Personal Cyber Security Checklist | Full List

1. Your Passwords
2. 2-Factor Authentication
3. Your Browser & Search
4. Your Internet Connection
5. Your Emails
6. Your Social Media Accounts
7. Your Smartphone
8. SMS and Calling
9. Your Desktop/ Laptop
10. Your Router
11. Your Online Shopping

Passwords

There'd be no point in implementing the rest of this guide, if a hacker can crack or get hold of your password to get direct access into your online accounts. Most reported data breaches (see this Verizon report) are caused by weak, default or stolen passwords. Massive amounts of private data has been stolen because of this.

If this list looks quite daunting, you'll probably find a password manager very helpful, since it will do most of this for you.

For everything you could ever want to know about passwords, check out this guide.

Security	**Priority**	**Details and Hints**
Use a strong password	Recommended	Check how strong your password is at: HowSecureIsMyPassword.net. Try to get a got mixture of upper and lower-case letters, numbers and symbols. Avoid names, places and dictionary words where possible, and aim to get a decent length. Have a look at How Long will it take to Crack my Password.
Don't save your password in browsers	Recommended	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 can allow

		easy access into your accounts. Also do not store passwords in a .txt file or any other unencrypted means. Ideally use a password manager.
Use different passwords for each account you have	Recommended	If one password gets compromised, it can give hackers access to your other online sites, so it is highly recommended not to reuse the same passwords. In order to manage having hundreds of different passwords, use a password manager. Have a look at LastPass, DashLane, KeePassor Robo Forms 8.
Be cautious when logging in on someone else's device	Recommended	Ideally you wouldn't ever log into any of your services on someone else's device, since you can't be sure that they don't have any malware. If you do, ensure that your in a private session (like Incognito mode) so that nothing gets saved
Change your passwords regularly	Recommended	The passwords for for any important sites should ideally be updated at least annually.
Avoid password hints	Optional	Hints often give away a lot more than you may realise of a password. If possible don't use a hint.
Never answer online security questions truthaly	Optional	It's usually a reasonably easy task for a hacker to work out which high school you went to, what your Mums name is, or what your first car was. So instead of giving the correct answers to these questions, create a note inside your password manager to store your fictitious answers.
Don't use a 4-digit pin to access your phone or accounts	Optional	Don't use a short pin to access your smartphone, computer or apps. Instead use a text password. 4 digit pins are considerably easier to crack.
Use an offline password manager	Advanced	Consider an offline password manager, encrypted by a strong password. If you work across two or more computers, this could be stored on an encrypted USB. KeePass is a strong choice
If possible, try to avoid bio-metric and hardware-based authentication	Advanced	Fingerprint sensors, face-detection and voice-recognition are all hackable. Where possible replace these with traditional passwords, strong passwords.

2-Factor Authentication

This is a secure method of logging in, where you supply not just your password, but also an additional code usually from a device that only you'd have access to.

Security	**Priority**	**Details and Hints**
Use an authenticator.	Recommended	Use Google Authenticator where sites offer 2-FA. Alternative authenticators include: Authy, FreeOTP, LastPassAuthenticatorand AuthenticatorPlus. SMS codes are ubiquitous, but easy to break so although better than nothing, not ideal. Another option is a hardware-based 2FA, such as Yubico, although with limited compatibility and of course a physical cost. Check out this list of apps/ sites which provide the option of 2FA.

Your Browser and Search

Modern web browsers are packed with tons of features which improve our experience of surfing the web, in terms of both speed and convenience. Be aware that ever website that you interact with, including search engines will likely be keeping records of all your activity, and not being aware of what's being collected can put you at risk. Last year Kaspersky reportedover a million data exploits caused by malicious sites.

For more browser security pointers, check out: Here's How To Get Solid Browser Security

Security	**Priority**	**Details and Hints**
Deactivate ActiveX	Recommended	ActiveX is barley used nowadays, but Microsoft browsers have it enabled by default. It acts as a middleware between Java and Flash applications and your PC. But it is commonly used for malicious sites to run scripts directly on your PC. See this article for more details.
Disable Flash	Recommended	Adobe Flash has been around since the dawn of the internet, however it has been falling in popularity

