

21st Century Cyber Security for the Layperson or Business

Practical, straight-forward steps in preparing PC users for World War 3.0 online

Sf. R. Careaga, BSEE, CS minor (ECE)

V.2.3.2021

A Resilient Firm Publication <http://bit.ly/2KGotJJ>
www.resilientfirm.com

2020 Executive Notice

*This is the second year of the Layperson's Guide to Cybersecurity. It had a tremendous first year, rising to an excellent paper rank on Academia. But the end result is still disappointing, because so few people are considering their personal, financial, and privacy data and security as important as securing the lives of their children or homes. People are, by nature, procrastinators. But with cybersecurity threats on the rise and accelerating, from foreign sources, it is all the more important to consider means and ways (as well as the source of need) to protect ones' livelihood and small businesses from cyberspace threats. Those may be automated DDOS like threats to a website, malware, etc., or they might be ransomware attacks on medical servers. It doesn't really matter the end goal is **your money and identity** and the threat is as real as any mugger.*

*So this year we are going to talk more about encryption and blockchain, as well as describe how to be involved in cryptocurrencies, safely, for the common person. Also this is the year AI will take over all sorts of daily aspects of lives in a more visible way. It'll be on the tips of every tongue. The shift is now, and while the threat of Coronavirus seems all-important, the reality is that more livelihoods will be threatened **daily** than all the lives currently affected by Coronavirus (as of 3/6/2020) since its epidemic began. So please take the time to print out this document from page 3 to end, and to secure your home computer!*

-Shifu Ramon Careaga

Forward

When you have a brush with a pretend hacker who works for Google, and threatens to rob your bank account if you don't pay them in BTC (bitcoin), you start to get concerned about the state of the internet 3.0 situation. This paper is in the spirit of providing the common person security, and advanced knowledge of new (and if possible, free) techniques in a series of practical steps. There are innumerable services and programs available, so this is not an exhaustive list. It is also limited to my experience which is with PC/Windows and Linux OS, although many steps will be available to Apple OS users as well, by nature of being remote/3rd Party services, or cross-OS platforms. One more caveat need be specified: I am not a gamer, and so online gaming accounts may constitute any number of vulnerabilities, and users of Steam, Discord, and other online gaming services should take steps to keep their anonymity.

A lot of this will seem redundant or self-obvious to the younger generations or savvy, but please bear in mind that unsecured email and server accounts were responsible for quite a lot of espionage and conspiracy in 2016. Famously several important things, including nuclear launch codes, have had passwords of 12345... !!

It is recommended you use the checkboxes as you have gone through this document, and that you complete 100% of the document.

Informative Articles

The following articles may be of added value to the learning and reference:

- ❑ <https://www.pcmag.com/article/360806/12-simple-things-you-can-do-to-be-more-secure-online>
- ❑ <https://www.popsoci.com/how-to-be-more-secure-online>
- ❑ <https://www.techradar.com/vpn/best-free-vpn>
- ❑ <https://www.androidauthority.com/how-to-set-up-chromebook-vpn-876213/>
- ❑ <https://www.techradar.com/news/the-best-free-anti-ransomware-tools>
- ❑ <https://www.pcmag.com/roundup/353231/the-best-ransomware-protection>
- ❑ <https://www.pcmag.com/roundup/331555/the-best-free-password-managers>
- ❑ <https://www.techradar.com/news/best-email-provider>
- ❑ <https://support.google.com/accounts/answer/3466521?hl=en>
- ❑ <https://www.facebook.com/help/262314300536014/>
- ❑ <https://www.thesimpledollar.com/what-is-private-browsing-and-can-it-protect-you-online/>
- ❑ <https://www.online-tech-tips.com/computer-tips/how-to-protect-your-computer-from-hackers-spyware-and-viruses/>
- ❑ <https://www.online-tech-tips.com/computer-tips/how-to-encrypt-your-computers-hard-disk-data-and-files-for-free/>
- ❑ <https://searchenterprisedesktop.techtarget.com/essentialguide/The-complete-guide-to-Windows-10-security-tools>
- ❑ <https://www.thewindowsclub.com/free-security-tools-microsoft>
- ❑ <https://hackernoon.com/the-2017-pentester-guide-to-windows-10-privacy-security-cf734c510b8d>
- ❑ <https://www.csoononline.com/article/3253899/the-best-new-windows-10-security-features.html>

Links to Open Immediately

- ❑ <https://myaccount.google.com/permissions>
- ❑ <https://myaccount.google.com/security>

Adblocker

Several of the above articles have websites (just as many media companies do) which prefer no ad blockers. Nevertheless, while you may pause them for trusted sites, or even disable them there, please continue to use adblocker or similar extensions, as popups may be externally inserted programs to common download sites such as cnet etc. Once the pop-up inserts, it is possible for code to continue running which takes advantage of the cookie download to track your information. This may lead to phishing attacks which attempt to take advantage over you via prior knowledge of your habits, identity information, etc. Additionally, you should learn to recognize phishing emails, and report them as spam. Although far less common nowadays, it can happen that fake versions of PayPal, eBay, Amazon, etc. emails would arrive, and when you hover over their links, you can see that they are **not** to the domains of the real companies, but to fake and randomized websites.

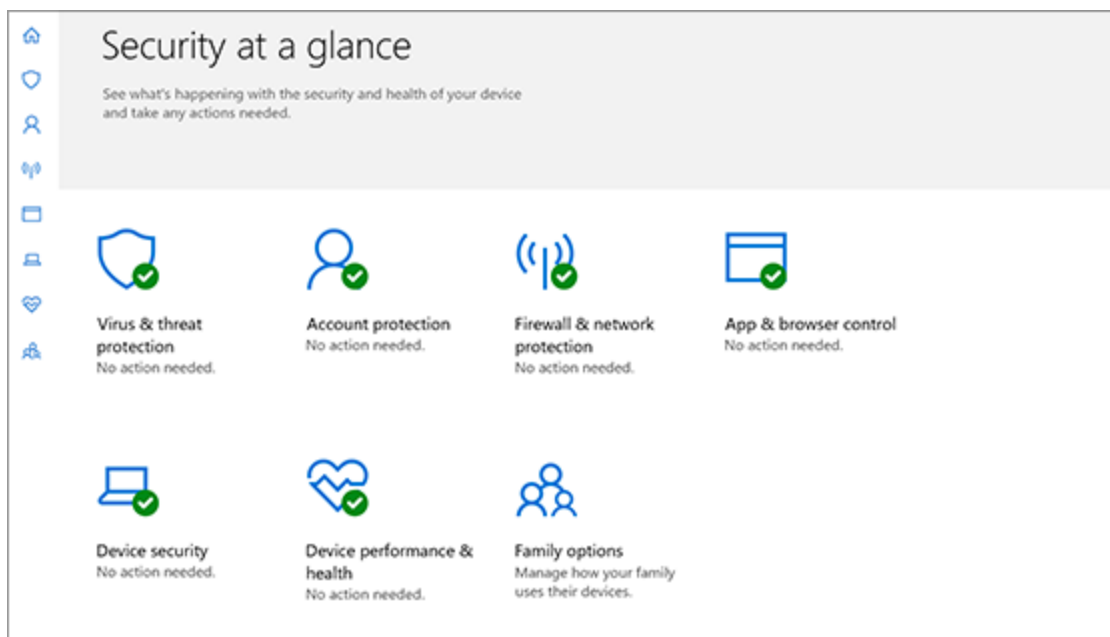
Please visit this website to download a free, and trustworthy basic Adblocker that I use:

<https://www.getadblock.com/>

Windows Defenders

The best thing to make use of is the free, nascent security services in Windows. Note - for those using Windows 7, please [download Microsoft Security Essentials](#).

Windows Security Center & Firewall



Windows Security Center may be accessed via the Control Panel (search Cortana or find via the Menu). If you should wish to turn it off, the following article describes how, along with several other options. <https://www.askvg.com/fix-disable-turn-on-windows-security-center-service-notification-in-windows-10/>

From Microsoft:

<https://support.microsoft.com/en-us/help/4013263/windows-10-stay-protected-with-windows-security>

"You can customize how your device is protected with these Windows Security features. To access

them, select the Start button, then select Settings > Update & Security > Windows Security . Then select the feature you want to explore.

- ❑ [Virus & threat protection](#). Monitor threats to your device, run scans, and get updates to help detect the latest threats. (Some of these options are unavailable if you're running Windows 10 in S mode.)
- ❑ Account protection. Access sign-in options and account settings, including Windows Hello and dynamic lock.
- ❑ [Firewall & network protection](#). Manage firewall settings and monitor what's happening with your networks and internet connections.
- ❑ [App & browser control](#). Update settings for Windows Defender SmartScreen to help protect your device against potentially dangerous apps, files, sites, and downloads. You'll have exploit protection and you can customize protection settings for your devices.
- ❑ [Device security](#). Review built-in security options to help protect your device from attacks by malicious software.
- ❑ [Device performance & health](#). View status info about your device's performance health, and keep your device clean and up to date with the latest version of Windows 10.
- ❑ [Family options](#). Keep track of your kids' online activity and the devices in your household.

Status icons indicate your level of safety:

- Green means your device is sufficiently protected and there aren't any recommended actions.
- Yellow means there is a safety recommendation for you.
- Red is a warning that something needs your immediate attention."

The following articles provides a number of results that will answer most queries

<https://www.windowscentral.com/beginners-guide-windows-defender-security-center-windows-10>

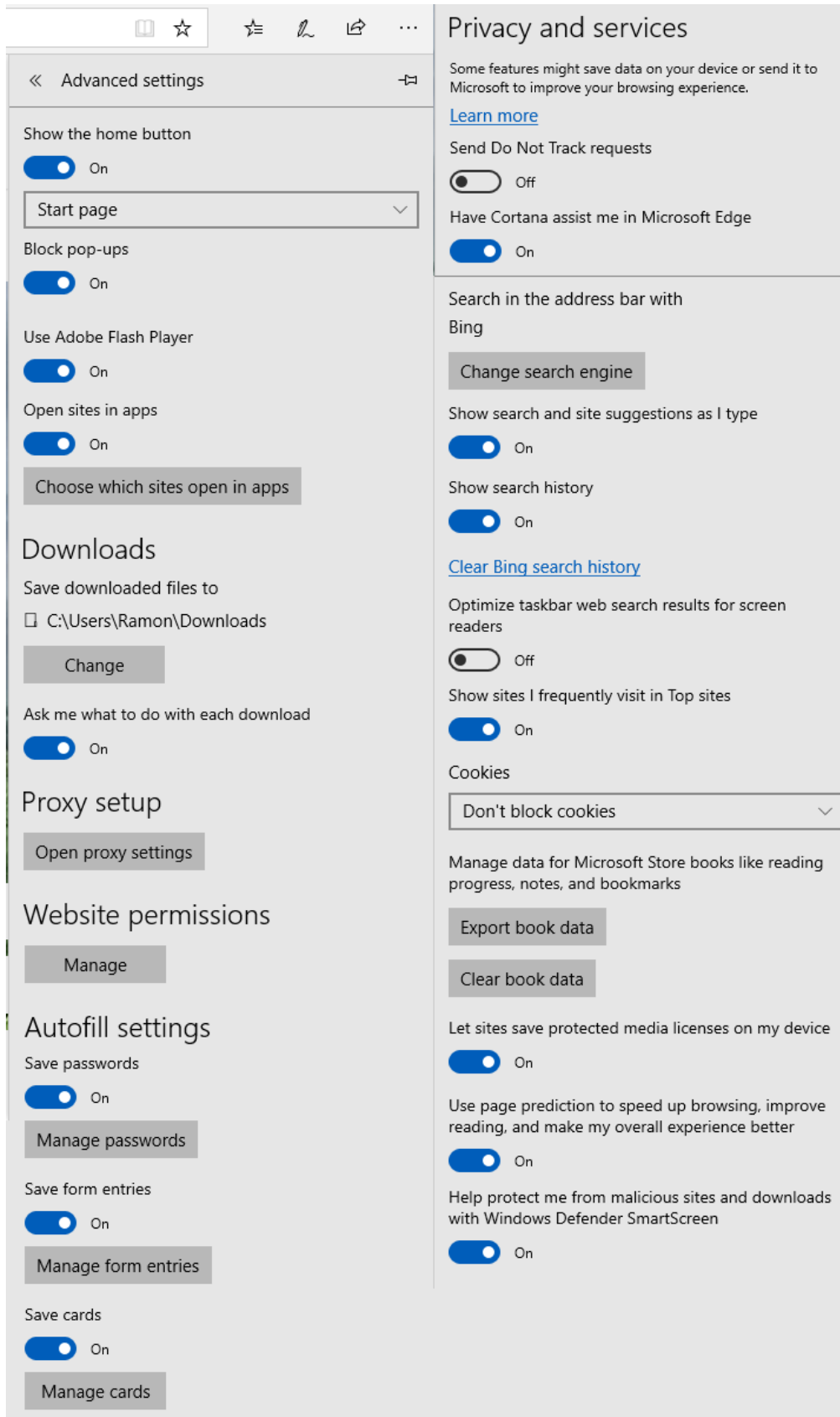
- ❑ [Windows Defender Security Center vs. Windows Defender Antivirus](#)
- ❑ [How to navigate Windows Defender Security Center](#)
- ❑ [How to scan your PC for malware using Windows Defender Antivirus](#)
- ❑ [How to view scan history using Windows Defender Antivirus](#)
- ❑ [How to temporarily disable Windows Defender Antivirus](#)
- ❑ [How to view health and performance report of your PC](#)
- ❑ [How to manage network security with Windows Defender Firewall](#)
- ❑ [How to protect your PC against malicious code](#)
- ❑ [How to manage parental control and keep track of your PCs](#)

"Windows Defender Security Center includes five areas of protection that you can manage and monitor.

- ❑ Virus & threat protection: includes the Windows Defender Antivirus settings, and it allows you to monitor the malware protection, scan your device for threats, and set up its [advanced anti-ransomware feature](#).
- ❑ Device performance & health: allows you to check the health and performance of your computer, and provides a mechanism to clean up your device to fix errors and slowdown problems."

It is my recommendation that the average person turn on both the Defender/Antivirus and all firewall options. If you purchase an antivirus suite and it appears to replace the Windows Defender, or clashes with it, if the suite is known to be very powerful (see above article on best antivirus software), then you may turn off the Defender. However, the best suites should modify the settings automatically.

Internet Security Options



Aside from the Security Center and Firewall, there are Microsoft Edge/Explorer security options which can turn down or up the trustworthiness of various websites, and manage all sorts of security. This is something that can be done no matter what browser you choose to use (for Windows 10 users).

Aside from managing Website Permissions, you might try blocking cookies, pop ups, Cortana, and turn on the Windows Defender SmartScreen. Most of these settings are automatic, and you have to manually set them if you want anything different.

