Authentication

Most reported data breaches are caused by the use of weak, default or stolen passwords (according to this Verizon report).

Use long, strong, and unique passwords, manage them in a secure password manager, enable 2-factor authentication, keep on top of breaches and take care while logging into your accounts.

Security	Priority	Details and Hints
Use a Strong Password	Recommended	If your password is too short, or contains dictionary words, places or names- then it can be easily cracked through brute force or guessed by someone. The easiest way to make a strong password, is by making it long (12+ characters)- consider using a 'passphrase', made up of many words. Alternatively, use a password generator to create a long, strong random password. Have a play with HowSecureIsMyPassword.net, to get an idea of how quickly common passwords can be cracked. Read more about creating strong passwords: securityinabox.org
Don't reuse Passwords	Recommended	If someone was to reuse a password, and one site they had an account with suffered a leak (data breaches occur approx. every 39 seconds), then a criminal could easily gain unauthorized access to their other accounts. This is usually done through large-scale automated login requests, and it is called Credential Stuffing. Unfortunately this is all too common, but it's simple to protect against- use a different password for each of your online accounts
Use a Secure Password Manager	Recommended	For most people it is going to be near-impossible to remember hundreds of strong and unique passwords. A password manager is an application that generates, stores and auto-fills your login credentials for you. All your passwords will be encrypted against 1 master passwords (which you must remember, and it should be very strong). Most password managers have browser extensions and mobile apps, so whatever device you are on, your passwords can be auto-filled. A good all-rounder

		is BitWarden, or see Recommended Password Managers
Enable 2-Factor Authentication	Recommended	2FA is where you must provide both something you know (a password) and something you have (such as a code on your phone) to log in. This means that if anyone has got your password (e.g. through phishing, malware or a data breach), they will no be able to log into your account. It's easy to get started, download an authenticator app onto your phone, and then go to your account security settings and follow the steps to enable 2FA. Next time you log in on a new device, you will be prompted for the code that displays in the app on your phone (it works without internet, and the code usually changes every 30-seconds)
Sign up for Breach Alerts	Optional	After a website suffers a significant data breach, the leaked data often ends up on the internet. There are several websites that collect these leaked records, and allow you to search your email address to check if you are in any of their lists. Firefox Monitor, Have i been pwned and Breach Alarm allow you to sign up for monitoring, where they will notify you if your email address appears in any new data sets. It is useful to know as soon as possible when this happens, so that you can change your passwords for the affected accounts. Have i been pwned also has domain-wide notification, where you can receive alerts if any email addresses under your entire domain appear (useful if you use aliases for anonymous forwarding)
Keep Backup Codes Safe	Optional	When you enable multi-factor authentication, you will usually be given several codes that you can use if your 2FA method is lost, broken or unavailable. Keep these codes somewhere safe, to prevent loss or unauthorised access. You could store them in your password manager, in an encrypted note, or write them down somewhere safe
Shield your Password/ PIN	Optional	When typing your password in public places, ensure you are not in direct line of site of a CCTV camera and that no one is able to see over your

		shoulder. Cover your password or pin code while you type, and do not reveal any plain text passwords on screen
Update Passwords Periodically	Optional	Database leaks and breaches are common, and it is likely that several of your passwords are already somewhere online. Occasionally updating passwords of security-critical accounts can help mitigate this. But providing that all your passwords are long, strong and unique, there is no need to do this too often- annually should be sufficient. Enforcing mandatory password changes within organisations is no longer recommended, as it encourages colleagues to select weaker passwords
Don't save your password in browsers	Optional	Most modern browsers offer to save your credentials when you log into a site. Don't allow this, as they are not always encrypted, hence could allow someone to gain access into your accounts. Instead use a dedicated password manager to store (and auto-fill) your passwords
Be cautious when logging in on someone else's device	Optional	When using someone else's machine, ensure that you're in a private/ incognito session (Use Ctrl+Shift+N/ Cmd+Shift+N). This will ensure that none of your credentials, cookies, browsing history of session data gets saved. Ideally you should avoid logging into your accounts on other people's computer, since you can't be sure their system is clean. Be especially cautious of public machines, as malware and tracking is more common here
Avoid password hints	Optional	Some sites allow you to set password hints. Using this feature can make it easier for social engineers to guess your credentials
Never answer online security questions truthfully	Optional	If a site asks security questions (such as place of birth, mother's maiden name or first car etc), don't provide real answers. It is a trivial task for hackers to find out this information online or through social engineering. Instead, create a fictitious answer, and store it inside your password manager
Don't use a 4-digit PIN	Optional	Don't use a short PIN to access your smartphone or computer. Instead, use a text password or much

		longer pin. Numeric passphrases are easy crack, (A 4-digit pin has 10,000 combinations, compared to 7.4 million for a 4-character alpha-numeric code)
Avoid using SMS for 2FA	Optional	When enabling multi-factor authentication, opt for app-based codes or a hardware token, if supported. SMS is susceptible to a number of common threats, such as SIM-swapping and interception. There's also no guarantee of how securely your phone number will be stored, or what else it will be used for. From a practical point of view, SMS will only work when you have signal, and can be slow
Avoid using your PM to Generate OTPs	Advanced	Many password managers are also able to generate 2FA codes. It is best not to use your primary password manager as your 2FA authenticator as well, since it would become a single point of failure if compromised. Instead use a dedicated authenticator app on your phone or laptop
Avoid Face Unlock	Advanced	Most phones and laptops offer a facial recognition authentication feature, using the camera to compare a snapshot of your face with a stored hash. It may be very convenient, but there are numerous ways to fool it and gain access to the device, through digital photos and reconstructions from CCTV footage. Unlike your password- there are likely photos of your face on the internet, and videos recorded by surveillance cameras
Watch out for Keyloggers	Advanced	A hardware keylogger is a physical device planted between your keyboard and the USB port, which intercepts all key strokes, and sometimes relays data to a remote server. It gives a hacker access to everything typed, including passwords. The best way to stay protected, is just by checking your USB connection after your PC has been unattended. It is also possible for keyloggers to be planted inside the keyboard housing, so look for any signs that the case has been tampered with, and consider bringing your own keyboard to work. Data typed on a virtual keyboard, pasted from the clipboard or auto-filled by a password manager can not be intercepted by a hardware keylogger, so if you are

		on a public computer, consider typing passwords with the on-screen keyboard
Consider a Hardware Token	Advanced	A U2F/ FIDO2 security key is a USB (or NFC) device that you insert while logging in to an online service, in to verify your identity, instead of entering a OTP from your authenticator. SoloKey and NitroKey are examples of such keys. They bring with them several security benefits, since the browser communicates directly with the device and cannot be fooled as to which host is requesting authentication, because the TLS certificate is checked. This post is a good explanation of the security of using FIDO U2F tokens. Of course it is important to store the physical key somewhere safe, or keep it on your person. Some online accounts allow for several methods of 2FA to be enabled
Consider Offline Password Manager	Advanced	For increased security, an encrypted offline password manager will give you full control over your data. KeePass is a popular choice, with lots of plugins and community forks with additional compatibility and functionality. Popular clients include: KeePassXC (desktop), KeePassDX (Android) and StrongBox (iOS). The drawback being that it may be slightly less convenient for some, and it will be up to you to back it up, and store it securely
Consider Unique Usernames	Advanced	Having different passwords for each account is a good first step, but if you also use a unique username, email or phone number to log in, then it will be significantly harder for anyone trying to gain unauthorised access. The easiest method for multiple emails, is using auto-generated aliases for anonymous mail forwarding. This is where [anything]@yourdomain.com will arrive in your inbox, allowing you to use a different email for each account (see Mail Alias Providers). Usernames are easier, since you can use your password manager to generate, store and auto-fill these. Virtual phone numbers can be generated through your VOIP provider

Recommended Software: Password Managers | 2FA Authenticators

Web Browsing

Most websites on the internet will use some form of tracking, often to gain insight into their users behaviour and preferences. This data can be incredibly detailed, and so is extremely valuable to corporations, governments and intellectual property thieves. Data breaches and leaks are common, and deanonymizing users web activity is often a trivial task

There are two primary methods of tracking; stateful (cookie-based), and stateless (fingerprint-based). Cookies are small pieces of information, stored in your browser with a unique ID that is used to identify you. Browser fingerprinting is a highly accurate way to identify and track users wherever they go online. The information collected is quite comprehensive, and often includes browser details, OS, screen resolution, supported fonts, plugins, time zone, language and font preferences, and even hardware configurations.

This section outlines the steps you can take, to be better protected from threats, minimise online tracking and improve privacy. A summarized shorter version of this list can be found here

Security	Priority	Details and Hints
Ensure Website is Legitimate	Basic	It may sound obvious, but when you logging into any online accounts, double check the URL is correct. When visiting new websites, look for common signs that it could be unsafe: Browser warnings, redirects, on-site spam and pop-ups. You can also check a website using a tool, such as: Virus Total URL Scanner, IsLegitSite, Google Safe Browsing Status if you are unsure
Watch out for Browser Malware	Basic	Your system or browser can be compromised by spyware, miners, browser hijackers, malicious redirects, adware etc. You can usually stay protected, just by: ignoring pop-ups, be wary of what your clicking, don't proceed to a website if your browser warns you it may be malicious. Common sighs of browser malware include: default search engine or homepage has been modified, toolbars, unfamiliar extensions or icons, significantly more ads, errors and pages loading much slower than usual. These articles from Heimdal explain signs of browser malware, how browsers get infected and how to remove browser malware

Use a Privacy-Respecting Browser	Recommended	Firefox and Brave are secure, private-by-default browsers. Both are fast, open source, user-friendly and available on all major operating systems. Your browser has access to everything that you do online, so if possible, avoid Google Chrome, Microsoft IE and Apple Safari as (without correct configuration) all three of them, collect usage data, call home and allow for invasive tracking. See more: Privacy Browsers
Use a Private Search Engine	Recommended	Using a privacy-preserving, non-tracking search engine, will ensure your search terms are not logged, or used against you. Consider DuckDuckGo, Quant, or SearX (self-hosted). Google implements some incredibly invasive tracking policies, and have a history of displaying biased search results. Therefore Google, along with Bing, Baidu, Yahoo and Yandex are incompatible with anyone looking to protect their privacy. It is recommended to update your browsers default search to a privacy-respecting search engine
Remove Unnecessary Browser Addons	Recommended	Extensions are able to see, log or modify anything you do in the browser, and some innocent looking browser apps, have malicious intentions. Websites can see which extensions you have installed, and may use this to enhance your fingerprint, to more accurately identify/ track you. Both Firefox and Chrome web stores allow you to check what permissions/access rights an extension requires before you install it. Check the reviews. Only install extensions you really need, and removed those which you haven't used in a while
Keep Browser Up-to-date	Recommended	Browser vulnerabilities are constantly being discovered and patched, so it’s important to keep it up to date, to avoid a zero-day exploit. You can see which browser version your using here, or follow this guide for instructions on how to update. Some browsers will auto-update to the latest stable version
Check for HTTPS	Recommended	If you enter information on a non-HTTPS website, this data is transported unencrypted and can therefore be read by anyone who intercepts it. Do not enter

