SPY-SUPPLY

PRACTICAL HANDBOOK

OPSEC GUIDE

Understand your risks.
Protect your information.
Stay in control of access.

THREAT MODELS / SCENARIOS / RECOVERY

EN / EDITION 3.0 / SEPTEMBER 2026

spy-supply.com

Your route to better OPSEC

Protect what matters, limit access and prepare for recovery. This guide turns specific risks into safeguards you can verify. Start with chapters 1-3; use chapter 12 during an incident and chapters 16-18 to practise and take action.

Not a product manual or a guarantee of anonymity. A practical framework for informed decisions, with checks and clear limitations.

Contents

01 Decide what you want to protect

Security starts with a specific question: what do you want to prevent?

You may want to stop someone taking over your accounts, finding your home address, reading confidential conversations or obtaining business files. Different risks call for different measures.

Answer these five questions:

1. **What matters?** Consider messages, photos, identity, location, finances and work information.
2. **Who might gain access?** An online scammer, an unwanted observer or someone who finds your device, for example.
3. **What access do they have?** Only public information, access to your email, or physical access to your phone as well?
4. **What would the consequences be?** Inconvenience, financial loss, reputational damage or danger to you or someone else?
5. **Which measures can you maintain?** An impractical system will eventually be bypassed.

This is called a threat model: a realistic assessment of your risks. Review it when your circumstances change. [1]

Turn a risk into a verifiable safeguard

Describe a risk as a specific event: 'Someone who finds my phone can access my email and use it for account recovery.' Avoid broad labels such as 'hackers' without identifying a route to access.

For each risk, record four fields: event, possible consequences, existing protection and next improvement. Rate likelihood and impact separately as low, medium or high; do not invent precise percentages without evidence.

Prioritise a plausible risk with serious consequences, or a low-cost improvement that reduces several risks. Record what remains: a screen lock limits access to a lost phone, but does not stop a recipient forwarding a message.

Check: can you name one safeguard and one way to verify it for each of your three main risks? If not, your plan is still too general.

02 Understand privacy, security and anonymity

These concepts are related, but they mean different things.

Concept	Meaning	Practical example
Privacy	Control over who receives information about you.	An app can access only selected photos.
Security	Protection against unwanted access, misuse or loss.	Your account uses a passkey and has a recovery method.
Anonymity	An activity cannot easily be linked to your identity.	A publication contains no identifying account or personal details.

A well-secured account can still use your real name. A restricted profile may still be identifiable through photos, contacts or what you say.

Distinguish between **the content**, **access to it** and **the surrounding information**. A conversation can be encrypted while details such as its timing or participants remain visible. These details are called metadata. What metadata is available varies by service. [2]

Small clues can reveal much more together

A username, a recognisable background and a recurring time may each seem harmless. Together, they can connect a profile to a workplace or routine. Combining clues can reveal more sensitive information than any individual detail.

Do not assess a post only by asking 'does it contain my name?'. Also ask 'what does this add to information that is already public?'. Consider combinations of faces, locations, contact details and habits. Removal reduces future visibility but does not recall existing copies.

03 Secure your most important accounts first

Your primary email, password manager and cloud account may unlock many other services. Secure these dependencies first, then the remaining accounts. Use unique, random passwords where passkeys are unavailable. Keep them in a well-protected password manager. [3]

Choose your sign-in method deliberately

Method	Strength	Main limitation
Passkey / FIDO2 key	Domain-bound authentication; resists entering a secret into a fake website.	Recovery and protection of the device or synchronisation account still matter.
Password + authenticator code	Additional protection if only the password is exposed.	A phishing page can capture and immediately relay a code.
Password + push approval	Requires a separate approval.	Unexpected requests may prompt accidental approval; number matching helps but is not domain binding.
Password + SMS	An additional barrier beyond a password alone.	Depends on control of the phone number; the code remains vulnerable to phishing.

