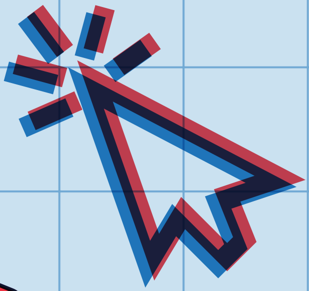
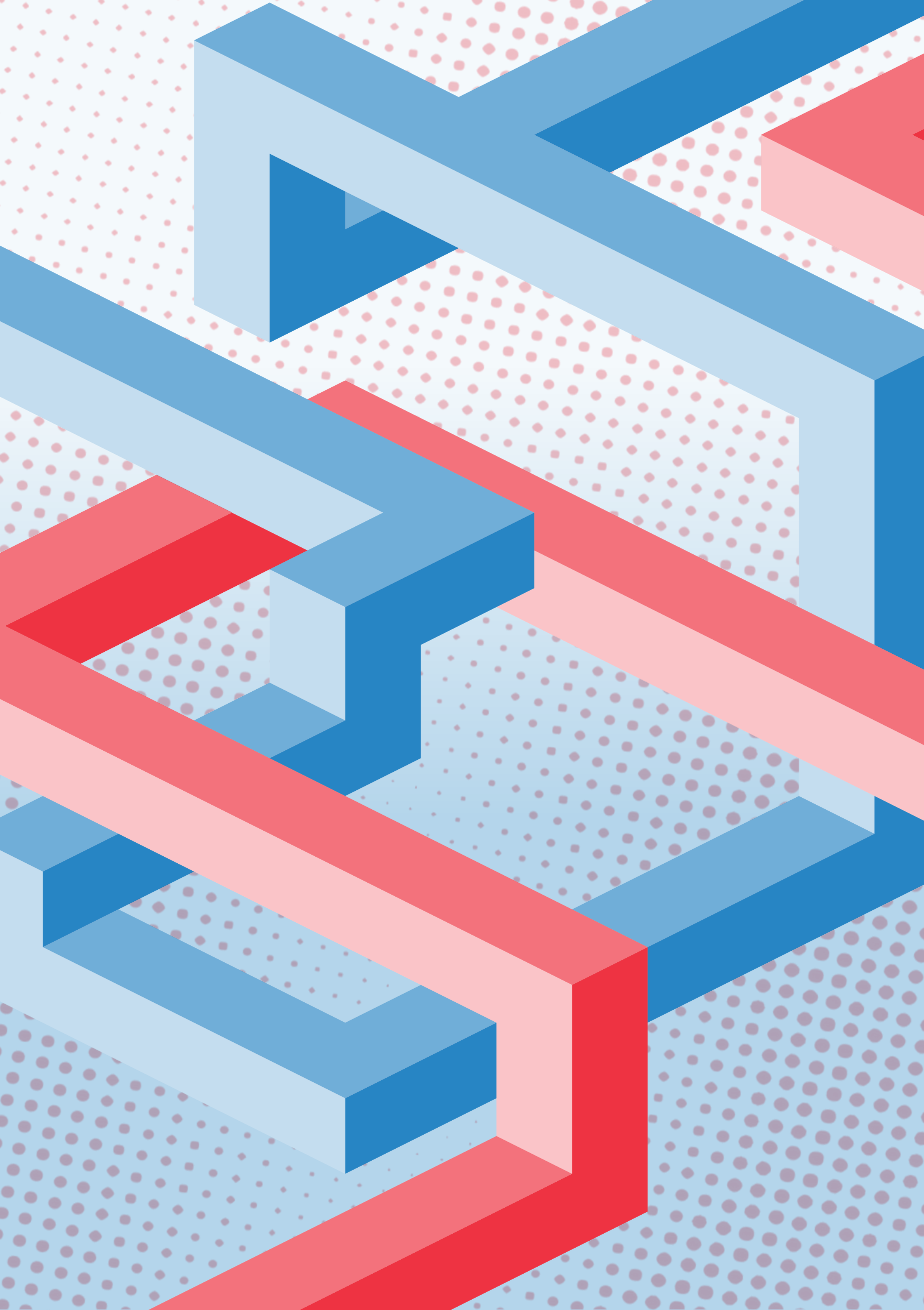


