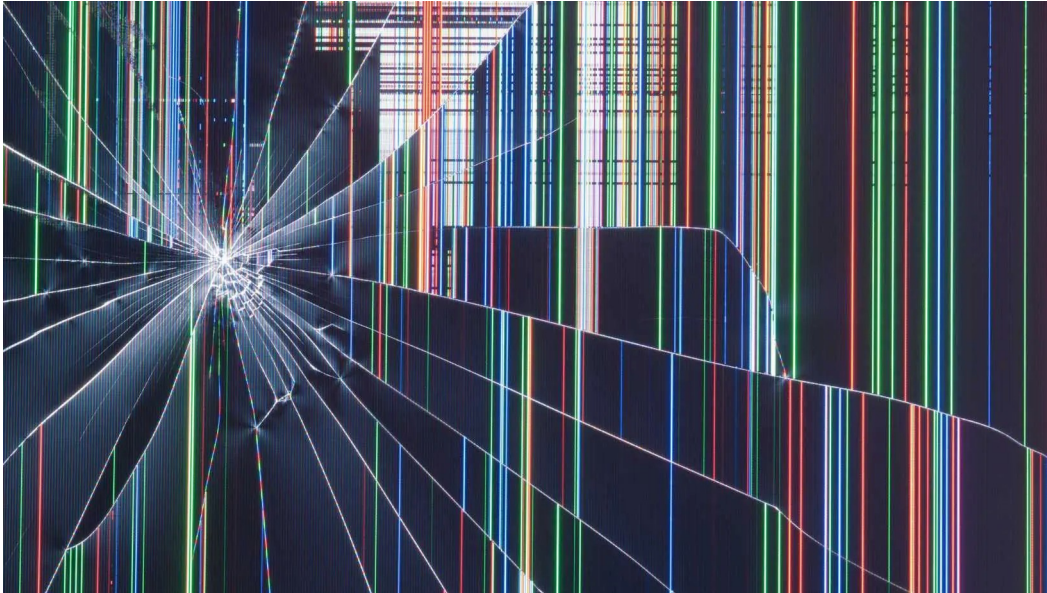




A Beginner's Guide: Control Your Technology

Ways to reduce device from hijacking:

Random Weirdo: Question "if you have nothing to hide, then why worry?"

Subtle Substance: Answer "If you have nothing to hide, why worry about using doors and windows in your home?"

Speaking of windows, it is probably unreasonable to suddenly tell people to change their dear beloved MS Windows or Apple operating system to Linux since even I have only been using Linux for only 4 years, and I know that feeling of comfort of already having something in front of you rather than thinking of something else. So I won't be doing that here, maybe. I am aware most prefer comfort over change. Below are the listed things you need minimally if you intend to be "private" using your own Windows or Apple device --mostly Windows in 2026.

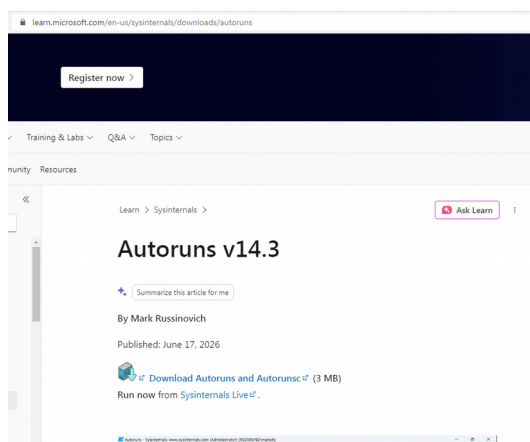
Overall, know that the twinkling promise of "no government will be able to breach your technological privacy and security" is very scarce. If a State actor is determined enough to tag you, there are slim chances of getting away since they have not just the monies to develop the technology, but to also hire the most robotic single track minded smart people to accomplish their intent.

1. PC Protection

Don't Use Admin Account on the PC: If you are an admin user, the malware has admin privileges. Straight forward, so do not use admin user account on your PC, so the malware will hit a UAC prompt (This is the little panel box that pops up to request password in order for permission to be granted) requesting permission to run and it dies there as you will say “no”.

