THREAT INTELLIGENCE REPORT

Personal Security Checklist

Ref. **PD-TI-2026-32825** Published **10 July 2026** Source **phishdestroy.io/security-checklist**

258 battle-tested tips for protecting your digital security and privacy. Track your progress as you harden your defenses.

~25 min read · Updated **March 2026** · PhishDestroy Intelligence

Your Progress

0%
0 completed 258 total

Categories

Click to jump to section

Authentication
21 items
Securing your online account login credentials
0 /21 done
Web Browsing
39 items

Avoiding tracking, censorship, and data collection online
0 /39 done
Email
21 items
Protecting the gateway to your online accounts
0 /21 done
Messaging
19 items
Keeping your communications private and secure
0 /19 done
Social Media
15 items
Minimizing the risks associated with using online communities
0 /15 done
Networks
25 items
Safeguarding your network traffic
0 /25 done
Mobile Devices
23 items
Reduce invasive tracking for cells, smartphones and tablets
0 /23 done
Personal Computers
35 items
Securing your PC's operating system, data & activity
0 /35 done
Smart Home
13 items
Using IoT devices without compromising your privacy
0 /13 done
Personal Finance
10 items
Protecting your funds, financial accounts and transactions
0 /10 done
Human Aspect
21 items
Avoiding social engineering security risks
0 /21 done
Physical Security
16 items
Taking measures to prevent IRL security incidents
0 /16 done

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.

0 / 21 6 Essential 9 Optional 6 Advanced

Use a Strong Password

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 Security.org's How Secure Is My Password? , to get an idea of how quickly common passwords can be cracked. Read more about creating strong passwords: securityinabox.org .

Essential

Don't Reuse Passwords

If someone were to reuse a password and one site they had an account with suffered a leak, 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.

Essential

Use a Secure Password Manager

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 password (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 .

Essential

Avoid Sharing Passwords

While there may be times that you need to share access to an account with another person, you should generally avoid doing this because it makes it easier for the account to become compromised. If you absolutely do need to share a password — for example, when working on a team with a shared account — this should be done via features built into a password manager.

Essential

Enable 2-Factor Authentication

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 your password (e.g., through phishing, malware, or a data breach), they will not 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 is displayed in the app on your phone (it works without internet, and the code usually changes every 30 seconds).

Essential

Keep Backup Codes Safe

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 unauthorized access. You should store these on paper or in a safe place on disk (e.g., in offline storage or an encrypted file/drive). Don't store these in your password manager as 2FA sources and passwords should be kept separately.

Essential

Sign Up for Breach Alerts

After a website suffers a significant data breach, the leaked data often ends up on the internet. Several websites 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 DeHashed 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).

Optional

Shield your Password/PIN

When typing your password in public places, ensure you are not in direct line of sight of a CCTV camera and that no one can see over your shoulder. Cover your password or pin code while you type, and do not reveal any plain text passwords on your screen.

Optional

Update Critical Passwords Periodically

Database leaks and breaches are common, and, likely, 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.

Optional

Don’t Save your Password in Browsers

Most modern browsers offer to save your credentials when you log into a site. Don’t allow this, as they are not always encrypted and could allow someone to gain access to your accounts. Instead, use a dedicated password manager to store (and auto-fill) your passwords.

Optional

Avoid Logging In on Someone Else’s Device

Avoid logging in on other people's computers since you can't be sure their system is clean. Be especially cautious of public machines, as malware and tracking arr more common here. Using someone else's device is especially dangerous with critical accounts like online banking. When using someone else's machine, ensure that you're in a private/incognito session (Use Ctrl+Shift+N/ Cmd+Shift+N). This will request the browser to not save your credentials, cookies, and browsing history.

Optional

Avoid Password Hints

Some sites allow you to set password hints. Often, it is very easy to guess answers. In cases where password hints are mandatory, use random answers and record them in your password manager (

`Name of the first school: 6D-02-8B-!a-E8-8F-81`).

Optional

Never Answer Online Security Questions Truthfully

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. Using real words is better than random characters, as explained here .

Optional

Don’t Use a 4-digit PIN

Don’t use a short PIN to access your smartphone or computer. Instead, use a text password or a much longer PIN. Numeric passphrases are easy to crack (A 4-digit pin has 10,000 combinations, compared to 7.4 million for a 4-character alpha-numeric code).

Optional

Avoid Using SMS for 2FA

When enabling multi-factor authentication, opt for app-based codes or a hardware token if supported. SMS is susceptible to several 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 a signal and can be slow. If a website or service requires the usage of an SMS number for recovery, consider purchasing a second pre-paid phone number only used for account recovery for these instances.