DIGITAL SELF DEFENCE

#1



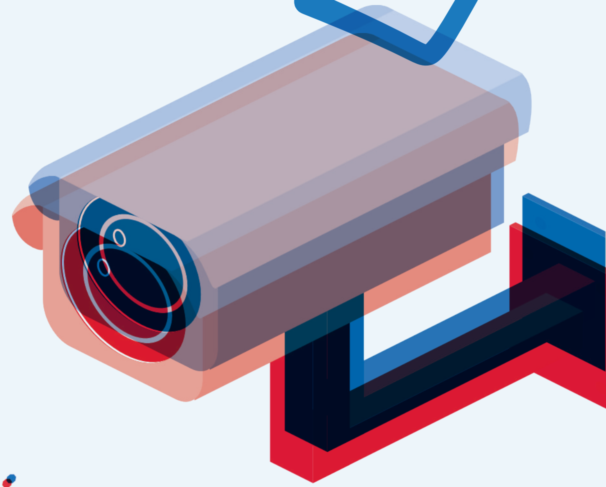
CONTENTS

let us INTRODUCE ourselves

This zine is for political organisers in the UK. It was written in December 2025. It will become out of date quickly. Make sure that you are always accessing up-to-date information.

We are a collective of "tech people" based in Scotland and England working around computer systems in radical political spaces. Our aim is to provide up-to-date, practical and accessible information about digital rights, security, and tools.

how to think about Security



SECURITY NIHILISM VS DEBILITATING PARANOIA

Nihilism and Paranoia are two attitudes which commonly arise in organising spaces which they should be avoided.

Security Nihilism

Security Nihilism is the belief that no matter what lengths you go to to protect your information, it will inevitably be compromised. You may be thinking of your typical hacker, but it could be someone such as the police etc. Essentially the belief is that there is nothing you can do to keep your secrets safe and that you have to take an 'all or nothing' approach to digital security. You may hear people say 'They know everything about us already' or 'I'm not a person of interest, so I don't need to worry about it' to justify their beliefs, but security is solidarity and we all keep each other safer by being careful.

Debilitating Paranoia

You may come across spaces where there is a culture of paranoia with regards to security. This can look like strict organisational policies, secretive, insular or hierarchical culture, arbitrary security procedures etc. These can often act as barriers for grassroots communities to organise effectively, as they may lead to inaccessibility of the movement, low trust, an unwelcoming culture and many digital hoops to jump through that can impede the growth of your group. Crucially, if we are unable to act because we don't trust each other, we are doing the job of our opponents for us.

How *SHOULD* we think about it?

You should take a contextual approach to thinking about digital security. Nothing is completely secure; measures that you take to secure your digital assets are merely a deterrent to those who want to access them. Steps that you take to secure something in one context may be ineffective in another. Security is a practice. You should be constantly revising your security measures and responding to changes quickly. Think about the needs of your group and those that use your tech. Apply threat modelling to strike a balance between security and accessibility.

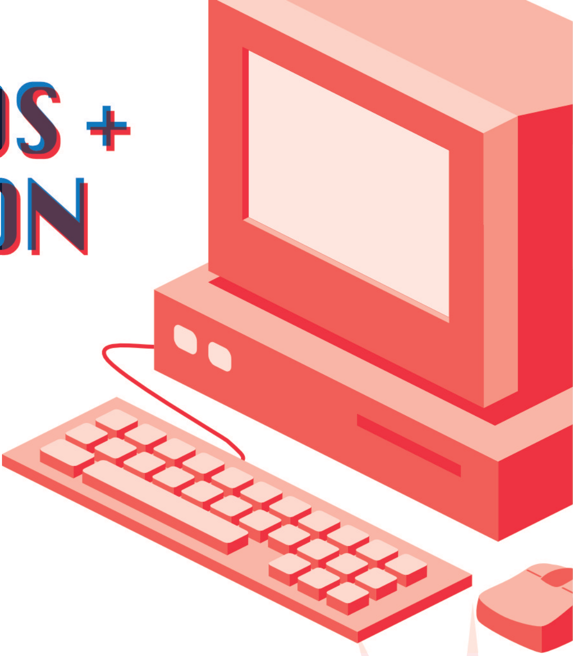
PROPERTY

Take a moment to think about where data about you exists. On your phone, laptops and PCs, notebooks, jotters, diaries, and indeed on far-away servers owned by corporations. Digital property comes in many forms, and you have to take good care to ensure it doesn't fall into the wrong hands.

Data generated by your usage of computers is worth a lot of money to tech companies, especially now that the entire US economy is underpinned by generative AI. So this data can exist for long periods of time in these companies' servers, where it may be used to train AI models, or accessed by third parties, such as advertisers, hackers, or the police.