Microsoft Baseline Security Analyzer

From this article, we see that there are some nascent Microsoft security analysis tools which are free, and just require a download:

<https://www.komando.com/tips/460504/3-security-program-that-should-be-on-every-computer-or-laptop>

“The Microsoft Baseline Security Analyzer is a free download that will help you assess your computer's security. It will make sure Windows and Office are updated with all the necessary security patches. You can also learn about other security issues that you might otherwise overlook. For example, it will check for multiple administrator accounts to see if other users have more control over the machine than they should. And what about your account password? If your password is weak, others might be able to access your account. The Microsoft Baseline Security Analyzer will alert you if account passwords aren't strong enough. Microsoft Baseline Security Analyzer gives you a detailed assessment that will be quite lengthy. Take the time to read it thoroughly and fix any problems listed. It is another tool in your arsenal to protect your machine.

Warning: This is a tool geared for advanced users. Following some of its recommendations could break other programs or Windows if done incorrectly. Before you make any changes to your system, be sure you understand what you are doing.

❑ [Click here to download the Microsoft Baseline Security Analyzer.”](#)

BitLocker

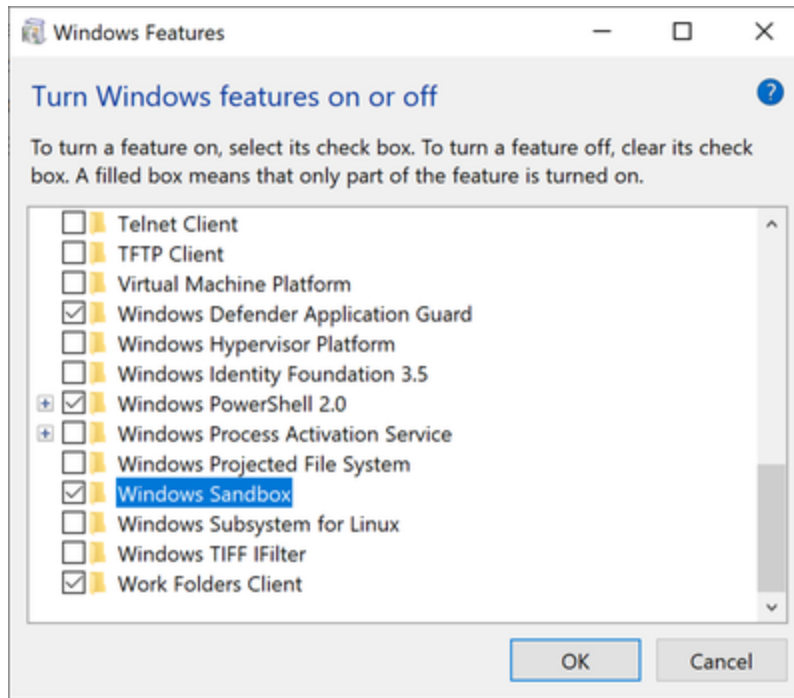
In Windows Vista through 8.1, BitLocker was standard, but in Windows 10 it is not available in the Home Edition. However, here are two articles on how to set up free encrypted Hard Drives for Windows:

- ❑ [Windows Vista, 7, and 8.1](#)
- ❑ [Windows 10](#)
- ❑ [Security Warnings and tips](#)
- ❑ Alternative: [VeraCrypt for Windows](#)

Windows Sandbox

A sandbox is a tool where you can run or test a feature before implementing it in the real OS environment. It is sort of like using a virtual machine, in that everything is supposed to be isolated from the rest of your system. [Windows Sandbox](#) is a Windows 10 feature only. But Linux and other OS may have options for the same function.

1. “Install Windows 10 Pro or Enterprise, [Insider build 18305](#) or newer
2. Enable virtualization:
 - If you are using a physical machine, ensure virtualization capabilities are enabled in the BIOS.
 - If you are using a virtual machine, enable nested virtualization with this PowerShell cmdlet:
 - `Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true`
3. Open Windows Features, and then select Windows Sandbox. Select OK to install Windows Sandbox. You might be asked to restart the computer.



4. Using the Start menu, find Windows Sandbox, run it and allow the elevation
5. Copy an executable file from the host
6. Paste the executable file in the window of Windows Sandbox (on the Windows desktop)
7. Run the executable in the Windows Sandbox; if it is an installer go ahead and install it
8. Run the application and use it as you normally do
9. When you're done experimenting, you can simply close the Windows Sandbox application. All sandbox content will be discarded and permanently deleted
10. Confirm that the host does not have any of the modifications that you made in Windows Sandbox.

Windows Update Changes to End Automatic Updates

From the article:

<https://www.csoonline.com/article/3253899/the-best-new-windows-10-security-features.html?page=2>

"Windows update notifications

Microsoft is making small changes to Windows update notifications so that it is much more obvious that an update is going to take place and reboot your system. It has also added settings to assist with installing. When your computer is on, Windows Update will keep an inactive computer from going to sleep for two hours when installing an update.

Windows update changes

Administrators get more group policy and registry adjustments to better throttle Windows update bandwidth in a network setting. New features are located under Administrative Templates > Windows Components > Delivery Optimization. These new controls allow you to adjust bandwidth used by foreground downloads. The amount of bandwidth can now be limited for both Windows Update and Microsoft Store updates. Previously, you could only limit the download bandwidth. Now you can specify Maximum Foreground Download Bandwidth (percentage) or Maximum Background Download Bandwidth (percentage). The process of installing feature updates has been [designed to be faster](#) to allow your machine to get back to functional access after the feature update has been triggered.

Administrators have been given the ability to customize the roll-back window. Before it was programmed at 10 days whereby the system kept your old version, now the administrator has dism commands to customize the number of days the system will keep the prior version.

The following commands can be used to customize the roll-back window:

DISM /Online /Initiate-OSUninstall

Initiates an OS uninstall to take the computer back to the previous installation of windows.

DISM /Online /Remove-OSUninstall

Removes the OS uninstall capability from the computer.

DISM /Online /Get-OSUninstallWindow

Displays the number of days after upgrade during which uninstall can be performed.

DISM /Online /Set-OSUninstallWindow

Sets the number of days after upgrade during which uninstall can be performed.”

Windows 10 Enterprise Advanced Threat Protection

On occasion a person will purchase a refurbished computer with Win10EE, or perhaps you are a medium sized business owner reading this and have a fleet of computers with it on there. It is important, therefore, that you know about anti-ransomware opportunities. One such you must get is [Defender ATP](#), which you can get by [clicking here to sign up for it](#).

“Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

- Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.
- Cloud security analytics: Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections and recommended responses to advanced threats.
- Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.”

- ❑ Given the good track record of Windows Defender lately, you can probably dispense with other anti-malware product purchases, if you can get this tool.
- ❑ IT administrators and the more tech savvy [may enjoy this article from a hacker/IT professional](#), which acts as a guide for setting up a battle-hardened network.

Device Guard

- ❑ Again Windows 10 Enterprise and Education version users are enabled to use this feature, [Device Guard, which will give them program control of the Windows Security system](#). For more information, advanced users may consult [this article on Windows Defender Application Control](#).

Secure email

While hacking into google is nearly impossible, gmail, and other services like it are far from secure, from the perspective of a user desiring to be anonymous, and to have encrypted emails. Gmail is not encrypted, though the links for the web-data for each email be randomized. With the right knowledge of tokens and servers, emails can be found on the Dark Web where everything has been stored. However, if one desires to be totally anonymous, one can refer to the services provided by companies mentioned in this article:

<https://restoreprivacy.com/secure-email/>

❑ My recommendation is this:

1. Open a Tutanota or similar account. Store the restore code provided temporarily on a screen.
 - a. The purpose of the Tutanota is to be anonymous, so do not associate it with any other accounts than the Protonmail, which is also secure mail.
2. Open a [protonmail account](#), using the first account as the restore account.
 - a. All passwords for these should be written down, rather than stored in browser. But a Password Manager is a good option from trusted devices.
 - b. **Important** - when you reset protonmail passwords you lose old emails, so try to avoid this if possible.
3. Send the code from #1 to #2, and **write it down; use the encrypted email option and a simple password only you would know to lock the restore code up.**
 - a. Optional/Recommended: setup a BitWarden account and extension to memorize these, as they will probably be easy to forget.
4. Use the protonmail account as the restore account for a mainstream email.
 - a. Optional: install ProtonVPN and use your protonmail account to open it on your phone.
5. If you already have a gmail account, open a secondary one which you can share your Drive contents to, or even transfer ownership.
 - a. You may consider changing your Facebook and Instagram, etc. logins to the newer email so that you can restore your social media accounts securely anytime. Remember, the restoration for this email **should be your secure mail account**. Should that be compromised, your second and totally anonymous secure mail account can restore it. So keep the password for #1 totally separate from all other accounts.
6. Turn on all the security options available for the emails above.
 - a. For gmail, review your security settings at <http://myaccounts.google.com/security>
 - b. Remove any identifying security questions, such as old phone numbers, high schools, etc.
7. Use the protonmail to open a secondary cloud service, which may backup the Google Drive or Dropbox contents; this will not be free.
 - a. My recommendation is pCloud for several reasons discussed later.

Anonymous email

On very rare occasions, it may be necessary to send a totally anonymous email with no identifying characteristics. In such cases realize two things: the keystrokes and cache on your computer may **not** be secure, despite the service offered. Also, if you are using TOR/Onion routing or VPN, these will afford you no protection in the case of mainstream services which can, do, and will log your activity. Therefore you should utilize only your completely anonymous Tutanota (or other) account, or, if the matter be temporary,

Guerilla-mail: <https://www.guerrillamail.com/>

2-step and 3-step (factor) Validation

For all the email services which are important for your passports (single click logins using gmail or facebook), you should as of 2018 really have on 2 factor authentication, if you have a smartphone. If you do not have a smartphone, you will need to create a second factor login, or perhaps change the password monthly. As we go along using the internet, giving permissions, our digital footprint and more importantly: fingerprints get left in all sorts of nooks and crannies of the web. From time to time a critical security breach at a company (such as the famous Yahoo breach from 2012) may expose all other accounts to extreme vulnerabilities.

A 2 factor authentication will send you a code to your phone whenever a new device (or one that has been silent awhile) attempts to login to an account. Important accounts to consider adding 2 factor authentication to:

- ☐ Email
- ☐ Bank
- ☐ Brokerage
- ☐ Cloud service
- ☐ Antivirus or firewall settings
- ☐ Cryptocurrency accounts

In some cases, a third factor, such as an encrypted keystore of randomized characters, provided only once, may be needed. This is especially true for crypto accounts not using wallet services.

NOTE - pCloud and similar services which offer military grade encryption can be used - if the password is kept personally or with a hint only yourself and a spouse or trusted relative recognize - to store information about passwords and accounts, or secure strings. You should never identify the existence of the meaning of these with the entire login details or mention of the word password (use pw instead). Should you forget to logout of your pCloud, it may be that someone following after you may decipher the meaning and use of these, and sabotage your account. You may optionally also store the details in an added layer of security via **steganography** (see below), within the encrypted folder. This would add a fourth layer of authentication to get at certain details. The multiple forms of encryption should prove very difficult for even the NSA to crack, unless they have keystrokes. You must rely upon the security of your modem, or strengthen it, in order to keep any advantage you wish over snoopers.

Revoking Licenses & App Privileges

This is important for gmail users: when you add multi-factor authentication, you should scroll to the bottom and click "Revoke all Devices" This appears once. Afterwards, you can review your devices by running the [Security Checkup](#)

Regarding App Privileges, we will cover this as it pertains to the two most important passport types, google and facebook. From time to time, you should peruse your authorizations, and revoke authentication and sharing permissions with companies that can use your data without your further permission. Perhaps you did it to play a game you no longer play. You can always give permission again. After you first set up multi factor authentication, however, you should revoke all permissions that are *not essential* to your daily activities. The links were provided above, and are simple enough in gmail by going to <https://myaccount.google.com/permissions>

But for Facebook, there may be a couple of other steps. [Following CNET](#):

❑ "Log on to Facebook."

1. Click the drop-down arrow next to Home in the upper right, then select "Account Settings."

The screenshot shows the Facebook homepage for a user named Rob Lightner. The top navigation bar includes the Facebook logo, a search bar, and links for 'Rob Lightner', 'Find Friends', and 'Home'. A dropdown menu is open next to the 'Home' link, displaying options: 'Account Settings', 'Privacy Settings', 'Log Out', and 'Help'. The left sidebar contains sections for 'FAVORITES' (News Feed, Messages, Events, Find Friends), 'APPS' (flicfy, Xbox LIVE, Music, D&D: Heroes of Neverwinter, PayPal Send Money, Apps and Games), and 'GROUPS' (Pacific Science Center, PSC-current and past empl..., New Group...). The main content area shows a status update from Rob Lightner about archiving 2011 work folders, followed by a link to a list of fun holiday recipes for self-sufficient singles. The right sidebar shows a list of friends and their recent activity, including a post from 'Ch sta' and a comment from 'An Ma'.

2. Account Settings.

3. Select "Apps" on the left sidebar.

4. Scan the list and click the "x" on the right of any app you want to clear. Its permissions will be revoked and you won't see it anymore (unless you decide to give it another go one day).

5. Revoke permissions."

Passcode/PIN

On phones and Windows login, many people use PIN for passwords. This is acceptable. Google also now has the option to turn on finger tap pass-pin for two factor authentication.

← → ↻ https://myaccount.google.com/signinoptions/two-step-verification?utm_source=google-account&utm_medium=web&rapt=AEjHL4Nuk77W2GHQ

Google Account


← 2-Step Verification

2-Step Verification is ON since May 30, 2019

TURN OFF

Your second step

After entering your password, you'll be asked for a second verification step. [Learn more](#)



Tired of typing verification codes?

Get a Google prompt on your phone and just tap Yes to sign in.

[ADD GOOGLE PROMPT](#)

Add Google prompt

This is **not** fingerprint verification, and so it is not considered by the author to be an option for high level security. It would however, lock out foreign intrusions.

- ❑ **NOTE - take the time while you are here to add two or more recovery phone numbers; also verify your email restoration account and if possible change to your new gmail/email or protonmail account.**

Push Notifications

Another option is you can download a 2FA app, such as Google Authenticator or BitWarden Authenticator, etc. and turn on push notifications, to eliminate the hassle of 6 digit codes.

Secure an E-mail Client

Not many people use email clients anymore, but some businesses still use Outlook. If you'd like secure, encrypted messages, one option that remains still is [Gpg4win](#).

Antivirus, Firewall, Etc.

I use AVG Internet Security, because I am familiar with its system. Other than McAfee (terrible) and Norton (overpriced), I have no secondary favorites. I am familiar with ZoneAlarm, Avast, Panda, Total360, Malwarebytes, and Spybot S&D. There are innumerable options.