This comparison describes properties, not certification of individual products. One-time codes are not phishing-resistant. [4]

Passkeys: synced or device-bound

A synced passkey can be available on several devices through a protected ecosystem. This makes recovery easier, but protecting access to that ecosystem becomes important. A device-bound passkey stays on one authenticator, such as a security key; losing it requires another access route arranged beforehand. Both types can provide phishing-resistant authentication. [5]

Choice: use a passkey where it is well supported. Otherwise, use a unique password with the best available additional factor. Keep SMS protection until you have a working alternative; arrange the replacement first.

03 Secure your most important accounts first / continued

Recovery is part of security

Map the chain: which account recovers which other account? Avoid keeping the only recovery code on the phone you could lose, or having two accounts that can only recover each other.

- Store recovery codes separately from your everyday device, in a protected place.
- Register a spare security key where appropriate and check which services accept it.
- Test an alternative sign-in route while your normal session remains available.
- Review old numbers, recovery addresses, app permissions and email forwarding.
- Remove an existing recovery route only after an alternative demonstrably works.

Passkeys and additional factors do not prevent every misuse of an already signed-in session. Changing a password does not revoke every session or permission at every service. If takeover is suspected, separately end unwanted sessions and connected access.

Check: can you recover your most important account if your phone is lost, without a stranger being able to do the same using only your public personal details?

04 Keep your devices trustworthy

Your device is where messages are read, files are opened and accounts are used. Its security therefore affects how much protection your apps can provide.

Make these habits part of everyday use:

- Install operating system, browser and app updates promptly.
- Use devices that still receive security updates.
- Choose a strong screen lock and enable automatic locking.
- Hide sensitive notification content on the lock screen.
- Install software from its official source or a trusted distribution channel.
- Remove apps and browser extensions you no longer need.
- Allow access to your camera, microphone, contacts, location and files only when necessary.

Updates fix known vulnerabilities; postponing them leaves avoidable risks in place. A familiar sender does not automatically make an installer or attachment trustworthy. [6]

Check that device encryption is enabled. It helps protect stored data, particularly when a device is powered off or properly locked. It does not stop someone opening files on an unlocked device or malicious software reading information while the device is in use. [7]

Example: a locked phone may still reveal private information if full messages appear on the lock screen. Check what someone can actually see without unlocking it.

05 Communicate consciously

For confidential conversations, use a service that provides end-to-end encryption for the type of communication you are using. Check whether that also covers group conversations, linked devices and any backups. A marketing term such as 'secure' does not answer these questions.

End-to-end encryption protects the content between participants. Transport encryption protects the connection to a service, but does not by itself mean the provider cannot read the content. [8]

Before sharing, make three checks:

1. **The right person:** do not rely solely on a name, photo or familiar writing style. Confirm an unexpected sensitive request through a contact channel you already trust.
2. **The right conversation:** check the recipient and the members of a group. Do not share confidential information in an old group without knowing who can still read it.
3. **The right amount:** send only what is needed. A complete folder of records is rarely necessary to answer one question.

Where an app supports contact verification using security codes or keys, you can check them together through an independent, trusted channel before sensitive communication.

Encryption does not prevent a recipient from forwarding information, photographing it or reading it on an insecure device. Agree on how information will be retained and whether it may be shared further.

Does a message really disappear?

Disappearing messages reduce the amount of conversation history left behind. They do not guarantee that information has not been saved: a recipient could photograph the screen with another device. Use them to manage retention without assuming that every copy will disappear. [9]

Remember linked devices

A desktop app or tablet may also have access to your communications. Regularly review linked devices and remove unfamiliar or unused connections. Signal provides an overview in the app. [10]

Define what trust means in practice

Checking a security code helps establish which cryptographic identity you are communicating with. It does not by itself prove that someone is honest or authorised to receive information. Verify both identity and the purpose of a request.

For sensitive collaboration, agree on four things: who participates, what may be shared, how long information is needed and how unexpected changes will be confirmed. A new number, changed payment details or a request for extra access requires independent verification.

Check: a second message in the same potentially compromised account is not independent confirmation. Use a previously trusted number, an in-person conversation or an agreed alternative.

06 Recognise manipulation and false urgency

Social engineering tries to influence your behaviour: pay quickly, share a code, install software or give someone access. The request may arrive through email, chat, a phone call, a QR code or a convincing fake website.