		any data on a non-HTTPS website, but also do not let the green padlock give you a false sense of security, just because a website has SSL certificate, does not mean that it is legitimate or trustworthy. HTTPS-Everywhere (developed by the EFF) is a lightweight, open source (on GitHub) browser addon, that by enables HTTPS encryption automatically on sites that are known to support it. Is included in Brave, Tor and mobile Onion-Browser, and is available for Chromium, Firefox and Opera
Use DNS-over-HTTPS	Recommended	Traditional DNS makes requests in plain text for everyone to see. It allows for eavesdropping and manipulation of DNS data through man-in-the-middle attacks. Whereas DNS-over-HTTPS performs DNS resolution via the HTTPS protocol, meaning data between you and your DNS resolver is encrypted. A popular option is CloudFlare's 1.1.1.1, or compare providers- it is simple to enable in-browser. Note that DoH comes with it's own issues, mostly preventing web filtering
Multi-Session Containers	Recommended	Compartmentalisation is really important to keep different aspects of your browsing separate. For example, using different profiles for work, general browsing, social media, online shopping etc will reduce the number associations that data brokers can link back to you. One option is to make use of Firefox Containers which is designed exactly for this purpose. Alternatively, you could use different browsers for different tasks (Brave, Firefox, Tor etc). For Chromium-based browsers, you can create and use Profiles, or an extension such as SessionBox, however this addon is not open source
Use Incognito	Recommended	When using someone else's machine, ensure that you're in a private/ incognito session (Use Ctrl+Shift+N/ Cmd+Shift+N). This will prevent browser history, cookies and some data being saved, but is not fool-proof- you can still be tracked
Understand Your Browser Fingerprint	Recommended	Browser Fingerprinting is an incredibly accurate method of tracking, where a website identifies you based on your device information, including: browser and OS versions, headers, time zone, installed fonts, plugins and applications and

		sometimes device hardware among other data points. You can view your fingerprint at amiunique.org- The aim is to be as un-unique as possible
Manage Cookies	Recommended	Clearing cookies regularly is one step you can take to help reduce websites from tracking you. Cookies may also store your session token, which if captured, would allow someone to access your accounts without credentials (often called Session Hijacking). To mitigate this you should clear cookies often. Self Destructing Cookies is a browser addon, which will kill cookies when you close the browser
Block Third-Party Cookies	Recommended	Third-party cookies placed on your device by a website other than the one you're visiting. This poses a privacy risk, as a 3rd entity can collect data from your current session. This guide explains how you can disable 3rd-party cookies, and you can check here ensure this worked
Block Ads	Recommended	Using an ad-blocker can help improve your privacy, by blocking the trackers that ads implement. uBlock Origin is a very efficient and open source browser addon, developed by Raymond Hill. When 3rd-party ads are displayed on a webpage, they have the ability to track you, gathering personal information about you and your habits, which can then be sold, or used to show you more targeted ads, and some ads are plain malicious or fake. Blocking ads also makes pages load faster, uses less data and provides a less cluttered experience
Block Third-Party Trackers	Recommended	Blocking trackers will help to stop websites, advertisers, analytics and more from tracking you in the background. Privacy Badger, DuckDuckGo Privacy Essentials, uBlock Origin and uMatrix (advanced) are all very effective, open source tracker-blockers available for all major browsers. Alternatively you can block trackers at the network level, with something like Pi-Hole (on your home server) or Diversion (Asus routers running Merlin firmware. Some VPNs offer basic

		tracking blocking (such as TrackStop on PerfectPrivacy)
Beware of Redirects	Optional	While some redirects are harmless, others, such as Unvalidated redirects are used in phishing attacks, it can make a malicious link seem legitimate. If you are unsure about a redirect URL, you can check where it forwards to with a tool like RedirectDetective. It is also recommended to disable redirects in your browser settings.
Do Not Sign Into Your Browser	Optional	Many browsers allow you to sign in, in order to sync history, bookmarks and other browsing data across devices. However this not only allows for further data collection, but also increases attack surface through providing another avenue for a malicious actor to get hold of personal information. For Chrome users, you can get around forced sign-in by navigating to chrome://flags and disabling the account-consistency flag. If you still need to sync bookmarks + browser data between devices, there are open source alternatives, such as xBrowserSync
Disallow Prediction Services	Optional	Some browsers allow for prediction services, where you receive real-time search results or URL auto-fill. If this is enabled then data is sent to Google (or your default search engine) with every keypress, rather than when you hit enter. You may wish to disable this to reduce the amount of data collected
Avoid G Translate for Webpages	Optional	When you visit a web page written in a foreign language, you may be prompted to install the Google Translate extension. Be aware that Google collects all data (including input fields), along with details of the current user. Instead use a translation service that is not linked to your browser
Disable Web Notifications	Optional	Browser push notifications are a common method for criminals to encourage you to click their link, since it is easy to spoof the source. Be aware of this, and for instructions on disabling browser notifications, see this article

Disable Automatic Downloads	Optional	Drive-by downloads is a common method of getting harmful files onto a users device. This can be mitigated by disabling auto file downloads, and be cautious of websites which prompt you to download files unexpectedly
Disallow Access to Sensors	Optional	Mobile websites can tap into your device sensors without asking. If you grant these permissions to your browser once, then all websites are able to use these capabilities, without permission or notification, take a look at the sensor-js study for more. The best solution is to not grant any permissions to your browser, and to use a privacy browser such as FireFox Focus (Android / iOS) or DuckDuckGo (Android / iOS)
Disallow Location	Optional	Location Services lets sites ask for your physical location to improve your experience. This should be disabled in settings (see how). Note that there are still other methods of determining your approximate location (IP address, time zone, device info, DNS etc)
Disallow Camera/ Microphone access	Optional	Check browser settings to ensure that no websites are granted access to webcam or microphone. It may also be beneficial to use physical protection such as a webcam cover and microphone blocker
Disable Browser Password Saves	Optional	Do not allow your browser to store usernames and passwords. These can be easily viewed or accessed. Chrome does protect this data behind your Windows credentials, but these can be simple to obtain thanks to password reset utilities such as Offline NT Password and Registry Editor. Instead use a password manager
Disable Browser Autofill	Optional	Turn off autofill for any confidential or personal details. This feature was designed to make online shopping and general browsing more convenient, but storing this sensitive information (names, addresses, card details, search terms etc) can be extremely harmful if your browser is compromised in any way. Instead, if essential, consider using your

		password manager's Notes feature to store and fill your data
Protect from Exfil Attack	Optional	The CSS Exfiltrate attack is a where credentials and other sensitive details can be snagged with just pure CSS, meaning even blocking JavaScript cannot prevent it, read more this article by Mike Gualtieri. You can stay protected, with the CSS Exfil Protection plugin (for Chrome and Firefox) which sanitizes and blocks any CSS rules which may be designed to steal data. Check out the CSS Exfil Vulnerability Tester to see if you could be susceptible.
Deactivate ActiveX	Optional	ActiveX is a browser extension API that built into Microsoft IE, and enabled by default. It's not commonly used by legitimate sites any more, but since it gives plugins intimate access rights, and can be dangerous, therefore you should disable it (see how)
Deactivate Flash	Optional	Adobe Flash is infamous for its history of security vulnerabilities (with over 1000 issues!). See how to disable Flash and Flash alternatives. Adobe will end support for Flash Player in December 2020
Disable WebRTC	Optional	WebRTC allows high-quality audio/video communication and peer-to-peer file-sharing straight from the browser. However it can pose as a privacy leak, especially if you are not using a proxy or VPN. In FireFox WebRTC can be disabled, by searching for, and disabling media.peerconnection.enabled in about:config. For other browsers, the WebRTC-Leak-Prevent extension can be installed. uBlockOrigin also allows WebRTC to be disabled. To learn more, check out this guide
Spoof HTML5 Canvas Sig	Optional	Canvas Fingerprinting allows websites to identify and track users very accurately though exploiting the rendering capabilities of the Canvas Element. You can use the Canvas-Fingerprint-Blocker extension to spoof your fingerprint or use Tor - Check if you are susceptible here

Spoof User Agent	Optional	The user agent is a string of text, telling the website what device, browser and version you are using. It is used in part to generate your fingerprint, so switching user agent periodically is one small step you can take to become less unique. You can switch user agent manually in the Development tools, or use an extension like Chameleon (Firefox) or User-Agent Switcher (Chrome)
Disregard DNT	Optional	Do Not Track is a HTTP header, supported by all major browsers, once enabled is intended to flag to a website that you do not wish to be tracked. Enabling Do Not Track has very limited impact, since many websites do not respect or follow this. Since it is rarely used, it may also add to your signature, making you more unique, and therefore actually easier to track
Prevent HSTS Tracking	Optional	HTTP Strict Transport Security (HSTS) was designed to help secure websites, by preventing HTTPS downgrading attacks. However privacy concerns have been raised, as it allowed site operators to plant super-cookies, and continue to track users in incognito. It can be disabled by visiting chrome://net-internals/#hsts in Chromium-based browsers, or following this guide for Firefox, and this guide for other browsers
Prevent Automatic Browser Connections	Optional	Even when you are not using your browser, it may call home to report on usage activity, analytics and diagnostics. You may wish to disable some of this, which can be done through the settings, see instructions for: Firefox, Chrome, Brave
Enable 1st-Party Isolation	Optional	First party isolation means that all identifier sources and browser state are scoped (isolated) using the URL bar domain, this can greatly reduce tracking. In Firefox (under network.cookie.cookieBehavior), it is now possible to block cross-site and social media trackers, and isolate remaining cookies. Alternatively, to enable/disable with 1-click, see the First Party Isolation add-on

Strip Tracking Params from URLs	Advanced	Websites often append additional GET paramaters to URLs that you click, to identify information like source/ referrer. You can sanitize manually, or use an extensions like ClearUrls (for Chrome / Firefox) or SearchLinkFix (for Chrome / Firefox) to strip tracking data from URLs automatically in the background
First Launch Security	Advanced	After installing a web browser, the first time you launch it (prior to configuring it's privacy settings), most browsers will call home (send a request to Microsoft, Apple, Google or other developer) and send over your device details (as outlined in this journal article). Therefore, after installing a browser, you should first disable your internet connection, then launch it and go into settings and configure privacy options, before reenabling your internet connectivity. This does not apply to all browsers, in this article Brave claims to be the on of the only browser to call out to a single, controlled TLD exclusively
Use The Tor Browser	Advanced	The Tor Project provides a browser that encrypts and routes your traffic through multiple nodes, keeping users safe from interception and tracking. The main drawbacks are speed and user experience, as well as the possibility of DNS leaks from other programs (see potential drawbacks) but generally Tor is one of the more secure browser options for anonymity on the web
Disable JavaScript	Advanced	Many modern web apps are JavaScript-based, so disabling it will greatly decrease your browsing experience. But if you really want to go all out, then it will really reduce your attack surface, mitigate a lot of client-side tracking and JavaScript malware

Recommended Software

- Privacy Browsers
- Non-Tracking Search Engines
- Browser Extensions for Security
- Secure Browser & Bookmark Sync

Emails

Nearly 50 years since the first email was sent, it's still very much a big part of our day-to-day life, and will continue to be for the near future. So considering how much trust we put in them, it's surprising how fundamentally insecure this infrastructure is. Email-related fraud is on the up, and without taking basic measures you could be at risk.

If a hacker gets access to your emails, it provides a gateway for your other accounts to be compromised (through password resets), therefore email security is paramount for your digital safety.

The big companies providing "free" email service, don't have a good reputation for respecting users privacy: Gmail was caught giving third parties full access to user emails and also tracking all of your purchases. Yahoo was also caught scanning emails in real-time for US surveillance agencies Advertisers were granted access to Yahoo and AOL users messages to "identify and segment potential customers by picking up on contextual buying signals, and past purchases."