- ❑ <https://www.pcmag.com/roundup/267984/the-best-free-antivirus-protection>
- ❑ <https://www.techradar.com/best/best-antivirus>
- ❑ <https://www.avg.com/en/signal/best-free-antivirus-software>

The best part about AVG free is it is free, and it does work. However, AVG Free will not detect malware very well, so it is not comprehensive. The AVG Internet Security is a great option, while (as discussed later) AVP PC Tuneup is a **must**. Sometimes AV providers have true freeware programs, such as Malwarebytes Anti-rootkit. But most of them want you to pay. The goal is to get as many programs that will work together, with as few \$\$ spent. You do not need two anti-viruses, which will only compete. Some single PC users (grandparents and such) will opt to purchase one large suite, such as Avast or Norton AV, which is supposed to be comprehensive. To choose, please rely upon performance reports published yearly, as to the quality, speed, reliability, and user friendliness of various options. Anyone savvy enough to click the “advanced install” on programs will not likely need this advice, so if you are prone to using recommended settings, you are not an advanced user, and should follow program recommendations for almost all security options.

Special AV Tools

- ❑ [VirusTotal is an online file upload or url scanner](#) which you can use before making a choice to download or press install.
- ❑ [Qihoo Total 360 has anti-ransomware decryption tools built in](#), along with several other tools, a few of which are free, some of which are not and may act like malware, and eat up memory. Choose wisely which tools you download. Note that this company may be vulnerable to Chinese backdoors.
- ❑ Panda Free AV has no immunization vault, or malware protection, but it is cloud based and has a free VPN client (for now) though only 150MB daily. [Its reliability may be questionable](#). However it is free and no strings attached, and not controlled by China
- ❑ [Avira Free comes with a built in Firewall and quarantine section](#)
- ❑ [rKill](#) or [rKill for IE](#) are useful standalone tools to search for malware
- ❑ [WinThruster](#) can be used to remove HEUR related trojans not fixed by MalwareBytes (unpopular)
- ❑ [Farbar](#) has a free [scan toolkit](#) and [Toolbar toolkit](#) which creates log files to look for explorer.exe malware
- ❑ **Important:** your antivirus may disable restores and backups, or interfere. When you purchase a new computer, immediately create a backup before installing these software. To create one after, [refer to this howto article regarding creating windows backups with security installed](#).

Firewall

A firewall blocks intrusive connections and trojan attacks. Therefore it is as important to have a firewall as it is to have an anti-virus. All modern high-speed internet modems come with firmware (pre-built) firewalls, and your ISP will also run intrusion detection on their servers. Also they will attempt to keep you from hacking out, as well. However, as these can all be circumvented, it is recommended you install a software firewall, or at least rely upon Windows Defender Firewall. A custom made firewall is better, however, and usually free. If you purchase an internet security suite, it will come with one, automatically.

- ❑ [Read about the best free firewalls - you only need to choose one.](#)
- ❑ [This article includes one for Mac Users, AvastFree](#)
- ❑ In the past I used ZoneAlarm, but found it quirky with various software installations. It may have improved since then, as it ranks high in that article. It has been valuable to me in the mid 2000's if that has any sway to the reader.

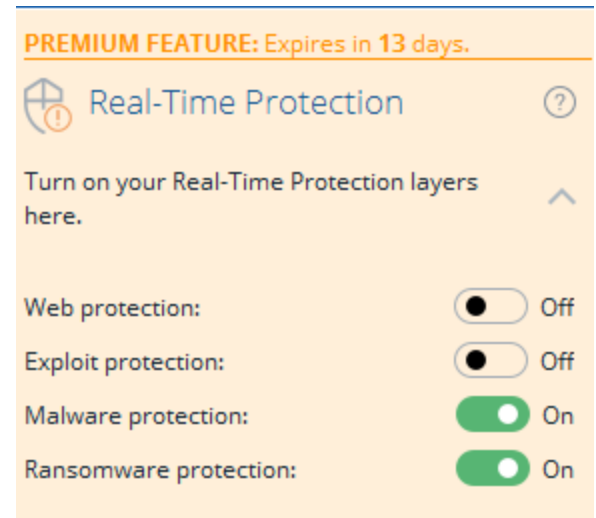
Anti-Malware

Malware are software programs inserted onto your computer to track, trace, or snoop on you, and report your behaviors and private information back to third parties - like Eastern European hackers, or China.

This data is useful to them financially, and typically doesn't harm your computer, except for speed. The most common malware of the 90s and 00s were little programs or processes with quirky names in your Task Manager (ctrl+alt+del). However, they are quite a bit more advanced now, and can hide within your Windows Registry, or in the background. So while it is useful to search your TaskMan from time to time for odd RAM or Disk behavior, it's better to search for it directly.

You can pay for Malware protection, but the author only uses two programs:

- ❑ [Malwarebytes](#) - no longer free after a month, but worth a first time install and scan. The "free" version isn't real-time, and has annoying pop-ups. It may slow down older computers.
- ❑ [Malwarebytes now provides a browser extension](#)
- ❑ [Spybot Search & Destroy](#) - free, comes with Immunization protection, and free scan forever, premium upgrades available. This is a program that has been very useful to me in the past and I can always recommend.
- ❑ Also available is the [Microsoft Malicious Removal Tool](#)
- ❑ Malwarebytes [Anti-Ransomware BETA](#) and [Anti-Exploit BETA](#) are two tools you can use if you do not have Malwarebytes 3.0+ installed, and they are free
- ❑ [Unchecky](#) (helps keep PUPs from being installed, or unwanted options)
- ❑ [Hitman Pro](#) is an option that has a mobile app version or [can be used instead of Malwarebytes](#).
- ❑ [MalwareFox](#) can be installed without run-time, and is light install (only 5mb) in case you have an emergency. It allows file/folder drag and drop scan, which is very handy.



Anti-Rootkit

- ❑ [Malwarebytes has a free rootkit scan tool. you must acquire.](#) It works fine with all installed anti-malware, and is a standalone program in their C:/Program Files directory. Make sure to "send to desktop (create shortcut)" so you can find the program again, later.

Anti-Bootkit

Kaspersky makes a free utility called [TDSSkiller which you should download](#) and run on any fresh computer, especially before locking down the BIOS and Hard Drive with BitLocker. <https://support.kaspersky.com/5350>

- ❑ <https://support.kaspersky.com/viruses/utility#TDSSKiller>

Anti-Ransomware

Ransomware is a small segment of attack, and mostly targeted at Medical Office Software users. I personally know a chiropractor office targeted, and who could not pay, and lost all their data. Assuming the Total360 tool is useless in real time, there are a number of options for download, please go here to read:

- ❑ <https://www.pcmag.com/roundup/353231/the-best-ransomware-protection#>

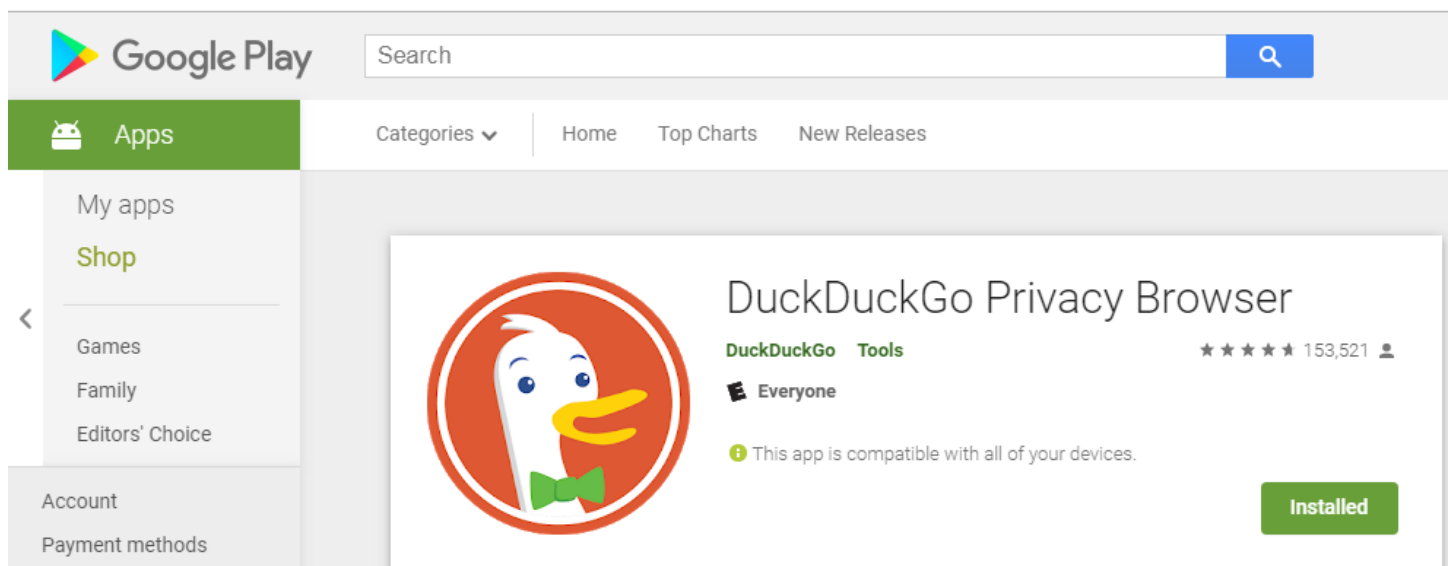
As you can see, none of them are very good. If you are concerned, purchase the full versions. My hunch is they will not work against a coordinated, and concerted attack, so a strong firewall, AV, and malware

defense is much more important. However, for a free version, [you can download the Trend Micro software](#), which is after all only half good, but better than nothing. It might have a memory hole issue in Windows 7.

Internet Browsing

There's something you need to know about using Google or Bing. When you do, you are no longer on the true internet, known as the Deep Web. You are on a synthetic copy, owned basically, by Google or Microsoft, except the pages which you go to. But everywhere you search, go, click, login, and leave text or scroll data via cookies, is available to Google AI and to intelligence agencies - **worldwide**. Your habits are known, stored, and targeted. This can help or hurt you, depending on your political and social stances.

As such, you may be interested to know there are viable options to alternative search engines, such as [Duck, Duck, Go](#) which does not store your data and can perform in many cases better jobs (because it has no political or financial bias, nor track your habits). You can even install it as an app or extension on your devices:



It will ask you to specify which device you want it installed on, however. It may be you do not trust them, but regardless assume that your Android and iOS and MSOS devices are tracking you, anyhow.

Virtual Private Networks

Which brings us to the invention of a lifetime (for now): VPN. VPN has actually been around since the 1990s, but it was not very popular except for remote management and conferencing, etc. In the 2000s it became popular with people doing unsavory things and then those who wanted onto the Dark Web (to buy illegal items, like drugs), and finally it has come mainstream. Just about every YouTube channel is sponsored - it seems - by a VPN provider. The two most common advertisers being NordVPN and ExpressVPN¹. A third popular program that I support is Hotspot Shield, as it seems pretty reliable.

So why is this important? You may not be aware but your address is vulnerable right now via your ISP IP address, which either looks like this:

[37.120.130.4](#) or [2600:1005:b062:61e4:74d7:f292:802c:fbfd](#) (neither of these are me, I am on VPN!)

The long and short of it is that these can be turned into physical addresses. Someone can map out where you are and then track you down, personally. Take for example some angry rando who is an ex-military type looking to suicide by cop or commit a school-shooting. And you just *made them mad!*. Or more classically, a pedophile

¹ Both of which have no log policies for VPN users; <https://ucp.nordvpn.com/audit-report/>

who is interested in your daughter. This is all scary but real stuff that has happened. So use a VPN, and use it on your phone, computers, laptops, and other devices! Once installed it's as easy as a click. Alternatively, or perhaps at any rate, you can install extensions for the VPN right into Chrome or Firefox. Ones I trust:

- ❑ [NordVPN](#) (pain though, it keeps requiring signin)
- ❑ [Free VPN](#)
- ❑ [Browsesec](#) (very very fast)
- ❑ [ProtonVPN](#) (perfect for phone and computer, especially if you have a protonmail account, it's easy to add this feature. Right now it's free, one day it may not be.)
- ❑ [uVPN](#) (not free for westerners, but a good option if you're traveling or from India, etc.)

Double-VPN

You can run two VPN programs back-to-back, or with NordVPN, it is a single click option. This puts you into a slower connection with more bounces, but does add an extra layer of security.

Alternatively, you can actually run two VPN extensions or programs in tandem, and if one is turned on after the other, this should, in theory, give you a double VPN.

TOR/Deep Web

The Onion Router was developed by the military for security connections that were basically untraceable worldwide. Websites using TOR encryption end with .onion or similar suffixes. Their domains are often also randomized, but with the TOR browser you can find them readily enough if you know the exact name of the illicit website you plan to visit. Very soon TOR routing will be commonplace for everyday use, which will make law enforcement very difficult, but for you good people, it will only protect you from a worsening internet environment. So, how can you safely get on the Deep Web? If you use TOR on your windows, you will, of course, expose your machine and burn your OR identity. There are only two methods I advocate, and only two I have used:

TAILS OS

Tails is a Linux based OS specifically created to use the Dark Web in secret. You can create a login, and use it like an OS. It is loaded onto a personal thumb drive/USB stick or similar. You have to make sure to download a verified single-owner copy of the OS installation file, otherwise it could already be infiltrated by the NSA/CIA or other world government intelligence agencies. They change the keys daily, so you can generally trust the website procuring it, unless you have been routed via hack to an NSA server. That would mean they were onto you, beat all your home PC protection, and planted a clever trojan that backdoors through all your security. This is more common than you'd imagine, but nevertheless not usual - yet. Once the AI meets the quantum computers, it probably won't matter anyhow, they will be able to slice through encryption no matter what, and only governments and institutions will be capable of affording those!

Once the OS is on the stick you can create a first time login. Write down the details on paper somewhere, and keep them. Otherwise, you can always use the OS as a guest. All your files will be lost each time you logout. It is a dedicated stick, so if you have a large one, you probably want to keep your details. Here are the steps, in specific, to do this:

<https://www.techrepublic.com/article/getting-started-with-tails-the-encrypted-leave-no-trace-operating-system/>



“Before getting started you will need:

- ❑ Two 4GB USB drives. One USB drive will be used to prepare and install Tails; the second USB drive will run the OS.
- ❑ A mobile device, like a phone or tablet, and an app that scans QR codes.
- ❑ Two to three hours of time. The installation process is relatively painless, but make sure you allocate enough time to read all the documentation, download software, and to prepare your machine.

Step 1: Learn

Tails is not a magic bullet, and it cannot protect against compromised hardware, compromised software, or user error. These steps may seem simple, but for Tails to provide proper protection it's essential you follow the most current documentation on the [boum.org](https://tails.boum.org) website. Installing Tails is fast and simple. Understanding how to use the security tools inside the operating system takes planning and preparation.