Watch especially for the combination of **pressure, an unusual request and an unverifiable sender**. A perfectly written message can still be fraudulent.

Use a consistent response:

- **Pause.** Do not act immediately because someone claims it is urgent.
- **Open the service yourself.** Use the official app or an address you saved previously.
- **Verify independently.** Call back using a number you already knew.
- **Limit access.** Do not install support software or approve a sign-in request you did not initiate.

When signing in, check the actual domain. A logo, name or HTTPS connection does not prove you are on the intended website. [6]

07 Know what a VPN protects

A VPN encrypts traffic between your device and the VPN provider. This can limit what the local network can see and changes the IP address websites see for that traffic.

It also shifts trust towards the VPN provider. A VPN does not prevent phishing, malicious software or identification when you sign in to a personal account. It does not remove cookies or other recognition methods either.

Assess a provider's technical explanations, ownership, data policies and independent reviews. An audit provides information about a particular scope and period; it is not an unlimited guarantee. [11]

Use HTTPS, keep your browser updated and do not ignore certificate warnings just to proceed. Treat unfamiliar networks and unexpected sign-in portals cautiously.

A different IP address does not mean your identity is hidden everywhere.

Match the protection to the problem

Measure	Helps with	Does not solve
HTTPS	Protecting the connection to the website you visit.	A fraudulent website can also use HTTPS.
VPN	Protecting the connection as far as the VPN provider.	Signed-in accounts, untrustworthy recipients or compromised devices.
Private window	Limiting locally retained browsing history after closing, depending on the browser.	Invisibility to websites or the network; downloads remain.
Fewer accounts and permissions	Fewer places where access or information can remain.	Copies already made by others.

When a connection fails, establish what actually stopped working first. Do not disable several protections blindly to restore access. After a necessary temporary change, restore the original setting and verify the result.

[12]

08 Share less personal information

Review your digital presence from the perspective of someone who does not know you. What is public, and what could someone work out by combining small clues?

Check for:

- Profiles displaying a home address, date of birth or personal phone number.
- Public calendars, participant lists and shared documents.
- Photos showing number plates, shipping labels, screens or recognisable locations.
- Posts about regular routines, absences or your current whereabouts.
- Old accounts and posts that no longer reflect what you want to share.

Choose consciously who can see a post. Ask permission before publishing someone else's location, face or contact details. Where appropriate, share sensitive information about your whereabouts only after you have left.

A private account limits the audience, but does not prevent someone in that audience making a copy.

Check files before sending

A document may contain more than its visible pages: comments, tracked changes, author information or hidden sheets. A photo may contain location data. The exact information depends on the file and how it is sent.

Send a checked copy and open it yourself one more time. Inspect both the visible content and the file properties. Do not assume every app automatically removes all metadata.

Uploading to a tool is also sharing

An online translator, PDF converter, AI assistant or public scanning service receives what you upload. Check whether the content is appropriate and how the service handles files. Use an approved environment for sensitive documents and provide only what is necessary.

Remove names and identifying details where possible, but do not assume this guarantees anonymity. A unique situation or combination of details may still identify someone. Do not upload passwords, recovery codes or complete client records to explain one small problem.

09 Keep personal life and work clearly separated

Separation limits accidental mixing and the consequences of a mistake. Choose the level based on the access you need to restrict; a new profile is not automatically a new identity.

Separation	Useful when	Boundary
Separate accounts and folders	Keeping personal and work data apart; granting individual permissions.	The same device and administrator may affect both environments.
Separate browser profiles	Organising cookies, sessions and bookmarks separately.	Not a strong barrier against a compromised operating system.
Separate OS user profiles	Separating app data and users' everyday access.	Isolation varies by system; administrators and system compromise remain relevant.
Separate devices	Isolating sensitive work from riskier everyday activity.	Shared accounts, synchronisation and files can reconnect the environments.

Decide in three steps

1. **Start simply:** separate accounts, individual permissions and clearly labelled storage locations.
2. **Increase separation for a specific reason:** for example, confidential client information on a shared computer. Verify what the chosen system actually isolates.
3. **Choose a separate device for a clear need:** when a mistake in the everyday environment must not immediately reach sensitive work. Arrange updates, backup and recovery for that device too.