Optional

Avoid Using your PM to Generate OTPs

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.

Advanced

Avoid Face Unlock

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.

Advanced

Watch Out for Keyloggers

A hardware keylogger is a physical device planted between your keyboard and the USB port, which intercepts all keystrokes 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.

Advanced

Consider a Hardware Token

A U2F/FIDO2 security key is a USB (or NFC) device that you insert while logging in to an online service 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, it 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.
Advanced
Consider Offline Password Manager
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.
Advanced
Consider Unique Usernames
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.
Advanced

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.

0 / 39 13 Essential 20 Optional 4 Advanced
Block Ads
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.

Essential

Ensure Website is Legitimate

It may sound obvious, but when you logging into any online accounts, double check the URL is correct. Storing commonly visited sites in your bookmarks is a good way to ensure the URL is easy to find. 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 , IsLegitSite , Google Safe Browsing Status if you are unsure.

Basic

Watch out for Browser Malware

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 signs 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 .

Basic

Use a Privacy-Respecting Browser

Firefox (with a few tweaks) and Brave are secure, private-respecting 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, Edge and Safari as (without correct configuration) all three of them, collect usage data, call home and allow for invasive tracking. Firefox requires a few changes to achieve optimal security, for example - arkenfox or 12byte 's user.js configs. See more: Privacy Browsers .

Essential

Use a Private Search Engine

Using a privacy-preserving, non-tracking search engine, will reduce risk that your search terms are not logged, or used against you. Consider DuckDuckGo , or Qwant . 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.

Essential

Remove Unnecessary Browser Addons

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.

Essential

Keep Browser Up-to-date

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 you're using here , or follow this guide for instructions on how to update. Some browsers will auto-update to the latest stable version.
Essential
Check for HTTPS
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) used to be a browser extension/addon that automatically enabled HTTPS on websites, but as of 2022 is now deprecated. In their accouncement article the EFF explains that most browsers now integrate such protections. Additionally, it provides instructions for Firefox , Chrome, Edge and Safari browsers on how to enable their HTTPS secure protections.
Essential
Use DNS-over-HTTPS
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 its own issues, mostly preventing web filtering.
Essential
Multi-Session Containers
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).
Essential
Use Incognito
When using someone else's machine, ensure that you're in a private/ incognito session. This will prevent browser history, cookies and some data being saved, but is not fool-proof- you can still be tracked.
Essential
Understand Your Browser Fingerprint
Browser Fingerprinting is an incredibly accurate method of tracking, where a website identifies you based on your device information. You can view your fingerprint at amiunique.org- The aim is to be as un-unique as possible.
Essential
Manage Cookies
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. To mitigate this you should clear cookies often.
Essential
Block Third-Party Cookies

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.

Essential

Block Third-Party Trackers

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.

Essential

Beware of Redirects

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.

Optional

Do Not Sign Into Your Browser

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.

Optional

Disallow Prediction Services

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.

Optional

Avoid G Translate for Webpages

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.

Optional

Disable Web Notifications

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.

Optional

Disable Automatic Downloads

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.

Optional

Disallow Access to Sensors

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.

Optional

Disallow Location

Location Services lets sites ask for your physical location to improve your experience. This should be disabled in settings. Note that there are still other methods of determining your approximate location.

Optional

Disallow Camera/ Microphone access

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.

Optional

Disable Browser Password Saves

Do not allow your browser to store usernames and passwords. These can be easily viewed or accessed. Instead use a password manager.

Optional

Disable Browser Autofill

Turn off autofill for any confidential or personal details. This feature can be harmful if your browser is compromised in any way. Instead, consider using your password manager's Notes feature.

Optional

Protect from Exfil Attack

The CSS Exfiltrate attack is a method where credentials and other sensitive details can be snagged with just pure CSS. You can stay protected, with the CSS Exfil Protection plugin.

Optional

Deactivate ActiveX

ActiveX is a browser extension API that built into Microsoft IE, and enabled by default. It's not commonly used anymore, but since it gives plugins intimate access rights, and can be dangerous, therefore you should disable it.

Optional

Disable WebRTC

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. To learn more, check out this guide.

Optional

Spoof HTML5 Canvas Sig

Canvas Fingerprinting allows websites to identify and track users very accurately. You can use the Canvas-Fingerprint-Blocker extension to spoof your fingerprint or use Tor .

Optional

Spoof User Agent

The user agent tells the website what device, browser and version you are using. Switching user agent periodically is one small step you can take to become less unique.

Optional

Disregard DNT

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.