- ❑ Make sure you read the Tails [About](#) and [Warning](#) pages to understand what Tails does and does not do.
- ❑ Read the [Documentation](#) and [FAQ](#). Make sure that your system meets the minimum requirements.
- ❑ Join the Tails XMPP chat, and communicate with developers and community members
 - ❑ Server: conference.riseup.net
 - ❑ Room: tails
 - ❑ TLS/SSL

Step 2: Download and authenticate

- ❑ Make sure your local machine is secure and virus-free.
- ❑ Download and install Firefox.
- ❑ Install the Tails [browser addon](#). This plugin will be used to verify the OS image file download.
- ❑ Download Tails by navigating directly to <https://tails.boum.org/install/index.en.html> and selecting your operating system.
- ❑ Or download the Tails torrent file here: <https://tails.boum.org/torrents/files/tails-i386-2.5.torrent>.
- ❑ After you download, to prevent man-in-the-middle attacks you must [verify Tails](#).

Step 4: Install

- ❑ Insert your first USB drive.
- ❑ Download the [Universal USB Installer](#) from the Installation page.
- ❑ Windows users will be guided through an installation wizard and prompted to install the Tails image on the USB drive.
- ❑ Important: use your mobile device to open the [Instructions URL](#). In the next step you will need to restart your machine. This instruction list will walk you through getting back online fast.

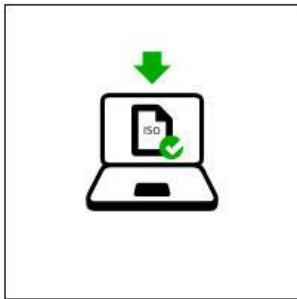
- ❑ Restart your computer. During the bootup process, press the Boot Menu Key, usually F12 or esc, and select Boot Tails from your USB drive.
- ❑ Follow the instructions on the Welcome to Tails prompt.
- ❑ Next, insert your second USB drive.
- ❑ Under Applications click Tails Installer and follow the prompts to install Tails on your second USB drive.
- ❑ After the installation completes, shut down your computer.
- ❑ Remove your first USB drive, leaving the second USB drive attached.
- ❑ Repeat the startup process and run Tails.”

There is a visual howto on this article <https://www.maketecheasier.com/create-bootable-tails-usb/>

“Download and Verify Tails

There are a couple of ways to do this. By far, the easiest is to use the Firefox add-on that the Tails project set up.

Download and verify



You will download Tails as an ISO image: a single file containing the whole operating system. For your security, it is very important to also verify your download. We propose you two techniques to do this verification automatically.

We detected that you are running Firefox or Tor Browser.

You can download the ISO image via our Firefox add-on. The add-on verifies your download automatically.

1. Install Firefox add-on

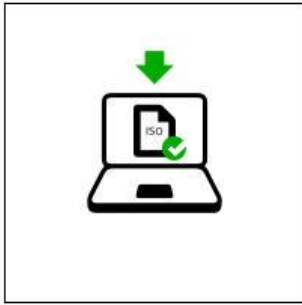
No restart

or [Download and verify via BitTorrent](#)

or [Download and verify using OpenPGP](#)

- ❑ Go to the [Tails download page](#) using Firefox. You'll see a couple of steps listed. The first will be highlighted purple, and it will prompt you to install the Firefox add-on.

Download and verify



You will download Tails as an ISO image: a single file containing the whole operating system. For your security, it is very important to also verify your download. We propose you two techniques to do this verification automatically.

1. Install Firefox add-on



2. Download Tails 3.0.1 ISO image

3968 KB/s — 46.5/1153.1 MiB, 4 minutes



Downloading to /home/nick/Downloads/tails-amd64-3.0.1.iso



Cancel

3. Verify ISO image

- ❑ The next button will light up purple, after the add-on installs. Click on it to begin the download. The download will take a bit of time, so relax.



1. Install Firefox add-on



2. Download Tails 3.0.1 ISO image

Downloaded to /home/nick/Downloads/tails-amd64-3.0.1.iso



3. Verify ISO image



You downloaded and verified the ISO image successfully!

If you are knowledgeable about OpenPGP, you can do additional verification using the [OpenPGP signature](#).

[Download again](#)

- ❑ When the download finishes, you should automatically see a check on the page next to “Verify ISO image.” If you do, great! Your Tails ISO is downloaded and ready to go.

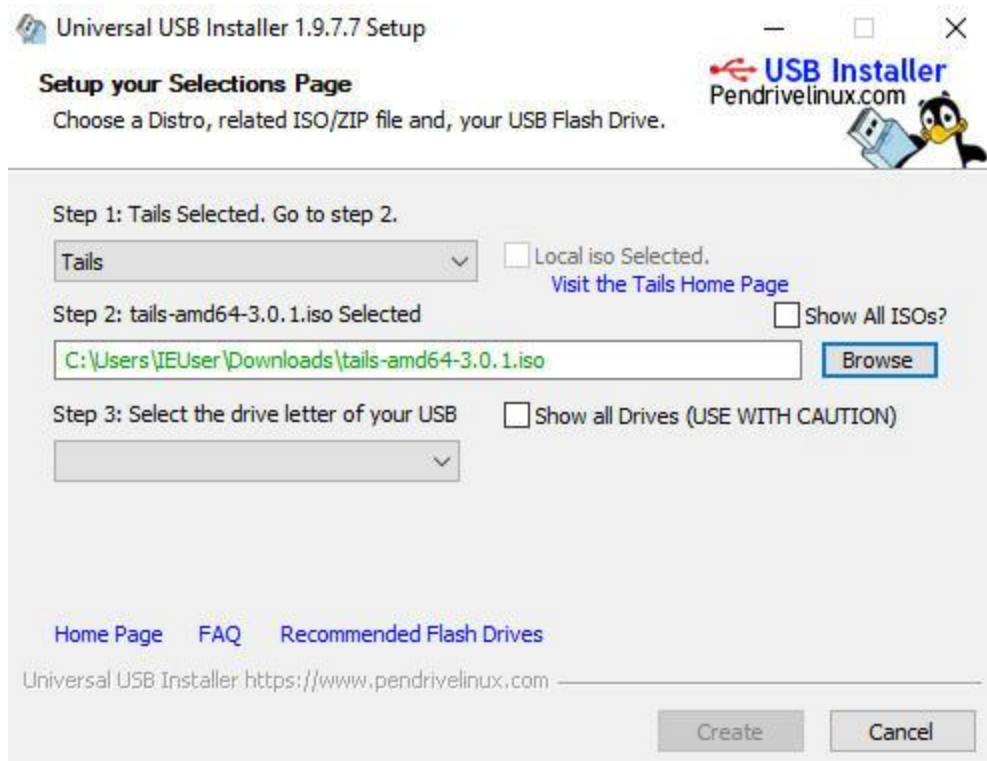
Create the First USB

This step is going to be different, depending on which operating system you’re using. The goal here is to create the first USB, the intermediary one, using the image that you just downloaded.

- ❑ Insert the first USB into your computer.

Windows

- ❑ Before you can create the USB, you need to [download a utility](#) to install your Tails image. If you have a utility that you prefer, use that. Otherwise, use the [Universal USB Installer](#) provided by Tails.
- ❑ Download the program and install it. After you’ve done that, open it.



- ❑ In the first drop-down, select “Tails.” Then, in the second, click on “Browse.” Browse to the Tails image that you just downloaded and select it.
- ❑ Finally, find and select the USB drive that you inserted. When everything looks the way you want it to, click “Create.”
- ❑ The installer will ask you to confirm. Click “Yes” and close the installer when it finishes.

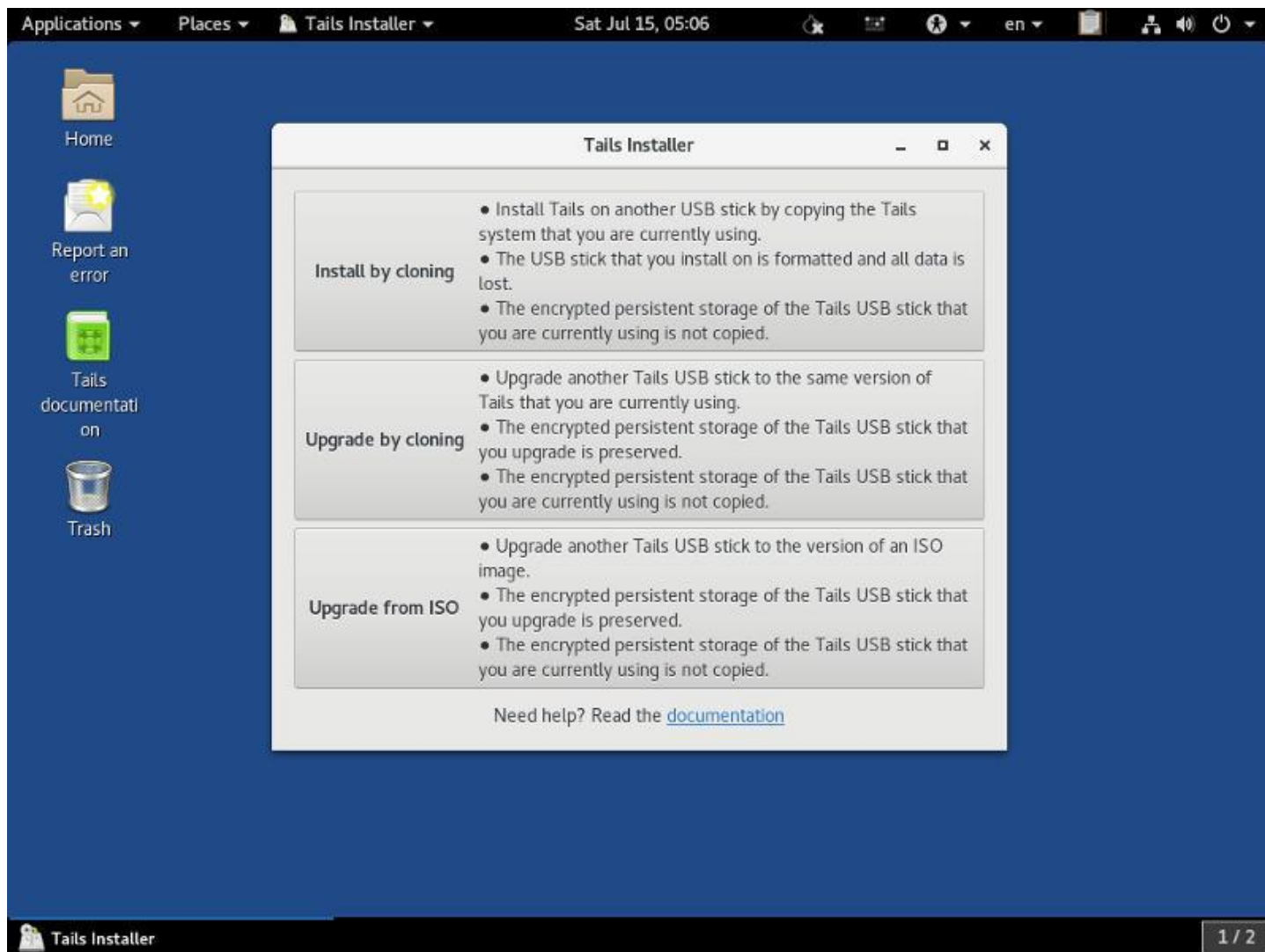
Linux

- ❑ Open a terminal. You’ll need to find where your USB is mounted. If you don’t know, run the following to list everything mounted on your computer.
- ❑ `ls /dev/ | grep sd`
- ❑ You’re going to be looking for the drive with the last letter in the alphabet that has a number after it. If you’re really unsure, open a program like GParted. It’ll be much easier to figure out which one is the USB that way.
- ❑ Once you’re absolutely sure that you have the right drive, you can clone the image onto the USB.
- ❑ `sudo dd if=Downloads/tails-amd64-3.0.1.iso of=/dev/sdc bs=8M`

- ❑ Make sure that if is set equal to the path to the image file and of is set to the path of your USB.

Create the Final USB

- ❑ After the first USB is done, you can reboot your computer into Tails. As it's rebooting, make sure that your computer is set to boot to USB.
- ❑ Select Tails from the boot menu. Then, when Tails boots, select your language and region. After a few seconds, you'll see the Tails desktop.
- ❑ Insert your second USB now.
- ❑ Click on "Applications" in the upper-left corner of the screen. Click on "Tails," then find "Tails Installer."



- ❑ The first option is "Install by cloning." That's the one you want. Once you click that, you'll be able to select your second USB to install on.
- ❑ Confirm your install. After the installer finishes, you'll have a working Tails USB. Shut down your computer, unplug the first USB, and power it back on. You'll find yourself in your working install.
- ❑ For true anonymity and security, remember common sense and best practices, and as always, only use Tails for good."

Virtual Machine

A virtual machine (VM) - [usually run on VMWare](#), but can be other software - is a complete simulation of a computer, in a software window on your current machine. So in essence, a computer within a computer. You can secretly download a VM and an OS to run it on - such as TAILS or other Linux - and then install it on your computer. Once there and logged in (say it was Windows XP, so you'd call it your XP Machine), you can again download VPN software or use what you have bought (along with all the internet security you need these days, as it is a totally different machine than your desktop²), and even run double VPN. I have heard that certain nutjobs with a lot to hide, like pedophiles, are even running virtual machines within virtual machines, double VPN, and then TOR. What a lot of work! At that stage the fear you must live with is too tremendous to be worth the risk. But as a scientific experiment it would be interesting to know the drop in computing power and connection latency. If the FBI is tapped into your connection at the local junction between you and the ISP, it may be pointless, for anything unencrypted - which is most of the internet - would still be exposed.

To install VMWare, [visit their website](#). As said before you need to install an OS, so if you have an old disc of Windows XP or 7 laying around, fine. Otherwise I'd advise downloading a free copy of Ubuntu. Not much reason to use Ubuntu Linux except for software developers. So instead we will include directions on running TAILS on your VMWare:

- ❑ Follow all these steps in this article:
<http://fortysomethinggeek.blogspot.com/2014/09/proper-way-to-run-tor-and-tails-in.html>
- ❑ For Linux/VirtualBox, please use this article:
https://tails.boum.org/doc/advanced_topics/virtualization/virtualbox/index.en.html
- ❑ [Read up about security concerns and the breaking of Tails security when using VMWare/VirtualBox etc.](#)

Password Manager

A Password Manager acts just like GoogleSync, and keeps track of your data, except that it is third party. There are only a few worth using, as covered by this article:

<https://www.pcmag.com/roundup/331555/the-best-free-password-managers>

- ❑ BitWarden is the product I most recommend, after the LastPass forced upgrade fiasco. You can easily [export your LastPass data, and import to BitWarden](#), and use on all platforms, and the extension is a little better, too.
- ❑ Myki has almost the same number of features, sans "Digital Legacy". It seems like a good product, as it received Editor's Choice.
- ❑ 1U Password is a distant third, and only use this if you have had bad interactions with the first two programs.
- ❑ Symantec has more features than 1U Password, but has a much lower rating, probably indicating weak user friendliness

Authenticators

At this time the author recommends you create a Microsoft Live account for cloud, and install Microsoft Authenticator, and use it (top reviews) for all your alt.2FA needs. It is easy to use and secure.