This data can be quite compromising; phone numbers, location history, biometric data, (sensitive) conversations, interests and habits, the list is endless. It depends on what digital services you use and their privacy policies, and how good you are at limiting data being generated about you through good digital security practice. Let's look at how we can protect our digital property.

PASSWORDS + ENCRYPTION



You use passwords and encryption to keep your data safe from unauthorised access. Think of them like the locks on your front door.

More complex locks and more of them = more security.

Encrypting data causes it to become scrambled and unreadable without a 'key' which is able to reverse the process.

You can read more about asymmetric encryption here.

Before the invention of Password Managers, passwords were typically reused, memorised, or written down by the user, leading to weak passwords (MyFavouriteBook1990!) and insecure storage (remember post-it notes on monitors?).

You wouldn't want the same lock on every house on your street for the same reason you don't use the same password for every account.

For any user accounts you have open, such as email, youtube, facebook etc., you should store your passwords in a ...

Password Manager.

This will make your life much easier and much more secure - all you have to do is remember the password to unlock your password manager.

WE RECOMMEND:

- KeepassXC / KeePassDX,
- Vaultwarden
- Proton Pass

For your devices, such as phones, laptops, and PCs, you should enable disk encryption.

This makes the contents of your device unreadable without first providing a decryption key (you will need to remember this too). Read more about disk encryption here.

Password Managers:

- Generate strong passwords (such as yjJtn7&Me"Gbzb2b)
- Store all of your passwords securely
- Auto-fill them for you when you log in.

Don't use biometric lock, such as FaceID or your Fingerprint to open your devices, as they can be taken from you under duress, and will work on all devices where you have enabled it,

forever.

Passwords that aren't appropriate to store in your password manager (device passwords, decryption keys) can be made memorable by using a series of words that paint a picture or tell some arbitrary story (IWentToTheShopThereWasNoBread!, for example). Passwords like this (known as 'passphrases') are often more secure than gibberish passwords.

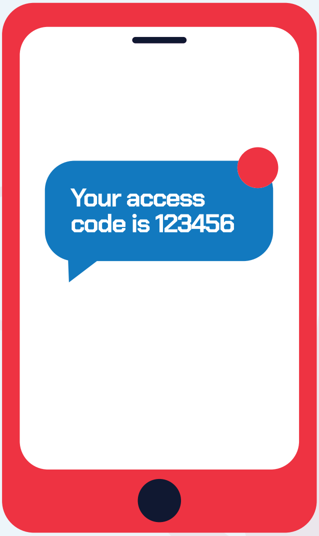
Read more about PASSPHRASES here:

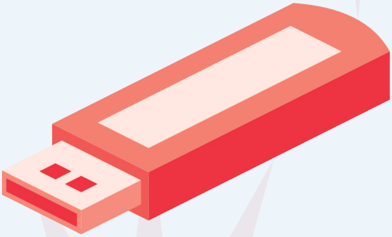
MULTI-FACTOR AUTHENTICATION

In our current era, a password alone is no longer enough to secure a given account.

Two-Factor Authentication (2FA or Multi-Factor Authentication) is a highly effective way to prevent unauthorised access, by adding an additional layer of security to the process of logging in. If your password was leaked in a data-breach, your account may remain uncompromised in this case long enough for you to recover it.

The most common factor used today is an SMS message sent to your phone number with a secret code in it that you provide to finish logging in. This is known as a 'Temporary One-Time Password' or TOTP token.





Note - SMS is not an encrypted means of receiving messages, and so if someone had your password and intercepted this message, they could still gain access to your account. For this reason, you should use an app, such as Proton Authenticator, to receive TOTP tokens securely.

Passkeys are a more modern form of 2FA. Passkeys are only associated with a single device rather than an account, which enhances their security.

They come in different forms - they can prompt you to unlock your phone to prove your identity, or they can be physical USB devices which you have to plug into the device you're trying to log into.

