Online Privacy Checklist ☑️ - Search Encrypt Blog

Step-By-Step Privacy Checklist

Follow these steps to ensure you have the best privacy and security protection possible. If you're like most people you spend a ton of time connected to the internet, so it's essential that you keep your sensitive information protected.

☑️ Use a password manager

Password managers do more than just storing your passwords. Since you won't have to memorize all of your passwords, these tools let you use more complex and unique passwords for all of your accounts. Many password managers also have password generators built in, so you can easily use long passwords with a mix of letters, numbers and symbols. Using a password isn't a perfect solution to keeping your data secure, but the longer and more complex your password, the longer it will take a hacker to crack into your accounts.

Resources:

- ***Best Password Manager & Password***

Generator Tools

☑ Create Strong Passwords

Using a strong password is vital if you want to keep your accounts and information secure. The best passwords are long and include a combination of letters, numbers and symbol characters. Using a reliable password manager makes these kinds of passwords simpler to use. Strong passwords will be at least 12 characters long, and isn't a simple word or phrase.

Examples of Strong Passwords: "AmazingStates909!!","{B#vjj-!@WyQ[)8X","Number #0ne is too fa$t"

Examples of Weak Passwords: "passw0rd","Stars1″ ,"Login","Smith22″

Resources:

- ***How Do I Create a Strong and Unique Password – Webroot***
- ***How to Create a Strong Password and Beat the Hackers – Avast***

☑ Enable Two-Factor Authentication

(2FA)

Using a strong password is important, but a password is just a single line of defense against unwanted access to your information. Two-factor authentication requires anyone trying to access your account to provide a second form of identity verification. That could be a code sent via text message or email, a fingerprint, or a PIN number.

Resources:

- ***What is Two-Factor Authentication (2FA)? – Authy***
- ***Two-Factor Authentication Blocks Potential Security Threats***

☑️ Freeze Your Credit

The benefit of freezing your credit is that identity thieves or anyone who has accessed your data cannot get credit in your name. While your credit is frozen, you also will be unable to receive new credit, but you can usually unfreeze your credit in 15 minutes or less. In the event that your financial information is hacked, in an event like the Equifax breach, you won't be at risk for having someone steal your identity.

Resources:

- ***How To Get a Free Credit Freeze – Experian***

☑️ Use an Alternative DNS

DNS stands for Domain Name Service. This system is what allows your browser to navigate to URLs. For example, when you go to "www.searchencrypt.com" you are actually going to its IP address of "52.207.202.196". Domain names are much easier to remember and easier for users to type in. ISPs typically offer their own Domain Name Services to their customers. Running your ISP's DNS service can lead to less security, less privacy, slower browsing and content blocking. It's better to use an alternative DNS that doesn't keep traffic logs, lets you encrypt your browsing, and that offers other security features like phishing prevention.

Resources:

- ***The Top 5 Best DNS Servers for Improving Online Privacy & Security – Security Trails***

☑️ Use a VPN

Virtual Private Networks, or VPNs, make it look like your internet connection is coming from somewhere else besides your actual location. It redirects your network connection through a "virtual" network so

websites and trackers online will have a harder time determining your actual location. VPNs are also useful tools for accessing blocked websites from school or work networks.

Resources:

- ***The Best VPNs for Privacy in 2019***

☑️ Cover Your Webcam and Protect Your Screen

In some cases, hackers can access your computer and access your webcam and microphone without your knowledge. The best way to combat this is by covering your webcam and microphone with a piece of tape when you aren't using them. Another important thing to consider if you're using your computer in a public area is to be careful viewing sensitive information as anyone snooping over your shoulder could use it to access your accounts or other private information.

☑️ Use a Private Browser

Your browser is like your computer's window into the internet. Almost all of your internet activity will flow through your browser. It's important to choose a browser that prioritizes keeping your activity

private and secure. The most secure browsers use encryption and range of other features to protect your browsing from security threats.