² But it **will** paginate and store files on your HDD, even with Tails. It should remove those files when finished, unless from a Virtual Machine

AdBlockers

There are many other adblocker software than the version already posted. For a review of the best options, see: <https://www.comparitech.com/blog/vpn-privacy/best-free-ad-blockers/>

“From our research, the best free adblockers of 2019 are:

1. Stands Fair Adblocker
2. AdGuard
3. Opera Browser
4. AdLock
5. [AdBlock Plus](#)
6. uBlock Plus Adblocker
7. Incognito Adblocker for Firefox
8. AdBlocker Genesis Plus
9. Trustnav Adblocker
10. Adblocker Ultimate
11. NoScript

When researching the best free ad blockers, we looked for the following criteria

- ☐ Always free, without a paywall for important features
- ☐ Good user ratings
- ☐ Do not require an account to use services
- ☐ Recently updated (within the past 12 months)
- ☐ Readily available as a plugin for at least one browser or operating system
- ☐ Blocks “display ads” (floating, pop-up, banner, video, static image, wallpaper, text ads)
- ☐ Blocks streaming video ads (such as on YouTube)”

You should be able to find all blockers on their site, or in Play Store / Apple Store. **You should not have to ever download one via an ftp or account signin website.** This would indicate a scammer or phishing attack.ected

Web Extensions, Cookies, Scripts, etc.

Kids and randos in your family (lol) will install extensions, usually by accident or clicking yes/agree to anything they happen upon while surfing for games, porn, movies, news, etc. It is important to open the advanced settings in your Browser, and view the extensions that are presently installed:

- ☐ [Chrome](#) or chrome://extensions/
- ☐ [Firefox](#) or ctrl+shift+A in Firefox
- ☐ [Edge](#) > (three dots ---) > [Extensions](#)
- ☐ Explorer > Tools > Manage Addons (generally remove anything that isn't Microsoft or Adobe)
- ☐ [Opera](#) and [Watch this video](#)
- ☐ [Signal Desktop](#) (end-to-end message [encryption to work with Signal on Android/iOS](#))

As far as removing cookies, scripts, and clearing cache this is all contained in the Tools/Settings and manager sections of the browsers. In the case of Chrome, however, there are three places to visit:

- ☐ Ctrl+shift+del to clear browsing Data
- ☐ History > Clear History if it is insecure, and learn to use Incognito Mode
- ☐ chrome://settings/ > Advanced and check all of your settings

In general you should disable extraneous javascript extensions and add-ons unless you know exactly which website it is for (such as a game or forum website you frequent)

Surfing Blockers

The scripts that you can use - and there are many options - will be those which block, track, or totally [eradicate the threats from typical daily browsing](#). Try out some of these scripts, and see which you trust the most, or prefer:

- ☐ [uBlock Origin](#)
- ☐ [uMatrix](#) (advanced!)
- ☐ [NoScript/Safe](#)
- ☐ [HTTPS Everywhere](#)
- ☐ [Disconnect.Me](#)
- ☐ [Social Book Post](#)
- ☐ [Privacy Badger](#)
- ☐ [Lightbeam \(Firefox\)](#)
- ☐ [FacebookDisconnect \(Firefox\)](#)
- ☐ [Web of Trust](#) (not always

reliable, but can be quite useful. Won't be able to handle small business web-pages with unfamiliarity)

– Privacy (2)

- ☒ [Basic tracking list by Disconnect](#) 29 used out of 34 ⓘ
- ☒ [EasyPrivacy](#) 🏠 13,261 used out of 13,303 ⓘ
- ☒ [Fanboy's Enhanced Tracking List](#) 🏠 ⚠️

– Malware domains (5)

- ☒ [Malvertising filter list by Disconnect](#) 647 used out of 5,073 ⓘ
- ☒ [Malware Domain List](#) 1,122 used out of 1,152 ⓘ
- ☒ [Malware domains](#) 🏠 26,784 used out of 26,785 ⓘ
- ☒ [Malware domains \(long-lived\)](#) 🏠 2,380 used out of 3,204 ⓘ
- ☒ [Malware filter list by Disconnect](#) 3 used out of 2,331 ⓘ
- ☒ [Spam404](#) 🏠 ⚠️

– Social (3)

- ☒ [Anti-ThirdpartySocial \(see warning inside list\)](#) 🏠 66 used out of 66 ⓘ
- ☒ [Fanboy's Annoyance List](#) 🏠 10,802 used out of 26,246 ⓘ
- ☒ [Fanboy's Social Blocking List](#) 🏠 15,368 used out of 15,400 ⓘ

Incognito Mode, fact and fiction

IM used to mean Instant Messenger³, but precious few people use those anymore with the advent of SMS and Facebook (and other) messengers). Now the main IM is Incognito Mode, which is accessed when you open a new tab in Chrome Ctrl+shift+N instead of Ctrl+N or Ctrl+T. But despite its billing you need to know that [IM is not anonymity, completely](#). Not like TOR on Tails OS.

- Your movements are still logged by Google
- Your clicks can be tracked, like keystrokes
- Your IP is not incognito, only your browser history
- Websites may still install cookies and malware on your computer while using IM.

Therefore it may still be of value to clear your browsing history, from time to time.

More Secure Browsers

Some people no longer trust Chrome, Firefox, Edge/Explorer, and Safari, and [want to seek alternatives](#). Here's a short list to look into which are either considered more secure or more lightweight and able to disable vulnerable features:

- ☐ [Tor Browser](#) (not as secure as on TAILS OS, and a bit slow, but if you use "configure" it can be secure)
- ☐ Waterfox
- ☐ Opera

³ Look into [Jitsi](#) for more secure IM, if you plan to continue using instant messaging. Like P2P, I don't recommend IM.

- ❑ Quantum
- ❑ Falcon
- ❑ More [Windows Security for browsing](#)

Decrypto Browsing and Decentralized Browsing

New developments in blockchain means new ways of browsing. For more information on this, see “Unstoppable Domains”. For now, you can consider using [their extension “decrypt.co”](#) OR you can look into other ways to [encrypt and decrypt web components like gmail](#) with [extensions](#). Beware, however, that by nature these types of endeavors attract hackers and scammers, who could be running phishing outfits disguised as cybersecurity. Also, even well-intentioned firms may have poor security themselves. Until they have several years of tested and reputable value, the author cannot recommend adding them to your cybersecurity repertoire.

Decentralized Web 3.0 (Blockstack)

First, you can find a link to all the blockstack Chrome, Firefox, or developer code, at <https://www.blockstack.org/install>

From there you can find Various Apps at <https://www.app.co/> and Webby: <https://heywebby.app/webby>

There are many potential apps to use here, be sure you have your password storage going to store your Blockstack ID and any other secure phrases!

Blockchain/Crypto Currencies A to Z

Understanding Blockchain

Blockchain is an algorithmic protocol which is open sourced and evolving. Sometimes there are multiple layers. It involves a decentralized spreading of data, and “mining” algorithms to verify encrypted data, and because it is decentralized there is data security.

CryptoExchanges and Your Bank

First, create your first account at Coinbase, a trusted corporation, and go through the verification steps and link to your bank account. NOTE - you will pay taxes or have tax credits one your gains/losses are reported back into your bank account. NOTE! The IRS does not tax your internal gains in the crypto world, and you **can legally pay for things with crypto**.

Second, learn to secure your Coinbase password with your password storage (and never store in email or on computer), and then also turn on your 2FA (consider using an Authenticator).

Third, consider purchasing an external wallet or other method to store your crypto off server as Coinbase can theoretically be hacked and your crypto stolen. Millions of dollars in crypto are stolen every month as attacks are brute forced but nonpersonal.

Fourth, when you transfer from and to your bank, expect delays. When you do purchases and transfers between coins, expect data mining delays for verification. These can take seconds to minutes, even 10 minutes.

ICOs and Investing

I am not a crypto expert, but it is a fact that most of them are practically or literally worthless. Even with inflation most will amount to nothing. BitCoin/Cash is different because it has a limited supply and is an accepted gold standard. This makes it an ideal hedge - the ideal hedge - and there are BitCoin Futures on the major stock exchanges, and platforms like TDAmeritrade. Furthermore coins go up and down in value 24/7/365 and this doesn't stop. Sometimes it is affected by the stock markets, the money markets, and large purchases and sales, but the number one connection is via Google Search Trends. You can track the Trend here: <https://trends.google.com/trends/explore?q=bitcoin> and you can yourself decide when it may rise or fall, relatively speaking to the [dying] dollar. Bear in mind during extraordinary circumstances, like the Coronavirus Shutdown, it may become unhinged from this fundamental analysis. But primarily coins rise in value with hype and interest, and crash as it wanes. News stories may fuel their prices.

Hype and Underlying

One of the most important indicators is hype, and there is an entire ICO marketplace, and a dedicated (and zealous) group of techy/nerdy followers. Don't let them lead you or scare you, they are always Bulls. There is no underlying value to any coin, with the sole exception of the hedge value and limited supply of BitCoin, the grandfather. The only real value at all is the security the technology offers, and anonymity. You can use - and will be required to use - BTC on the Dark Web for illicit or private purchases you don't want police or governments to know about.

Plausible Uses

Whether you choose to use it to purchase BTC related stuff, to buy and hold, to order a pizza, or order cocaine, the bottom line is that BTC is useful and liberating. However, in the world of investing, you should not think of it like a stock or even like a currency. Unlike metals it changes value by the second and for often unrealistic reasons. A buy and hold strategy is for 98% of people. As it inflates, occasionally take from your wallet.

Another strategy is the pig rolling in mud.

1. Purchase BTC
2. Transfer to another coin, such as ETH, XRP, LNK, etc. when BTC is high and those coins are low
3. Transfer again to another coin, so long as you cover service fees, again once your coin rises and the other is low.
4. At the end of a period of time, doing this "roll around" you transfer back to BTC at Coinbase
5. Transfer back out to your bank when satisfied, or roll into a BTC Futures or other account.
 - a. If you have a Metals account you might convert it to bank then immediately to your metals account and buy a Metals IRA.
 - b. Or into a Health Savings Account, etc.
 - c. Or Mutual Fund/IRA/401-K (not recommended)

Please follow the laws of your state or country and consult an attorney before engaging in anything illegal.

Top Currencies to Consider and Become Familiar With

These are the top coins to track: <https://coinmarketcap.com/> and <https://www.worldcoinindex.com/>

I only trade in BTC, ETH, XRP, and coins that are commonly listed at Coinbase. I can only recommend these, and have no interest in others. Be careful and remember: nothing above should be construed as direct advice for investing, but is merely informative information.

Social Media


Social Media is the fastest growing arena of the internet, in terms of interaction programming concerns, and security/safety threats. Everything from cyber-bullying to doxxing (revealing private identifying data publicly and to angry hordes for the purpose of retribution) to credit card or identity fraud. People have live streamed suicides, murders, hate crimes, robberies, political attacks, and more. Needy trolls and lonely people, many of whom are starved for attention or think that life is a movie script, would love nothing more than to have a “A Few Good Men” moment IRL. Or, they may perhaps hate your personal political stances, and seek to have an anonymous revenge upon you. Also, there are armies of hacking groups that need likes and to generate “organic likes” by stealing your account login. For this reason many people are turning away from using their real names for social media, despite company policies, and returning to anonymous user ID’s. However, there are some ways to better safeguard your accounts, using (if you trust them) the security features provided by the companies are usually more than sufficient to protect you against concentrated attacks.

Facebook Security

- ☐ Quick: check your [Security and Account Settings](#).
- ☐ Read about [Facebook storage and tracking of your web browsing](#)
- ☐ Firefox users might install Facebook Disconnect
- ☐ Install Social Book Post adblocker

Security and Login

Recommended


 **Set up two-factor authentication**
We recommend that you add an extra layer of security to make your account even more secure.

Edit


If you’ve had trouble with break ins, then you can decide to set up 2 factor authentication. Otherwise, it’s probably likely to drive you crazy to use it. So long as you have a restore email, it shouldn’t be very hard to take back your account. However, there is a chance they might change some of your details, in which case if you’re not likely to notice for days, then you should absolutely use two-factor authentication. However, there is another way to know quickly that your account has a new sign-in on a new device: add email notification.

On top of that, take the time to add three to five friends that can help you if you are locked out. If you’re very paranoid, then you can use encrypted email notifications to tell you when someone is in your account.

Setting Up Extra Security



Get alerts about unrecognized logins
On • We'll let you know if anyone logs in from a device or browser you don't usually use

Edit



Choose 3 to 5 friends to contact if you get locked out
On • Your trusted contacts can send a code and URL from Facebook to help you log back in

Edit


Advanced


Encrypted notification emails
Add extra security to notification emails from Facebook (only you can decrypt these emails)

Edit



Recover external accounts
Recover access to other sites with your Facebook account

Edit



See recent emails from Facebook
See a list of emails we sent you recently, including emails about security

View

Login



Change password
It's a good idea to use a strong password that you're not using elsewhere

Edit



Save your login info
It will only be saved on the browsers and devices you choose

Edit


Two-Factor Authentication


Use two-factor authentication
We'll ask for a security code if we notice a login from an unusual device

Edit


Authorized Logins
Review a list of devices where you won't have to use a login code

View


App passwords
Use special passwords to log into your apps instead of using your Facebook password or login codes.

Add

- ☐ In case you are traveling you can set up USB/U2F or (up to 10) personal codes [to get into your account if you don't have your phone](#).

Control Friends and Sharing Privileges

- ☐ Set your [share privilege levels](#) (privacy) within the Settings of your Facebook. In light of the current environment I am recommending tighter restrictions than I have used in the past.

General
 Security and Login
 Your Facebook Information

Privacy
 Timeline and Tagging
 Stories
 Location
 Blocking
 Language


Notifications
 Mobile
 Public Posts

Apps and Websites
 Instant Games

Privacy Settings and Tools

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Friends except...	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

Download data

- ☐ If you are not using pCloud, or for some reason want to download your data and close your account forever (instead of just putting it on ice), you can do so [by downloading a copy following these steps](#):
1. “Go to the top right of Facebook and click .

2. Click Settings.

3. Click Your Facebook Information.

4. Go to Download Your Information and click View.

5. To add or remove categories of data from your request, click the boxes on the right side of Facebook.

6. Select other options, including:

■ The format of your download request.

