“Friendly Neighborhood IT Guy”

– ON SCHOFIELD BARRACKS –

8+ years IT experience, and privacy and security enthusiast!

DIY Guide – Jet speed + Privacy and security suite

Required materials:

x2 USB Drives – one that can be wiped and one to back up your stuff – At least 8gb and more for your back up. I don’t recommend buying one off of amazon, either buy one from a reputable manufacturer or go to Best buy.
https://www.bestbuy.com/site/pny-128gb-turbo-attache-4-usb-3-0-flash-drive-black/3198009.p?skuId=3198009
x1 iFix it kit https://www.amazon.com/iFixit-Pro-Tech-Toolkit-Electronics/dp/B01GF0KV6G
x1 Canned air – even better get a hand held blower that can clean out your computer
https://www.amazon.com/Compressed-Electric-Computer-Replaces-Electronics/dp/B09KKN4T3N
x1 Computer + Charger

This guide assumes that you’re using Windows 10/11 and you’d like to continue to use it. The steps will be similar if you decide on a Linux distribution with some quirks here and there. If you’re already using Linux, good job! For linux users check out this link and utilize the alternatives, do that and you probably won’t need me. https://www.privacytools.io/
Keep in mind that this guide, while it will assist in keeping your computer more secure… there is no substitute for safe and security conscious browsing. See here for the bare minimum: https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221

“The solution to government surveillance is to encrypt everything” — Eric Schmidt

1. Back up everything you want to keep.

2. If you’re upgrading your computer with new storage (hopefully a solid state drive) do this step after steps 3-8. Get your iFix it kit or something similar. Find a how to video on your computer model that will teach you how to open it up. Watch it so you don’t damage your computer. ← Particularly if you have a laptop. Turn it off and open your computer. With your handheld electric blow or canned air clean it out.

3. Close it up and bust out the Lysol wipes and clean your computer.

4. Take your blank usb and plug it into your computer.
Go here: https://www.microsoft.com/en-us/software-download/windows10

5. Download the tool. Run the tool. Create installation Media using the USB. You should now have a USB capable of installing a clean version of windows.

6. Turn off your computer and get into the BIOS, change your boot order to boot from USB first. Save it and exit the BIOS.

BIOS Keys by Manufacturer

Here's a list of common BIOS keys by brand. Depending on the age of your model, the key may be different.

- **ASRock:** F2 or DEL
- **ASUS:** F2 for all PCs, F2 or DEL for Motherboards
- **Acer:** F2 or DEL
- **Dell:** F2 or F12
- **ECS:** DEL
- **Gigabyte / Aorus:** F2 or DEL
- **HP:** F10
- **Lenovo (Consumer Laptops):** F2 or Fn + F2
- **Lenovo (Desktops):** F1
- **Lenovo (ThinkPads):** Enter then F1.
- **MSI:** DEL for motherboards and PCs
- **Microsoft Surface Tablets:** Press and hold volume up button.
- **Origin PC:** F2
- **Samsung:** F2
- **Toshiba:** F2
- **Zotac:** DEL

7. Make sure you've got the USB plugged in and boot from it. Install Windows 10 Pro N. MAKE SURE you select Windows 10 Pro N! This is free from all the bloatware your computer has on it from the factory. If it doesn't give you the option and it installs Windows Home – no worries, it'll buff. You'll just uninstall all the nonsense manually.

NOTE: IF YOU AREN'T USING A WINDOWS PRODUCT KEY, OR JUST DONT HAVE ONE: Prepare your backgrounds and profile picture of choice by putting them on some form of storage, maybe a USB. When going through the setup, don't connect to the internet. Change those before you connect to the internet, or they'll be stuck at the default until you get a product key.

8. Once Windows 10 Pro N is installed, you'll begin setup. Create a local account, don't connect your email. Don't use your real name. Create a strong password. DO NOT use the

same password you probably use for everything. Turn off Cortana, Location Services, anything that looks like Microsoft can collect information on you.