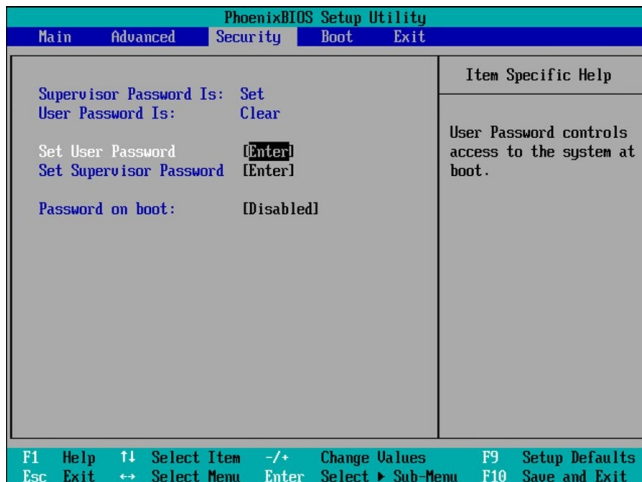


Start Up : Find apps that has already been there that runs when PC starts. Scheduled task, registry, startup folder, root are locations of usual suspects. Get the app “Autoruns” from Microsoft sys internal suit. Open it in admin and look at the pink (no digital signature) or yellow (missen) highlight, find the “scheduled” or “Logon” tab and find anything that appears off. If you see “update” or “helper” it runs from temp folder which is a massive red flag. Real software lives in “Program” file or “User” folder. Right click on it and check virus total



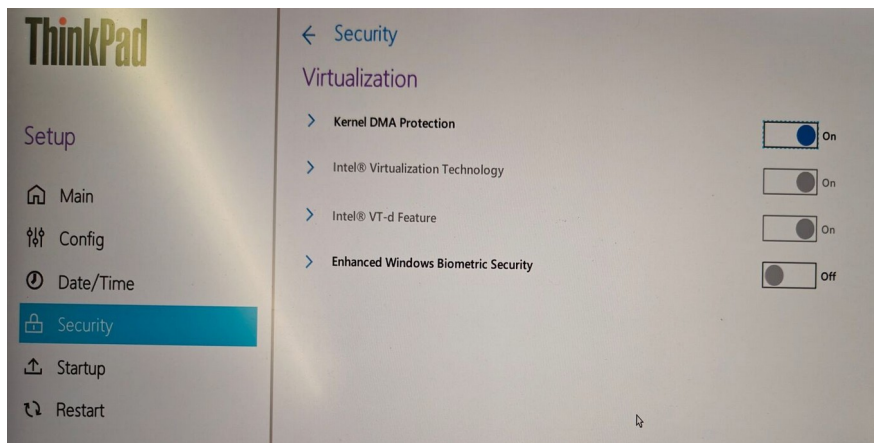
VirusTotal: Delete anything that the Autoruns app reveals as bs.

Enable password for BIOS UEFI: Prevent anyone from booting specialized mess into your device if they physically possess your device if you leave it for any moment. It locks the boot order, preventing the hijack before it starts.



Enable Secured Boot: First line of defense against boot kits. Each laptop model differs on how this is done. Just spam F12, F2, Del, F10, or F100 to start up and it will take you to the Boot Settings. In some devices you may hold down "Fn" and something else. Find what yours requires to access Boot menu

Enable Kernel DMA Protection: Prevents malicious hardware implants from reading encryption keys from memory; it ensures you are the one who manages these requests. A barrier from ports to your information. Ports are basically doors used to accept addresses/websites. It works both ways, not just you going through them to search for a nose hair twizzler. These same doors can be used to access your device. Some devices require you to restart them and tap the aforementioned keys, go under BIOS or Advanced, or Security and enable it. Each laptop's look will differ.