		for a while. It brings with it many unpatched vulnerabilities (a few of which you can read about here). See this guide, on how to disable Flash player, or this guide for more details on how dangerous it can be.
Block Trackers	Recommended	Consider installing a browser extension, such as Privacy Badger, to stop advertisers from secretly tracking you
Block scripts from bad origin	Recommended	Use an extension such as uBlock Origin, to block anything being loaded from an external or unverified origin.
Force HTTPS only traffic	Recommended	Ensure that you only use websites through https. It's recomended to use an extension such as HTTPS Everywhere, to force all sites to load securely.
Only use trusted browser addons and extensions	Recommended	Both Firefox and Chrome webstore allow you to check what permissions access rights an extension requires before you install it. Check the reviews. Only install extensions you really need.
Always keep your 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.
Clear Browsing Cookies	Optional	The browsing history and cookies in your browser can sometimes be a security risk. It's a good practice to clear these regularly. *In Chrome (History -> History -> Clear Browsing Data), or in Safaris (Settings -> Safari -> Clear History and Website Data)*
Delete data stored on old accounts	Optional	If you no longer use a certain cloud service, log in, delete your data, and then consider closing that account.
Watch out for trash	Optional	Some account store your deleted data in a trash folder (sometime called deleted items, recycle bin or archive). If you no longer need this data, delete it.
Use a private search engine	Optional	Take a look at DuckDuckGo or StartPage. Neither store cookies or cache anything.
Consider a privacy browser	Optional	Google openly collects usage data on Chrome usage. There are several privacy browsers out there which minimise the amount of data collected. Have a look at Brave Browser, Yandex, or Comodo. As a more extreme choice, consider Tor.
Disable JavaScript	Advanced	Many modern web apps, are JavaScript based, so disabling it will greatly reduce your browsing

		experience, most websites just won't work. But if you really want to go all out, then it will reduce your attack surface. Read more about the growing risk of JavaScript malware.
Use Tor	Advanced	The onion routing in the Tor network will greatly improve your security. It will also decrease the user experience while browsing though.

Your Internet Connection

A Virtual Private Network (VPN) allows you to securely connect to the internet, when you visit a site, your visiting it through the secure VPN connection and not broadcasting your own IP address, therefore hiding your identity on the sites you visit, to both your ISP anyone else trying to track you, they can also encrypt your traffic so you can browse more securely on public networks. They're really easy to setup. To learn more about what a VPN is, how it works and how to choose one, checkout this PC Mag article.

Security	**Priority**	**Details and Hints**
Use a VPN	Recommended	Ideally use a paid-for VPN, as they're considerably better quality so won't affect your speeds, nor show adds. Take a look at VyprVPN, NordVPN, IPVanishand TunnelBear.
Host your own VPN	Advanced	It's not too hard to set up OpenVPN, on any cloud platform, and it does mean that you have control over your data. You can also tweak the security setting to your needs, you could even set the instance to destroy itself every night and spin up a new node for the morning.

Your Emails

Nearly 50 years since the first email was sent, they're still very much a big part of our day-to-day life, and will probably 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. (For basic enterprise pointers, see this article).

In the words of Andy Chen, https://www.ted.com/talks/andy_yen_think_your_email_s_private_think_again#t-22541 "Emailis like a Postcard". It is easily readable by all the servers it travels through. Keep this in mind when sending anything sensitive, and were necessary take precautions.

Further more, if a hacker gets access to your emails, it provides a gateway for your other accounts to be compromised (through password resetting and other methods), therefore email security is paramount for your digital safety.

These links are also useful for additional simple measures that you can take to specifically protect a Yahoo, GMail, Outlook and AOL account.

Security	**Priority**	**Details and Hints**
Have more than one email address	Recommended	Keeping your important and safety-critical messages separate from trivial subscriptions such as newsletters, is a very good idea. Be sure to use different passwords. This will also make recovering a compromised account after an email breach easier.
Keep security in mind when logging into emails	Recommended	Your email account is one of the most important to protect with a secure password. Only sync your emails with your phone, if it is secured (encrypted with password). Don't allow your browser to save your email password. Prevent man-in-the-middle attacks by only logging in on a secured network.
Always be weary of phishing and scams	Recommended	If you get an email from someone you don't recognize, don't reply, don't click on any links, and absolutely don't download an attachment. Keep an eye out for senders pretending to be someone else, such as your bank, email provider or utility company. Check the domain, read it, ensure it's addressed directly to you, and still don't give them any personal details. Check out this guide, on how to spot phishing emails.
Don't store emails for longer than necessary	Optional	Delete all emails regularly, being sure to not store anything for more than a year. If a message contains something important (such as a legal contract, or finance information), then download and store it securely offline, deleting the original version.
Don't share sensitive information over email	Optional	Emails are very very easily intercepted. Also you can't know how secure your recipients environment is. Don't share anything personal, such as bank details, passwords, confidential information over email. Ideally, don't use email as any primary method of communication.

Don't connect third-party apps to your email account	Optional	If you give a third-party app (like Unroll.me) full access to your inbox, this makes you vulnerable to cyber attacks. The app can be compromised and, as a consequence, cyber criminals would gain unhindered access to all your emails and their contents.
Consider switching to a more secure email provider	Optional	Email providers such as ProtonMail, CounterMail, HushMailhttps://www.hushmail.com(for business users) or MailFence allow for end-to-end encryption, full privacy as well as more security-focused features.