Passkeys offer a lot of flexibility and accessibility without compromising on security. Remember though not to use a biometric passkey! Read more:

HOW TO SEND SECURE MESSAGES

You should always try to send messages to people securely. ***Security is solidarity!*** *You can assume that anything you send which isn't encrypted will be read by another party, be it your network provider, a marketing firm, AI, or other authorities.*

End-to-end encryption *is a type of encryption which scrambles your message before it leaves your device, and only reverses the process when it arrives on your intended recipient's device. This means that if the message is intercepted in transit, the contents* ***cannot be read****. Use end-to-end encryption when sending text messages or emails.*

Signal *is the obvious choice for sending messages to individuals and groups of people as it is open source and highly secure. Note that messages which remain on your phone are not strictly encrypted, which is why* ***device encryption is so important.***

Emails are also not strictly encrypted in transit. They can be an effective way to communicate, but you must observe good security. Use a mail service provider which is end-to-end encrypted such as Proton (though note that an email's subject and other metadata in an email sent by proton is not encrypted) to send and receive encrypted emails when you have to use emails.

Read More

What is metadata?

Metadata is information which describes a given piece of data. In the case of an email, this is normally the sender, recipient, timestamp, and other technical details. On an image file, you may see location data, timestamp, resolution etc.

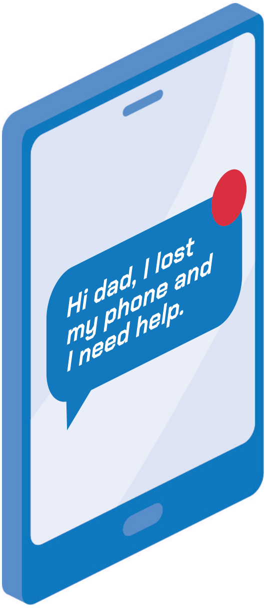
Search for "removed EXIF" for how to clean your files, and note Signal does this automatically.

Wherever possible, **enable disappearing messages** for sensitive conversations. This means that the messages are deleted from your device after a given period of time has passed (assuming the device is switched on so as to delete the message).

If the device were then to become compromised, the messages would not be discovered. Signal and WhatsApp have these features. Always be careful when you choose to send a message - practice sensible sending. If you're on Android, use **Molly** to store your messages securely.

VERIFYING MESSAGES

Send sensibly, receive critically.



It is a good idea to verify messages that you receive if you aren't sure that they are real. Assume your phone number is not a secret.

You may receive calls and messages from scammers or hackers looking to manipulate or steal information from you.

If you receive an unexpected message, reach out to the person by another means to verify that they have contacted you.

Signal provides a safety number which they can give you to prove that the account belongs to them (Chat Header > View Safety number: they should match).

'Sensible Sending' is the principle that the chance of some information being leaked to an unauthorised party increases with the number of authorised parties which the information is sent to. If you send a message about a picket line to 200 colleagues, the chances that a manager is going to see it become exponentially higher. Read the checklist on the next page to see how you can secure your signal account correctly.

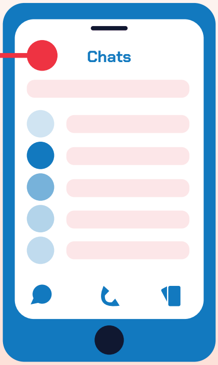
In cyber-security, it's always a good idea to err on the side of caution. Be sceptical of communications which you weren't anticipating. Fact check information, and double check that you know who you're talking to, and that you trust them. Be careful with messages which you send and receive and store them safely. Practising this mindfulness will give you confidence that you can trust your comrades and get the job done!

It's time to secure your

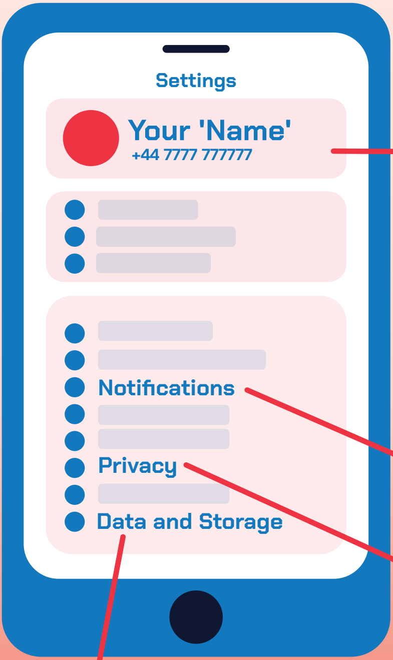
SIGNAL MESSENGER

Some sensible suggestions for Signal setup.

Tap your profile image in the left hand corner to access SETTINGS



Follow these steps and tick them off as you go!



Profile □

- Avoid personally identifying information in your photo and signal name.
- Set a username which doesn't reflect your identity so you can share your contact without a phone number.

Notifications ---> Notification Content □

- Show: Name only OR No name or content.