Security	Priority	Details and Hints
Have more than one email address	Recommended	Consider using a different email address for security-critical communications from trivial mail such as newsletters. This compartmentalization could reduce amount of damage caused by a data breach, and also make it easier to recover a compromised account
Keep Email Address Private	Recommended	Do not share your primary email publicly, as mail addresses are often the starting point for most phishing attacks
Keep your Account Secure	Recommended	Use a long and unique password, enable 2FA and be careful while logging in. Your email account provides an easy entry point to all your other online accounts for an attacker
Disable Automatic Loading of Remote Content	Recommended	Email messages can contain remote content such as images or stylesheets, often automatically loaded from the server. You should disable this, as it exposes your IP address and device information, and is often used for tracking. For more info, see this article
Don't connect third-party apps to your email account	Optional	If you give a third-party app or plug-in (such as Unroll.me, Boomerang, SaneBox etc) full access to your inbox, they effectively have full unhindered

		access to all your emails and their contents, which poses significant security and privacy risks
Don't Share Sensitive Data via Email	Optional	Emails are very easily intercepted. Further to this you can't be sure of how secure your recipient's environment is. Therefore emails cannot be considered safe for exchanging confidential or personal information, unless it is encrypted/ or both parties are using a secure mail provider
Consider Switching to a Secure Mail Provider	Optional	Secure and reputable email providers such as ProtonMail and Tutanota allow for end-to-end encryption, full privacy as well as more security-focused features. Unlike typical email providers, your mailbox cannot be read by anyone but you, since all messages are encrypted. Providers such as Google, Microsoft and Yahoo scan messages for advertising, analytics and law enforcement purposes, but this poses a serious security threat
Use Smart Key	Advanced	OpenPGP also does not support Forward secrecy, which means if either your or the recipient's private key is ever stolen, all previous messages encrypted with it will be exposed. Therefore, you should take great care to keep your private keys safe. One method of doing so, is to use a USB Smart Key to sign or decrypt messages, allowing you to do so without your private key leaving the USB device. Devices which support this include NitroKey, YubiKey 5 (See Yubico Neo), Smart Card (See guide), OnlyKey
Use Aliasing / Anonymous Forwarding	Advanced	Email aliasing allows messages to be sent to [anything]@my-domain.com and still land in your primary inbox. Effectively allowing you to use a different, unique email address for each service you sign up for. This means if you start receiving spam, you can block that alias and determine which company leaked your email address. More importantly, you do not need to reveal your real email address to any company. Anonaddy and SimpleLogin are open source anonymous email forwarding service allowing you to create unlimited email aliases, with a free plan

Subaddressing	Optional	An alternative to aliasing is subaddressing, where anything after the + symbol is omitted during mail delivery, for example you the address yourname+tag@example.com denotes the same delivery address as yourname@example.com. This was defined in RCF-5233, and supported by most major mail providers (inc Gmail, YahooMail, Outlook, FastMail and ProtonMail). It enables you to keep track of who shared/ leaked your email address, but unlike aliasing it will not protect against your real address being revealed
Use a Custom Domain	Advanced	Using a custom domain, means that even you are not dependent on the address assigned my your mail provider. So you can easily switch providers in the future and do not need to worry about a service being discontinued
Sync with a client for backup	Advanced	Further to the above, to avoid loosing temporary or permanent access to your emails during an unplanned event (such as an outage or account lock). Thunderbird can sync/ backup messages from multiple accounts via IMAP and store locally on your primary device
Be Careful with Mail Signatures	Advanced	You do not know how secure of an email environment the recipient of your message may have. There are several extensions (such as ZoomInfo) that automatically crawl messages, and create a detailed database of contact information based upon email signitures, and sometimes message content. If you send an email to someone who has something like this enabled, then you are unknowingly entering your details into this database
Be Careful with Auto-Replies	Advanced	Out-of-office automatic replies are very useful for informing people there will be a delay in replying, but all too often people reveal too much information- which can be used in social engineering and targeted attacks

Choose the Right Mail Protocol	Advanced	Do not use outdated protocols (below IMAPv4 or POPv3), both have known vulnerabilities and out-dated security.
Self-Hosting	Advanced	Self-hosting your own mail server is not recommended for non-advanced users, since correctly securing it is critical yet requires strong networking knowledge - read more. That being said, if you run your own mail server, you will have full control over your emails. Mail-in-a-box and docker-mailserver are ready-to-deploy correctly-configured mail servers that provide a good starting point
Always use TLS Ports	Advanced	There are SSL options for POP3, IMAP, and SMTP as standard TCP/IP ports. They are easy to use, and widely supported so should always be used instead of plaintext email ports. By default, the ports are: POP3= 995, IMAP=993 and SMTP= 465
DNS Availability	Advanced	For self-hosted mail servers, to prevent DNS problems impacting availability- use at least 2 MX records, with secondary and tertiary MX records for redundancy when the primary MX record fails
Prevent DDoS and Brute Force Attacks	Advanced	For self-hosted mail servers (specifically STMP), limit your total number of simultaneous connections, and maximum connection rate to reduce the impact of attempted bot attacks
Maintain IP Blacklist	Advanced	For self-hosted mail servers, you can improve spam filters and harden security, through maintaining an up-to-date local IP blacklist and a spam URI realtime block lists to filter out malicious hyperlinks. You may also want to activate a reverse DNS lookup system

Recommended Software:

- Encrypted Email Providers
- Anonymous Mail Forwarding
- Pre-Configured Mail Servers

Secure Messaging

Security	Priority	Details and Hints
Only Use Fully End-to-End Encrypted Messengers	Recommended	End-to-end encryption is a system of communication where messages are encrypted on your device and not decrypted until they reach the intend recipient. This ensures that any actor who intercepts traffic cannot read the message contents, nor can the anybody with access to the central servers where data is stored. Note that if an app is not completely open source, the extent to which the encryption is implemented cannot be verified, and it should not be trusted.
Use only Open Source Messaging Platforms	Recommended	If code is open source then it can be independently examined and audited by anyone qualified to do so, to ensure that there are no backdoors, vulnerabilities, or other security issues. Therefore propriety applications should not be trusted for communicating sensitive information. In open source echosystems, bugs are raised transparently and are usually fixed quickly, and version histories can show who added what, and when. When downloading a pre-built package, you can verify that it has not been tampered with by doing a hash check and comparing the digital signatures. It's important to note that, no piece of software that it totally bug free, and hence never truly secure or private- being open source, is in no way a guarantee that something is safe
Use a "Trustworthy" Messaging Platform	Recommended	When selecting an encrypted messaging app, ensure it's fully open source. It should be stable and actively maintained. Ideally it should be backed by reputable developers or at least be fully clear where funding originates from and/or what their revenue model is. It should have undergone an independent code audit, with results publicly published
Check Security Settings	Recommended	Enable security settings, including contact verification, security notifications and

		encryption. Disable optional non-security features such as read receipt, last online and typing notification. If the app supports cloud sync either for backup or for access through a desktop or web app companion, this increases the attack surface and so should be disabled
Ensure your Recipients Environment is Secure	Recommended	Your conversation can only be as secure as the weakest link. Often the easiest way to infiltrate a communications channel, is to target the individual or node with the least protection. They may not even be aware that their environment has been compromised, leading to sensitive information being captured by an adversary. The best solution to this is to educate and inform the participants in your conversation, about good security practices. Focus on secure authentication, device encryption, network security and malware prevention
Disable Cloud Services	Recommended	Some mobile messaging apps offer a web or desktop companion. This not only increases attack surface, but it has been linked to several critical security issues, and should therefore be avoided, if possible. Some messaging apps also offer a cloud backup feature. Again there a serious security issues with many of these implementations, for example WhatsApp backups are not encrypted, and so with this feature available, you chat history may be breached. Again, this should be disabled.
Secure Group Chats	Recommended	That the risk of compromise will rise exponentially, the more participants are in a group, as the attack surface increases. There is also a higher chance that an adversary lurking among the members can go unnoticed. Periodically check that all participants are legitimate, and ensure only trusted members have admin privileges. It may sometimes be worth only sharing sensitive information within smaller groups. Note that with some messengers, not all group chats are encrypted

		(especially if one recipient is on an older version)
Create a Safe Environment for Communication	Recommended	There are several stages where your digital communications could be monitored or intercepted. This includes: Your or your participants device, your ISP, national gateway or government logging, the messaging provider, the servers. You can help protect from these risks by: paying attention to your surroundings, keeping your devices up-to-date, avoiding malware, watching out for phishing attacks, relying on trustworthy services, creating strong passwords and second-factor authentication, using encryption and helping those with whom you communicate do the same. If you are concerned about your communications being intercepted, consider using a reputable VPN provider, or routing traffic through Tor
Agree on a Communication Plan	Optional	In certain situations (such as attending a protest, communicating with a source or traveling to a risky location), it may be worth making a communication plan. This should include primary and backup methods of securely getting in hold with each other, (in order to avoid falling back on insecure technologies). You may wish to include procedures to implement in potential situations, e.g. to signal for help or assistance
Strip Meta-Data from Media	Optional	Metadata is "Data about Data" or additional information attached to a file or transaction. When you send a photo, audio recording, video or document you may be revealing more than you intended to, or leaking your location. For example Exif data attached to images typically includes: Device name and model, author, time & date taken, GPS location (latitude & longitude) and photography information. In order to protect privacy, you should remove this data before uploading and file or media item. Some apps strip this

		information out automatically, but they may be logging it before doing so
Defang URLs	Optional	Sending links via WhatsApp, Slack, Apple Messenger, Wire, Facebook and other services can unintentionally expose your personal information. This is because, when a thumbnail or preview is generated- it happens on the client-side, and therefore causes your IP, user-agent, device info to be logged. This broadcasts to the website owner that you are discussing that website. One way around this, is to defang your URLs (e.g. https://www.example.com --> hxxps://www[.]example[.]com), using a VPN will also help protect your IP
Verify your Recipient	Optional	Your communication is only as secure as it's weakest link- Always ensure you are talking to the intended recipient, and that they have not been compromised. One method for doing so is to use an app which supports contact verification. This is a powerful feature that enables users to trust the destination, and ensure the conversation has not been hijacked. It usually takes the form of comparing fingerprint codes, even over a phone call or in real life via scanning a QR code. If you believe you may be targeted, use a secure messenger that provides reliable indicators of compromise, where both parties will be notified if there have been any changes
Enable Ephemeral Messages	Optional	You cannot always rely on the physical security of your device. Self-destructing messages is a really neat feature the causes your messages to automatically delete after a set amount of time. This means that if your device is lost, stolen or seized, an adversary will only have access to the most recent communications. Unlike remote erase, disappearing messages does not require your device to be remotely accessible or have signal. You are able to vary this time frame from weeks all the way down to just a few seconds, depending on your threat model.

		Without disappearing messages enabled, you should periodically delete conversation history, in case your device is breached
Avoid SMS	Optional	SMS may be convenient, but it's not secure. It is susceptible to threats, such as interception, sim swapping, manipulation and malware. If you must use SMS, then you should encrypt messages before sending. One option is to use Silence, an Android app that provides end-to-end encryption for SMS
Watch out for Trackers	Optional	A tracker is a piece of software meant to collect data about you or your usages. Be wary of messaging applications with trackers, as the detailed usage statistics they collect are often very evasive, and can sometimes reveal your identity as well as personal information that you would otherwise not intend to share. You can check how many, and which trackers a given app uses, by searching it in Exodus Privacy
Consider Jurisdiction	Advanced	The jurisdictions where the organisation is based, and data is hosted should also be taken into account. As in some territories, organisations are forced to comply with local government regulations, which can require them to keep logs of all users interactions and metadata, or hand over encryption keys. Where possible, avoid Five Eyes and other International Cooperatives, and countries with poor respect for user privacy such as China, Russia, Singapore and Malaysia.
Use an Anonymous Platform	Advanced	If you believe you may be targeted, you should opt for an anonymous messaging platform that does not require a phone number, or any other personally identifiable information to sign up or use. Even using false or temporary information (such as a burner sim, VOIP number, temporary or forwarding email address, made-up details etc) cannot be grantee anonymity, and may put you at risk. As well as this you should download the app over Tor, outside of Google Play / Apple App Store, create an anonymous identity, only run the app while connected

		through Tor and ideally sandbox it to prevent data leaks (using a separate profile, virtual machine or even a secondary device)
Ensure Forward Secrecy is Supported	Advanced	Opt for a platform that implements forward secrecy. This is where your app generates a new encryption key for every message. It means that if your adversary has obtained the private encryption key from one party, they will not be able to use it to decrypt any previously captured messages
Consider a Decentralized Platform	Advanced	If all data flows through a central provider, you have to trust them with your data and meta-data. You cannot verify that the system running is authentic without back doors, and they may be subject to local laws, court orders or censorship, and if that provider ceases to operate, the entire network will be unavailable for that duration. Whereas with a decentralized system, there are no central servers to compromise, and no single point of failure. It cannot be raided, shut down, or forced to turn over data. Some decentralized platforms also route traffic through the Tor network, which provides an additional layer of anonymity and security.