Resources:

- ***Top Secure Browsers to Protect Your Privacy (2019)***
- ***4 Free Anonymous Web Browsers That Are Completely Private – MakeUseOf***

☑️ Use a Private Search Engine

Private search engines will return useful results without tracking what you search for or which websites you visit. Since these search engines generally don't use your history to determine which results you see, they will offer more objective and less "censored" search results than traditional search engines.

Resources:

- ***Why Using a Private Search Engine Actually Matters***

☑️ Use Ad & Tracker Blockers

Ads and tracking scripts embedded in the web pages you visit can slow down your browsing, in addition

to being threats to your privacy. Use ad blockers and tracker blockers to keep these from loading and using your network resources. You may be surprised after you start blocking ads how distracting and annoying these can be.

Resources:

- ***Best Ad Blockers for Chrome***

☑️ Clear Your Cookies Often

Cookies are small files that websites store in your browser to recognize you when you come back to their website. They let you stay logged in on social media sites and other website that you login to. While cookies often make browsing more convenient, they are also another way for websites to track you and your browsing behavior. Go into your browser settings and clear your cookies on a regular basis to prevent unwanted tracking.

Resources:

- ***How to Clear Cookies in Chrome, Firefox, Safari, and Other Browsers – Norton***

☑️ Use a Private Email Provider

If you use Gmail, you are likely handing over

information about your interests and your purchase behavior to Google. Other mainstream email services track you in similar ways. Private email services use encryption to keep the contents of your emails secure and only visible to you and the intended recipient.

Resources:

- ***11 Private Email Services to Keep Your Emails Confidential***

☑️ Review Location Data Permissions

Whenever you install a mobile app on Android or iOS, the app will often prompt you to give it access to your location data. To make sure you aren't giving unnecessary access to your location data, it's a good idea to review which apps you have granted access to track you. If an app doesn't need your location for its core functionality, it likely is only using that data to sell to advertisers or other third parties.

☑️ Manage Other App Permissions

To keep your information private from the apps you have installed on your phone, make sure you aren't granting them access to unneeded data. For example,

many apps request access to your microphone, camera, photo library and contacts. In many cases the app doesn't need access to this information all the time, even though it asks for constant access.

☑️ Use Encrypted Messaging Apps

Encrypted messaging apps are private alternatives to basic texting or instant messaging apps. These apps use encryption, and other features like expiring messages, to keep the contents of your messages private.

Resources:

- ***Private Messaging Platforms for Confidential Communication***

☑️ Avoid Public Wi-Fi Networks if Possible

While public Wi-Fi networks are often our only choice, especially if you're travelling a lot or working remotely, it's best to avoid these networks if possible. While a network may appear to be secure, it's hard to know the network's actually security. A password protected network is not necessarily secure, as WEP and WPA security protocols both use passwords. WEP is an older

version of WPA which has many vulnerabilities. Not all networks will encrypt your internet browsing, and an unencrypted network leaves you open to Man-In-the-Middle attacks.

☑️ Secure All Your Devices, Not Just Your Computer

Security and privacy doesn't just apply to your desktop computer. Some people may not realize that they actually are sharing the majority of their data through using their smartphones. You're more likely to keep your phone with you wherever you go than to bring your computer everywhere. Since you use your phone for more and more everyday tasks, there is a ton of information that needs to be kept private on these devices, in addition to your desktop computers.

Resources:

- ***How to Make Android as Secure as Possible – How-To Geek***
- ***10 Tips to Make Your iPhone Even More Secure – Kaspersky Lab Daily***

☑️ Delete Your Unused Accounts

If you've stopped using a particular service online,

you shouldn't let your account sit unused. The best way to prevent any privacy or security issues is to delete any accounts you no longer use. If you let you account sit dormant, the company may still collect information from any devices you're still logged in to. Often times when websites lose their user base, they will stop making security and bug fixes. This leaves your old unused account vulnerable to hacks and data breaches.

Resources:

- ***Should You Delete Old Unused Accounts? The Answer is Yes. – Cyclonis***

While these steps will help you be more private, they don't guarantee that your data is 100% safe. We recommend thinking twice and using a little common sense when sharing your information online. Good luck!