read mail in a browser, keep extensions minimal.

PART 3 · PROTON PASS

Install it in this order.

If you only do one thing in this guide, do this. Password reuse is how one breach turns into ten.

iPhone or iPad

1. Install Proton Pass from the App Store and sign in.
2. When prompted, tap **Go to Settings**.
3. In Passwords, open **Password Options**.
4. Turn on **AutoFill Passwords** and select Proton Pass.
5. Enable Face ID or Touch ID when Pass offers.

Android

1. Install Proton Pass from Google Play and sign in.
2. Choose the autofill option in the app.
3. In Android's Autofill service settings, select Proton Pass.
4. Confirm the change.
5. Enable fingerprint unlock when Pass offers.

Computer

1. Install the desktop app for Windows, macOS or Linux from proton.me/pass/download.
2. Sign in, then use it to organize and review your vault.
3. **Optional:** add the official extension for autofill, from that same page.
4. If you add it, pin it to your toolbar, allow site access so autofill can work, and set a PIN (page 16).

EXPERT MOVE

Make Pass your phone's default password manager and turn off your browser's offer to save passwords. If two managers keep offering, you'll end up with logins in the wrong place.

FREE PLAN, REAL PROTECTION

Pass Free includes unlimited logins, notes and devices, a password generator, passkeys, weak and reused password alerts, and 10 aliases. For most people, it's enough to get started.

PART 3 · PROTON PASS

Bring your passwords across.

Pass imports from browsers and other password managers. Here's how it works from Chrome.

1. In Chrome, click your profile picture → **Passwords and autofill** → **Google Password Manager** → **Settings**.
2. Choose **Export passwords** → **Download file**. You now have a .csv file.
3. Upload that file to Proton Pass using its import option.
4. Open your bank and email logins in Pass to check they arrived correctly.
5. **Permanently delete the .csv file,** and empty your trash. Passwords in a .csv aren't encrypted.
6. Once you're sure, go back to Google Password Manager → Settings → **Delete Data**.
7. Turn off your browser's offer to save passwords.

READ THIS BEFORE DELETING

Proton notes that Delete Data removes all of your Google Password Manager data, not just passwords. Confirm that your import worked before you click it.

Fix what you imported, by priority

DO FIRST	THEN	LATER
Email accounts	Cloud storage	Forums and newsletters
Bank and investment accounts	Shopping sites with saved cards	Old apps: delete the account if you don't need it
Phone provider	Social accounts	
Government accounts	Work tools	

What makes a password hard to guess

- **Unique:** a different one for every site, so one leak stays one leak.
- **Long:** let Pass generate a long random password wherever a site allows it.
- **Random:** "P@ssw0rd2026!" follows a pattern attackers already try.
- **Memorized only when needed:** you should only need to remember a few, including your Proton password.

EXPERT MOVE

Pass flags weak and reused passwords for free. Fix five a day when you're already logging in anyway, and within a few weeks the list is short.

PART 3 · PROTON PASS

Aliases, passkeys and 2FA.

Hide-my-email aliases

An alias is a separate address that forwards to your inbox. If a store leaks it or sells it, you turn off that one alias instead of changing your email. It also helps keep your real address out of more databases.

USE AN ALIAS	USE YOUR REAL ADDRESS
Stores and loyalty programs	Banks and government
Newsletters and free downloads	Your doctor, lawyer or accountant
Apps you're trying out	People you know
Contests and Wi-Fi sign-ups	Anything you must recover by email

ON THE FREE PLAN

You get 10 aliases, so spend them on the things most likely to spam you or leak. Pass Plus has unlimited aliases and custom domains. Create one while signing up by choosing **Generate alias** in the Username field.

Passkeys

A passkey replaces your password with a cryptographic key pair and is designed to resist phishing. Pass supports them on all devices, on the free plan too. When an important site offers one, try it and save it in Pass.

2FA codes for your other accounts

PLAN	WHERE CODES LIVE	HOW
Free	Proton Authenticator	Scan each site's QR code in the Authenticator app (page 17)
Pass Plus or higher	Pass, or Authenticator	In Pass: edit the login → **2FA secret (TOTP)** → scan the code. Pass then displays and fills it.

CONVENIENCE OR SEPARATION?

Keeping codes in Pass is convenient. Keeping them in a separate app means someone who gets into your vault still doesn't have your second factor. For email and banking, we prefer the separate app, or a hardware key.