Recommended Software

- Secure Messaging Apps
- P2P Messaging Platforms

Social Media

Online communities have existed since the invention of the internet, and give people around the world the opportunity to connect, communicate and share. Although these networks are a great way to promote social interaction and bring people together, that have a dark side - there are some serious Privacy Concerns with Social Networking Services, and these social networking sites are owned by private corporations, and that they make their money by collecting data about individuals and selling that data on, often to third party advertisers.

Secure your account, lock down your privacy settings, but know that even after doing so, all data intentionally and non-intentionally uploaded is effectively public. If possible, avoid using conventional social media networks.

Security	**Priority**	**Details and Hints**
Secure your Account	Recommended	Profiles media profiles get stolen or taken over all too often. To protect your account: use a unique and strong password, and enable 2-factor authentication. See the Authentication section for more tips
Check Privacy Settings	Recommended	Most social networks allow you to control your privacy settings. Ensure that you are comfortable with what data you are currently exposing and to whom. But remember, privacy settings are only meant to protect you from other members of the social network- they do not shield you or your data from the owners of the network. See how to set privacy settings, with this guide
Think of All Interactions as Public	Recommended	There are still numerous methods of viewing a users 'private' content across many social networks. Therefore, before uploading, posting or commenting on anything, think "Would I mind if this was totally public?"
Think of All Interactions as Permanent	Recommended	Pretty much every post, comment, photo etc is being continuously backed up by a myriad of third-party services, who archive this data and make it indexable and publicly available almost forever. Sites like Ceddit, and /r/undelete, Politwoops, The Way Back Machine allow anyone to search through deleted posts, websites and media. Therefore it's important to not unintentially reveal too much information, and to consider what the implications would be if it were to go 'viral'

Don't Reveal too Much	Recommended	Profile information creates a goldmine of info for hackers, the kind of data that helps them personalize phishing scams. Avoid sharing too much detail (DoB, Hometown, School etc)
Be Careful what you Upload	Recommended	Status updates, comments, check-ins and media can unintentionally reveal a lot more than you intended them to (such as location, preferences, contacts/ relationships etc). This is especially relevant to photos and videos, which may show things in the background (documents, road names/ signs, credit cards, electronic devices), even more so when there are multiple images uploaded
Don't Share Email or Phone Number	Recommended	Posting your real email address or mobile number, gives hackers, trolls and spammers more munition to use against you, and can also allow seperate alliases, profiles or data points to be connected
Don't Grant Unnecessary Permissions	Recommended	By default many of the popular social networking apps will ask for permission to access your contacts, call log, location, messaging history etc.. If they don't need this access, don't grant it. For Android users, check out Bouncer - an app that gives you the ability to grant permissions temporarily
Be Careful of 3rd-Party Integrations	Recommended	Avoid signing up for accounts using a Social Network login, revoke access to social apps you no longer use, see instructions for: Facebook, Twitter, Insta and LinkedIn
Avoid Publishing Geo Data while still Onsite	Recommended	If you plan to share any content that reveals a location (such as 'checking in', sharing photos, or status updates that reveal your location), then wait until you have left that place. This is particularly important when you are taking a trip, at a restaurant, campus, hotel/ resort, public building or airport- as it may alert the wrong people to your exact whereabouts
Remove metadata before	Optional	Most smartphones and some cameras automatically attach a comprehensive set of additional data (called EXIF data) to each photograph. This usually includes things like time,

uploading media		date, location, camera model, user etc. It can reveal a lot more data than you intended to share. Remove this data before uploading. You can remove meta data without any special software, use a CLI tool, or a desktop tool like EXIF Tage Remover
Consider Spoofing GPS in home visinity	Advanced	Even if you yourself never use social media, strip geo-data from all media and disable device radios- there is always going to be others who are not as careful, and could reveal your location. For example, if you have guests, family members or visitors to your home residence, their device will likley be recording GPS and logging data. One method around this, is to use an SDR to spoof GPS signals, causing all devices in the visinity to believe they are in a different, pre-defined location
Consider False Information	Advanced	If you just want to read, and do not intend on posting too much- consider using an alias name, and false contact details. Remember that there are still methods of tracing your account back to you, but this could mitigate a lot of threats. Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities. Don't link accounts in any way- don't comment on / liking inter-account posts, avoid logging in from the same IP and use different passwords (so the accounts cannot be linked in the case of a data breach)
Don't have any social media accounts	Advanced	Social media is fundamentally un-private, so for maximum online security and privacy, avoid using any mainstream social networks

Recommended Software

- Alternative Social Media
- Alternative Video Platforms
- Alternative Blogging Platforms
- News Readers and Aggregation

Networking

This section covers how you connect your devices to the internet securely, including configuring your router and setting up a VPN.

Security	**Priority**	**Details and Hints**
Use a VPN	Recommended	Use a reputable, paid-for VPN. This can help protect sites you visit logging your real IP, reduce the amount of data your ISP can collect and increase protection on public WiFi. However VPNs alone do not make you anonymous or stop tracking, it's important to understand their limitations. ProtonVPN and Mullvad may be good options for many, but for an unbiased comparison, see: That One Privacy Site. Select a service with a good reputation, that does not keep logs, and is not in the 5-eyes jurisdiction
Change your Router Password	Recommended	After getting a new router, change the password. Default router passwords are publicly available (see default-password.info), meaning anyone within proximity would be able to connect. See here, for a guide on changing router password
Use WPA2, and a strong password	Recommended	There are different authentication protocols for connecting to WiFi. Currently the most secure is options are WPA2 and WPA3 (on newer routers). WEP and WPA are moderately easy to crack. Ensure it is strong: 12+ alpha-numeric characters, avoiding dictionary words. You can set this within your routers admin panel
Keep router firmware up-to-date	Recommended	Manufacturers release firmware updates that fix security vulnerabilities, implement new standards and sometimes add features/ improve the performance your router. It's important to have the latest firmware installed, to avoid a malicious actor exploiting an un-patched vulnerability. You can usually do this by navigating to 192.168.0.1 or 192.168.1.1, entering the admin credentials (on the back of you of your router, not your WiFi password!), and follow the instructions, see: Asus, D-Link, Linksys (older

		models), NetGear and TP-Link. Some newer routers update automatically
Implement a Network-Wide VPN	Optional	If you configure your VPN on your router, firewall or home server, then traffic from all devices will be encrypted and routed through it, without needing individual VPN apps. This reduces the chance: of IP leaks, VPN app crashes, and provides VPN access to devices which don't support VPN clients (TV's, Smart Hubs, IoT devices etc)
Protect against DNS leaks	Optional	When using a VPN, it is extremely important to exclusively use the DNS server of your VPN provider or secure service. For OpenVPN, you can add: block-outside-dns to your config file (which will have the extension .ovn or .conf). If you are unable to do this, then see this article for further instructions. You can check for leaks, using a DNS Leak Test
Use a secure VPN Protocol	Optional	OpenVPN and WireGuard are open source, lightweight and secure tunneling protocols. Avoid using PPTP or SSTP. L2TP can be good, but only when configured correctly
Secure DNS	Optional	Use DNS-over-HTTPS which performs DNS resolution via the HTTPS protocol, encrypting data between you and your DNS resolver. Although DoH is not perfect, it does remove the need for trust - see CoudFlares 1.1.1.1 Docs for more details
Avoid the free router from your ISP	Optional	Typically they're manufactured cheaply in bulk in China, with insecure propriety firmware that doesn't recieve regular security updates. Consider an open source router (such as Turris MOX) or a comercial router with secure firmware
Whitelist MAC Addresses	Optional	You can whitelist MAC addresses in your router settings, disallowing any unknown devices to immediately connect to your network, even if they know your credentials. Note that a malicious actor may be able to bypass this, by cloning their address to appear the same as one of your trusted devices, but it will add an extra step

Change the Router's Local IP Address	Optional	It is possible for a malicious script in your web browser, to exploit a cross site scripting vulnerability, accessing known-vulnerable routers at their local IP address and tampering with them (known as CSRF Attack). Updating your routers local IP address, so that it is not the default (usually 192.168.0.1 or similar), can help protect you from some of these automated attacks
Don't Reveal Personal Info in SSID	Optional	You should update your network name, choosing an SSID that does not identify you, include your flat number / address, and does not specify the device brand/ model. It may be beneficial to avoid something very unique, as services like Wigle's WiFi map can link an SSID directly back to your home address. This may also slightly aid in deterring an opportunistic attacker, as it indicates the router is being conscientiously administered. See, how to update SSID
Opt-Out Router Listings	Optional	WiFi SSIDs is scanned, logged and then published on various websites (such as Wiggle WiFi SSID Map), which is a serious privacy concern for some. You can opt-out of many of these listings, by adding _nomap to the end of your SSID (WiFi network name)
Hide your SSID	Optional	Your routers Service Set Identifier is simply the network name. If it is not visible, it may receive less abuse. However understand that finding hidden networks is a trivial task (e.g. with Kismet). See, how to hide SSID
Disable WPS	Optional	Wi-FI Protected Setup provides an easier method to connect, without entering a long WiFi password, it often involves a physical button on your router, entering an 8-digit PIN, or tapping an NFC. It may be convenient, but WPS introduces a series of major security issues, allowing an attacker to bypass the password, and gain easy access into your network. See, how to disable WPS
Disable UPnP	Optional	Universal Plug and Play allows applications to automatically forward a port on your router, saving you the hassle of forwarding ports

		manually. However, it has a long history of serous security issues, and so it is recommended to turn this feature off. See, how to disable UPnP
Use a Guest Network for Guests	Optional	Do not grant access to your primary WiFi network to visitors, as it enables them to interact with other devices on the network (such as printers, IoT/ smart home devices, network-attached storage/ servers etc). Even if it is someone you trust, you cannot guarantee that their device has not been compromised in some way. Some routers offer the ability to enable a separate 'guest' network, which provides isolation and is able to expire after a given time frame. For a more comprehensive network, the same outcome can be achieved using a VLAN and separate access point. See, how to enable guest network
Change your Router's Default IP	Optional	Modifying your router admin panels default IP address will makes it more difficult for malicious scripts in your web browser targeting local IP addresses, as well as adding an extra step for local network hackers
Kill unused processes and services on your router	Optional	Services like Telnet and SSH (Secure Shell) that provide command-line access to devices should never be exposed to the internet and should also be disabled on the local network unless they're actually needed. In general, any service that's not used should be disabled to reduce attack surface
Disable UPnP	Optional	Universal Plug and Play may allow you to save time with Port Forwarding, but it opens doors to many security risks. It can be disabled from your routers admin panel
Don't have Open Ports	Optional	Close any open ports on your router that are not needed. Open ports provide an easy entrance for hackers. You can use a port scanner (such as AngryIP), or a web service
Disable Unused Remote Access Protocols	Optional	When protocols such as PING, Telnet, SSH, UPnP and HNAP etc are enabled, they allow your router to be probed from anywhere in the world,

		and so should be disabled if not in use. Instead of setting their relevant ports to 'closed', set them to 'stealth' so that no response is given to unsolicited external communications that may come from attackers probing your network
Disable Cloud-Based Management	Optional	You should treat your routers admin panel with the upmost care, as considerable damage can be caused if an attacker is able to gain access. You should take great care when accessing this page, ensuring you always log out, or considering Incognito mode. Most routers offer a 'remote access' feature, allowing you to access the admin web interface from anywhere in the world, using your username and password. This greatly increases attack surface, and opens your network up to a host of threats, and should therefore be disabled. You could also take it a step further, disable the admin interface over WiFi, meaning the settings can only be modified when using a direct Ethernet connection. Note that disabling cloud management may not be possible on some modern mesh-based routers
Manage Range Correctly	Optional	It's common to want to pump your routers range to the max, and often this is necessary, especially if you live in a large house, or desire coverage in outdoor spaces. But if you reside in a smaller flat, and have neighbors close by, your attack surface is increased when your WiFi network can be picked up across the street. It maybe worth carefully configuring your networks, and device antennas to provide coverage only within your operating area/ apartment. One method of doing so, it to utilize the 5-GHz band, which provides a faster link speed, but a lesser range, and is easily blocked by thick walls
Route all traffic through Tor	Advanced	VPNs have their weaknesses- you are simply moving your trust from your ISP/ mobile carrier to a VPN provider- Tor is much more anonymous. For optimum security, route all your internet traffic through the Tor network. On Linux you can use TorSocks or Privoxy, for Windows you can use Whonix, and on OSX follow thsese

		instructions, for Kali see TorGhost. Alternativley, you can use OnionPi to use Tor for all your connected devices, by configuring a Raspberry Pi to be a Tor Hotspot
Disable WiFi on all Devices	Advanced	Connecting to even a secure WiFi network increases your attack surface. Disabling your home WiFi and connect each device via Ethernet, and turning off WiFi on your phone and using a USB-C/ Lightening to Ethernet cable will protect against WiFi exploits, as Edward Snowden says here.