For elevated or targeted risk, specialist assessment is more useful than continually adding layers yourself. Separation you routinely bypass provides little benefit.

Review the connections

Check synchronisation, shared mailboxes, cloud folders, extensions and linked devices. Prevent work photos automatically reaching a personal cloud account. Give collaborators only the permissions needed for the task and assign someone to revoke access afterwards.

Check: inspect the membership and sharing settings of one important file. Does every person, group and public link match your intention? Separate folder names alone do not change access permissions.

10 Store deliberately and prepare for recovery

Information you keep needs protection. Information stored on only one device can be lost.

Distinguish between:

Type of information	Recommended approach
Temporary information	Delete it when it is no longer needed.
Important documents	Keep them organised, restrict access and maintain a backup.
Passwords and recovery details	Use an appropriate secure storage method with a recovery plan.
Confidential files	Limit access and protect backup copies too.

For important files, aim to keep multiple copies, including at least one outside your everyday device and one that cannot be continually modified from that device. Choose a method appropriate to the sensitivity and amount of information.

Test your recovery plan in practice:

1. Can you restore a test file?
2. Do you still have the password or key needed for the backup?
3. Can you access it if both your phone and laptop are unavailable?
4. Do you know which apps and files are not included automatically?
5. Is an old, unprotected backup still stored somewhere?

Synchronisation and backup are different. Syncing can propagate a deletion or change to other devices; version history and recovery options vary by service.

Think about erasure in advance

An erase function may be irreversible. Distinguish between erasing local data, revoking account access and deleting copies held by others. One does not automatically accomplish the others.

A remote erase request may depend on connectivity and the service used. Never make it your only protection. Arrange screen locking, encryption and secure recovery beforehand.

Decide how much loss you can tolerate

A weekly backup may mean losing several days of work. Decide how much recent information you can afford to lose and how long you can manage without access. Match backup frequency and recovery methods to those needs.

Test with an unimportant file: create a copy, restore it to a different folder and open the result. Record the date, what worked and what was missing. A 'backup completed' message does not prove you can recover everything.

Do not store the key for an encrypted backup only inside that same backup. A good recovery plan works even when the everyday device is lost, without weakening your protection.

11 Take physical access seriously

Privacy also matters away from the screen. A conversation can be overheard, a document can be left behind and a visitor can use an unlocked computer.

Lock devices when you step away. Consider who can see your screen in public spaces and shared workplaces. Store recovery codes, sensitive paperwork and spare devices appropriately.

Do not casually hand over a fully unlocked device for a simple task. Where possible, open only what is needed and stay present.

Prepare carefully for repair or sale: make sure you have a usable backup, follow the official handover procedure and remove your data before a device changes ownership. Revoke existing account sessions where necessary.

12 Respond calmly when something goes wrong

An unfamiliar sign-in, a missing phone or a file shared by mistake calls for a targeted response. Not every unusual event proves a hack. Record what you actually know and work from a device you trust.

You entered a password on a suspicious page

Open the real service yourself. Change the password, end unfamiliar sessions and review recovery details and connected access. Replace that password anywhere else you reused it. For an email account, also inspect forwarding rules and delegates.

You installed software you do not trust

Do not use the suspect device to change important passwords. Disconnect it from the network where practical and seek qualified help to establish what happened. Removing an app alone does not always provide enough assurance about what remains.

Your phone or laptop is missing

Use previously configured finding or locking features where available. Review important sessions from another trusted device and contact your mobile provider if necessary. Identify which accounts are immediately at risk and revoke access accordingly. Do not confront a suspected thief yourself.

12 Respond calmly when something goes wrong / continued

You sent information to the wrong person

Revoke a shared link where possible. Ask the recipient to delete the information, but do not assume this removes every copy. Replace exposed passwords or codes and inform affected people when their information is at risk.

You suspect targeted monitoring

Use another trusted device to seek help. If someone close to you may be monitoring your activity, sudden changes could be noticed. Plan your next steps around your personal safety.