Optional

Prevent HSTS Tracking

HSTS was designed to help secure websites, but privacy concerns have been raised as it allowed site operators to plant super-cookies. It can be disabled by visiting chrome://net-internals/#hsts in

Chromium-based browsers.
Optional
Prevent Automatic Browser Connections
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.
Optional
Enable 1st-Party Isolation
First Party Isolation means that all identifier sources and browser state are scoped using the URL bar domain, this can greatly reduce tracking.
Optional
Strip Tracking Params from URLs
Websites often append additional GET parameters to URLs that you click, to identify information like source/referrer. You can sanitize manually, or use an extension like ClearURLs to strip tracking data from URLs automatically.
Advanced
First Launch Security
After installing a web browser, the first time you launch it (prior to configuring its privacy settings), most browsers will call home. Therefore, after installing a browser, you should first disable your internet connection, then configure privacy options before reenabling your internet connectivity.
Advanced
Use The Tor Browser
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.
Advanced
Disable JavaScript
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.
Advanced

Email

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.”

0 / 21 4 Essential 5 Optional 12 Advanced
Have more than one email address

Consider using a different email address for security-critical communications from trivial mail such as newsletters. This compartmentalization could reduce the amount of damage caused by a data breach, and also make it easier to recover a compromised account.

Essential

Keep Email Address Private

Do not share your primary email publicly, as mail addresses are often the starting point for most phishing attacks.

Essential

Keep your Account Secure

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.

Essential

Disable Automatic Loading of Remote Content

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 .

Essential

Use Plaintext

There are two main types of emails on the internet: plaintext and HTML. The former is strongly preferred for privacy & security as HTML messages often include identifiers in links and inline images, which can collect usage and personal data. There's also numerous risks of remote code execution targeting the HTML parser of your mail client, which cannot be exploited if you are using plaintext. For more info, as well as setup instructions for your mail provider, see UsePlaintext.email .

Optional

Don’t connect third-party apps to your email account

If you give a third-party app or plug-in 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.

Optional

Don't Share Sensitive Data via Email

Emails are very easily intercepted. Furthermore, you can’t be sure of how secure your recipient's environment is. Therefore, emails cannot be considered safe for exchanging confidential information, unless it is encrypted.

Optional

Consider Switching to a Secure Mail Provider

Secure and reputable email providers such as Forward Email , 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.

Optional

Use Smart Key

OpenPGP 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.

Advanced

Use Aliasing / Anonymous Forwarding

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.

Advanced

Subaddressing

An alternative to aliasing is subaddressing, where anything after the `+` symbol is omitted during mail delivery. This 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.

Optional

Use a Custom Domain

Using a custom domain means that you are not dependent on the address assigned by your mail provider. So you can easily switch providers in the future and do not need to worry about a service being discontinued.

Advanced

Sync with a client for backup

To avoid losing 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.

Advanced

Be Careful with Mail Signatures

You do not know how secure of an email environment the recipient of your message may have. There are several extensions that automatically crawl messages, and create a detailed database of contact information based upon email signatures.

Advanced

Be Careful with Auto-Replies

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.

Advanced

Choose the Right Mail Protocol

Do not use outdated protocols (below IMAPv4 or POPv3), both have known vulnerabilities and out-dated security.

Advanced

Self-Hosting

Self-hosting your own mail server is not recommended for non-advanced users, since correctly securing it is critical yet requires strong networking knowledge.

Advanced

Always use TLS Ports

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.

Advanced

DNS Availability

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.
Advanced
Prevent DDoS and Brute Force Attacks
For self-hosted mail servers (specifically SMTP), limit your total number of simultaneous connections, and maximum connection rate to reduce the impact of attempted bot attacks.
Advanced
Maintain IP Blacklist
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.
Advanced

Messaging

0 / 19 8 Essential 7 Optional 4 Advanced
Only Use Fully End-to-End Encrypted Messengers
End-to-end encryption is a system of communication where messages are encrypted on your device and not decrypted until they reach the intended recipient. This ensures that any actor who intercepts traffic cannot read the message contents, nor can anybody with access to the central servers where data is stored.
Essential
Use only Open Source Messaging Platforms
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.
Essential
Use a "Trustworthy" Messaging Platform
When selecting an encrypted messaging app, ensure it's fully open source, stable, actively maintained, and ideally backed by reputable developers.
Essential
Check Security Settings
Enable security settings, including contact verification, security notifications, and encryption. Disable optional non-security features such as read receipt, last online, and typing notification.
Essential
Ensure your Recipients Environment is Secure
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.
Essential
Disable Cloud Services
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.
Essential
Secure Group Chats

The risk of compromise rises exponentially, the more participants are in a group, as the attack surface increases. Periodically check that all participants are legitimate.

Essential

Create a Safe Environment for Communication

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.