Recommended Software

- Virtual Private Networks
- Mix Networks
- Router Firmware
- Open Source Proxies
- DNS Providers
- Firewalls
- Network Analysis Tools
- Self-Hosted Network Security Tools

Mobile Devices

Smart phones have revolutionized so many aspects of life and brought the world to our fingertips. For many of us, smart phones are our primary means of communication, entertainment and access to knowledge. But while they've brought convenience to whole new level, there's some ugly things going on behind the screen.

Geo-tracking is used to trace our every move, and we have little control over who has this data- your phone is even able to track your location without GPS. Over the years numerous reports that surfaced, outlining ways in which your phone's mic can eavesdrop, and the camera can watch you- all without your knowledge or consent. And then there's the malicious apps, lack of security patches and potential/ likely backdoors.

Using a smart phone generates a lot of data about you- from information you intentionally share, to data silently generated from your actions. It can be scary to see what Google, Microsoft, Apple and Facebook know about us- sometimes they know more than our closest family. It's hard to comprehend what your data will reveal, especially in conjunction with other data.

This data is used for far more than just advertising - more often it's used to rate people for finance, insurance and employment. Targeted ads can even be used for fine-grained surveillance (see ADINT)

More of us are concerned about how governments use collect and use our smart phone data, and rightly so, federal agencies often request our data from Google, Facebook, Apple, Microsoft, Amazon, and other tech companies. Sometimes requests are made in bulk, returning detailed information on everybody within a certain geo-fence, often for innocent people. And this doesn't include all of the internet traffic that intelligence agencies around the world have unhindered access to.

Security	**Priority**	**Details and Hints**
Encrypt your Device	Recommended	In order to keep your data safe from physical access, use file encryption. To enable, for Android: Settings --> Security --> Encryption, or for iOS: Settings --> TouchID & Passcode --> Data Protection. This will mean if your device is lost or stolen, no one will have access to your data
Turn off connectivity features that aren’t being used	Recommended	When you're not using WiFi, Bluetooth, NFC etc, turn those features off. There are several common threats that utilise these features

Keep app count to a minimum	Recommended	Uninstall apps that you don't need or use regularly. As apps often run in the background, slowing your device down, but also collecting data.
App Permissions	Recommended	Don't grant apps permissions that they don't need. For Android, Bouncer is an app that allows you you to grant temporary/ 1-off permissions.
Only install Apps from official source	Recommended	Applications on Apple App Store and Google Play Store are scanned and cryptographically signed, making them less likely to be malicious. Avoid downloading .apk or .ipa files from unverified source, unless you know it is safe. Also check the reviews, and app info before downloading a new application.
Be Careful of Phone Charging Threats	Optional	Juice Jacking is when hackers use public charging stations to install malware on your smartphone or tablet through a compromised USB port. You can mitigate this, either by using a power bank or AC wall charger, or by using a simple data blocker device (See USB Condom or PortaPow Blocker)
Set up a mobile carrier PIN	Recommended	SIM hijacking is when a hacker is able to get your mobile number transferred to their sim (often through social engineering your mobile carrier). This then allows them to receive 2FA SMS codes (enabling them to access your secure accounts, such as banking), or to pose as you. The easiest way to protect against this is to set up a PIN through your mobile provider, thus disallowing anyone without this PIN to make any changes to your account. Using a non-SMS based 2FA method will reduce the damage, Read more about the sim swap scam.
Opt-out of Caller ID Listings	Optional	When one of your friends or colleagues has your number in their contacts, and also has a caller ID app, then your Name, Phone Number and any other saved contact details will be uploaded. To keep your details private, you can unlist it here: TrueCaller, CallApp, SyncMe, cia-app, Hiya. Note that it is possible to opt-out, even before your number has been added, and this will prevent your details being uploaded in the future.

Opt-out of personalized ads	Optional	In order for ads to be personalized, Google collects data about you, you can slightly reduce the amount they collect by opting-out of seeing personalized ads. See this guide, for Android instructions.
Erase after too many login attempts	Optional	To protect against an attacker brute forcing your pin, if you lose your phone, set your device to erase after too many failed login attempts. See this iPhone guide. You can also do this via Find my Phone, but this increased security comes at a cost of decreased privacy.
Monitor Trackers	Optional	A tracker is a piece of software meant to collect data about you or your usages. εxodus is a great service which lets you search for any app, by its name, and see which trackers are embedded in it. They also have an app which shows trackers and permissions for all your installed apps.
Use a Mobile Firewall	Optional	To prevent applications from leaking privacy-sensitive data, you can install a firewall app. This will allow you to block specific apps from making data requests, either in the background, or when on WiFi or mobile data. Consider NetGuard (Android) or LockDown (iOS), or see more Firewalls
Reduce Background Activity	Optional	For Android, SuperFreeze makes it possible to entirely freeze all background activities on a per-app basis. Intended purpose is to speed up your phone, and prolong battery life, but this app is also a great utility to stop certain apps from collecting data and tracking your actions while running in the background
Sandbox Mobile Apps	Optional	Prevent permission-hungry apps from accessing your private data with Island. It is a sandbox environment to clone selected apps and isolate them from accessing your personal data outside the sandbox (including call logs, contacts, photos and etc.) even if related permissions are granted
Tor Traffic	Advanced	Orbot provides a system-wide Tor connection, which will help protect you from surveillance and public WiFi threats

Avoid Custom Virtual Keyboards	Optional	Android and iOS allow you to download and use third-party keyboard apps. These apps will be able to access everything that you type on your phone/ tablet: passwords, messages, search terms etc. It is recommended to stick with your devices stock keyboard. If you choose to use one of these apps, ensure it is reputable, block internet access (can be done with a firewall app), don't grant it permissions it does not need, and turn off analytics or other invasive features in it's settings. This article by Lenny Zelster explains things further
Restart Device Regularly	Optional	Over the years there have vulnerabilities relating to memory exploits (such as CVE-2015-6639 + CVE-2016-2431). Restarting your phone at least once a week will clear the app state cached in memory. A side benefit is that your device may run more smoothly after a restart.
Avoid SMS	Optional	SMS may be convenient, but it's not particularly secure. It is susceptible to threats, such as interception, sim swapping (see this article), manipulation and malware (see this article). SMS should not be used to receive 2FA codes, (as demonstrated in the video in this article), instead use an authenticator app. SMS should not be used for communication, instead use an encrypted messaging app, such as Signal
Keep your Number Private	Optional	MySudo allows you to create and use virtual phone numbers for different people or groups. This is great for compartmentalisation. Alternativley, use a VOIP provider like Google Voice or Skype, or for temporary usage you can use a service like iNumbr. Where possible, avoid giving out your real phone number while creating accounts online.
Watch out for Stalkerware	Optional	This is a malware that is installed directly onto your device by someone you know (partner, parent, boss etc.). It allows them to see your location, messages and other app data remotely. The app likely won't show up in your app draw, (but may visible in Settings --> Applications --> View All). Sometimes they can be disguised as a non-conspicuous app (such as a game, flashlight or

		calculator) which initially don't appear suspicious at all. Look out for unusual battery usage, network requests or high device temperature. If you suspect that stalkerware is on your device, the best way to get rid of it is through a factory reset. See this guide for more details
Favor the Browser, over Dedicated App	Optional	Where possible, consider using a secure browser to access sites, rather than installing dedicatd applications. Both Android and iOS applications often have invasive permissions, allowing them intimate access to sensitive data and your devices sensors and radios. But the extent to what these apps can access is often not clear, and even zero-permission apps can see more data than you think: accessing phone sensors, vendor ID's and determine which other apps you have installed. All this is enough to identity you. In some situations you can still use a service, without having to install an application, through accessing it via the browser, and this can help mitigate a lot of the issues cause by untrustworthy apps
Consider running a custom ROM (Android)	Advanced	For Android users, if your concerned about your device manufacturer collecting too much personal information, consider a privacy-focused custom ROM, such as Lineage or GrapheneOS - see more

Recommended Software

- Mobile Apps, for Security + Privacy
- Encrypted Messaging
- Mobile Operation Systems

Personal Computers

Although Windows and OS X are easy to use and convenient, they both are far from secure. Your OS provides the interface between hardware and your applications, so if compromised can have detrimental effects.

Security	**Priority**	**Details and Hints**
Keep your System up-to-date	Recommended	New vulnerabilities are constantly being discovered. System updates contain fixes/ patches for these security issues, as well as improve performance and sometimes add new features. You should install new updates when prompted, to avoid any critical issues on your system from being exploited
Encrypt your Device	Recommended	If your computer is stolen, seized or falls into the wrong hands, without full disk encryption anyone is able to access all of your data, without a password (by booting to a live USB or removing the hard drive). You can enable encryption very easily, using BitLocker for Windows, FileVault on MacOS, or by enabling LUKS on Linux, during install. Or using an open source, program, such as VeraCrypt or DiskCryptor. For encrypting cloud files, consider Cryptomator or CryFS. Note that you should select a long and strong password, and keep it somewhere safe, as there is no way to recover your password if you loose it
Backup Important Data	Recommended	Maintaining a copy of important data will prevent loss in the case of ransomware, theft or damage to your system. You should encrypt these backups, to keep the data safe. One solution would be to use Cryptomator to encrypt files, and then sync them to a regular cloud storage provider. Or you could have a USB drive, with an encrypted volume (e.g. using VeraCrypt). The best backup solution, should include 2 additional copies of your data- such as a physical off-site copy, and a cloud copy of your data
Be Careful Plugging USB Devices into your Computer	Recommended	Think before inserting a USB device into your PC, as there are many threats that come in the form of a USB device. Something like a USB Killer will destroy your computer, by rapidly charging and discharging capacitors. A Bad USB (such as Malduino or Rubber Ducky), will act as a keyboard, once plugged in, it will proceed to rapidly type commands at lighning speed, often with severe consequences. There's also remote