Use already embedded securities: Windows Browwer Control> Exploit Protection> Enable All. It performs check from indirect call instructions that people use to load your computer with their own program

ASR Rule Defend (Words with Win 10 above): Go to GitHub and get “Configure Defender”, set it to ‘high’. It block behaviors exclusively used for malware like powershell scripts “it enabled ASR attack reduction rules”. Only you can launch cmd and powershell, no one else can do so behind you, these are required to attack a system using ASR.

github.com/AndyFul/ConfigureDefender

File	Update	Time
README.md	Update README.md	10 months ago
What_is_new.txt	Update What_is_new.txt	10 months ago

README License

ConfigureDefender stable version 4.1.0.0 - December 2025

<https://github.com/AndyFul/ConfigureDefender/raw/master/ConfigureDefender.exe>

Overview

ConfigureDefender is a small utility for configuring Windows 10/11 (and Windows Server) built-in Defender Anti-Virus settings. It is a part of the Hard_Configurator project (including source files), but it can be used as a standalone application (portable).

ConfigureDefender sources

Releases
No releases published

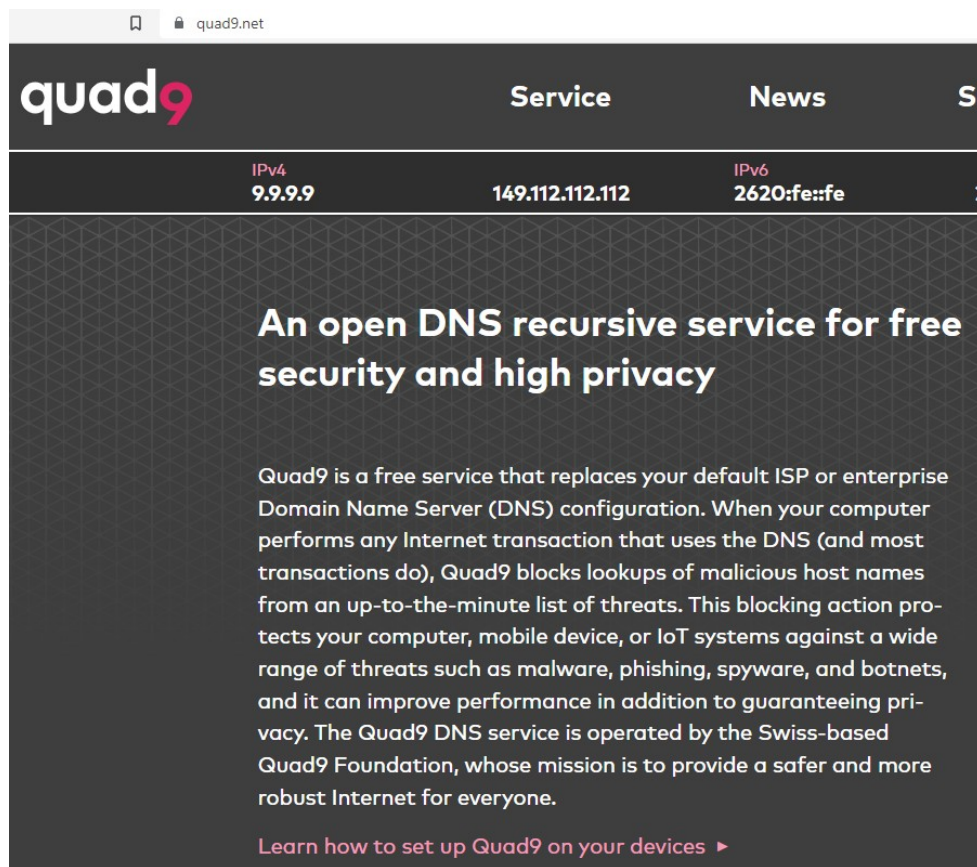
Contributors 1
AndyFul

Disable Telemetry and Background Services in Windows: Use “Chris Titus Tech’s Windows Utility”.

VBS and Core isolation (Win 10 above): Windows> Device Security> Core Isolation. Each device that runs will be verified and isolated in a bubble so that infections don’t affect other parts from one part.

2. Network Protection:

Change DNS to Quad9: It prevents spoofing and interception of domains. A nonprofit organization that specializes in threat security each time you connect to a domain, the double check it with a global base of malware command control serves, if it is bad, then it won't connect. Note that this is not a VPN. It does not hide or encrypt IP like a VPN, it does not change location appearance of device. All it does is block malicious and phishing sites and software as you browse.