REMINDER

Your Proton Account's own 2FA never goes in Pass. Use Authenticator or a security key.

PART 3 · PROTON PASS

Lock down the vault.

Your vault is encrypted, but anyone holding your unlocked device can still open it. These settings fix that.

SETTING	WHERE	DO THIS
Biometric unlock	iPhone, iPad and Android apps	Turn on Face ID, Touch ID or fingerprint unlock in your Profile
PIN and auto-lock	Browser extension and web app	Settings → Security → PIN code. Set 6 digits and a short auto-lock time.
Extra password	Extension and mobile apps	Adds a second password just for Pass. See the warning below.
Manual autofill	Default behaviour	Keep it. Check the site, then choose the login.
Password health alerts	Free	Fix weak and reused logins as you go
Dark web monitoring	Pass Plus and up	Turn it on if you have a paid plan

EXTRA PASSWORD: ONLY IF YOU CAN KEEP IT

Setting it signs you out of Pass everywhere, and you can't access Pass without it. Store it safely, or skip this if you're likely to forget it.

Why manual autofill matters

Some attacks use hidden fields on malicious pages to trick password managers into filling credentials without you noticing. Proton says Pass uses manual autofill by default, which gives you a moment to confirm where you are.

Share passwords safely

- **Family:** create a shared vault for streaming, Wi-Fi and utilities. Free lets you share a vault with 2 people; Plus allows 10.
- **Everything else stays private.** Keep personal logins in your main vault.
- **Paid extras:** share single items, send secure links, and set up Emergency Access for someone you trust.

Also worth doing

- Store Wi-Fi passwords and software licences in Pass, not your notes app.
- Save your cards in Pass instead of your browser.
- If you lose a device, revoke its session (page 8).

OUR VERDICT

Biometrics on your phone, PIN and short auto-lock on the extension, manual autofill on, and five password fixes a day. That's most of the value.

PART 4 · PROTON AUTHENTICATOR

Your second factor.

A free 2FA app for iOS, Android, macOS, Windows and Linux. You don't need a Proton Account to use it. You sign in only if you want to sync.

Set it up

1. Install it from proton.me/authenticator.
2. Coming from another app? Import from Google Authenticator, 2FAS, Aegis, Bitwarden Authenticator, Ente Auth or LastPass Authenticator.
3. On each site, find the security settings, turn on 2FA and scan the QR code.
4. Enter the code it shows, and save that site's recovery codes.
5. Turn on encrypted backup or sync, or export your codes to another safe location.

TEST BEFORE YOU DELETE THE OLD APP

Sign in to a few accounts using the new codes before removing your old authenticator. Keep each site's recovery codes somewhere offline.

Which 2FA method is strongest?

METHOD	STRENGTH	USE FOR
Hardware key or passkey	Strongest. Designed to resist phishing.	Email, banking and crypto
Authenticator app	Strong, but you can still be tricked into typing a code	Most accounts
Text message	Better than nothing, but open to SIM swaps	Only when there's no other option

Do these first

- Your recovery email account
- Your bank and investment accounts
- Apple or Google account
- Social accounts, especially ones you run a business from
- Your domain and website hosting

EXPERT MOVE

Nobody legitimate will ask you to read out a 2FA code. If someone says "read me the code we just sent" (support, your bank, even a friend), treat it as a takeover in progress. Hang up, and call back on a number you trust.

PART 5 · PROTON VPN

What it does, and what it doesn't.

A VPN encrypts traffic between your device and the VPN server, and hides your IP address from the sites you visit. It's useful, but often oversold.

GOOD FOR

- Public Wi-Fi at hotels, airports and cafés
- Keeping your browsing from your internet provider or local network
- Hiding your IP address from websites

DOESN'T DO

- Stop phishing or scams
- Make you anonymous: sites can still identify you when you sign in
- Remove malware
- Replace 2FA or good passwords

Set it up with the app

1. Install Proton VPN from protonvpn.com/download on the device you use most.
2. Sign in with your Proton account.
3. Press **Connect** and use the recommended option.
4. Turn on the kill switch using the table on the next page.
5. Visit a "what is my IP" page to confirm your address changed.