Essential

Agree on a Communication Plan

In certain situations, it may be worth making a communication plan. This should include primary and backup methods of securely getting in hold with each other.

Optional

Strip Meta-Data from Media

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.

Optional

Defang URLs

Sending links via various services can unintentionally expose your personal information. This is because, when a thumbnail or preview is generated- it happens on the client-side.

Optional

Verify your Recipient

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.

Optional

Enable Ephemeral Messages

Self-destructing messages is a feature that 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.

Optional

Avoid SMS

SMS may be convenient, but it's not secure. It is susceptible to threats such as interception, sim swapping, manipulation, and malware.

Optional

Watch out for Trackers

Be wary of messaging applications with trackers, as the detailed usage statistics they collect are often very invasive, and can sometimes reveal your identity as well as personal information that you would otherwise not intend to share.

Optional

Consider Jurisdiction

The jurisdictions where the organisation is based, and data is hosted should also be taken into account.

Advanced

Use an Anonymous Platform

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.
Advanced
Ensure Forward Secrecy is Supported
Opt for a platform that implements forward secrecy. This is where your app generates a new encryption key for every message.
Advanced
Consider a Decentralized Platform
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.
Advanced

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.

0 / 15 10 Essential 1 Optional 4 Advanced
Secure your Account
Social 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.
Essential
Check Privacy Settings
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.
Essential
Think of All Interactions as Public
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?"
Essential
Think of All Interactions as Permanent
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.
Essential
Don't Reveal too Much
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).
Essential

Be Careful what you Upload
Status updates, comments, check-ins and media can unintentionally reveal a lot more than you intended them to. This is especially relevant to photos and videos, which may show things in the background.
Essential
Don't Share Email or Phone Number
Posting your real email address or mobile number, gives hackers, trolls and spammers more munition to use against you, and can also allow separate aliases, profiles or data points to be connected.
Essential
Don't Grant Unnecessary Permissions
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.
Essential
Be Careful of 3rd-Party Integrations
Avoid signing up for accounts using a Social Network login, revoke access to social apps you no longer use.
Essential
Avoid Publishing Geo Data while still Onsite
If you plan to share any content that reveals a 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.
Essential
Remove metadata before uploading media
Most smartphones and some cameras automatically attach a comprehensive set of additional data (called EXIF data) to each photograph. Remove this data before uploading.
Optional
Implement Image Cloaking
Tools like Fawkes can be used to very subtly, slightly change the structure of faces within photos in a way that is imperceptible by humans, but will prevent facial recognition systems from being able to recognize a given face.
Advanced
Consider Spoofing GPS in home vicinity
Even if you yourself never use social media, there is always going to be others who are not as careful, and could reveal your location.
Advanced
Consider False Information
If you just want to read, and do not intend on posting too much- consider using an alias name, and false contact details.
Advanced
Don’t have any social media accounts
Social media is fundamentally un-private, so for maximum online security and privacy, avoid using any mainstream social networks.
Advanced

Networks

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

0 / 25 4 Essential 19 Optional 2 Advanced

Use a VPN

Use a reputable, paid-for VPN. This can help protect sites you visit from logging your real IP, reduce the amount of data your ISP can collect, and increase protection on public WiFi.

Essential

Change your Router Password

After getting a new router, change the password. Default router passwords are publicly available, meaning anyone within proximity would be able to connect.

Essential

Use WPA2, and a strong password

There are different authentication protocols for connecting to WiFi. Currently, the most secure options are WPA2 and WPA3 (on newer routers).

Essential

Keep router firmware up-to-date

Manufacturers release firmware updates that fix security vulnerabilities, implement new standards, and sometimes add features or improve the performance of your router.

Essential

Implement a Network-Wide VPN

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.

Optional

Protect against DNS leaks

When using a VPN, it is extremely important to exclusively use the DNS server of your VPN provider or secure service.

Optional

Use a secure VPN Protocol

OpenVPN and WireGuard are open source, lightweight, and secure tunneling protocols. Avoid using PPTP or SSTP.

Optional

Secure DNS

Use DNS-over-HTTPS which performs DNS resolution via the HTTPS protocol, encrypting data between you and your DNS resolver.

Optional

Avoid the free router from your ISP

Typically they’re manufactured cheaply in bulk in China, with insecure propriety firmware that doesn't receive regular security updates.

Optional

Whitelist MAC Addresses

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.

Optional

Change the Router’s Local IP Address

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.

Optional

Don't Reveal Personal Info in SSID

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.

Optional

Opt-Out Router Listings

WiFi SSIDs are scanned, logged, and then published on various websites, which is a serious privacy concern for some.

Optional

Hide your SSID

Your router's Service Set Identifier is simply the network name. If it is not visible, it may receive less abuse.