■ The quality of photos, videos and other media.

■ A specific date range of information. If you don't select a date range, you'll request all the information for the categories you've selected.

7. Click Create File to confirm the download request.

After you've made a download request, it will appear as Pending in the [Available Files](#) section of the [Download Your Information Tool](#). It may take several days for us to finish preparing your download request

Once we've finished preparing your download request, we'll send a notification letting you know it's ready. To download a copy of the data you requested:

1. Go to the Available Files section of the Download Your Information tool.

2. Click Download and enter your password.”
- ☐ Be sure to place a backup copy on the cloud, and on an external HDD/SDD

Manage Applications

Remember when you gave access to AngryBirds in 2012? Do you remember turning that off? I didn't think so.

- ☐ So [go here and start sifting through Apps that have access to your photos, media, and friends](#).

YouTube Privacy






It is important in these days of angry mobs, doxxing, and creepy perverts who may prey on your children, to keep all sorts of history and tendencies hidden.

Therefore, I recommend not tracking, or at least not sharing your YouTube viewing history and channel preferences. You can change these from the Google side (what used to be Google Plus settings), but here's how in YouTube:

Open your YT account. Select the Menu button on the right, and "Manage your Google Account"

- ☐ [Open your Data and Privacy Personalization](#)
- ☐ Switch off all sharing options (see below)
- ☐ Take the [Privacy Checkup](#)
- ☐ [Open People and Sharing](#) to ensure you are not visible through other means.
- ☐ [Go to AboutMe to choose what people see](#) about you on Google and lock everything up.













Manage your Google Account

-  Your channel
-  Paid memberships
-  YouTube Studio (beta)
-  Switch account >
-  Sign out

Activity controls

You can choose to save your activity for better personalization across Google. Turn on or pause these settings at any time.




 Web & App Activity	 Paused	>
 Location History	 Paused	>
 Voice & Audio Activity	 Paused	>
 Device Information	 Paused	>
 YouTube Search History	 Paused	>
 YouTube Watch History	 Paused	>

[Manage your activity controls](#)

- ☐ Take the time to Manage or download, etc. your Google Data while you are here.


Ad personalization

You can make ads more useful to you



Ad personalization


Ads Google shows you are personalized

 On

[Go to ad settings](#)

Account storage




Your account storage is shared across Google services, like Gmail and Photos



0% used – 0 GB of 15 GB

[Manage storage](#)

Download, delete, or make a plan for your data

	<p>Download your data</p> <p>Make a copy of your data to use it with another account or service</p>	>
	<p>Make a plan for your account</p> <p>Use Inactive Account Manager to plan what happens to your data if you stop using your account</p>	>
	<p>Delete a service or your account</p> <p>You can do this if you no longer use a service or your account</p>	>

- ❑ You can , lastly, [set up a Google Alert](#) to keep you in the look about changes to your identity online.

Google Maps

It is highly recommended that you either [turn off your Google Maps Tracking/Location History](#)...

- ❑ First, go to [myaccount.google.com/privacycheckup](#). This is a good page to bookmark, since it gives you granular control over lots of privacy settings.
- ❑ Next, scroll down to “Location History” and choose “Manage Location History.”
- ❑ This is where you’ll see everywhere you’ve been. It’s a freaky level of detail.
- ❑ Tap “Manage Location History” at the bottom of the screen again.
- ❑ Toggle the button to turn off Location History.

Or change the settings to where it [deletes tracking history after 3 months](#)...

- ❑ Open Google Maps on iPhone or Android.
- ❑ Tap the menu bar on the top-left of the app.
- ❑ Choose “Your Timeline.”
- ❑ Tap the three dots on the top-right of the screen.
- ❑ Choose “Settings and privacy.”
- ❑ Select “Automatically delete location history.”
- ❑ Change the setting from “Keep until I delete manually” to “Keep for 18 months” or “Keep for 3 months.”

Securing Webpages

If you are the owner of a WordPress or Joomla site, or some other custom built site that is not run by Wix or another template provider, you will need to install backdoor entry and services to get in. I personally hire a trustworthy *wizard* I found on Fiverr.com, who has done work on several sites for me, very cheaply, very fast. He has always provided screenshots of work and fixed problems with my website. He locks it down, and it's worth every penny. But at a very minimum, with the way attacks happen these days, I must recommend two things:

1. Regular Backup by website manager
2. Regular Updates to the Wordpress (or other) theme.

If you do have a template based website, consider your login details. With Wix, my websites are accessed with the Google or Facebook passports, which saves me a lot of worry about passwords and 2 factor authentication.

Those who are security savvy will find this section tedious, but I suspect **most** small business owners, after they get a website, do not think about it, or its security for years. Locally, a small-time professional baseball league had a website that was taken over by pornography, so that when you visited, you immediately had porn on your phone or screen. That would be professionally embarrassing, and for a league trying to attract fans, probably a career ender. No players or coaches will want to be associated with smutting kids in the face.

Cloud Backup

The backup of your fields and personal data, is extremely important. Never has it been easier, or more dangerous. While in the old days removable media could be lost, broken, stolen, or burned up in a fire, and had to be duplicated multiple times, it was, at least, not ransomable by hackers. Nowadays, your cloud account has to be protected via multiple ways. For one thing, Dropbox is not considered a very secure account, though it is passable for most applications/uses. This article will explain to you the best cloud services⁴, by security: <https://www.tenorshare.com/top/top-secure-cloud-storage.html>

Although Dropbox is listed at the top, that is because it is so popular and easy to use. But realistically, it is not known for security. Nor is Google Sync. Instead, choose those services as your primary two backup centers for data which does not absolutely require encrypted backup. But pCloud has an advantage of being both encrypted, and with Military deep encryption available, and of working directly with your Facebook, Instagram, Google Drive, OneDrive (Microsoft), and Gmail to backup. In the future it will probably work with other services as well. It also comes with a public folder, which can be used to give open access or even host HTML based websites. This was a feature DropBox had, and got rid of, to their detriment. That's when they lost me as a client. Now my only reason for a DropBox account is people sharing something to me.

- ❑ NEW!: try out [Google Drive File Streaming](#), instead of the online suite or [Backup Drive](#) tool.
- ❑ Alternative: [Microsoft OneDrive](#) comes standard in many computers. I do not use it, and I do not trust it (no more or less than Google) the same way I do not trust the [Apple iCloud](#). But while I have utility loyalty to Google Drive, it is understandable many are leaving the app. So these other big services may hold answers for you.

⁴ Interestingly enough there are other companies which create cloud-based security software for companies, and they are all different companies. <https://www.softwaretestinghelp.com/cloud-security-companies/>

Military Encryption Options

While it costs extra for pCloud to add the Military Grade Encryption, there are some cloud services which have strong encryption from the get-go. The main thing to look for is 256 bit encryption or greater or zero-knowledge options, meaning employees of the company cannot search your files, like Google or Amazon can! Sync, iDrive, MEGA, and of course pCloud offers this. But MEGA does not charge extra (being already expensive). I anticipate with the fall of some of the early encrypt cloud services in the last few years, more - and better - options will be entering the market soon with impossible to beat encryption, and competing by offering it for free.

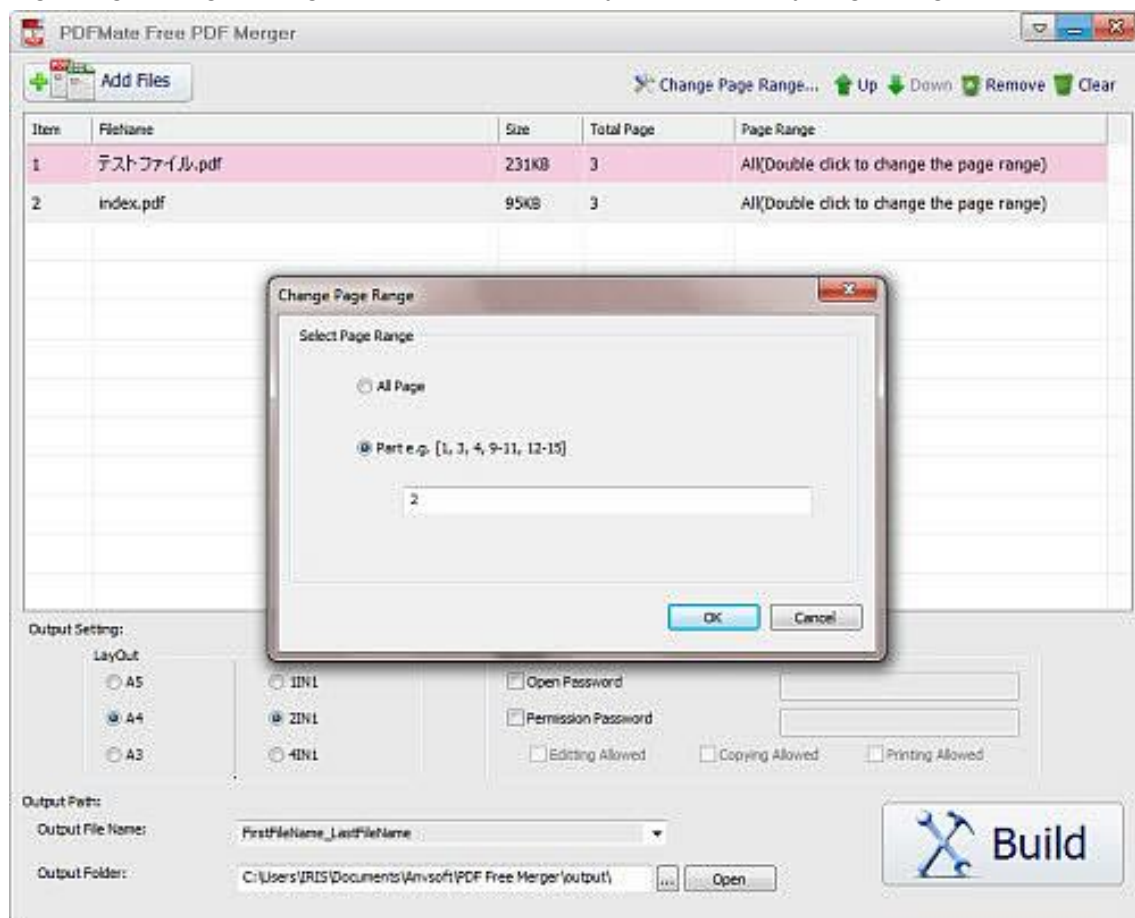
PDF Security

Although it is not as important with secure mail, there may arise a need for time to time, to have encrypted PDF. If you use Acrobat, then you can set up a Digital Signature, and [encrypt the file with Acrobat's internal password protection](#).

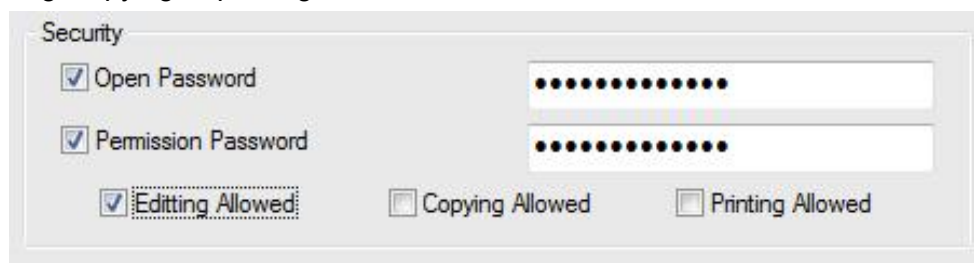
For a free method, [use this article's steps](#):

“PDFMate [Free PDF Merger](#) is an easy but powerful program for merging multiple PDF files into a single one, converting images to PDF files, split PDF pages, and encrypt PDF with new password for protection.

- ❑ Step 1. Preparation. [Download this Free PDF Encryption Software](#), install and run it.
- ❑ Step 2. Add source files. Click the button "Add PDF", and add the PDF files you want to add password. If you only want to extract some specific part of the original PDF files and encrypt, click “Change Page Range” or right click the PDF, then you can specify page ranges in the pop-up window.



- ❑ Step 3. Customize output settings. Below the file list, there is an area marked as Output Setting with which you can customize PDF output. LayOut area in this section is for defining the PDF printing paper types. You can choose to output PDF in A3, A4, and A5 style sheet. You are also able to choose output of pages with 1-in-1, 2-in-1 or even 4-in-1 arrangement. By doing so, you can print PDF in more economically and environment-friendly way, saving lots of time and sheets of paper.
- ❑ Encrypt PDF File. On the right is a Security section which allows you to set password for protecting PDF file.
 - ❑ Check Open Password, you can set password for opening PDF.
 - ❑ Check Permission Password, you can set password for either PDF processing actions like editing, copying or printing.



With these settings, you can output confidential PDF file with high security assurance. No one could read or process your PDF file without your permission.

If all options are well set and the PDF is ready for export, you can go to Output Path section.

- ❑ Step 4. Start to create and encrypt PDF. After inputting a name for your PDF file in "Output File Name" and defining the output path in "Output Folder", just click on "Build" button. Then this [Free PDF Encrypt Software](#) will do the rest for you. When conversion finished successfully, a window will pop out and show you the encrypted PDF file location."

Mobile Payment Apps

There are numerous options for mobile payment apps to replace putting in your credit card, bank, or debit account numbers. According to [this article, these are the top 6](#):

1. PayPal
2. Venmo (PayPal social)
3. Square Cash
4. Zelle
5. Google Wallet
6. Facebook Messenger

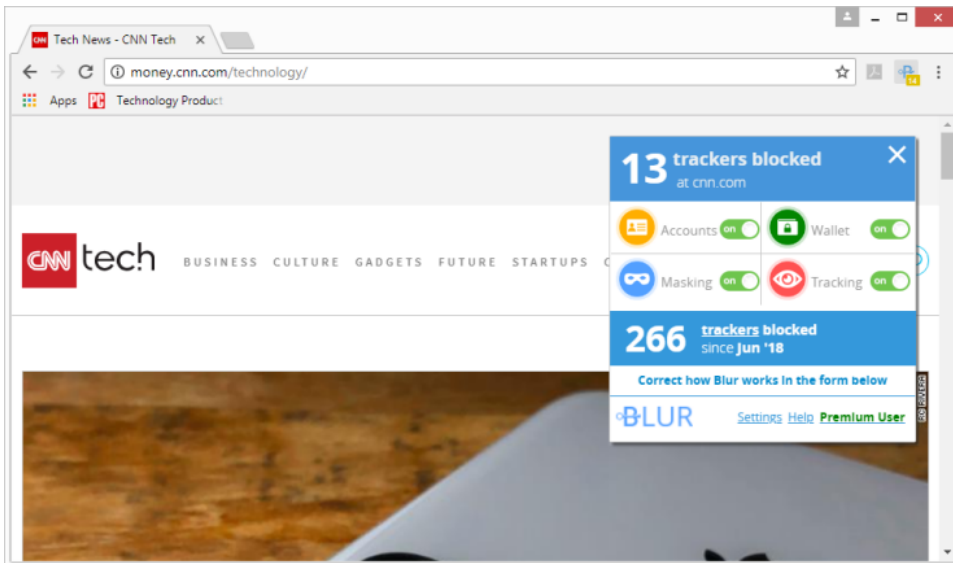
In my opinion you should shy away from the latter two, after all we are trying to secure against a hostile takeover of your life. PayPal has also been involved in some shady business both politically as well as not helping certain vendors. So Venmo, Square, or Zelle will be the optimal choices for this. [Other options](#) are Alipay and Samsung Pay, if you are unable to use these first three for any reason. Most sites will accept Square or Venmo. The goal here is to be able to stop swiping your card and inputting your personal cc# on websites. This may be a difficult transition for some, but necessary in the new Internet 3.0

Square Cash does Bitcoin transactions as well, although the exchange fee is probably very high.