Privacy □

- Phone Number
Who can see my number: Nobody
Who can find me by number: Nobody
- Disappearing Messages
Default timer for new chats: [something sensible e.g. 1 week]

Data and Storage □

---> Manage Storage

- Keep Messages: [something sensible e.g. 1 month or 6 months]

Please Note! This only applies to android users.

On android? Use MOLLY instead of the standard signal app so you can encrypt your messages while they are sitting on your device.

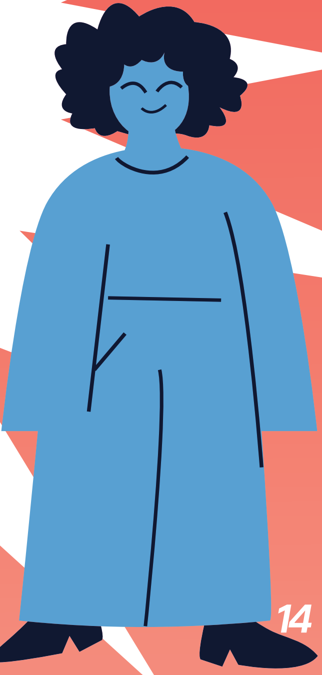
USAGE

There are some good digital hygiene practices it is worth getting used to doing:

1. **Cleaning up old chats**: leave then delete chats that you are no longer using.

2. **Multiple admins**: make sure at least two people are an admin on all group chats you are using.

3. **Remove inactive accounts:** remove old or inactive accounts from signal groups you are an admin for.



EMERGENCY! Monica has been arrested with their phone! What do I do?

Arrests, raids, and tech seizure are becoming increasingly common. Our phones and laptops get targeted.

Hold up! Check with people there at the protest/raid if their phone was taken.

Check with their peers that their device has really been seized. Try to reach out to someone that you can trust as opposed to Monica themself, as their device may be in the hands of the police.

Their phone was taken.

Okay. Here's what to do...

Find out which Signal account is potentially compromised. Most people only have one.

On active chats:

1. Change the chat description to remove sensitive info (you can copy to clipboard)
2. For messages in the last 24 hours you have sent, use the "delete for everyone" option to delete private messages.
3. Remove them LAST - this has to be done last or these changes will not take effect on the stolen phone.

Only if the arrested person is the only admin on the chat...

1. Follow steps (1) and (2) above.
2. Set up a new chat (with two or more admins!).
3. Add everyone other than the arrested person into this chat.
4. THEN stop using the old group and close it as you normally would do.

DON'T remove everyone from a chat just because the seized phone was or is in it.

This does NOT prevent anyone with access to the taken phone's Signal seeing those contacts. Not only does destroying chats not have any security advantages, it also fosters a culture of fear whilst potentially destroying networks and groups.

Share

Find a copy paste message to share in group chats here:

FAQs

What does this do?

- Prevent further messages falling into the cops' hands
- If the phone was connected to the internet, then it potentially reduces access to your signal description and some incriminating messages (the ones you delete)

What do the police get access to?

If the police get through the phone's encryption, then this can the following may be accessed:

- Taken account's contacts
- Taken account's chat descriptions & names
- Taken account's message history (i.e. messages that have already been sent and not deleted by the phone)

Should I leave the chat?

Generally, no. Your contact can't be hidden from the taken phone, and the fact you left would come through and link to your contact. Only leave the chat as during normal cleaning up of inactive chats.

What about if a computer with Signal desktop is taken?

Do you have access to the linked phone?

- **Yes**: change the descriptions and delete messages on chats as above. Then unlink the Signal on the phone app. No further messages will be received on the computer.
- **No**: same process as above.

Does this always work?

No, if the police duplicate the unencrypted device while it is offline these steps have no useful effect. This is why careful Signal usage and device encryption is so important! A well encrypted device that is turned off, or a Molly-Signal that has been locked with a strong password makes the police's job much, much harder.

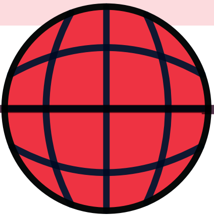
PRIVACY

The digital world is filled with little monsters who want your secrets. You may think that you have nothing to hide, but the modern surveillance state is becoming creepier by the day, and the information that they gather can compromise you and your comrades' security. Let's look at how to protect your privacy online.

BROWSING THE INTERNET SECURELY

Cookies

Cookies are little pieces of data which websites place on your device so that they can refer to it later. Their main purpose is to remember things like login details and settings, but they are also often used for marketing and tracking purposes because websites can read cookies from other places. This makes you easy to identify and gather data about as you continue to browse the web.