Optional

Disable WPS

Wi-Fi Protected Setup provides an easier method to connect, without entering a long WiFi password, but WPS introduces a series of major security issues.

Optional

Disable UPnP

Universal Plug and Play allows applications to automatically forward a port on your router, but it has a long history of serious security issues.

Optional

Use a Guest Network for Guests

Do not grant access to your primary WiFi network to visitors, as it enables them to interact with other devices on the network.

Optional

Change your Router's Default IP

Modifying your router admin panel's default IP address will make it more difficult for malicious scripts targeting local IP addresses.

Optional

Kill unused processes and services on your router

Services like Telnet and SSH 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.

Optional

Don't have Open Ports

Close any open ports on your router that are not needed. Open ports provide an easy entrance for hackers.

Optional

Disable Unused Remote Access Protocols

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.

Optional
Disable Cloud-Based Management
You should treat your router's admin panel with the utmost care, as considerable damage can be caused if an attacker is able to gain access.
Optional
Manage Range Correctly
It's common to want to pump your router's range to the max, but if you reside in a smaller flat, your attack surface is increased when your WiFi network can be picked up across the street.
Optional
Route all traffic through Tor
VPNs have their weaknesses. For increased security, route all your internet traffic through the Tor network.
Advanced
Disable WiFi on all Devices
Connecting to even a secure WiFi network increases your attack surface. Disabling your home WiFi and connect each device via Ethernet.
Advanced

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.

0 / 23 6 Essential 15 Optional 2 Advanced
Encrypt your Device
In order to keep your data safe from physical access, use file encryption. This will mean if your device is lost or stolen, no one will have access to your data.
Essential

Turn off connectivity features that aren’t being used
When you're not using WiFi, Bluetooth, NFC etc, turn those features off. There are several common threats that utilise these features.
Essential
Keep app count to a minimum
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.
Essential
App Permissions
Don’t grant apps permissions that they don’t need. For Android, Bouncer is an app that allows you to grant temporary/ 1-off permissions.
Essential
Only install Apps from official source
Applications on Apple App Store and Google Play Store are scanned and cryptographically signed, making them less likely to be malicious.
Essential
Be Careful of Phone Charging Threats
Juice Jacking is when hackers use public charging stations to install malware on your smartphone or tablet through a compromised USB port.
Optional
Set up a mobile carrier PIN
SIM hijacking is when a hacker is able to get your mobile number transferred to their sim. The easiest way to protect against this is to set up a PIN through your mobile provider.
Essential
Opt-out of Caller ID Listings
To keep your details private, you can unlist your number from caller ID apps like TrueCaller, CallApp, SyncMe, and Hiya.
Optional
Use Offline Maps
Consider using an offline maps app, such as OsmAnd or Organic Maps, to reduce data leaks from map apps.
Optional
Opt-out of personalized ads
You can slightly reduce the amount of data collected by opting-out of seeing personalized ads.
Optional
Erase after too many login attempts
To protect against an attacker brute forcing your pin, set your device to erase after too many failed login attempts.
Optional
Monitor Trackers
Îµxodus is a great service which lets you search for any app and see which trackers are embedded in it.
Optional
Use a Mobile Firewall

To prevent applications from leaking privacy-sensitive data, you can install a firewall app.
Optional
Reduce Background Activity
For Android, SuperFreeze makes it possible to entirely freeze all background activities on a per-app basis.
Optional
Sandbox Mobile Apps
Prevent permission-hungry apps from accessing your private data with Island , a sandbox environment.
Optional
Tor Traffic
Orbot provides a system-wide Tor connection, which will help protect you from surveillance and public WiFi threats.
Advanced
Avoid Custom Virtual Keyboards
It is recommended to stick with your device's stock keyboard. If you choose to use a third-party keyboard app, ensure it is reputable.
Optional
Restart Device Regularly
Restarting your phone at least once a week will clear the app state cached in memory and may run more smoothly after a restart.
Optional
Avoid SMS
SMS should not be used to receive 2FA codes or for communication, instead use an encrypted messaging app, such as Signal .
Optional
Keep your Number Private
MySudo allows you to create and use virtual phone numbers for different people or groups. This is great for compartmentalisation.
Optional
Watch out for Stalkerware
Stalkerware is malware that is installed directly onto your device by someone you know. The best way to get rid of it is through a factory reset.
Optional
Favor the Browser, over Dedicated App
Where possible, consider using a secure browser to access sites, rather than installing dedicated applications.
Optional
Consider running a custom ROM (Android)
If you're concerned about your device manufacturer collecting too much personal information, consider a privacy-focused custom ROM.
Advanced

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.