Your Social Media Accounts

Security	**Priority**	**Details and Hints**
Check permissions before posting from a mobile app	Recommended	By default most of the main social networks attach your current location to a post made from your phone. Think first about who will be able to see this post, and therefore your location.
Check your privacy settings	Recommended	Most social networks allow you to control your privacy settings. Regularly review these settings (as they do change frequently). Ensure you feel comfortable with who can see your posts, photos and interactions.
Only put info on social media that you wouldn't mind being public	Recommended	Even with tightened security settings, don't put anything online that you wouldn't want to be seen by anyone other than your friends. Don't reply soley on the social networks security. Any organisation can be hacked.
Don't give social networking apps permissions they don't need	Recommended	By default many of the popular social networking apps, will ask for permission to access your contacts, your call log, your location, your messaging history etc.. If they don't need this access- don't grant it.
Revoke access for apps your no longer using	Recommended	Instructions: Facebook, Twitter, LinkedIn, Instagram.
Don't be tricked into a false sense of security	Recommended	Many social apps claim that your content will be secure, or only visible to certain people, when this can be simply bypassed by a mediocre hacker. For example Snapchat's disappearing photos, are in fact stored on your phones memory, and easily retrievable if you

		know where to look.
Don't share publicly	Optional	Ideally your profile should only be viewed by people who you are in your friends list, and you know personally. Check before you post, that there is no personal information in what you are sharing beyond your close friends.
Remove meta data before uploading media	Optional	Most smartphones and some cameras automatically attach a comprehensive set of additional data to each photograph., This usually includes things like time, date, location, camera model, user etc. Remove this data before uploading. See this guide for more info.
Don't have any social media accounts	Advanced	It may seem a bit extreme, but if your serious about data privacy and security, stay away from entering information on any social media platform.

Your Smart Phone

Security	**Priority**	**Details and Hints**
Don't grant apps permissions that they don't need	Recommended	If an app doesn't need access to your camera- don't grant it access. Same with any features of your phone (such as hardware access to gyrometer, microphone or biometric sensor as well as access permissions of contacts, calendar or messages). Be very wary about what each app has access to.
Turn of connectivity features that aren't being used	Recommended	When your not using WiFi, Bluetooth, NFC or anything else- turn those features off. These are commonly used in many simple hacks.
Uninstall apps that you don't need	Recommended	Don't have apps that your not using on your phone, as they can be collecting data in the background. Don't install apps from non-legitimate sources, or apps with few reviews.
Require the passcode immediately	Recommended	Both Android and iOS by default don't require the password if you unlock your phone immediately after it's been locked. You can turn this off or minimise the amount of time the phone stays unlocked after use.

Be aware of which apps have location permissions	Recommended	If an app doesn't have a completely valid reason to know your exact location, or is not from a trusted publisher- then don't grand it GPS permissions. App collected locations, can be used by criminals to know when your home is unoccupied, or exactly where you are at all times.
Turn off location services when you don't need it	Optional	Location data, if leaked can make it clear where you live and work, as well as your general daily routine.
Data Retention Policies	Optional	By default most apps keep collected data forever, but this can nearly always be adjusted to say, just 30 days. iMessage for example is a treasure trove of personal information, if you don't need this to be kept forever, then modify that in settings.
Explore in-app Privacy Settings	Optional	Many apps, which deal with personal data have the option to add an app-specific passcode or other authentication methods. Although these shouldn't be purely relied upon, they can be useful in deterring someone you've given access to your device from reading about your prescriptions, investment balance or emails.
Data made available when your phone is locked	Optional	Check which data is readable on your lock screen (such as messages, calendar and notifications), and ensure your okay with it.
Don't use Touch ID to log into your phone	Optional	A thumbprint can be compelled by law enforcement as a search in the US and several other countries, whereas a passcode is protected by fifth amendment self incrimination protections.
Limit Add Tracking	Optional	Your phone, and the apps on it constantly track what you do in order to better target adverts. This can usually be tweaked by going to Settings -> Privacy -> Advertising -> Limit Ad Tracking (Turn on). Be aware that you will still see adds, they just won't be so relevant!
Consider not connecting phone messages to your computer	Optional	Mobile messages (such as WhatsApp, iMessage, Telegram and Hangouts…) usually have the option to sync up with your PC or Mac. However they leak a lot of information

		unnecessarily, which can be easily intercepted by a hacker. (Signal Messenger for desktop is pretty secure though)
Set the phone to erase after 10 failed unlock attempts are made	Optional	It may sound extreme, but this way even if a thief were able to gain access to your phone (either through brute force, or physically removing the memory). They can't capture any personal details which are stored on your device.
Consider running a custom ROM if you have an Android device	Advanced	Your default OS tracks information about your usage, and app data, constantly. Consider a security-focused custom ROM, such as Lineage or CopperheadOS.