	FREE	PAID
Devices at once	1	10
Countries	10, chosen for you	140+
Bandwidth and ads	Unlimited data, no ads	Unlimited data, no ads
Kill switch and DNS leak prevention	Included	Included
NetShield ad and malware blocker	No	Yes
Secure Core	No	Yes
Streaming, P2P	No	Yes

WHY THIS FREE VPN IS DIFFERENT

Proton says its free plan is funded by paid subscribers, with no ads and a strict no-logs policy.

PART 5 · PROTON VPN

Turn on the kill switch.

If your VPN drops, a kill switch helps stop your traffic from going out unprotected. It's available on free plans too.

DEVICE	HOW	KNOW THIS
iPhone, iPad	Settings → Security Options → Kill switch	Some Apple DNS requests can bypass the VPN
Android	Settings → Features → Kill switch, then in device settings turn on **Always-on VPN** and **Block connections without VPN**	Not on Android 7 or earlier. Works like an advanced kill switch.
Windows	Settings → Kill switch. Choose Standard or Advanced, then Apply.	Advanced blocks all internet unless connected, even after a restart
macOS	Kill switch icon on the Countries tab → Kill switch On	Your real IP may briefly show when switching servers
Linux	Menu → Settings → Features → Kill switch	Standard is the default; Advanced is stricter

Standard or Advanced?

TYPE	WORKS WHEN	BEST FOR
Standard	The connection drops unexpectedly	Most people
Advanced	Blocks all internet whenever the VPN isn't connected	Anyone who must never browse unprotected

IF YOUR INTERNET SUDDENLY "STOPS WORKING"

An Advanced kill switch may be why. Open the VPN app and reconnect, or turn it off. Local devices such as printers may also become unreachable.

When to run it

SITUATION	OUR CALL
Public or hotel Wi-Fi	Always on
Home Wi-Fi, normal browsing	Your choice; turn it on when you want more privacy
Banking	If your bank blocks it, disconnect and use a trusted network
Work laptop	Check your employer's rules first

EXPERT MOVE

On the free plan, you can only use one device at a time. Put it on the device you use on public networks, usually your phone. If you need more devices or a choice of country, that's the best reason to upgrade.

PART 6 · PROTON DRIVE

Encrypted storage that works.

Your files are end-to-end encrypted. Start with what would hurt most to lose.

DEVICE	USE IT FOR
Windows, macOS app	Syncing files automatically. On Windows, you can also pick folders to back up.
iPhone, Android app	Automatic photo backup and mobile access
Web app	Quick access, plus Docs and Sheets, albums and sharing

1. Install the app, then finish the get-started steps to boost your free storage from 2 GB to 5 GB.
2. Create folders: **Documents**, **Tax**, **Family**, **Photos**.
3. Upload your most important files first: tax records, IDs, contracts and insurance.
4. Turn on photo backup in the mobile app if you have room for it.
5. Move Google Drive files across using your Takeout download.

ON THE FREE PLAN

Up to 5 GB is great for documents, but a phone's photos can fill it fast. Paid plans go to 15 GB, 500 GB and up.

Share files without losing control

1. Share with specific people by email when you can. You can change their access later.
2. If you use a link, add a password and an expiry date.
3. Send the password by another route, such as text or a phone call.

EXPERT MOVE

Free users get link sharing with advanced sharing security, so stop emailing tax returns as attachments. Share a password-protected link with an expiry date instead.

REPLACE GOOGLE DOCS TOO

Proton Docs and Sheets live inside Drive, so sensitive documents can stay in your encrypted space. They're included on the free plan.

PART 6 · PROTON DRIVE

Cloud storage isn’t a backup plan.

Accidents, ransomware and lost accounts can affect synced files too. Use the 3-2-1 rule, which Proton recommends as well.

RULE	WHAT IT MEANS	EXAMPLE
3 copies	The original plus two backups	Laptop, Proton Drive and an external drive
2 storage types	Don't rely on one kind of storage	Cloud and an external drive
1 offsite	Protects against fire or theft	Proton Drive counts

A simple monthly routine

1. Plug in your external drive on the first of the month.
2. Copy your Documents, Family and Photos folders to it.
3. Open a random file to confirm that it works.
4. Unplug it, so ransomware can't reach it.

Moving out of Google Photos and Drive

1. Use **Google Takeout** to export your data, and check that it opens.
2. Back it up to an external drive first.
3. Upload what fits to Proton Drive, starting with the things you can't replace.
4. Only then consider removing it from Google.