0 / 35 11 Essential 13 Optional 11 Advanced

Keep your System up-to-date

System updates contain fixes/patches for security issues, improve performance, and sometimes add new features. Install new updates when prompted.

Essential

Encrypt your Device

Use BitLocker for Windows, FileVault on MacOS, or LUKS on Linux, to enable full disk encryption. This prevents unauthorized access if your computer is lost or stolen.

Essential

Backup Important Data

Maintaining encrypted backups prevents loss due to ransomware, theft, or damage. Consider using Cryptomator for cloud files or VeraCrypt for USB drives.

Essential

Be Careful Plugging USB Devices into your Computer

USB devices can pose serious threats. Consider making a USB sanitizer with CIRCLean to safely check USB devices.

Essential

Activate Screen-Lock when Idle

Lock your computer when away and set it to require a password on resume from screensaver or sleep to prevent unauthorized access.

Essential

Disable Cortana or Siri

Voice-controlled assistants can have privacy implications due to data sent back for processing. Disable or limit their listening capabilities.

Essential

Review your Installed Apps

Keep installed applications to a minimum to reduce exposure to vulnerabilities and regularly clear application caches.

Essential

Manage Permissions

Control which apps have access to your location, camera, microphone, contacts, and other sensitive information.

Essential

Disallow Usage Data from being sent to the Cloud

Limit the amount of usage information or feedback sent to the cloud to protect your privacy.

Essential

Avoid Quick Unlock

Use a strong password instead of biometrics or short PINs for unlocking your computer to enhance security.

Essential

Power Off Computer, instead of Standby

Shut down your device when not in use, especially if your disk is encrypted, to keep data secure.
Essential
Don't link your PC with your Microsoft or Apple Account
Use a local account only to prevent data syncing and exposure. Avoid using sync services that compromise privacy.
Optional
Check which Sharing Services are Enabled
Disable network sharing features you are not using to close gateways to common threats.
Optional
Don't use Root/Admin Account for Non-Admin Tasks
Use an unprivileged user account for daily tasks and only elevate permissions for administrative changes to mitigate vulnerabilities.
Optional
Block Webcam + Microphone
Cover your webcam when not in use and consider blocking unauthorized audio recording to protect privacy.
Optional
Use a Privacy Filter
Use a screen privacy filter in public spaces to prevent shoulder surfing and protect sensitive information.
Optional
Physically Secure Device
Use a Kensington Lock to secure your laptop in public spaces and consider port locks to prevent unauthorized physical access.
Optional
Don't Charge Devices from your PC
Use a power bank or AC wall charger instead of your PC to avoid security risks associated with USB connections.
Optional
Randomize your hardware address on Wi-Fi
Modify or randomize your MAC address to protect against tracking across different WiFi networks.
Optional
Use a Firewall
Install a firewall app to monitor and block unwanted internet access by certain applications, protecting against remote access attacks and privacy breaches.
Optional
Protect Against Software Keyloggers
Use key stroke encryption tools to protect against software keyloggers recording your keystrokes.
Optional
Check Keyboard Connection
Be vigilant for hardware keyloggers when using public or unfamiliar computers by checking keyboard connections.
Optional
Prevent Keystroke Injection Attacks

Lock your PC when away and consider using USBGuard or similar tools to protect against keystroke injection attacks.
Optional
Don't use commercial "Free" Anti-Virus
Rely on built-in security tools and avoid free anti-virus applications due to their potential for privacy invasion and data collection.
Optional
Periodically check for Rootkits
Regularly check for rootkits to detect and mitigate full system control threats using tools like chkrootkit .
Advanced
BIOS Boot Password
Enable a BIOS or UEFI password to add an additional security layer during boot-up, though be aware of its limitations.
Advanced
Use a Security-Focused Operating System
Consider switching to Linux or a security-focused distro like QubeOS or Tails for enhanced privacy and security.
Advanced
Make Use of VMs
Use virtual machines for risky activities or testing suspicious software to isolate potential threats from your primary system.
Advanced
Compartmentalize
Isolate different programs and data sources from one another as much as possible to limit the extent of potential breaches.
Advanced
Disable Undesired Features (Windows)
Disable unnecessary Windows "features" and services that run in the background to reduce data collection and resource use.
Advanced
Secure Boot
Ensure that Secure Boot is enabled to prevent malware from replacing your boot loader and other critical software.
Advanced
Secure SSH Access
Take steps to protect SSH access from attacks by changing the default port, using SSH keys, and configuring firewalls.
Advanced
Close Un-used Open Ports
Turn off services listening on external ports that are not needed to protect against remote exploits and improve security.
Advanced
Implement Mandatory Access Control

Restrict privileged access to limit the damage that can be done if a system is compromised.
Advanced
Use Canary Tokens
Deploy canary tokens to detect unauthorized access to your files or emails faster and gather information about the intruder.
Advanced

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.