8a. The next step will be encrypting your hard drive…. The best way to do this is to use the built in Windows Bitlocker… That requires you to activate Windows with a key, see here if you plan on activating Windows.
https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

9. Once you've logged in download Veracrypt from here:
https://www.veracrypt.fr/code/VeraCrypt/

10. Download the latest .zip and install it. Once you've gone through setup, open the program, Go to system, and select Encrypt System Partition/ Drive. Watch this video for a step by step. https://www.youtube.com/watch?v=i_WkMELC790

Your system partition should now be encrypted. You should be prompted to enter a password whenever your computer is restarted to decrypt. You can also use this software to encrypt files and protect them.

11. Now on to other software! Download Firefox. Get these add-ons: ublock, CleanURL, Decentraleyes, HTTPS Everywhere, Cookie AutoDelete. These will decrease the amount of data collection that happens… Keep in mind though that it gives your browsing a unique foot print. This may be something to consider based on your threat model.

12. Edit the privacy and security settings in Firefox. Make it private!

13. Set your homepage and default search engine to Startpage.com

13a. Download ProtonVPN. You'll prolly need to create an account. Turn on the perma Kill switch once you're booted in.

14. Download W10 Privacy here → https://www.w10privacy.de/english-home/

15. Run it as administrator, Click pretty much everything under the different options. It lays out the effect of each click, use your best judgment. Its kind of time consuming but it will cut out most if not all of the spying Windows does on you. Be careful though, too restrictive and you'll lose major functionality. If you want my preset settings, email me and I'll provide you a file you can just upload into it.

16. Download Edge deflector and install it. → https://github.com/da2x/EdgeDeflector/releases

17. Download the Windows Media Feature pack. → To install the Media Feature Pack, navigate to Settings > Apps > Apps and Features > Optional Features > Add a Feature and find the Media Feature Pack in the list of available Optional Features. Note, you will not be prompted to restart your computer, but you must restart in order to successfully complete installation of the Media Feature Pack. This is only necessary if you installed Win10 Pro N.

18. Download Bleachbit here, use it often!!! → https://www.bleachbit.org/

19. Download KeePass → https://keepass.info/

20. Download VLC, Libre Office, FreeTube, Spotify (Make sure to edit privacy settings), Signal, Tor Browser, ExifCleaner, Claws mail, Kleopatra, Calibre, 7zip and Portmaster. Claws takes some setup, so use Startpage and find a guide for your specific email. Reference this link for lots of ideas on privacy alternatives. https://www.privacytools.io/

21. Change your default programs!

22. Open up Task Manager and disable pretty much all of the startup programs under startup.

22. If you're using an HDD, defrag your computer and set the schedule. Also pin Disk cleanup to your quick access bar.

23. Delete all of these icons off of your desktop and pin them to quick start. It looks better.

24. Open Run → type msconfig → Enter → Services and check the hide all microsoft services box. Uncheck everything thats left.

25. Open Run → type regedit → Enter → Under Current user and Mouse change the Mouse hover time from 400 to 10. Do the same under Desktop and Menu show delay

26. Find Advanced System settings, Click settings on Performance. Click the circle that says Adjust for best performance. You may want to look at the button near the bottom that says smooth edges of screen font. Click it because windows is ugly otherwise.

27. At this point, I imagine your OS is finally done encrypting. Run Disk cleanup then Bleachbit. Restart and your computer is jammin' and ready to go.

Final Step:

Realize Windows is bad for privacy, switch to Linux Mint, Pop OS, or another Linux distro and do this all over again! Seriously though, consider switching to Linux.

Remember, use things from https://www.privacytools.io/

This is short and sweet. I may have forgotten some steps but this is the gist. You get some bonus freebies and additional polish if you pay for me, FN IT, to do this for you. But this will accomplish the mission of speeding up your computer and making it more private.

Reach out here if you have any questions:

fninfotech@protonmail.com
@fnit@noc.social ← Mastadon page → https://noc.social
@FnIT@metapixl.com ← Pixelfed page → https://metapixl.com/FnIT

Donations welcome!
XMR Address:

48VqyA9qGVLYDX5SnqfifnijLgSb2LdrzEqs9QjkWX4sFKacL8icq2QQz73T6nfteeN2wXSDsw9t2YvJyhPPKRPUAkQvdN2