Enable DNS over HTTPS: Windows Setting> Networks and internet> Ethernet and Wifi> DNS Setting> Set to Manual> Turn On DNS HTTPS. Prevents an intruder over a network from. DNS is wrapped in TLS encryption. ISP cannot see what domain you look and hackers cannot post up on DNS for high-jack.

Better Firewall (Outgoing and Incoming): Install SimpleWall, nothing happens until you say “yes”

3. Physical protection:

Prevent remote access Trojan via physical high jack or remote: It takes seconds for usb to download remote access Trojan. When moving away from your device it can be hijacked via a “rubber ducky”. Prevent this by running via windows “Run” program “gpedit.msc”> “Device Installation Restrictions”> Enable “Prevent Installation of device not described by other policy...”> “Enable”. Windows will refuse to install a new driver that attempts to enter via usb or external device It freezes the OS. You disable it when you are intentionally adding a new hardware like your own recognized mouse, keyboard, new usb etc.

Protect your USB from fake ports that download bs: Use USB condom. Seriously, this is actually a thing. It is called “PortaPow Data blocker”. It prevents data transfer which most usb can do, so there is no threat of downloading bs. To the untrained eyes (unless you are superman that can see the thermal images or have a tool that shows it) these days, there are regular looking usb in any place, or that yours can be replaced by which has wifi access, download and upload capacity and tracking means on that small space you plug into a charger or your laptop or your phone. **Use usb condom. Especially when in public spaces, airports etc.**



4. Browsing Risks and Exploitation:

Cookie tracking: Use browser isolation for sets of internet activities to prevent cross site tracking via tabs and cookies.

Script blocking: Most browsing hacks use Javascript, “NoScript” blocks all script. Note that you will have to allow script one at a time only on websites you like. It prevents drive by downloads and cross site scripting used to track and attack

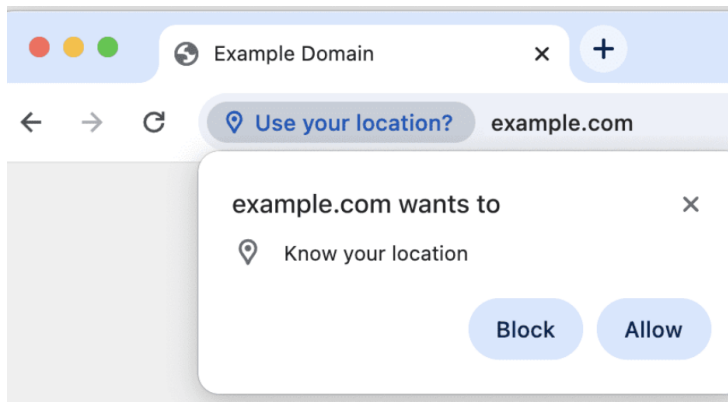


Delete cookies: This is how hijackers by pass your 2FA AND PASSWORDS because cookies store login credentials that “trusts” the device by adding cookies into the browser. Downside to this is you may need to continuously manually login to each page.

Use browser isolation: Have 3 different browsers (LibreWolf, Waterfox, Chrome). use chrome for all Youtube/Google related stuff. Librewolf for emails and work. Waterfox for anything else like banking, online shopping etc. Each tab you have on your window or phone browser right now as you read this is sharing data from all the other tabs, 3 or 60 of tabs. With browser isolation, each browser cannot see what the other browser is doing. So if you have an online banking tab open on the same browser while your beloved shopping website is opened on another tab, those two tabs are sharing data and activities of what is going on

within each of them. If only people knew how creepy the internet have gotten since the late 1900s.