Record times, warnings and specific events. Do not automatically erase a device if you still want someone to investigate what happened.

Work through four phases

Phase	Action	Record the outcome
1. Establish	Record specific alerts, times and affected accounts. Separate suspicions from facts.	What was observed, on which device and when?
2. Contain	Use a trusted device to stop unwanted access. Prioritise accounts that recover other accounts.	Which sessions, connections or sharing permissions were revoked?
3. Recover	Restore access and, if needed, the device with appropriate help. Check recovery details and unwanted settings.	What works again, and what remains uncertain?
4. Review	Identify the route to access and improve the missing safeguard. Watch for unwanted access returning.	Who will check again, and when?

Seek specialist help for persistent unfamiliar sessions, suspected malware, large amounts of sensitive information or an unclear recovery path. An unplanned factory reset can hinder investigation while leaving compromised cloud accounts unaffected.

For suspected financial fraud, promptly contact the relevant financial service through a known channel. In immediate physical danger, personal safety comes before technical investigation.

13 Build a manageable routine

Monthly

- Review active sessions and linked devices.
- Check updates and remove unused software.
- Review important app permissions and public profile information.
- Check that backups are actually being created.

Periodically and after important changes

- Test recovery of a file or account.
- Review recovery email addresses, phone numbers and backup codes.
- Revoke access from old devices and former collaborators.
- Reassess what you want to protect and who is involved.

This is a practical routine, not an official standard. Adjust the frequency to your risks. You do not need to replace a unique, strong password simply because time has passed; change it when exposure or unwanted access is suspected. [3]

14 Common misconceptions

Claim	What you need to know
'A VPN makes me anonymous.'	Accounts, cookies and other information can still identify you.
'An encrypted conversation cannot leak.'	Participants and their devices remain possible sources of exposure.
'Disappearing messages cannot be saved.'	A recipient can make a copy or take a photo beforehand.
'A private account makes everything private.'	People with access can share information further.
'A strong password is enough.'	Recovery methods, active sessions and additional sign-in protection also matter.
'Erasing my phone removes everything.'	Cloud files and copies held by others do not automatically disappear.
'More security apps mean more safety.'	Each additional app needs maintenance and may receive extra access. Choose purposefully.
'A secure device fixes unsafe behaviour.'	It cannot prevent you voluntarily giving away information or access.

15 Assess providers through evidence

A security claim is a starting point for questions. Ask what information the provider can see, who has administrative access, which components depend on third parties and what happens when you leave. 'Encrypted' does not tell you who controls the keys.

Five questions before trusting a service

1. **What is protected?** Does the claim cover storage, transport or the complete communication between participants?
2. **Who can access it?** Consider administrators, support, connected apps and subcontractors.
3. **What supports the claim?** Look for current documentation, a clear security design and research with a defined scope.
4. **What happens during an incident?** Is there a recognisable reporting channel and an explanation of recovery or communication?
5. **Can you leave?** Can you export information, revoke access and close your account?

An audit assesses what was examined within its stated scope and period. Source availability can enable inspection, but does not prove an inspection took place or that the installed version matches the code.

Decision rule: rely on a claim only as far as you understand its coverage. If an essential question remains unanswered, do not use the service for that particular sensitive task.

The boundary of support

A supplier can explain a feature without knowing your secret codes. During support, agree on what will be visible and end temporary access once the task is finished. Afterwards, review linked devices and permissions. For a simple error message, share a limited screenshot rather than a complete account export.

16 Practise realistic scenarios

The following scenarios are exercises. They show how basic principles work together to prevent or limit an incident.

Scenario A - An invoice with new payment details

Situation: a familiar supplier sends a convincing invoice from the usual account, but the bank details have changed.

Risk: the account may have been taken over. A familiar sender and previous correspondence are not sufficient confirmation.

Action: pause payment. Confirm the change through a previously known number or in person. Do not use the number in the suspicious message. Record the confirmation.

Residual risk: a trusted contact can also be deceived. A second authorised check may be appropriate for large or unusual payments.

Scenario B - A photo for a public sales listing

Situation: the product is clearly visible, but the background includes a label, a laptop screen and a recognisable view.