When you choose one, look into their encryption standards, as well as privacy standards. The fact that PayPal tries to interfere with the legal types of businesses and has a political bias is very concerning. Try to choose a company which will not hinder you, nor spy on you, either.

Online Payment Maskers

These function similarly to payment apps. They are paid for (only use ones you pay for) services, such as [Abine Blur](#), which enables you to become an anonymous shopper, and stop giving out personal data. Even your PayPal is linked to your email and bank account. Abine Blur can also turn on Do Not Track, and look for other vulnerabilities in your shopping. It has a built in basic password manager as well. By encrypting and storing your data locally, you avoid cloud server vulnerabilities - so long as you have an anti-virus and firewall! NOTE - the free version does not include the credit card masking.



It's not perfect, and there is something you must know before you purchase the item,

"The Backup and Sync features aren't available in the free edition; premium users can also opt for local-only storage. But be warned, local storage is iffy. The FAQ states "If you have your information stored locally (i.e. you do not have Backup & Sync authorized), DO NOT CLEAR YOUR CACHE, unless you are OK with having your accounts & passwords removed. If you lose your accounts due to a cache reset, there is no way to recover those lost accounts." That's pretty dire. If you must use local-only storage, be sure to export your data frequently."

ID Fraud Protection

I am not a fraud protection analyst or expert. For myself, the protection from fraud involves five things:

1. Use of LifeLock or similar type company
2. A Credit Card company that looks out for fraud and is on your side when it happens. I chose Discover. They have excellent customer service. I will never use American Express again.
3. A bank that has fraud insurance and guarantees a return of your money.
4. The use of Experian Deep Web search and Credit Card overview
5. Searching the web myself, or using BeenVerified/similar company to scour the web for my footprint.

DeleteMe

One of the services available, for those who want a more thorough search, is something done by 'experts' at Abine Blur. For \$129/year, they will search your name across a wide list of databases that store personal identifying information and get it removed from these databases. I have not used the service, but they have [an example report here](#).

Credit Scores/Overlooking

Most people I know do not generally know what their credit scores are. There are three credit bureaus, and each of them have credit score tests (also Discover Card and others give access to these):

- ❑ [Experian](#) After you join you can get a Dark Web free deepscan.
- ❑ [Equifax](#) Comes with [Credit Freeze](#)
- ❑ [Transunion](#) You can not only freeze credit, but lock out your identity from thieves
- ❑ Your report can also be had using [CreditKarma](#) which will check Transunion and Equifax for you at the same time.
- ❑ Once a year, you can also use [AnnualCreditScore and get all 3 at once](#). Please take the time to do it now. To fix credit issues, you should create accounts with each directly to address individual report concerns. NOTE: after you see your report, you must cancel your membership within 7 days. It will ask a lot of pointed questions to establish your identity is really you.
- ❑ [LifeLock](#) can also provide credit scores, as well as provide fraud and identity protection/monitoring. It is not a free service.
- ❑ [Home Title Lock](#) can help (for a monthly or annual fee), lock up your mortgage title and deed, and protect from a Title Fraud, which could potentially cost you your property. The first time creator of the account gets a report for up to one month, and then you can cancel.

Deep Web Searches

A Deep Web or [Dark Web](#) search usually involves looking up your social security or other identity number, driver's license, and birthdate (along with name), in order to look for your information being **sold** on the web for the black market. This is kind of important. If you've ever had your vehicle registration, license, or a credit/bank statement, or even a paystub stolen, all of that information can be sold to interested buyers selling fake IDs and passports, etc. on the Dark Web at sites that people using TOR visit. When 9/11 happened, several of the terrorists had fake IDs and certain men were arrested in foreign countries when their names were mentioned by the media. As it turns out, Al Qaeda was stealing Muslims' identities from countries in Africa and the Middle East to use in America. Bear in mind that your credit card details can also be stolen at gas pumps, fast food restaurants, and all sorts of vendor sites.

- ❑ [Experian free scan](#)
- ❑ [TruthFinder](#) (pay per search)
- ❑ [BeenVerified](#)

If you have had your reputation or identity compromised in a severe way, and it is affecting your life, it might be worth [hiring a company to defend your reputation and bury attacks online](#). It is **not** always successful, so do not have unrealistic expectations. They cannot suppress dedicated social media witch hunts, or if you are a criminal, for example [if you are a sexual predator/convict and are on a searchable database](#).

CryptoCurrency Howto

The following is not an endorsement of investing advice, or investment techniques. This document cannot and should not be construed as legal or financial advice regarding the use of cryptocurrencies for investments or international currency movement, which may be involved in laundering or circumventing state and federal laws. It should be seen solely as a guide as to how to use crypto to make legal purchases, or transfer money without a payment service like PayPal, safely and securely.

Cryptocurrencies are - other than BitCoin - without underlying value. They are propped up by volume and supply vs demand. Generally their scores will follow [Google Trend](#). There have been, and will be bubbles and abuse of the platforms to both make money, and to rob people of their own investments.

At any rate, these are some good general guidelines, based on the author reviewing dozens of howto videos, and reading security articles:

- ❑ Use hard wallet - purchase these on Amazon or other websites, like direct seller
- ❑ Secondary (cloud) storage - preferably an encrypted folder
- ❑ You may use the exchange [Coinbase/GDAX \(Coinbase Pro\)](#) for BTC, ETH, LTC and other top coins
- ❑ Trade to [Bittrex](#) for top altcoins
- ❑ Be careful during ICO's to not lose your currencies to scam currencies and hype
- ❑ Use 2FA verification or push notification apps to log in and protect your online wallets and exchanges.
- ❑ Freeze coins or put the into "cold storage" if you step away from a significant investment for a long time.

To start Coinbase Pro and Bittrex accounts you will require several days to verify your identity, and the account deposits. If you have trouble, don't worry that just means people cannot easily do it in your name, either. Be patient, you will need to prove your identity with your driver's license, and then link your bank accounts. You will also need to learn from the following videos how to actually engage in [depositing to your account](#), [purchasing crypto](#), [engaging in a trade](#), and [putting into your wallet](#), or [withdrawing back to your bank account](#). Just so you know **it is safe** to post your crypto reception address/key for deposits. It will not enable anyone to withdraw from your account!

If you choose to become a crypto investor, spend 90% of your time learning, and working with small values. It is absolutely vital that you avoid bubbles and hype, and becoming one of the suckers they count on to jump in with thousands, driving the price up so that big investors and ICO pioneers can dump the currency and capitalize on the bubble, which naturally causes the price to fall. When you decide to purchase a digital wallet, protect it with encrypted restore keys stored in encrypted folders. If you get a physical wallet, keep it in a fireproof safe, as it is the only access, and there is no insurance for crypto. As such, many people freeze their crypto, but that of course eats into your profits. It is my opinion that the technology is wonderful, but the market has not come of age, and is still the wild west. It is inherently dangerous for the common person.

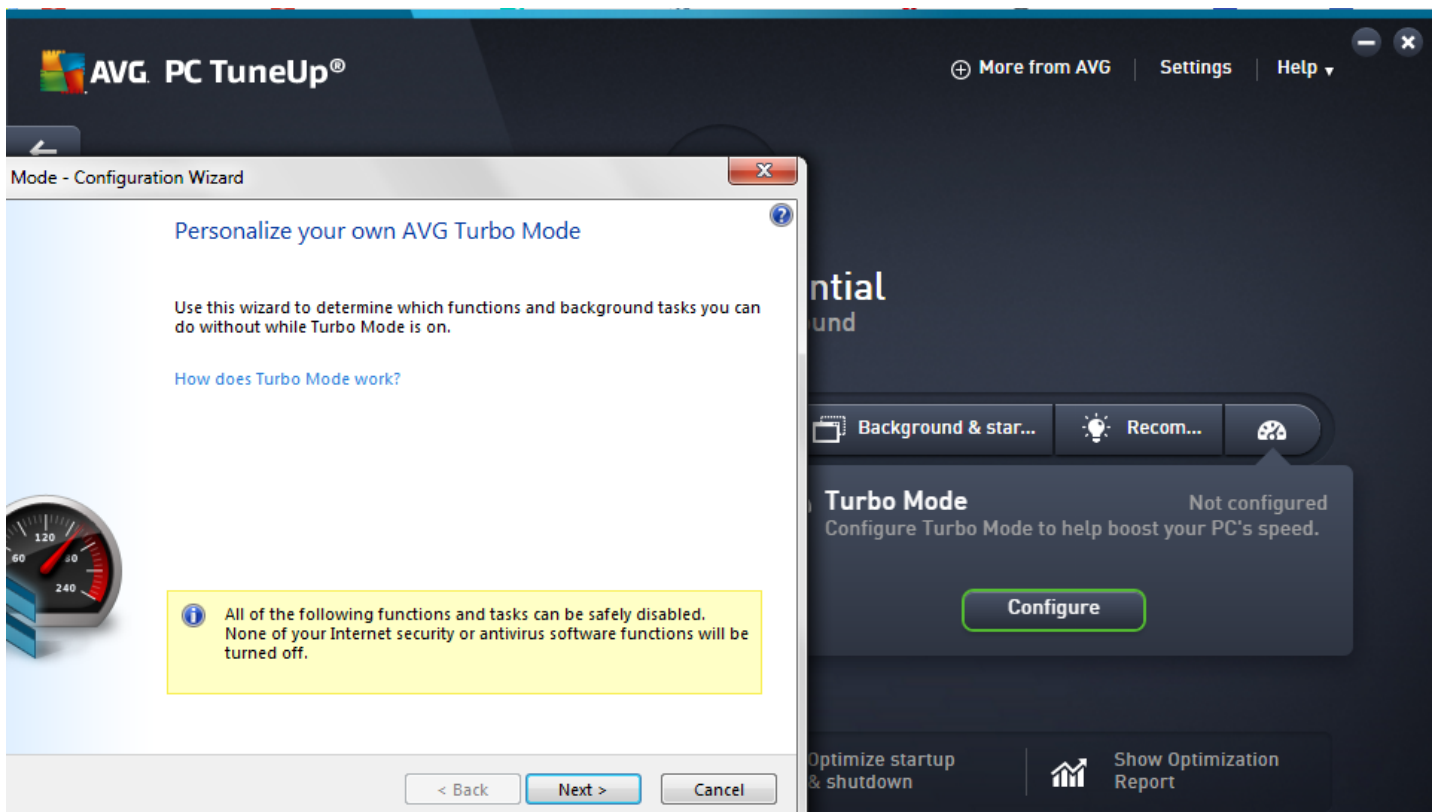
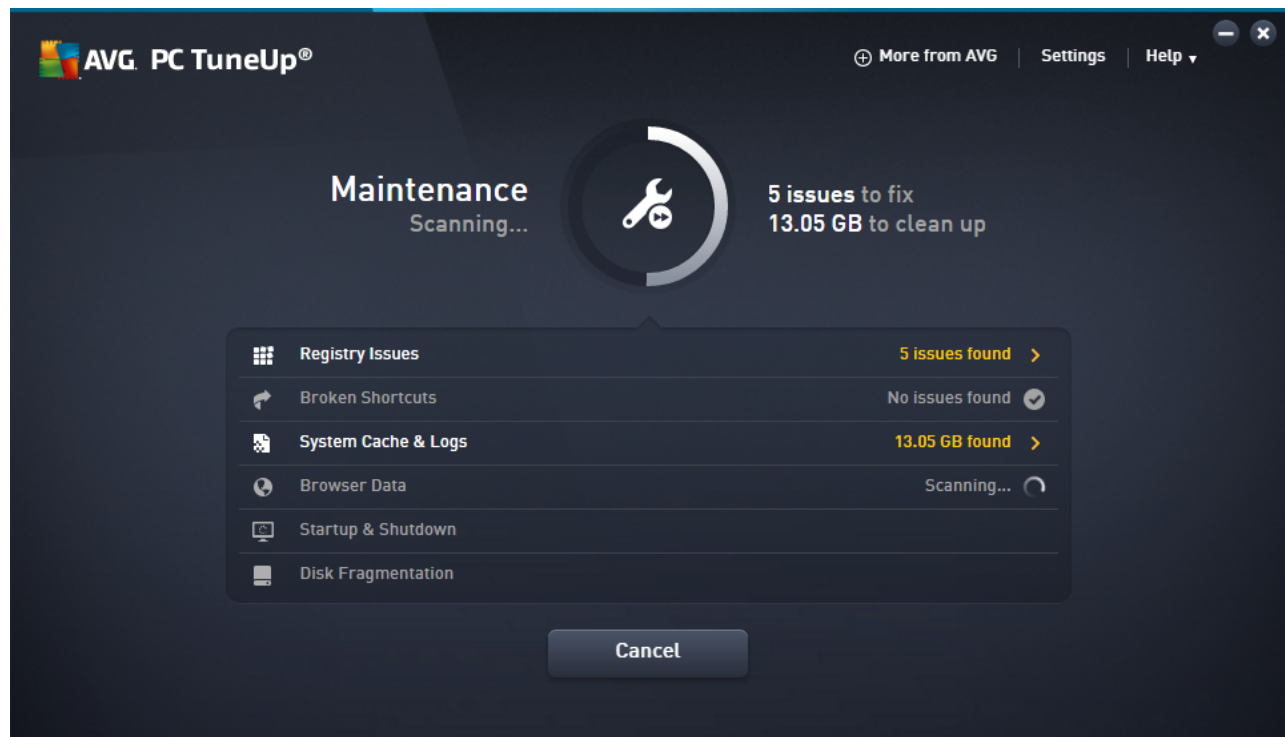
PC Tuneup Services

A PC Tuneup program searches your drivers and software installs to look for version history issues, and other regions that the computer's' performance is not optimal. My favorite program - by far - is AVG PC Tuneup⁵ because a single purchase then allows installation on any number of machines (unlimited license, for now). It is a comprehensive suite, with all the following features:


- ❑ Puts background programs to sleep (to reduce CPU load)
- ❑ Looks for duplicate files and old Windows Restore Backups
- ❑ Defrags HDD space safely
- ❑ Adjusts visual and speed performance, and overclocks certain functions (Boost)
- ❑ Checks drivers and security concerns in a single report
- ❑ Registry Scanner
- ❑ Browser Data cleanup
- ❑ Startup/Shutdown Management
- ❑ Comes with initial scan to start




⁵ If you have trouble finding it, all your AVG products are found at <https://subscriptions.avg.com/>

❏ Standard/Economy/Turbo/Flight Mode



Increase performance - details

 **AVG**
Increase performance

 Rescue Center  Change profile 

Overview

Hardware and software


Internet settings


Visual effects

The performance of your system can be optimized


There are **14 recommendations** for increasing the performance of your system. This page gives you an overview showing the parts of your system that were checked. You will find the detailed recommendations on the corresponding tab.