		access tools (such as the OMG Cable or P4wnP1_aloa), giving a hacker full remote access to your PC, even after the device has been removed. And of course, there's traditional USB drives, that contain malware that infect your device once inserted. One solution to this, is to make a USB sanitizer, using CIRCLean on a Raspberry Pi. It allows you to plug an obtained USB device into the Pi, and it'll convert the untrusted documents into a readable but disarmed format, and save them on a new USB key, which you can then safely insert into your computer
Activate Screen-Lock when Idle	Recommended	Get in the habit of locking your computer, whenever you step away from it. Reduce the amount of time that your computer is idle for, before the screensaver activates, and ensure that it will lock when the mouse is moved, so no one can access your data, when you step away from your desk. In Windows, check Personalization --> Screensaver --> On resume, display login screen, and in MacOS, check Security & Privacy --> General --> Require password immediately after screensaver starts. In Linux, Brightness & Lock --> Require my password when waking up from suspend. Better still, never leave your computer unattended, even in trusted environments
Disable Cortana or Siri	Recommended	Using a voice-controlled assistant, sends commands back to Microsoft or Apple as well as data about your files for local search, which have some serious privacy implications. They're always listening, waiting for the trigger word, and this can lead to parts of conversations being accidentally recorded. To disable this, in Windows, navigate to Settings --> Cortana and switch it to Off. You should also stop your speech, typing and handwriting patterns being sent to Microsoft, since this can be used to identify you, as well as potentially leaking sensitive data - navigate to Settings --> Privacy --> Speech, Inking, & Typing, and click Turn off. In Mac it's not easy to fully disable Siri, but you can stop it from always listening, go to System Preferences --> Siri, and uncheck Enable Siri
Review your Installed Apps	Recommended	It’s good practice to keep installed applications to a minimum. Not only does this keep your machine lean,

		it also reduces your exposure to vulnerabilities. You should also clear application cache's regularly. As well as looking through your application list manually, there are also tools that make this easier, such as BleachBit
Manage Permissions	Recommended	In a similar way to phones, your OS can grant certain permissions to applications. It's important to keep control over which apps and services have access to your location, camera, microphone, contacts, calendar and other account information. Some systems let you restrict which apps can send or recieve messages, as well as which apps can which processes can control radios such as Bluetooth and WiFi. In Windows, navigate to Settings --> Privacy, and for MacOS, go to System Preferences --> Security & Privacy --> Privacy. Note that there are other methods that apps can use to access this data, and this is just one step towards protecting it. You should check back regularly, as sometimes system updates can cause some privacy settings to be modified or reverted
Disallow Usage Data from being sent to the Cloud	Recommended	Both Windows and MacOS collect usage information or feedback, which is send to the cloud for analytics, diagnostics and research. Although this data should be anonymized, it can often be linked back to your identity when compared with other usage data. In Windows, there is no way to disable this fully, but you can limit it- navigate to Settings --> Privacy --> Feedback & diagnostics, and select Basic. You also have the option to disallow your advertising ID from being shared with apps on your system. In MacOS, it can be turned off fully, go to System Preferences --> Privacy --> Diagnostics & Usage, and untick both options
Avoid Quick Unlock	Recommended	Use a password to unlock your computer, ensure it is long and strong. Avoid biometrics such as facial recognition and fingerprint. These can be spoofed, allowing an intruder access to your account. Also, for Windows devices, avoid using a short PIN to unlock your machine.
Power Off Computer,	Recommended	You must shut down your device when not in use, in order for the disk to be encrypted. Leaving it in standby/ sleep mode keeps your data in an

instead of Standby		unencrypted state, and vulnerable to theft. Microsoft even recommends disabling the sleep functionality all together, once BitLocker is enabled. This only applies to encrypted disks, and is true for FileVault (MacOS), BitLocker (Windows), VeraCrypt, Self-Encrypting Drives and most other disk encryption methods. Another reason to shut down, is because the machine is completely offline while it is off, and cannot be hacked remotely. It also can't communicate with a command and control server, if it has already been infected with an exploit
Don't link your PC with your Microsoft or Apple Account	Optional	Create a local account only. This will prevent some data about your usage being uploaded and synced between devices. Avoid syncing your iPhone or Android device to your computer, as this will automatically lead to it being associated with your Apple, Microsoft or Google account. If sync is important to you, there are open source services that encrypt you data, and sync between devices. For example XBrowserSync for bookmarks, history and browser data, ETESync for calendar, contacts and tasks, Syncthing for files, folders and filesystems
Check which Sharing Services are Enabled	Optional	The ability to share files and services with other machines within your network, can be useful, but also acts as a gateway for common threats. You should disable the network sharing features that you are not using. For Windows, navigate to Control Panel --> Network and Internet --> Network and Sharing Center --> Advanced sharing settings, and for MacOS, just go to System Preferences --> Sharing and disable anything that you do not need. For Windows users, you should ensure that remote desktop is disabled. And also control apps' ability to sync with non-pairing devices, such as beacons that transmit advertising information- this is also in the privacy settings
Don't use Root/ Admin Account for Non-Admin Tasks	Optional	You should not use administrator / root account for general use. Instead, use an unprivileged user account, and temporarily elevate permissions when you need to make administrator changes. This will mitigate a large proportion of vulnerabilities, because a malicious program or an attacker can do

		significantly less damage without an administrator power. See this guide for Windows and MacOS, on how to implement this. You should also ensure that a password is required for all system wide changes, as this helps protect against malware doing widespread damage. In Windows this is enabled by default, in MacOS, navigate to System Preferences --> Security & Privacy --> General --> Advanced
Block Webcam + Microphone	Optional	To prevent the potential risk of being watched through your webcam, consider covering it with a sticker, slider or electrical tape, while it's not being used. There are also application solutions- such as Oversight (MacOS) or CamWings (Windows) - for ultimate protection, consider physically removing the webcam all together. Blocking unauthorized audio recording, can be done with a mic block, which works by disabling the primary sound input source- but is not fool proof
Use a Privacy Filter	Optional	A lot of information can be gleaned just from glancing at someones screen over their shoulder. When working in a public space (train, coffee shop, share office), use a screen privacy filter. This will allow you to see the content of your screen when looking straight on, but for anyone looking at a slight angle, your screen will appear black.
Physically Secure Device	Optional	When working from a laptop think about using a Kensington Lock to secure your device to a permanent fixture. To help protect against an opportunistic local attack, consider utilizing port locks, to prevent or slow down an intruder from dropping a malicious payload onto your device. Ideally never leave your laptop or other devices unattended
Don't Charge Devices from your PC	Optional	Connecting your smart phone to a computer can be a security risk, it's possible for a self-signed malicious app to be installed, without your knowledge. Also both iPhone or Android device have sync capabilities, which can lead to data being unintentionally shared. If you need to charge your device, consider using a USB data-blocker.
Randomize your hardware	Optional	A MAC Address is an identifier given to a device (specifically the Network Interface Controller), and is is one method used to identify, and track you across

address on Wi-Fi		different WiFi networks. Some devices allow you to modify or randomize how this address appears. See how, on Windows, MacOS and Linux. You should also disallow you device from automatically connect to open Wi-Fi networks
Use a Firewall	Optional	A firewall is a program which monitors incoming and outgoing traffic, and allows you to blocks internet access for certain applications. This is useful to stop apps from collecting data, calling home, or downloading unnecessary content- correctly configured, firewalls can help protect against remote access attacks, as well as protect your privacy. Your system will have a built-in firewall (Check it's enabled: Windows, Mac OS, Ubuntu and other Linux ditros). Alternatively, for greater control, consider: LuLu (MacOS), gufw (Linux), LittleSnitch, SimplеWall (Windows), there's plenty more firewall apps available
Protect Against Software Keyloggers	Optional	A software keylogger is a malicious application running in the background that logs (and usually relays to a server) every key you press, aka all data that you type (passwords, emails, search terms, financial details etc). The best way to stay protected, is to keep your systems security settings enabled, and periodically check for rootkits- which will detect most loggers. Another option, is to use a key stroke encryption tool. For Windows there is GhostPress, Spy Shelter or KeyScrambler (developed by Qian Wang) which encrypt your keystrokes at the keyboard driver level, and then decrypting them at the application level, meaning any software keylogger would just receive encrypted data.
Check Keyboard Connection	Optional	Check your keyboards USB cable before using, bring your own keyboard to work and watch out for sighs that it may have been tampered with. A hardware keylogger is a physical device that either sits between your keyboard and the USB connection into your PC, or is implanted into a keyboard. It intercepts and stores keystrokes, and in some cases can remotely upload them. Unlike a software logger, they can not be detected from your PC, but also they can not

		intercept data from virtual keyboards (like OSK), clipboard or auto-fill password managers.
Prevent Keystroke Injection Attacks	Optional	Always lock your PC when you step away from it (however this is not fool-proof, and can be circumvented). For Linux, there is USBGuard, and for Windows there's DuckHunt, which will detect super fast (badUSB-level super-fast) it will block input until the attack stops. Alternatively, Windows Group Policy can also be configured to not trust new devices by default. Port Blockers provide some level of physical protection, which may prevent an opportunistic attack, but can be circumvented fairly easily
Don't use Free Anti-Virus	Optional	The included security tools, which come with bundled your operating system (such as Windows Defender), should be adequate at protecting against threats. Free anti-virus applications are often more of a hinder than a help- as they require admin permissions, full access to all data and settings, and internet access. They usually collect a lot of data, which is uploaded to the cloud and sometimes sold to third-parties. Therefore, you should avoid programs such as Avast, AVG, Norton, Kasperky, Avira etc- even the paid plans come with privacy concerns. If you need a dedicated anti-virus application, consider CalmAV, which is open source. And for scanning 1-off files, VirusTotal is a useful tool
Periodically check for Rootkits	Advanced	You should regularly check for rootkits (which may allow an attacker full control over your system), you can do this with a tool like chkrootkit, once installed just run sudo chkrootkit. For Windows users, see rootkit-revealer or gmer
BIOS Boot Password	Advanced	A BIOS or UEFI password once enabled, will need to be entered before the system can be booted, which may help to prevent an inexperienced hacker from getting into your OS, booting from a USB, tampering with BIOS as well as other actions. However, it can be easy to bypass, don't put too much trust in this - it should only be used as an additional step, to exhaust your adversaries resources a little faster. Here is a guide on how to enable password.