SYNC ISN'T BACKUP

With sync, a deleted or encrypted file on your computer can change the cloud copy too. Version history helps, but it's a paid feature, so keep that offline copy.

EXPERT MOVE

Before you rely on any backup, try restoring from it. Your recovery details matter too: after a password reset, encrypted Drive files stay locked without a data recovery method (page 7).

PART 7 · PROTON CALENDAR

Your schedule says a lot about you.

Who you meet, where you go and when you're not home. It deserves the same protection as your inbox.

1. Install the app, or open it on the web using your Proton account.
2. Open Settings → **Import via Easy Switch** → More import options, choose Google, then select **Calendars**.
3. Pick whether to create a new calendar or merge into an existing one.
4. Check next month's events and repeating appointments.
5. Tell people who share calendars with you, before you stop updating the old one.

ON THE FREE PLAN

You get 3 personal calendars. Try **Personal**, **Work** and **Family**. Paid plans go up to 25.

BEFORE YOU LEAVE GOOGLE CALENDAR

Check anything connected to it, such as booking tools, video call links and work scheduling apps. They may need a new connection, or clients could book you at the wrong time.

Also in your account

TOOL	WHAT IT IS	FREE PLAN
Proton Docs and Sheets	Collaborative documents and spreadsheets	Included in Drive
Lumo	Proton's private AI assistant	Limited use and chat history
Proton Meet	Video conferencing	Up to 50 people, 60 minutes
SimpleLogin	Hide-my-email aliases, powered by Proton	Separate product
Standard Notes	Encrypted notes, powered by Proton	Separate product

EXPERT MOVE

Don't try to move everything at once. Mail, Pass and Authenticator give you most of the security value. Calendar, Docs and Lumo can come later, or not at all. A setup you keep using beats a perfect one you abandon.

PART 8 · PROTON WALLET · OPTIONAL

Only if you use Bitcoin.

Proton Wallet is self-custodial: Proton never has custody of your bitcoin. That's the appeal and the responsibility. Skip this section if you don't use Bitcoin. Nothing here is financial advice.

1. Before anything else, finish Part 1. Your Proton password, 2FA and recovery phrase protect your wallet.
2. Open wallet.proton.me or install the app, and sign in. If you don't see it, check Proton's current availability.
3. Choose **Create new wallet**.
4. Write down that wallet's seed phrase on paper and store it securely.
5. Decide whether you want an optional passphrase. You can only add one at creation, and Proton doesn't store it.
6. Turn on biometric unlock in the mobile app, and mask your balance if you like.
7. Send a small test transaction before sending more.

ITEM	WHAT IT DOES	IF YOU LOSE IT
Proton recovery phrase	Restores your Proton encrypted data, including wallets	You may need another recovery method
Wallet seed phrase	Controls that wallet's BTC, and works with any Bitcoin wallet provider	You could lose your BTC
Optional passphrase	Extra layer on that wallet	The wallet can't be recovered

SCAM ALERT

Never share your recovery phrase, seed phrase or passphrase with anyone, including someone claiming to be from Proton. Don't store them in photos, cloud notes or email.

Bitcoin via Email

- Lets Proton Wallet users send and receive bitcoin using an email address.
- **Transactions can't be reversed.** Check the recipient, because there's no undo.
- You need to be logged in for your wallet to generate new receiving addresses.
- Network fees go to miners, not Proton.

EXPERT MOVE

Proton suggests a split if you have a low risk tolerance: Proton Wallet for day-to-day use and a hardware wallet for long-term storage.

YOUR 30-DAY PLAN

Do it in order.

WHEN	DO THIS	DONE WHEN
Day 1	Create your account, write down the recovery phrase, turn on 2FA	You've saved your recovery codes offline
Day 2	Install the phone apps. Turn on app locks.	Pass unlocks with biometrics
Day 3	Import passwords into Pass and delete the .csv	Your browser no longer saves passwords
Day 4	Change your email, bank and phone provider passwords	Top accounts are unique
Day 5	Move your 2FA to an authenticator app	No text message 2FA on key accounts, where possible
Day 6	Clean up your browser extensions	Only what you use is left
Day 7	Connect Gmail with Easy Switch	New mail shows up in Proton
Week 2	Update critical accounts to your new email. Fix 5 passwords a day.	Bank and government accounts are updated
Week 3	Install VPN and turn on the kill switch. Upload key files to Drive. Move your calendar.	Your files have a second home
Week 4	Create aliases, make an offline backup, review sessions and test recovery	You could recover from a lost phone
Month 3+	Run a Google Takeout, then disconnect Gmail if it's gone quiet	Your old inbox is optional

Do you need to pay?