0 / 13 7 Essential 4 Optional 2 Advanced
Rename devices to not specify brand/model
Change default device names to something generic to prevent targeted attacks by obscuring brand or model information.
Essential
Disable microphone and camera when not in use
Use hardware switches to turn off microphones and cameras on smart devices to protect against accidental recordings or targeted access.
Essential
Understand what data is collected, stored and transmitted
Research and ensure comfort with the data handling practices of smart home devices before purchase, avoiding devices that share data with third parties.
Essential
Set privacy settings, and opt out of sharing data with third parties
Adjust app settings for strictest privacy controls and opt-out of data sharing with third parties wherever possible.
Essential
Don't link your smart home devices to your real identity
Use anonymous usernames and passwords, avoiding sign-up/log-in via social media or other third-party services to maintain privacy.

Essential
Keep firmware up-to-date
Regularly update smart device firmware to apply security patches and enhancements.
Essential
Protect your Network
Secure your home WiFi and network to prevent unauthorized access to smart devices.
Essential
Be wary of wearables
Consider the extensive data collection capabilities of wearable devices and their implications for privacy.
Optional
Don't connect your home's critical infrastructure to the Internet
Evaluate the risks of internet-connected thermostats, alarms, and detectors due to potential remote access by hackers.
Optional
Mitigate Alexa/ Google Home Risks
Consider privacy-focused alternatives like Mycroft or use Project Alias to prevent idle listening by voice-activated assistants.
Optional
Monitor your home network closely
Use tools like FingBox or router features to monitor for unusual network activity.
Optional
Deny Internet access where possible
Use firewalls to block internet access for devices that don't need it, limiting operation to local network use.
Advanced
Assess risks
Consider the privacy implications for all household members and adjust device settings for security and privacy, such as disabling devices at certain times.
Advanced

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.

0 / 10 2 Essential 3 Optional 5 Advanced
Sign up for Fraud Alerts and Credit Monitoring

Enable fraud alerts and credit monitoring through Experian, TransUnion, or Equifax to be alerted of suspicious activity.
Essential
Apply a Credit Freeze
Prevent unauthorized credit inquiries by freezing your credit through Experian, TransUnion, and Equifax.
Essential
Use Virtual Cards
Utilize virtual card numbers for online transactions to protect your real banking details. Services like Privacy.com and MySudo offer such features.
Optional
Use Cash for Local Transactions
Pay with Cash for local and everyday purchases to avoid financial profiling by institutions.
Optional
Use Cryptocurrency for Online Transactions
Opt for privacy-focused cryptocurrencies like Monero for online transactions to maintain anonymity. Use cryptocurrencies wisely to ensure privacy.
Optional
Store Crypto Securely
Securely store cryptocurrencies using offline wallet generation, hardware wallets like Trezor or ColdCard , or consider long-term storage solutions like CryptoSteel .
Advanced
Buy Crypto Anonymously
Purchase cryptocurrencies without linking to your identity through services like LocalBitcoins , Bisq , or Bitcoin ATMs.
Advanced
Tumble/ Mix Coins
Use a bitcoin mixer or CoinJoin before converting Bitcoin to currency to obscure transaction trails.
Advanced
Use an Alias Details for Online Shopping
For online purchases, consider using alias details, forwarding email addresses, VOIP numbers, and secure delivery methods to protect your identity.
Advanced
Use alternate delivery address
Opt for deliveries to non-personal addresses such as PO Boxes, forwarding addresses, or local pickup locations to avoid linking purchases directly to you.
Advanced

Human Aspect

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.

0 / 21 11 Essential 6 Optional 4 Advanced

Verify Recipients
Emails can be easily spoofed. Verify the sender's authenticity, especially for sensitive actions, and prefer entering URLs manually rather than clicking links in emails.
Essential
Don't Trust Your Popup Notifications
Fake pop-ups can be deployed by malicious actors. Always check the URL before entering any information on a popup.
Essential
Never Leave Device Unattended
Unattended devices can be compromised even with strong passwords. Use encryption and remote erase features like Find My Phone for lost devices.
Essential
Prevent Camfecting
Protect against camfecting by using webcam covers and microphone blockers. Mute home assistants when not in use or discussing sensitive matters.
Essential
Stay protected from shoulder surfers
Use privacy screens on laptops and mobiles to prevent others from reading your screen in public spaces.
Essential
Educate yourself about phishing attacks
Be cautious of phishing attempts. Verify URLs, context of received messages, and employ good security practices like using 2FA and not reusing passwords.
Essential
Watch out for Stalkerware
Be aware of stalkerware installed by acquaintances for spying. Look out for signs like unusual battery usage and perform factory resets if suspected.
Essential
Install Reputable Software from Trusted Sources
Only download software from legitimate sources and check files with tools like Virus Total before installation.
Essential
Store personal data securely
Ensure all personal data on devices or in the cloud is encrypted to protect against unauthorized access.
Essential
Obscure Personal Details from Documents
When sharing documents, obscure personal details with opaque rectangles to prevent information leakage.
Essential
Do not assume a site is secure, just because it is `HTTPS`
HTTPS does not guarantee a website's legitimacy. Verify URLs and exercise caution with personal data.
Essential