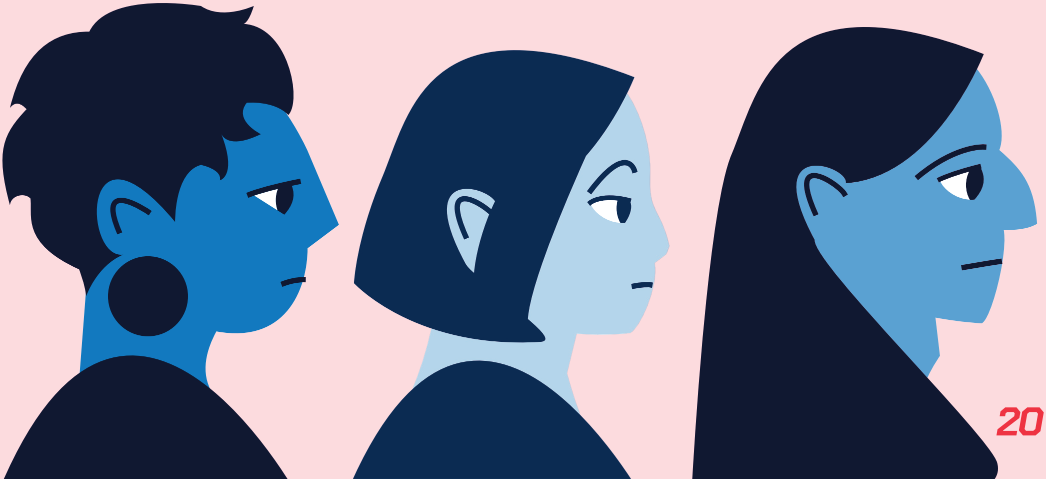
Trackers & Data Collection

Trackers are bits of code that follow you as you move between pages on the internet, gathering very valuable data about you as you go. Most browsers have security features or plugins which can stop these from working. You may also be tracked through hyperlinks, such as links in emails which you receive which are used to determine clickthrough rate and other things for marketing purposes. You can block these types of trackers with the uBlock Origin plugin.

Check out Uber's privacy policy for a great example of the types of data collected about you when you use a modern app (it's basically everything that they can possibly capture - and that's true of almost all apps).

Profiling

Profiling is an activity whereby someone will build up a profile about you based on the data which they have gathered on you. This is normally used for marketing i.e. targeted adverts, but a profile like this is useful for other things too, like testing software, or police intelligence in investigations. Your browsing habits, preferences, interests and hobbies, political influences, private browsing, digital accounts and more can all be factored into this depending on how much data is available to the digital profiler. So from a privacy perspective, it's important to minimise this dataset and ensure that if your data is being stored by anyone, they're storing it securely - and crucially, not selling it. Choosing a privacy-focused browser and using a VPN will help stop your data being leaked as you browse.



Browsers

There are lots of browsers to choose from in today's modern web era! A lot of them are owned by big tech companies, like Google Chrome. We recommend you use an open-source, privacy-focused browser, such as MullVad Browser, LibreWolf or Tor for the highest level of privacy. Try not to use Chrome, Safari or Edge - these browsers are not security or privacy focused.

READ MORE ☒

Websites often use the characteristics of your browser to figure out who you are, such as screen resolution, mouse movements, your plugins, cookies etc. This is Browser Fingerprinting - the act of identifying a user based on the technical characteristics of their device. **Learn more about fingerprinting in the EFF's fun browser tracking tester.** Using a privacy-focused browser limits the effects of browser fingerprinting.

BROWSER TESTER ☒

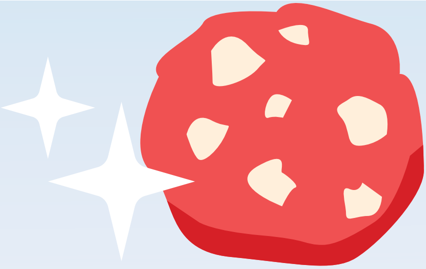
VPN

Virtual Private Networks (VPNs) use encryption to mask your network data from your ISP and other authorities which may be prying into your internet usage. They encrypt your data and send it to highly secure servers which then decrypt your request, handle it, and send you back what you were trying to access, which you then decrypt again. They may cause you to experience slow network speeds, since the request has to bounce around more servers, but they are useful when you are browsing materials that the state doesn't want you to look at (such as Imgur or archive.org) as you can send requests from other countries. **We recommend ProtonVPN or Mullvad VPN.**

Note: the anonymising effect of a VPN is limited by what you do online. If you connect through a VPN, but log into your personal Google account, Google and many others services will still be able to identify exactly who you are.