Risk: several small details expose contact information or identify a location.

Action: take a new photo against a simple background. Check the copy you will send and its metadata. Publish only the information needed to show the product.

Residual risk: earlier publications and copies made by others may remain.

Scenario C - A phone lost during a workday

Situation: the phone holds email, chat and your usual two-step verification method.

Risk: as well as unwanted access, you may lose your own ability to recover accounts.

Action: use your prearranged recovery method on a trusted device. Lock remotely where possible, assess sessions and contact your provider if necessary. Prioritise email and accounts that recover other accounts.

Residual risk: a remote lock or erase command may not arrive immediately. Protection configured beforehand and a usable backup access method remain important.

Scenario D - A collaboration ends

Situation: a former collaborator remains in groups and can still access shared files.

Risk: access survives after the business need has ended.

Action: review accounts, groups, file permissions and shared secrets. Remove permissions and replace shared passwords where they were used. Verify access through membership and permission lists.

Residual risk: you cannot technically recall earlier downloads. Limiting access in advance and agreeing on handling remain necessary.

17 From reading to implementation

Work through this plan at a pace you can maintain. The sequence is a suggestion; during an active incident, containment and recovery take priority.

When	Action	Evidence it is in place
Today	Choose three risks. Secure primary email. Review recovery details and unfamiliar sessions.	A short risk record and checked account settings.
This week	Update devices, review sharing and app permissions, document a recovery route.	Only expected people and devices have access.
Within a month	Test a backup and discuss one incident with someone you trust.	A file has actually been restored and first actions are clear.
Afterwards	Review periodically and after loss, a move, new devices or changed collaboration.	A date and specific next action for every unresolved item.

Verify outcomes, not just settings

'Backup enabled' is a setting; 'file restored and opened' is an outcome. 'Two-step verification enabled' is a setting; 'I have a protected recovery route outside my phone' says something about resilience.

Keep a small review log: date, check, result, exception, action and next review date. Do not record passwords, backup codes or sensitive incident content in it. An overview of your security also deserves restricted access.

Limit complexity

Add a tool only when you can explain which risk it reduces, what new trust it requires and how you will check that it works. Remove duplication that has no demonstrable benefit.

Goal: a manageable system you can maintain, recover and explain to the people you share information with.

18 Your personal OPSEC checklist

Use this list to identify your most important improvements. The number of ticks is not a security score.

- ☐ I know which information matters most to me.
- ☐ My most important accounts use unique passwords or passkeys.
- ☐ My email account and recovery methods are well protected.
- ☐ I recognise the devices that can access my accounts.
- ☐ My devices receive updates and lock automatically.
- ☐ I check who receives my messages and files.
- ☐ I understand the limits of encryption, VPNs and disappearing messages.
- ☐ I avoid sharing unnecessary location, identity or recovery information.
- ☐ I have a usable backup of important information.
- ☐ I know how to respond to loss or suspected account takeover.

Choose the three points that would have the most serious consequences if they went wrong. Address those before making your setup more complicated.

My action plan

My main risk and safeguard

How I will verify it works

My recovery route and trusted support

Next action and review date

Store this privately. Do not record passwords or recovery codes here.

Sources & scope

Technical principles are linked to primary documentation, consulted on 19 September 2026. The titles below are clickable.

[1] EFF - Your Security Plan

[2] EFF - Metadata

[3] EFF - Creating Strong Passwords

[4] NIST - Digital Identity Guidelines

[5] FIDO Alliance - Passkeys

[6] EFF - Avoid Phishing Attacks

[7] EFF - Keeping Your Data Safe

[8] EFF - Communicating With Others

[9] Signal - Disappearing Messages

[10] Signal - Linked Devices

[11] EFF - Choosing a VPN

[12] Google Chrome - Incognito mode

Scope and maintenance

This guide supports individuals and small teams with everyday information security. Targeted attacks, suspected malware or personal danger require specialist help. Product features and recovery options change; consult current documentation. Scenarios and worksheets are practical tools, not certification or guarantees. No independent security audit has been performed.

Review your plan after incidents, new devices or services, and changes in access or collaboration.