IF YOU…	CONSIDER
Mostly want passwords, built-in 2FA and alias control	Pass Plus
Have a big inbox or want a custom domain	Mail Plus
Want it all: 500 GB, full VPN, Pass, Sentinel	Proton Unlimited
Are setting up with a partner or family	Duo or Family

Start with Proton →

Referral link. New paid subscribers and Adapted.ai can each receive $20 in Proton credit, subject to Proton's terms. Check current prices and refund terms on Proton's site.

IF SOMETHING GOES WRONG

Stay calm. Do this.

WHAT HAPPENED	DO THIS RIGHT AWAY
Lost your phone	Sign in using a recovery code or second 2FA device. Revoke the phone's session, then disable the lost 2FA device. Lock or erase it with Find My or Find Hub. Set up 2FA on your replacement.
Forgot your Proton password	Reset with a recovery method. Then unlock your data with your recovery phrase, recovery file or a trusted device.
Reset your password and data looks scrambled	It's locked, not necessarily gone. Under Recovery, choose Unlock data and use your phrase, file or old password. Try a trusted device first.
Strange sign-in alert	Don't click links in it. Open account.proton.me yourself, review your sessions, change your password and check your recovery details.
Clicked a phishing link	If you typed a password, change it right away from a trusted device, plus anywhere else you used it. Revoke sessions and check your 2FA methods.
Installed a bad extension	Remove it and scan your device. Change passwords from a clean device, starting with email. End all active sessions.
Someone asks for your code or phrase	Stop. Treat it as a scam, even if they claim to be from Proton.
VPN blocks your internet	Reconnect, or turn off the kill switch in the app.
Import looks incomplete	Run it again. Easy Switch skips what's already imported. Check Proton's troubleshooting guide if it keeps failing.

Keep this emergency sheet offline

On paper, somewhere safe, keep your: Proton address · recovery phrase · 2FA recovery codes · where your backup drive is · the name of your trusted contact.

AND TELL SOMEONE

Someone you trust should know this sheet exists. If something happened to you, your family may need your accounts. Paid Pass plans also offer Emergency Access.

THE FULL CHECKLIST

Tick these off.

- [ ] Account created, unique password
- [ ] Recovery phrase on paper
- [ ] Signed-in reset on
- [ ] Recovery email added
- [ ] 2FA on, separate app
- [ ] Recovery codes offline
- [ ] Second 2FA device or key
- [ ] Sessions reviewed
- [ ] Phone apps installed
- [ ] App locks on
- [ ] Browser extensions cleaned up
- [ ] Gmail connected
- [ ] Key accounts moved
- [ ] Passwords imported to Pass
- [ ] .csv file deleted
- [ ] Browser password saving off
- [ ] Top 10 passwords unique
- [ ] First aliases created
- [ ] Authenticator backup on
- [ ] VPN kill switch on
- [ ] Key files in Drive
- [ ] Photo backup chosen
- [ ] External backup made
- [ ] Recovery tested
- [ ] Calendar moved
- [ ] Emergency sheet stored

WANT THIS DONE FOR YOUR BUSINESS?

Adapted.ai builds AI automation, secured from day one. Cybersecurity and IT support are by application. Follow **@adaptedai** for plain-English privacy and security tips, or visit **adapted.ai**.

Sources

- proton.me/support/proton-plans
- proton.me/pricing
- proton.me/pass/pricing
- proton.me/support/set-account-recovery-methods
- proton.me/support/two-factor-authentication-2fa
- proton.me/support/pass-2fa
- proton.me/support/switch-from-gmail-to-proton
- proton.me/support/what-is-encrypted-within-protonmail
- proton.me/mail/security
- proton.me/blog/safe-to-autofill-passwords
- protonvpn.com/support/what-is-kill-switch
- proton.me/blog/how-to-backup-photos
- proton.me/support/wallet-protection
- answers.uillinois.edu/150192