VPN vs. Location Permission: Just as contact tracing is done with social media contact uploads and Flocks, Axon, and Leonardo's SignalTrace use mesh network to know you intimately, and just as how even if you use software Wifi, anyone connecting to your router who is not on Wifi attached VPN will reveal your location. The same applies to the use of VPN and something called "browser fingerprint". One of the main benefits of using VPN as most probably know by now is that it clouds your IP Address by sharing ports with many more people using the same IP Address. Assuming that the host of that VPN is not keeping a log of your data which is subject to subpoena, whenever you use a browser, always **disable the "location"**. **It is a slick widget box that shows up near the search bar that says "___wants to know your location 'Accept, Deny" or "Enable", "Disable", "Allow", "Deny". Never grant it, ever.**



Even if you use a VPN, the moment you grant this, a browser fingerprint of your location is leaked. Better yet, use browsers that block these from the get go like Waterfox, Librewolf, or go to GitHub and find a version of Chromium that has all telemetries removed.

A note to consider: Even when all these are done on Apple and Windows, the Operating System company itself then becomes your threat. They collect all your data in real time. Also, some of these methods may be a tad bit too controlling and too strong, so depending on how much control you desire, you may want some of these and not so much the other. If you are the type that does crypto on your devices *erhHh HhEem* you need all of them. You are a prime target, a sitting duck.

MS Windows will soon want you to upload an ID in order for you to use the OS. Linux from its inception, was privacy based and does not care for this.

MS Windows will continue to release different operating system and stop security updates for old ones, effectively forcing the obsolete versions to leave your life in the realm of technology vulnerable. Linux does not do this.

MS Windows forces "updates" on you without you having any option or say so in whether what is downloaded on your devices helps you or not. Linux does not require this.

MS Windows does not support security updates for anything below Windows 11. Linux does not have any of this mess.

MS Windows sells your "user data" to other big corps. Linux does not.

MS Windows is closed source, meaning you cannot inspect the origin of what you are using and depends on. Linux is open source, the opposite of that.

MS Windows cost you about \$200 minimally besides OneDrive, Office Suite etc. Linux cost you \$0.

MS Windows has trash customization to your taste. It locks you into a standard Windows shell.

Linux has endless personalization and customization.

MS Windows wears down your device. Linux is light weight and fast.

...and more.

I mean, the advantages are just too vast and it makes you wonder why anyone would even give a f*ck about MS Windows. The issue persists that in real life, would you give a f*ck about someone who treats you like sh*t and spit on your face? Likely not, unless there are other deficiencies and virus up there in that personal CPU of the individual.

Do not throw the baby out with the bath water. Keep your Windows devices, it has its use (You can use it as a home server when and if you learn the necessities of such with running your own Local Agent LLM and some more such as hostings of services or local storage with your own cloud/remote access by you attached to it). If you want to be free over the next few years with a device

you wake up and sleep with, which probably spends more time in your own house than you do, then consider Linux.

If all those seem like much to you, just for the basic right to privacy and security, then just start with Zorin OS (a type of Linux), it is the easiest to switch to for those coming from Apple devices and Windows. I may do a step by step of how to do so, along with caveats on what makes it all a smooth easy transition, but there are many videos already online on just that.

Either way, I think slowly doing so is the best way via dual boot where you keep your old operating system while also having some form of Linux on the same device. Better yet a dedicate a completely separate device to Linux used for private activities like email, work, banking etc, and use the other operating system just for other things like video editing, since starting anew with Linux may require some acclimation.

No it requires no special command line stuff you see in movies, especially if using Zorin or Ubuntu(Don't get Arch Linux yet if you are starting off, ease into it). It is quicker, easier, and already has all those mechanisms above mentioned for privacy and security embedded from the start without you worrying about them or how to configure the security and privacy aspects.

I am no computer guy, but if you use computers, I think minimally the onus is on you to know how they work, just like anything else you are involved in.

That is a basic summary right there. Put them to use if you do not want to change computer operating systems.

On the other hand, whether or not you realize, Linux is the OS for doing special things you see in movies that some character sitting in a hoodie in a dark room with a green and black terminal in front of him loading data. The moment you begin to use Linux, you are closer to it than you think -- if you have the patience to learn about it. Heck most servers on Earth run on Linux, including the space program. Think about that for a moment as to how powerful and important it is.