Hardware and software


 7 recommendations available

 Unused programs


5 recommendations

 Functions that negatively impact performance

2 recommendations

 Hardware


Optimized


 AVG services

Optimized


Details

Internet settings

 3 recommendations available

 Internet connection

Optimized


 Browser settings


3 recommendations

Details


Optimize all

Visual effects

 4 recommendations available

 Display effects

Optimized

 Animation effects

4 recommendations

Details

Optimize all

Rescue Center active

40

More from AVG
Settings
Help

←

18 programs are slowing down your PC

Safely put their background & startup services to sleep to boost speed. [How does it work?](#)

Name	Slowdown severity		Put all to sleep
Spybot - Search & Destroy	<div><div></div></div>	Ignore	<button>Sleep</button>
VMware Player	<div><div></div></div>	Ignore	<button>Sleep</button>
{034F0029-5249-4F8E-856...	<div><div></div></div>	Ignore	<button>Sleep</button>
{0469BD53-62E9-4A9B-BA...	<div><div></div></div>	Ignore	<button>Sleep</button>
Brother MFL-Pro Suite MF...	<div><div></div></div>	Ignore	<button>Sleep</button>
Intel(R) Common User Inte...	<div><div></div></div>	Ignore	<button>Sleep</button>
Adobe SVG Viewer 3.0	<div><div></div></div>	Ignore	<button>Sleep</button>
NordVPN	<div><div></div></div>	Ignore	<button>Sleep</button>

More from AVG
Settings
Help

←

Clean Up Potential

25.81 GB found

13.13 GB cleaned

System Cache & Logs

System Cache & Logs

24.23 GB found

Safely remove unnecessary junk files on your PC.

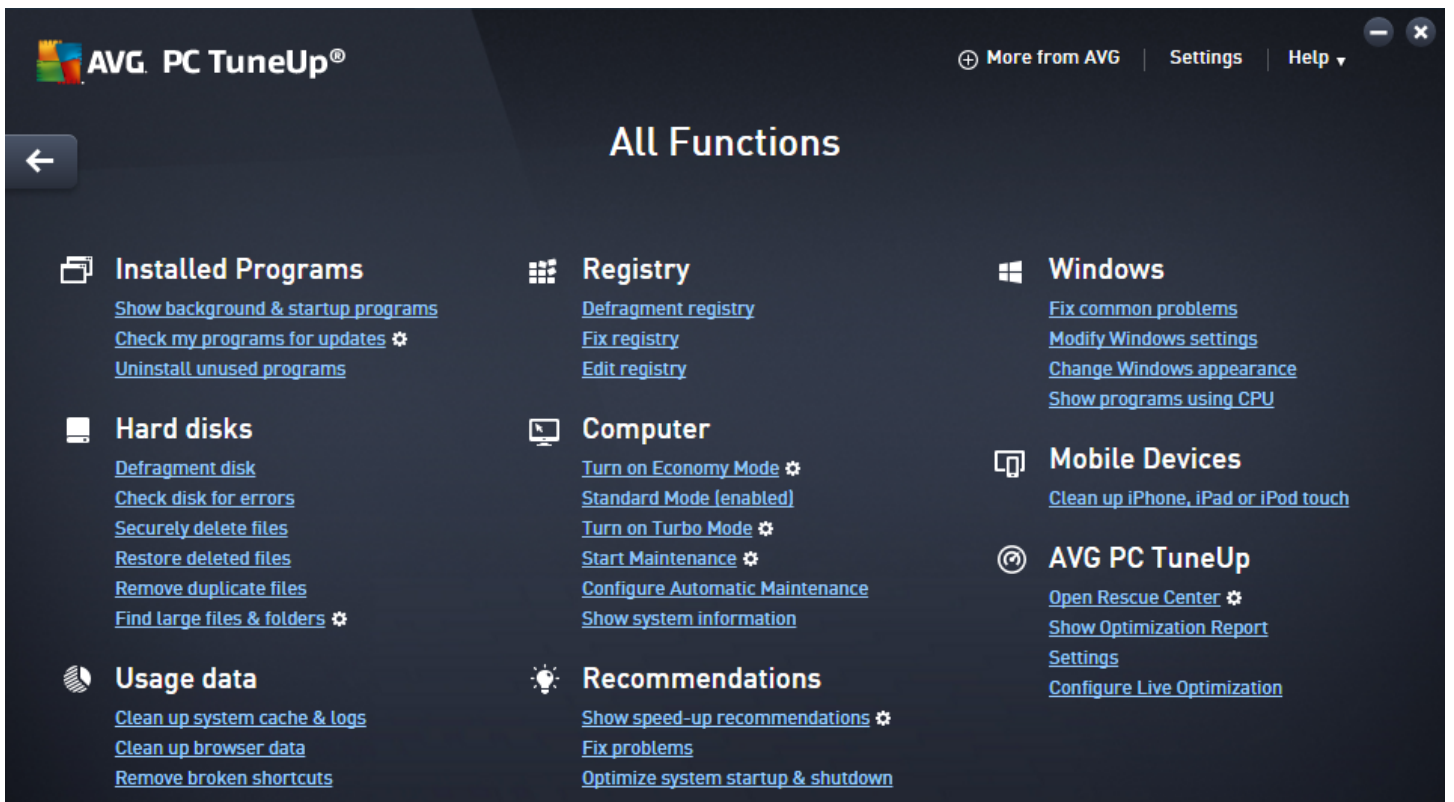
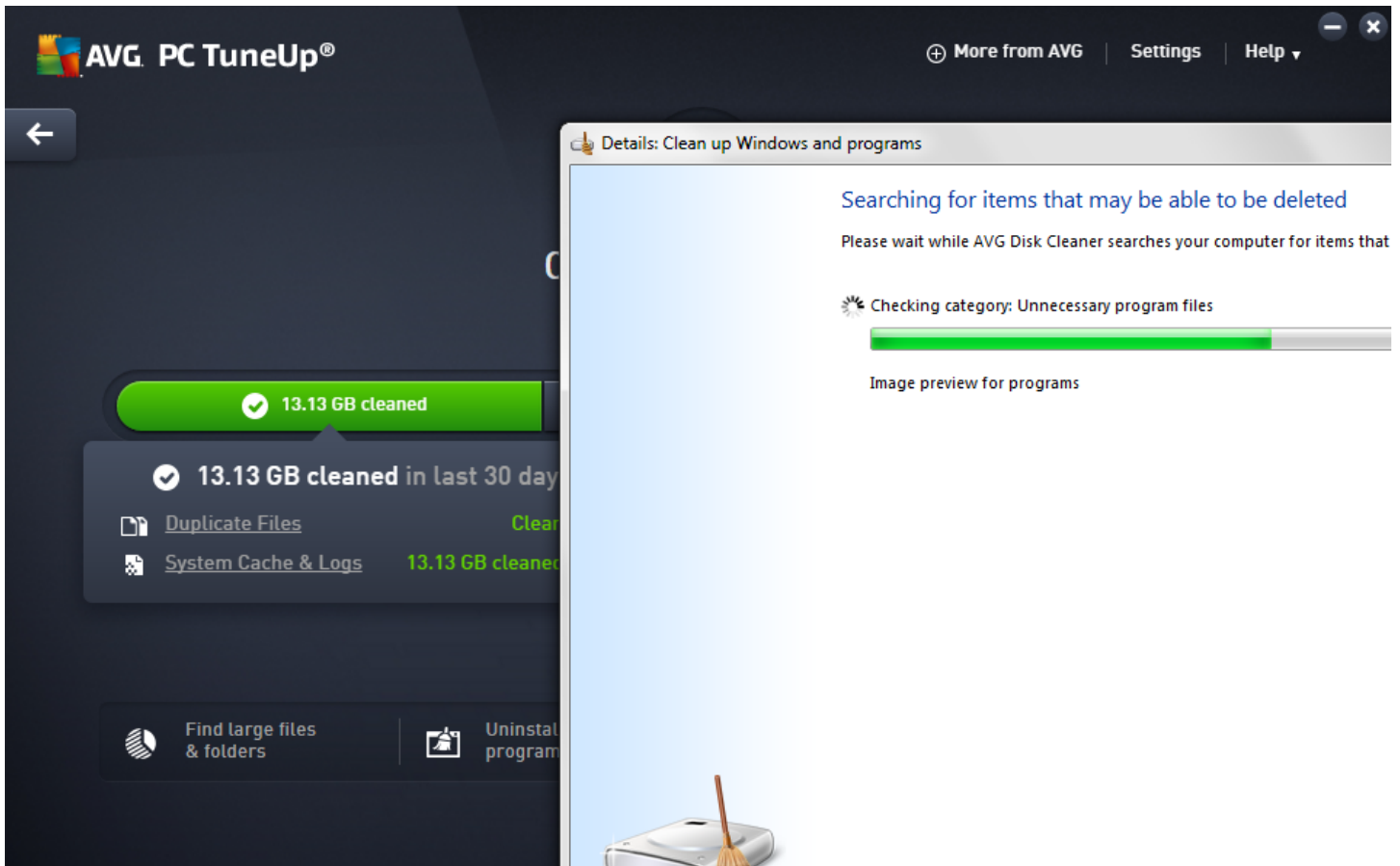
Show

Find large files & folders

Uninstall unused programs

Securely delete files

Remove broken shortcuts



More Linux Security

Read the [“Step-by-step guides on digital security tools for GNU/Linux:](#)

- ☐ [Basic security for Linux](#)
- ☐ [KeePassXC for Linux - Secure password manager](#)
- ☐ [VeraCrypt for Linux - Secure file storage](#)
- ☐ [Firefox and Security Add-Ons for Linux - Secure Web Browser](#)
- ☐ [Thunderbird, Enigmail and OpenPGP for Linux - Secure Email](#)
- ☐ [Tor Browser for Linux - Online anonymity and circumvention](#)
- ☐ [\[Unmaintained\] Jitsi for Linux - Secure instant messaging and VoIP”](#)

Remote PC Management (for the average person)

From time to time, it might be handy to quickly remote into one of your PCs, perhaps from your phone or laptop/chromebook. In the past that was the work of an IT or Tech Support guru. But today just about anyone could use this now with the free program [TeamViewer](#) to safely remote in, and transfer files, run updates, and perform security checks.

It is fairly self explanatory, however, here is an article regarding keeping your TeamViewer secure:

<https://www.howtogeek.com/257376/how-to-lock-down-teamviewer-for-more-secure-remote-access/>

- ☐ Exit the program (SysTray) when you are done using it
 - ☐ Turn off automatic startup
- ☐ Use SSL compatible password
- ☐ Turn on 2FA verification
 - ☐ Print or email to your secure mail the keycode to deactivate
- ☐ Keep it up to date
- ☐ Extra Personal passwords
- ☐ Enable/Assign Whitelists to specific accounts
- ☐ Set up granular login (very advanced) and limited user accounts
- ☐ Secure the Administrator Privileges and lockout changes from standard users

Other options for remote desktop winclude [Windows Remote Desktop](#) and [Chrome Remote Desktop](#) programs, and [Splashtop](#).

Steganography

This is an extra encryption technique which hides data - perhaps a text, PDF, or another image - inside a photo. While steganography won't fool the NSA, it will efficiently hide data from thieves, snoops, and most law enforcement (but not digital forensic specialists). For this you need three things:

- ☐ A steganography program [which is both free and reliable](#) (your friend will need the same program)
- ☐ A master password to share that is also strong

- ❑ An image which is neither so blasé that it is immediately suspicious, and yet not anything that begs attention. Classically a family photo, a very distracting pornographic photo, a beautiful and typical to keep nature photo, or a picture of a famous cityscape you'd like to visit, are ways to "hide in plain sight."
- ❑ Alternatively, you can use an audio or video file.

[This article is all about steganography](#), [this one all about their security concerns](#), and [this site is a step by step howto](#) for the [best programs](#) (and [this one for Linux users](#)). [This article has the history, etc.](#)

Disk Wiping

Most people think that formatting their computer will erase data, but actually it won't. Even using [Parted Magic](#) won't stop a true forensics specialist from getting data. But, generally speaking, the program will truly erase everything, because it will literally put 0's on every sector of the disk drive. There is a [bootable version from USB](#) to use to replicate the program's work, as well, and there is a Linux version, too.

Alternatively there are a few programs, such as [Ccleaner](#) and [Eraser](#), which are both out of date options, which may still work (especially for older Windows).

Download My Package

This entire thing is optional. But I keep a software folder, and for this paper I will keep a one stop shop collection of the latest programs I have installed. Whether or not this paper has been updated, the folder will have the latest versions I have downloaded, saved in one .zip file you can get. They will all be checked using VirusTotal, but you also can, and should, run that check yourself.

- ❑ [Shifu's .zip collection](#)⁶; link: <http://bit.ly/2WgAzch>

The screenshot shows a VirusTotal scan interface. At the top, the URL being scanned is https://drive.google.com/open?id=1_0nm_8iv2ppJeZm6kckarmQATcWGO9o8. The status is "200" and the content type is "text/html; charset=utf-8". The scan was performed on 2019-07-06 at 21:45:32 UTC. A green circle with the number "0" indicates no engines detected the URL as malicious. Below this, a table shows the results from various antivirus engines:

Engine	Result
ADMINUSLabs	Clean
AlienVault	Clean
Avira (no cloud)	Clean
AegisLab WebGuard	Clean
Antiy-AVL	Clean
BADWARE.INFO	Clean

Scan: <http://bit.ly/2Yv0otp>

You can utilize the extensions my firm recommends by going to this short document: <https://bit.ly/31XSSLG>

⁶ Again, I do not own the copyrights, I am simply putting all of them into a single download. You can download these tools individually, and if you don't trust the .zip, great! It's just an option of convenience.