OPTING OUT

Opting out of data collection is a great way to improve your digital hygiene and protect yourself from data breaches. Always deny cookies, opt out of personalisation, usage data and "telemetry"

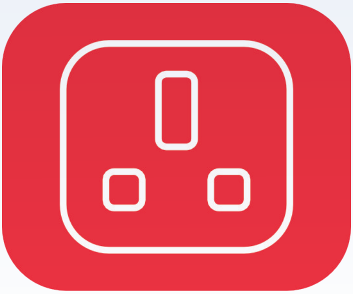


Cookies

When the next cookie banner comes out, take two extra steps to deny all cookies.

Search Engines

Use a search engine which has built in privacy features, such as DuckDuckGo. Google search has become deeply coupled with AI and is neither private nor secure.

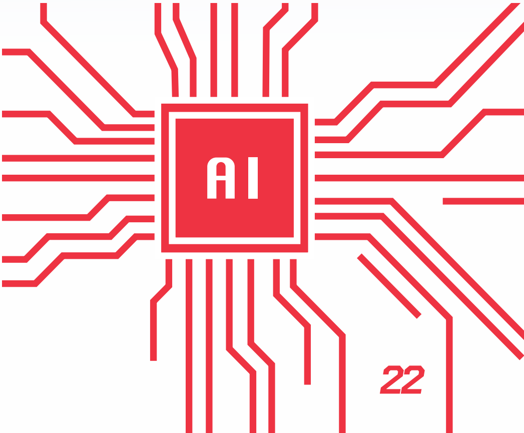


Plugins

Use plugins which block trackers and data collection, such as uBlock Origin, EFF's PrivacyBadger, Facebook Container and others. Only use reputable and widely used plugins, as they can theoretically contain malware.

AI

If you are using services which offer AI features, such as Google Workspace, you need to opt out of data collection for their AI models. GMail will automatically read all of your emails to train Gemini, and the implications of this are not yet fully known. We can't tell you exactly how to do this, so it may need some research on your part.