Can Linux still be hijacked? Yup, **anything can**. But, the default state of Linux is 1000% better than Windows. Windows even go as far as to place a key logger and screen recorder called "CoPilot" on your device now. The data collected by this slop AI you never asked for is shared with the government.

On the note of governmental entities hiring private corporations to harm people as an attempt to subvert the Constitution:

officials into the private sphere. Norms such as due process and freedom of speech do not regularly apply against private parties, except perhaps where the parties have agreed to observe them through private contracts and other devices of private ordering. Insofar as section 1983 litigation subjects some private defendants to public norms, the domain of these norms will tend to increase, perhaps ultimately spilling over into private contexts that are not subject to section 1983 litigation. This is especially relevant in the privatization context, in which private parties (such as the operators of a private prison) may be subject to section 1983 liability because they perform a government function.

West v. Atkins, 487 U.S. 42 (1988)

(a) If a defendant's alleged infringement of the plaintiff's constitutional rights satisfies the state action requirement of the Fourteenth Amendment, the defendant's conduct also constitutes action "under color of state law" for § 1983's purposes, since it is "fairly attributable to the State." *Lugar v. Edmondson Oil Co.*, **457 U. S. 922**, **457 U. S. 935**, **457 U. S. 937**. Thus, a state employee generally acts under color of state law when, while performing in his official capacity or exercising his official responsibilities, he abuses the position given to him by the State. *Polk County v. Dodson*, **454 U. S. 312**, distinguished. Pp. 487 U. S. 49-50.

(b) The Court of Appeals erred in concluding that defendants are removed from § 1983's purview if they are professionals acting in accordance with professional discretion and judgment, and that professionals may be liable under § 1983 only if exercising custodial or supervisory authority. The court's analogy between respondent and the public defender in *Polk County, supra*, is unpersuasive. Pp. 487 U. S. 50-54.

Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974)

of any greater connection here.

Petitioner next urges that state action is present because respondent provides an essential public service required to be supplied on a reasonably continuous basis by Pa.Stat.Ann., Tit. 66, § 1171 (1959), and hence performs a "public function." We have, of course, found state action present in the exercise by a private entity of powers traditionally exclusively reserved to the State. See, e.g., *Nixon v. Condon*, 286 U. S. 73 (1932) (election); *Terry v. Adams*, 345 U. S. 461 (1953) (election); *Marsh v. Alabama*, 326 U. S. 501 (1946) (company town); *Evans v. Newton*, 382 U. S. 296 (1966) (municipal park). If

Page 419 U.S. 353

The issue is that as time goes on and tech advances, the ability for us to use it and enjoy it is paired with being serfs. That is done either via (1) impeding your right to repair what you own, thereby turning you into a cash cow and wasting resources; (2) the technology limits your activities if certain actions are not performed such as embedding your intimate nature into it by attaching an ID to a hardware and a software, disclosing your financial health and medical health as prerequisites for using technological devices, or not being able to use specific applications unless you follow along with the crowd falling off a societal cliff; (c) the technology will "see what you see" and "hear what you hear" (Microsoft Co Pilot Agent AI) according to Microsoft AI CEO Mustafa Suleyman during an interview.

We ought to all strive for a life and a future where we enjoy technological advancement without some representatives of big entities using that attractive essence to enslave people. Once more, retain windows, as some programs are not native to Linux and may not run on it such as Adobe -- although new open source apps that does the same are now available--, but in the meantime, find alternative apps that can be used. I won't list them here, that is for you to find and get yourselves involved in. Take the steps to free yourself. Enough of waiting for others to hand us things. It was what got us here in the first instance.

One may even go as far as to say that a superior alternative to all the aforementioned is:

1. Use Linux OS for personal and intimate things in life which you have the right to privacy and security to.
2. Run Windows via a Virtual machine within it for typical nonsense.

Reap the benefit of both at the same time while sand-boxing the bs and its risks.

Done.

Just think about it for now with one thing in mind: Technology will be and has been for the past 5 years or so, the main medium of serfdom, but solutions exists that frees you completely from that.

Just keep that in mind.

Alright bye bye.