Use a Security-Focused Operating System	Advanced	Microsoft, Apple and Google all have practices that violate users privacy, switching to Linux will mitigate most of these issues. For more advanced users, consider a security-focused distro- such as QubeOS, which allows for compartmentalization of applications and data, and has strong encryption and Tor networking build in. For some actions, Tails a live operating system with no memory persistence is as close as you can get to not leaving a data trail on your system. BSD is also great for security, see FreeBSD and OpenBSD. Even a general purpose distro, will be much better for privacy compared to a propriety counterpart: Fedora, Debian, Arch / Manjaro, see more
Make Use of VMs	Advanced	If your job, or any of your activity could endanger your system, or put you at risk, then virtual machines are a great tool to isolate this from your primary system. They allow you to test suspicious software, and analyse potentially dangerous files, while keeping your host system safe. They also provide a host of other features, from quick recovery using snapshots, to the ability to replicate configurations easily, and have multiple VMs running simultaneously. Taking this a step further, VMs can be use for compartmentalization, with a host system performing the single task of spawning VMs (systems like ProxMox, is designed for exactly this). Be aware that virtual machines do not grantee security, and vulnerabilities, named VM-Escapes, may allow for data in memory to leak into the host system
Compartmentalize	Advanced	Security by Compartmentalization is a strategy, where you isolate different programs and data sources from one another as much as possible. That way, attackers who gain access to one part of the system are not able to compromise all of the user's privacy, and corporate tracking or government surveillance shouldn't be able to link together different compartments. At the simplest level, you could use separate browsers or multi-account containers for different activities, but taking it further you could have a virtual machine for each category (such as work, shopping, social etc). Alternativley, consider Qubes OS, which is designed for exactly this, and sandboxes

		each app in it's own Xen Hypervisor VM, while still providing great user experience
Disable Undesired Features (Windows)	Advanced	Microsoft Windows 10 is far from lean, and comes with many bundles "features" that run in the background, collecting data and using resources. Consider disabling are: Windows Script Host, AutoRun + AutoPlay, powershell.exe and cmd.exe execution via Windows Explorer, and the execution of commonly abused file extensions. In MS Office, consider disabling Office Macros, OLE object execution, ActiveX, DDE and Excel Links. There are tools that may make these fixes, and more easier, such as HardenTools, or ShutUp10. Note: This should only be done if you are competent Windows user, as modifying the registry can cause issues
Secure Boot	Advanced	For Windows users, ensure that Secure Boot is enabled. This security standard, ensures that your device boots only to trusted software when the PC starts. It prevents malware, such as a rootkit from maliciously replacing your boot loader, which could have serious consequences. Some Linux distros also work with secure boot (if they've applied to have their boot loaders signed by Microsoft), while others are incompatible (in which case, secure boot will need to be disabled)
Secure SSH Access	Advanced	If you access your system remotely, via SSH you should take steps to protect it from automated and targeted attacks. Change the port away from 22, use SSH keys to authenticate, disallow root login with a password and consider using a firewall, and only allow certain IPs to gain SSH access, consider using a Virtual Private Cloud as a gateway. Carry out regular service audits, to discover the services running on your system. For more info, see this guide, on OpenSSH security tweeks
Close Un-used Open Ports	Advanced	Some daemons listen on external ports, if they are not needed, then they are exposed to exploits. Turning off these listening services will protect against some remote exploits, and may also improve boot time. To check for listening services, just run netstat -lt
Implement Mandatory	Advanced	Restricting privileged access enables users to define rules, that limit how applications can run, or affect

Access Control		other processes and files. This means, that if a vulnerability is exploited, or your system is compromised, the damage will be limited. There are many options available, such as Rule Set Based Access Control, AppArmor or SELinux
Use Canary Tokens	Advanced	Breaches happen, but the longer it takes for you to find out about it, the more damage is done. A canary trap can help you know that someone's gained access to your files or emails much faster, and gain a bit of inform about the incident. A canary token is a file, email, note or webpage that's like a little hacker honeypot, something that looks appealing to them once they've gained access to your system. When they open the file, unknowingly to them, a script is run which will not only alert you of the breach, but also grab some of the intruders system details. These have been used to catch Dropbox employees opening users files, and Yahoo Mail employees reading emails. CanaryTokens.org and BlueCloudDrive are excellent sites, that you can use to generate your tokens. Then just leave them somewhere prominent on your system. Learn more about canary tokens, or see this guide for details on how to create them yourself.

Recommended Software

- Secure Operating Systems
- Linux Defenses
- Windows Defenses
- Mac OS Defenses
- Anti-Malware
- Firewalls
- File Encryption

Smart Home

Home assistants (such as Google Home, Alexa and Siri) and other internet connected devices collect large amounts of personal data (including voice samples, location data, home details and logs of all interactions). Since you have limited control on what is being collected, how it's stored, and what it will be used for, this makes it hard to recommend any consumer smart-home products to anyone who cares about privacy and security.

Security vs Privacy: There are many smart devices on the market that claim to increase the security of your home while being easy and convenient to use (Such as Smart Burglar Alarms, Internet Security Cameras, Smart Locks and Remote access Doorbells to name a few). These devices may appear to make security easier, but there is a trade-off in terms of privacy: as they collect large amounts of personal data, and leave you without control over how this is stored or used. The security of these devices is also questionable, since many of them can be (and are being) hacked, allowing an intruder to bypass detection with minimum effort.

The most privacy-respecting option, would be to not use "smart" internet-connected devices in your home, and not to rely on a security device that requires an internet connection. But if you do, it is important to fully understand the risks of any given product, before buying it. Then adjust settings to increase privacy and security. The following checklist will help mitigate the risks associated with internet-connected home devices.

Security	**Priority**	**Details and Hints**
Rename devices to not specify brand/model	Recommended	If your device name shows what brand or model it is, it will make it easier for a malicious actor launch an attack targeting a specific device. For example avoid names like "Nest Cam", "Yale Lock YRD 256" or "Hive Thermostat". It's usually easy to change the device's default name.
Disable microphone and camera when not in use	Recommended	Smart speakers and other voice controlled devices store sound clips on a server (and sometimes monitored by employees to improve the speech detection), any accidental recordings could disclose sensitive or personal data. A targeted attack could also allow someone to gain control of a microphone/ camera, so using the hardware switch to turn it off will help protect from that.
Understand what data is collected,	Recommended	Before purchasing any smart home device, do some research - and ensure that you

stored and transmitted		understand, and are comfortable with what is being collected and how it is stored and used. Don't buy devices that share anything with third parties, and check the data breach database.
Set privacy settings, and opt out of sharing data with third parties	Recommended	Once installed, go to settings in the app, and under privacy ensure the strictest options are selected. Usually by default, the most possible data is being collected.
Don't link your smart home devices to your real identity	Recommended	Use a unique user name and password which does not identify you, your family, your location or any other personal details. When creating an account for a new smart home device, do not sign up/log in with Facebook, Google or any other third-party service.
Keep firmware up-to-date	Recommended	Ensure firmware versions on smart devices are up-to-date and software patches have been applied. Most smart home apps will notify you when a new firmware version is available, so all you have to do it accept and install.
Protect your Network	Recommended	On many smart home devices, anybody connected to your home WiFi is able to view the device content (such as camera footages, or motion statistics). So ensure that your WiFi and home networks are properly secured with a strong password and up-to-date firmware. (See the Router Section for more details)
Be wary of wearables	Optional	Wearable smart devices allow companies to log even more data than ever before; they can track your every move to know exactly where you are and what you are doing at any given time. Again, you as the consumer have no control over what is done with that data.
Don't connect your home's critical infrastructure to the Internet	Optional	While a smart thermostat, burglar alarm, smoke detector and other appliances may seem convenient, they by design can be accessed remotely, meaning a hacker can gain control of your entire home, without even needing to be nearby. And by breaching

		multiple devices, the effects can be very serious.
Mitigate Alexa/ Google Home Risks	Optional	It is a known fact that voice-activated assistants collect a lot of personal data, and open the door to a mirage of security issues. Consider switching to Mycroft which is an open source alternative, with much better privacy. Alternativley, if you wish to continue using your current voice assistant, check out Project Alias, which prevents idle listening
Monitor your home network closely	Optional	Check your local network for suspicious activity. One of the easier methods to do this is with FingBox, but you can also do it directly through some routers.
Deny Internet access where possible	Advanced	If possible deny the device/ app internet access, and use it only on your local network. You can configure a firewall to block certain devices from sending or receiving from the internet.
Assess risks	Advanced	Assess risks with your audience and data in mind: Be mindful of whose data is being collected, e.g. kids. Manage which devices can operate when (such as turning cameras off when you are at home, or disabling the internet for certain devices at specific times of day)

Recommended Software

- Home Automation
- AI Voice Assistants

Personal Finance

Credit card fraud is the most common form of identity theft (with 133,015 reports in the US in 2017 alone), and a total loss of $905 million, which was a 26% increase from the previous year. The with a median amount lost per person was $429 in 2017. It's more important than ever to take basic steps to protect yourself from falling victim

Note about credit cards: Credit cards have technological methods in place to detect and stop some fraudulent transactions. Major payment processors implement this, by mining huge amounts of data from their card holders, in order to know a great deal about each persons spending habits. This data is used to identify fraud, but is also sold onto other data brokers. Credit cards are therefore good for security, but terrible for data privacy.

Security	**Priority**	**Details and Hints**
Sign up for Fraud Alerts and Credit Monitoring	Recommended	A Fraud Alert is a note on your credit report, that asks any business seeking your credit report to contact you to confirm your identity before granting credit in your name. Credit Monitoring tracks your credit history, and will alert you to any suspicious activity. You can enable fraud alerts and credit monitoring through credit the bureau's websites: Experian, TransUnion or Equifax
Apply a Credit Freeze	Recommended	A credit freeze will prevent anyone from requesting your credit report, hence stop someone applying for a financial product in your name, or a corporation requesting your details without your consent. You will need to temporarily disable your credit freeze before getting a loan, or any other financial product. You can freeze your credit through credit the bureau's website: Experian, TransUnion and Equifax
Use Virtual Cards	Optional	Virtual card numbers let you pay for items without revealing your real card or banking details. They also offer additional features, such as single-use cards and spending limits for each card. This means you will not be charged more than you specified, or ongoing subscriptions or in the case of a data breach. Privacy.com, MySudo and others offer this service

Use Cash for Local Transactions	Optional	Unlike any digital payment method, cash is virtually untraceable. Using cash for local and everyday purchases will prevent any financial institution building up a comprehensive data profile based on your spending habits
Use Cryptocurrency for Online Transactions	Optional	Unlike card payments, most cryptocurrencies are not linked to your real identity. Many blockchains have a public record, of all transaction matadata, on a public, immutable ledger. So where possible, opt for a privacy-focused currency, such as Monero or ZCash. If you are using a widley- supported currency (such as Tether, BitCoin, LiteCoin, Ripple, Etherium etc), take steps to distance yourself from the transaction details. See more privacy-respecting crypto currencies.
Store Crypto Securely	Advanced	Generate wallet address offline, never let your private key touch the internet and preferably avoid storing it on an internet-connected device. Use a secure wallet, such as Wasabi, or a hardware wallet, like Trezor or ColdCard. For long-term storage consider a paper wallet, or a more robust alternative, such as CryptoSteel
Buy Crypto Anonymously	Advanced	If you are buying a common cryptocurrency (such as BitCoin), purchasing it from an exchange with your debit/ credit card, will link directly back to your real identity. Instead use a service like LocalBitcoins, an anonymous exchange, such as Bisq, or buy from a local BitCoin ATM (find one here). Avoid any exchange that implements KYC
Tumble/ Mix Coins	Advanced	Before converting BitCoin back to currency, consider using a bitcoin mixer, or CoinJoin to make your transaction harder to trace. (Some wallets, such as Wasabi support this nativley)
Use an Alias Details for Online Shopping	Advanced	When you pay for goods or services online, you do not know for sure who will have access to your data, or weather it will be stored securley. Consider using an alias name, forwarding email address/ VOIP number, and don't reveal any of your true information. (For Amazon purchases,

		you can an Amazon gift card with cash, and use an Amazon Locker or local pickup location)
Use alternate delivery address	Advanced	When online shopping, if possible get goods delivered to an address that is not associated to you. For example, using a PO Box, forwarding address, corner-shop collection or pickup box

Recommended Software

- Virtual Credit Cards
- Cryptocurrencies
- Crypto Wallets
- Crypto Exchanges
- Other Payment Methods
- Budgeting Tools

Sensible Computing

Many data breaches, hacks and attacks are caused by human error. The following list contains steps you should take, to reduce the risk of this happening to you. Many of them are common sense, but it's worth takin note of.