Use Virtual Cards when paying online
Use virtual cards for online payments to protect your banking details and limit transaction risks.
Optional
Review application permissions
Regularly review and manage app permissions to ensure no unnecessary access to sensitive device features.
Optional
Opt-out of public lists
Remove yourself from public databases and marketing lists to reduce unwanted contacts and potential risks.
Optional
Never Provide Additional PII When Opting-Out
Do not provide additional personal information when opting out of data services to avoid further data collection.
Optional
Opt-out of data sharing
Many apps and services default to data sharing settings. Opt out to protect your data from being shared with third parties.
Optional
Review and update social media privacy
Regularly check and update your social media settings due to frequent terms updates that may affect your privacy settings.
Optional
Compartmentalize
Keep different areas of digital activity separate to limit data exposure in case of a breach.
Advanced
WhoIs Privacy Guard
Use WhoIs Privacy Guard for domain registrations to protect your personal information from public searches.
Advanced
Use a forwarding address
Use a PO Box or forwarding address for mail to prevent companies from knowing your real address, adding a layer of privacy protection.
Advanced
Use anonymous payment methods
Opt for anonymous payment methods like cryptocurrencies to avoid entering identifiable information online.
Advanced

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

0 / 16 10 Essential 1 Optional 5 Advanced

Destroy Sensitive Documents

Shred or redact sensitive documents before disposal to protect against identity theft and maintain confidentiality.

Essential

Opt-Out of Public Records

Contact people search websites to opt-out from listings that show persona information, using guides like Michael Bazzell's Personal Data Removal Workbook.

Essential

Watermark Documents

Add a watermark with the recipient's name and date to digital copies of personal documents to trace the source of a breach.

Essential

Don't Reveal Info on Inbound Calls

Only share personal data on calls you initiate and verify the recipient's phone number.

Essential

Stay Alert

Be aware of your surroundings and assess potential risks in new environments.

Essential

Secure Perimeter

Ensure physical security of locations storing personal info devices, minimizing external access and using intrusion detection systems.

Essential

Physically Secure Devices

Use physical security measures like Kensington locks, webcam covers, and privacy screens for devices.

Essential

Keep Devices Out of Direct Sight

Prevent devices from being visible from outside to mitigate risks from lasers and theft.

Essential

Protect your PIN

Shield your PIN entry from onlookers and cameras, and clean touchscreens after use.

Essential

Check for Skimmers

Inspect ATMs and public devices for skimming devices and tampering signs before use.
Essential
Protect your Home Address
Use alternative locations, forwarding addresses, and anonymous payment methods to protect your home address.
Optional
Use a PIN, Not Biometrics
Prefer PINs over biometrics for device security in situations where legal coercion to unlock devices may occur.
Advanced
Reduce exposure to CCTV
Wear disguises and choose routes with fewer cameras to avoid surveillance.
Advanced
Anti-Facial Recognition Clothing
Wear clothing with patterns that trick facial-recognition technology.
Advanced
Reduce Night Vision Exposure
Use IR light sources or reflective glasses to obstruct night vision cameras.
Advanced
Protect your DNA
Avoid sharing DNA with heritage websites and be cautious about leaving DNA traces.
Advanced

Related Research

Digital Fortress Guide
Comprehensive guide to building your personal cybersecurity fortress from the ground up.
Crypto Security Essentials
Essential protection against drainers, fake support, and common wallet traps.
Privacy Arsenal
Curated privacy tools, browsers, VPNs, and encrypted communication guides.

Related Resources

Privacy Arsenal & Tools
Secure browsers, VPNs, and OS recommendations to stay anonymous online.
Crypto Security Essentials
Protect your crypto from phishing, drainers, and social engineering attacks.
Digital Fortress Guide
Build your digital fortress — comprehensive guide to online security.
I Was Scammed — What Now?
Emergency steps to take if your wallet was drained or credentials stolen.
Can Your Wallet Be Hacked?
How crypto wallets get compromised and how to prevent it.