SMS and Calls

Both SMS texting and traditional phone calls are not secure. Avoid it whenever there is a reasonable alternative, and don't use these means to communicate anything secure. Be wary of who you share your phone number with

Security	**Priority**	**Details and Hints**
Don't use SMS - Use E2E encrypted messaging apps	Optional	iMessage is secure. For non-Apple users Signalis the most secure option. As of late 2016 WhatsAppis also end-to-end-encrypted using the Signal protocol. Keep in mind that although the transmission may be secured, breaches can still be cause if your, or your recipients device has been compromised.
Use a secure email provider	Optional	Most email providers completely invade your privacy intercepting both messages sent and received. ProtonMailis a secure email provider, that is open source and offers end-to-end encryption. There are alternative secure mail providers (such as CounterMail, HushMail and MailFence)- but ProtonMailhas both a clear interface and strong security record.
Avoid using your real phone number when signing up for an	Optional	Where possible, avoid giving out your real phone number while creating accounts online. You can create phone numbers using services such as Google

account or service		Voice or Skype. For temporary usage you can use a service like iNumbr that generates a phone number that forwards messages and calls to your main number.

Your Desktop or Laptop

Although Windows and OS X are easy 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 OS up-to-date	Recommended	Microsoft, Apple and ChromeOS release regular updates, which fix security risks. Always keep your device updated.
Encrypt your hard drive	Recommended	It's very easy to retrieve anything of an uncrypted hard drive, without knowing any passwords. Encrypt your hard drive via FileVault (Mac), BitLocker (Windows), or LUKS (Linux).
Locking your computer	Optional	Configure your computer to require a password after 5 minutes of inactivity, and on wake. Lock your computer when ever you get up from your desk, learn the shortcuts Windows logo + L (Windows), control + shift + power/escape (Mac), or ctrl + alt + L (Linux). Additionally on a Mac, add keychain status to your menu bar (open /Applications/Utilities/Keychain\ Access.app/Contents/Resources/Keychain.menu/) for easy screen locking.
Enable your OS's Firewall	Optional	Either with Windows Defender, or for OS X, stealth mode gives Apple Mac users a bit of additional network security. Here are additional details of how and why to enable.
P**assword protect your BIOS and drives**	Advanced	A BIOS or UEFI password helps to make an inexperienced hackers life a bit harder if they get hold of your PC, here is a guide on how to set one.
Consider Switching to Linux	Advanced	Linux is considerably more secure than both OSX and Windows. Some distros are still more secure than others, so it's worth choosing the right one to get a balance between security and convenience.

Your Router

Security	Priority	Details and Hints
Don't use a default password	Recommended	Change your router password- here is a guide as to how.
Use WPA2	Recommended	WPA and WEP make it very easy for a hacker to gain access to your router. Use a WPA2password instead. Ensure it is strong: 12+ alpha-numeric characters, avoiding dictionary words.
Ideally hide your SSID	Optional	An SSID (or Service Set Identifier) is simply your network name. If it is not visible, it is much less likely to be targeted. You can usually hide it after logging into your router admin panel, see here for more details.
Avoid using the free router you got from your ISP	Optional	Typically they're manufactured cheaply in bulk in China, and firmware updates which fix crucial security flaws aren't released regularly
Kill unused process and services	Advanced	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

Online Shopping

Security	Priority	Details and Hints
Consider using a pre-paid debit card, topped up with cash	Advanced	There are a lot of options out there, some are free, some are only available in certain locations, some do require identity checks, whereas others don't- so it's worth shopping round to find the one that's right for you.
Consider paying with a	Advanced	This is the most secure method of payment,

Crypto currency		although unfortunately not currently widley supported.
Consider not getting goods delivered to your home address	Advanced	Use a pickup service, such as Doddle, Amazon Click + Collect, eBay Argos collect etc.

References

Privacy.google.com. (2018). *Google Privacy | Why data protection matters*. [online] Available at: https://privacy.google.com/your-data.html [Accessed 17 Mar. 2018].

Privacy.microsoft.com. (2018). *Privacy – Microsoft privacy*. [online] Available at: https://privacy.microsoft.com/en-GB/ [Accessed 17 Mar. 2018].

Apple (United Kingdom). (2018). *Privacy*. [online] Available at: https://www.apple.com/uk/privacy/ [Accessed 17 Mar. 2018].

Burn-Murdoch, J. (2018). *Data security and privacy: can we have both?*. [online] the Guardian. Available at: https://www.theguardian.com/news/datablog/2013/jul/31/data-security-privacy-can-we-have-both [Accessed 18 Mar. 2018].

Ico.org.uk. (2018). *Home*. [online] Available at: https://ico.org.uk [Accessed 18 Mar. 2018].

Legislation.gov.uk. (2018). *Data Protection Act 1998*. [online] Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 18 Mar. 2018].