Security	**Priority**	**Details and Hints**
Verify Recipients	Recommended	Emails are easy for an attacker to spoof, and unfortunately happens all too often. So whenever an email asks you to take a sensitive action, first verify that the sender is authentic, and when possible enter the URL yourself (rather than clicking a link in the message)
Don't Trust Your Popup Notifications	Recommended	It is a trivial task for a malicious actor to deploy fake pop-ups, either on your PC, phone or browser. If you click a popup, ensure the URL is correct before entering any information
Never Leave Device Unattended	Recommended	Even with a strong password, it's straight-forward to retrieve the data from your phone or computer (unless it is encrypted). If you lose your device, and have find my phone enabled, then remotely erase it

Prevent Camfecting	Recommended	It is a good idea to invest in some webcam covers, and microphone blockers to protect against *camfecting*, where a malicious actor, or app is able spy on you and your physical space, without your knowledge. See this guide for more tips. Mute home assistants, (Alexa, Google Home and Siri) when you are not using them, or at least when you are discussing anything sensitive or anything conversation involving personal details
Stay protected from shoulder surfers	Recommended	Be sure to not let anyone 'shoulder surf' (read what is on your screen, when in public space). As they may be able to gather sensitive information about you. You could apply a privacy screen to your laptop and mobile, in order to restrict data being read from an angle
Educate yourself about phishing attacks	Recommended	Phishing is an attempt to obtain sensitive information (like an account password) by disguising as a trustworthy person or company. In recent years phishing attacks have become increasingly sophisticated and hackers are learning to use data that people put on the web to create highly specific and targeted attacks. Check the URL before entering any information. Understand the context- were you expecting the email or message, does it feel normal? Employ general good security practices will also help: Use 2FA, don't reuse passwords, close accounts you no longer use and backup your data. See these guides on: How to Protect against Common Phishing Attacks and The Anatomy of a Phishing Email
Watch out for Stalkerware	Recommended	This is a malware that is installed directly onto your device by someone you know (partner, parent, boss etc). It allows them to see your location, messages and other app data remotely. The app likely won't show up in your app draw, (but may visible in Settings --

		> Applications --> View All). Sometimes they can be disguised as a non-conspicuous app (such as a game, flashlight or calculator) which initially don't appear suspicious at all. Look out for unusual battery usage, network requests or high device temperature. If you suspect that stalker ware is on your device, the best way to get rid of it is through a factory reset
Install Reputable Software from Trusted Sources	Recommended	It may seem obvious, but so much of the malware many PC users encounter is often as a result of accidentally downloading and installing bad software. Also, some legitimate applications try to offer you slightly dodgy freeware (such as toolbars, anti-virus, and other utilities). Be sure to pay attention while completing the installation process. Only download software from legitimate sources (often this isn't the top result in Google) so it's important to double check before downloading. Before installing, check it in Virus Total, which scans installable files using multiple AV checkers
Store personal data securely	Recommended	Backing up important data is important. But ensure that all information that is stored on your phone/laptop, USB or in a cloud is encrypted. That way, if it is accessed by a hacker (which unfortunately is all too common), it will be almost impossible for them to get to your personal files. For USB devices, see VeraCrypt. For cloud backup, see Cryptomator, and for your phone and laptop, see this guide
Obscure Personal Details from Documents	Recommended	When sharing any document, photo or video- be sure to blank out text with an opaque rectangle. Be careful with blurring/ pixelating out text, as this could be recovered (using something like Depix). This is especially true for video footage (such as with license plates), since an adversary has more frames to work with

Do not assume a site is secure, just because it is HTTPS	Recommended	Unlike HTTP, data sent over HTTPS is encrypted. However that does not mean you should trust that website by default. HTTPS Certificates can be obtained by anybody, so a cloned or scam site may have a valid certificate (as denoted by the padlock icon). Always check the URL, and don't enter any personal details unless you are certain a website is legitimate. Avoid entering data on any site that is not HTTPS
Use Virtual Cards when paying online	Optional	There are risks involved in entering your card details on any website. Credit cards have better consumer protection, compared to debit or bank cards, meaning you are more likely to be recompensated for fraudulent transactions, however they collect and sometimes sell your transaction history. A better option would be to pay with a virtual, 1-time card. This will mean that even if those credentials are compromised a hacker will not be able to lift any of your money. You can also set limits, or create single-use cards, to prevent being over-charged. Privacy.com offer virtual payment cards for that you can use anywhere on the internet, as does Revolut Premium
Review application permissions	Optional	Ensure that no app have unnecessary access to your photos, camera, location, contacts, microphone, call logs etc. See these guides for how to manage app permissions on Android and iOS. On Android, there is a great app called Exodus Privacy, that displays all permissions, and trackers for each of your installed apps
Opt-out of public lists	Optional	In many countries there are public databases that include citizens names, addresses, contact numbers and more. This can often result in unwanted contact from marketing companies, but in some cases used for harassment, stalking and fraud. This guide from The World Privacy Forum provides good instructions for how to

		approach this. This includes opting out of: Marketing, Financial Institution Listings, Mail Spam, FERPA Education Listings, Data Brokers and Advertising, as well as joining the National Do Not Call Registry
Never Provide Additional PII When Opting-Out	Optional	When removing yourself from less mainstream data sharing services, do not enter any additional information in the opt-out form than what is already publicly availible through that site. There have been cases where this extra info is used elsewhere to add more details to your record
Opt-out of data sharing	Optional	Many apps, services and software automatically opt you in for data collection and sharing. You should opt-out of this, for instructions on how to opt-out, see Simple Opt Out. Often this collected data is sold onto third-parties, who combine multiple data sets together, allowing them to easily deduce your identity, along with your habits, purchases, personal details, location etc
Review and update social media privacy	Optional	Companies regularly update their terms, and that often leads to you being opted back. Check you Facebook, Twitter, Google etc. activity and privacy settings. See also re-consent and Jumbo which are tools aimed at making this clearer and easier
Compartmentalize	Advanced	Compartmentalization is where to keep several categories of digital activity and files totally separate from each other. It means that if one area is breached, then an attacker will only have a proportion of your data, and the rest will still be safe. For example, store your work and personal files on separate devices, or use different web browsers for different types of activity, or even run certain tasks in a contained VM or on a separate device (such as having a work phone, and personal phone, or using a separate browser for social media/ chat

		rooms, or even running a VM for using specialist software)
WhoIs Privacy Guard	Advanced	Owning your own domain can prevent you loosing access to your email addresses, or being locked-in with a certain provider. However if you do not use a privacy guard, or enter false web admin details, your data will be publicly accessible through a WhoIs search. Most reputable domain registrars will have a WhoIs Privacy option
Use a forwarding address	Advanced	Have all mail addressed to a PO Box or forwarding address, to prevent any commerce, utility, finance, media or other companies knowing your read address. This would give you an extra layer of protecting if they suffered a breach, sold on personal details or were presented with a court order
Use anonymous payment methods	Advanced	Paying online with credit or debit card involves entering personal details, including name and residential address. Paying with cryptocurrency will not require you to enter any identifiable information. Both Monero and Zcash are totally anonymous, and so best for privacy. See also: Anonymous Payment Methods

See also: Online Tools

Physical Security

Public records often include sensitive personal data (full name, date of birth, phone number, email, address, ethnicity etc), and are gathered from a range of sources (census records, birth/ death/ marriage certificates, voter registrants, marketing information, customer databases, motor vehicle records, professional/ business licenses and all court files in full detail). This sensitive personal information is easy and legal to access, which raises some serious privacy concerns (identity theft, personal safety risks/ stalkers, destruction of reputations, dossier society)

CCTV is one of the major ways that the corporations, individuals and the government tracks your movements. In London, UK the average person is caught on camera about 500 times per day. This network is continuing to grow, and in many cities around the world, facial recognition is being rolled out, meaning the state can know the identity of residents on the footage in real-time.

Strong authentication, encrypted devices, patched software and anonymous web browsing may be of little use if someone is able to physically compromise you, your devices and your data. This section outlines some basic methods for physical security

Security	**Priority**	**Details and Hints**
Destroy Sensitive Documents	Recommended	Instead of disposing of paperwork in the trash, you should first shred it, or take steps to redact any personally identifiable information. This will help protect you from identity theft, reduce the chance of blackmail and keep confidential data confidential
Opt-Out of Public Records	Recommended	People search websites (such as WhitePages, Spokeo and Radaris) list public records, including: full name, date of birth, address, and phone number. Some sites go further, showing place of work, previous addresses, criminal records and photos. This is bad for privacy, and can make you a target for fraud. It is recommended to contact these sites, and opt-out from these listings. Methods for doing so range considerably between countries and states, see Personal Data Removal Workbook by Michael Bazzell or Word Privacy Forum Opt-Out Guide or The LifeWire Remove Personal Information Guide to get started
Don't Reveal Info on Inbound Calls	Recommended	Only share sensitive personal data on outbound calls/ communications that you have initiated. Ensure the phone number is correct, and listen for anything that doesn't sound right. If a company phones you, and asks any questions, hang up and phone them back on their official number
Stay Alert	Recommended	Stay aware of your surroundings. Whenever you step into a new environment, take a moment to assess potential risks. Listen to your instincts, when approached by an unknown individual. Ensure you are not being followed, when you approach your home address. Understand basic self-defense principle, and know how to put them into practice to defend yourself, if needed
Secure Perimeter	Recommended	Maintain physical and structural integrity to all locations where devices with personal info are stored, and ensure steps have been put in place to

		stop any unauthorized access. Minimize external access: doors, windows, vents. Maintain locking devices responsibly: Keep keys safe, don't use guessable combinations, have multiple locks, change locks after a breach or potential risk. Consider intrusion detection systems, such as alarms and closed circuit monitoring. Make sure walls are structurally sound, and if there is a drop ceiling, ensure walls continue up into the ceiling. When inside - don't trust door chain lock and cover door peep hole
Physically Secure Devices	Recommended	Use a Kensington lock to secure your device. Never leave devices unattended. Cover your web cam, consider a microphone block or disable it when not in use, use a USB data blocker when charging devices, use a privacy screen when working in public spaces
Keep Devices Out of Direct Sight	Recommended	It is possible for an adversary to communicate with voice assistants with lasers at a certain frequency. This can be mitigated by keeping devices out direct line of sight from windows. Any electronics visible from outside, may also pose a risk from theft, and hence should be stored somewhere safe
Protect your PIN	Recommended	When entering a code or password (such as unlocking device, withdrawing money from an ATM, or inputting a building access code), ensure that no one is watching over your shoulder, and they you are not in direct line of sight of a camera. Cover the keypad while entering the code to shield your PIN. After entering your PIN on a touch screen device, wipe over the screen to ensure your PIN can not be determined from smudge marks left by skin.
Check for Skimmers	Recommended	Before entering your card into an ATM, check for any signs that it may have been tampered with. You could use a card skimmer detector, or try to pull the card intake device to ensure it's firmly fitted. Watch out for other signs of compromise, such as small cameras, keypad covers or blockage on the cash out slot. This also applies to any public device that requires biometric or personal data to complete an action.

Protect your Home Address	Optional	Don't set your home address in your phones settings, instead consider selecting a location in a similar region to where you live. Consider storing devices in faraday cage when at your home address. For deliveries, consider using an alias names, and if possible a forwarding or pickup address for receiving online deliveries. You could also combine this with anonymous payment (such as virtual card numbers/ privacy.com, cryptocurrency or cash), and a forwarding email address or VOIP number
Use a PIN, Not Biometrics	Advanced	For situations where law enforcement may be involved (such as a protest, or journalism), if your device is seized, authorities can not force you to hand over your device pin code, however they can ask for your fingerprint or face scan to unlock a device. Therefore in these situations disable biometric unlock.
Reduce exposure to CCTV	Advanced	Wearing a hat, hoodie, dark glasses or face cover can make it harder for your identity to be known. Less busy streets tend to have fewer cameras. Knowing where cameras in your local area are, can help you avoid being caught on them. See more in this article by Snälla Bolaget
Anti-Facial Recognition Clothing	Advanced	Most facial-recognition methods can be easily tricked with certain patterns. Example products from: Adversarial Fashion or this item on Redbubble.
Reduce Night Vision Exposure	Advanced	Infrared night vision cameras are very easy to block, by using a small IR light source, which is invisible to the human eye, but blinds night vision cameras. Alternatively super-reflective glasses (see Reflectacles) can also fool night vision cameras.
Protect your DNA	Advanced	DNA is totally unique person-to-person, and can directly identify you. Therefore it is important to avoid sharing this information, do not submit your DNA to heritage websites, be careful about where you leave your DNA.