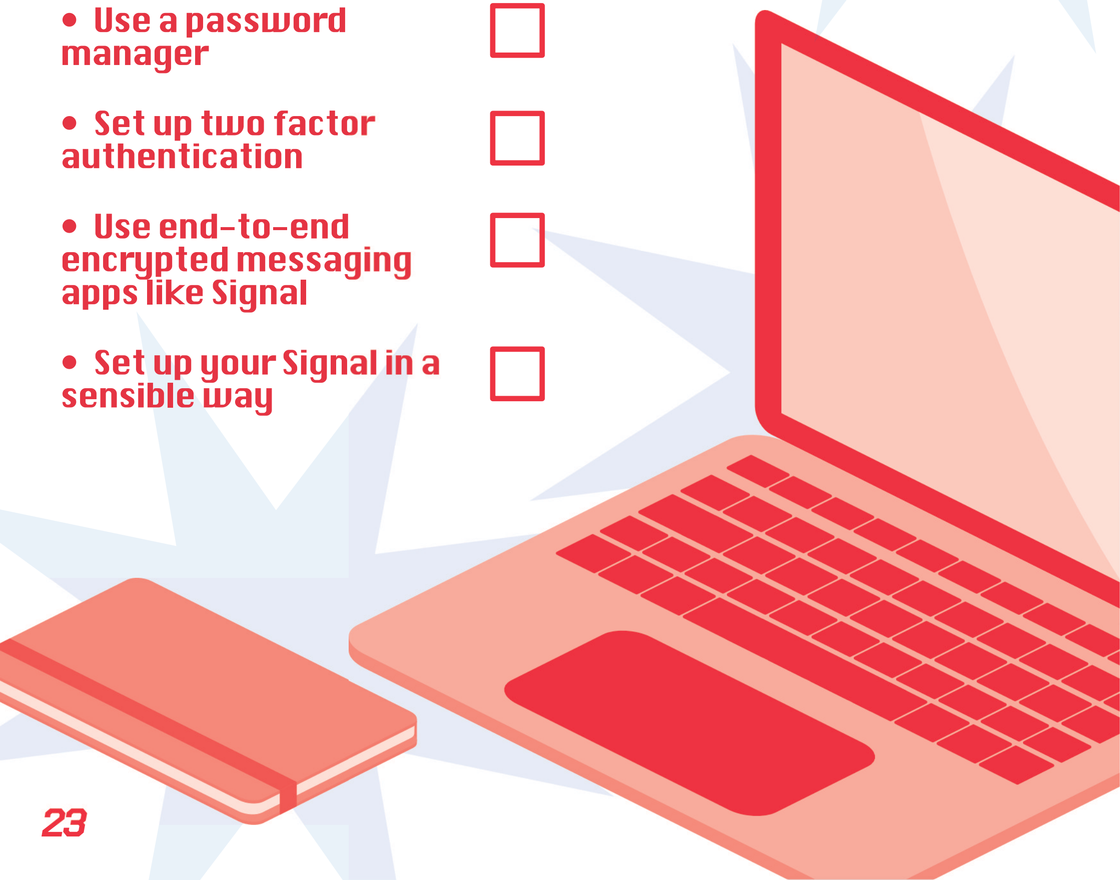


SUMMARY!

Checklist of takeaways!

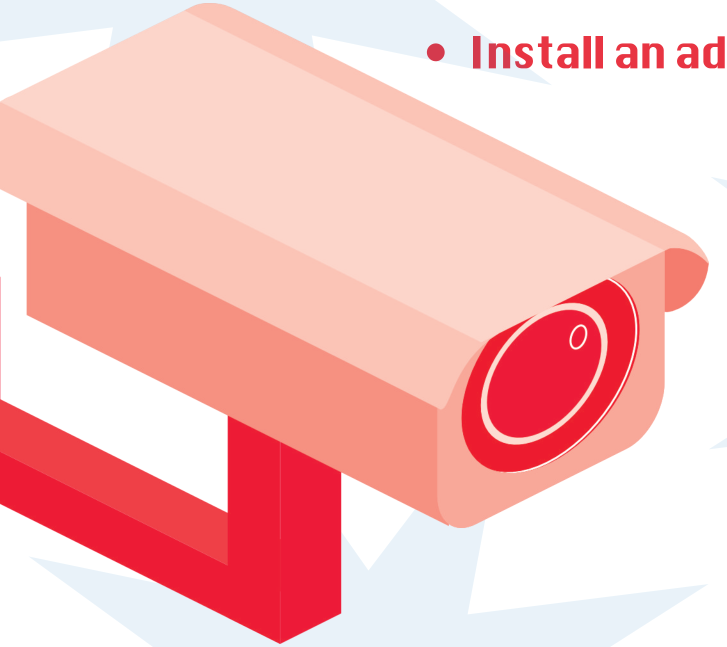
PROPERTY

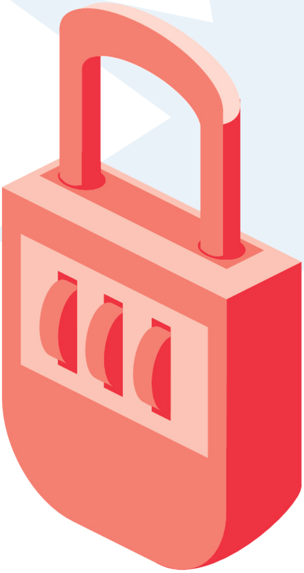
- Encrypt the disk of all of your devices (phone and laptop) □
- Use a password manager □
- Set up two factor authentication □
- Use end-to-end encrypted messaging apps like Signal □
- Set up your Signal in a sensible way □



PRIVACY

- Set up a recommended VPN □
- Opt-out of data gathering □
- Use a privacy focussed browser □
- Use DuckDuckGo □
- Install an ad blocker □





About this Zine

This zine was made by the Digital Self Defence Collective and is for political organisers in the UK. Written in December 2025, this information will go out of date in 2027.

Our focus is on political organisers in the UK in liberation struggles.

Although we touch on the concept of security in general, our focus is on digital security. There are areas of general security practices that you will have to seek education on elsewhere.

Donate Here

We are born from the grassroots movement, and all our money goes into resources and training. Any support will go far:

This zine is for political organisers in the UK. It was written in Dec 2025, and most security advice goes out of date quite quickly. We hope to refresh the content each year, so if you are reading this in 2027 or beyond then please...

BURN ME

[or compost me]

Head to digitalselfdefence.net
to see if there is a new one.

NET POL DSDC