




Cyber security, Morals and YOU!

A project by a coffee fueled Sean Anderson



So to start this off, let's talk about zoom and end-to-end encryption.

What is end-to-end encryption? End-to-End encryption is a method used by companies (Google, Apple, etc) that encrypts messages and files sent so that only the recipient and sender can read them. This means that no third party service can read the messages or modify them (this includes the service you are using to send said messages). In short: E2EE provides a massive boon to security and a service not having it can open you up to major risks.

Now let's talk about Zoom. Zoom does not have end-to-end encryption. This has led to people hacking into Zoom lobbies and causing chaos ([Zoom bombing](#)). Due to Zoom's lack of end-to-end encryption, this has forced various governments around the world to ban it from use.



How to safely run Zoom

Step 1: Download a VM (virtual machine). [VM Link](#)

Step 2: Download the windows 10 ISO (disc image).

Step 2.5: If you have windows, follow [this guide](#).

Step 3: Run the installation setup for the VM.

Step 4: Click New in the virtual machine once its fully installed and name it as well as set the version to windows 10.

Step 5: Click next and allocate memory (2gb is fine but I run 4gb).

Step 6: Click create and then click start, this will bring up a menu. Click on the folder looking icon with a green arrow. Find your windows 10 ISO file (put it on your desktop for easier access).

Step 7: Click on your windows 10 ISO and click open then click choose. You have just created A VM!



How to run Zoom Safely 2

Step 8: Install windows normally.

Step 9: pass your mic and webcam through the VM.

Step 9.5: to pass a mic and webcam through a VM, go to devices and find webcams and audio. The webcam will light up to tell you that you passed it through. To pass through audio, go to the audio section and select audio input, then pass through your mic.

Step 10: search up Zoom in the browser inside the VM and run it normally.

That is it, you can now run Zoom (and other programs) safely!



Tik Tok and safety: monitor your kids

In recent years, the popular app Tik Tok has been in constant hot water with accusations such as:

- .Not removing a suicide stream and talking to their PR team rather than calling the police.

- .shadowbanning children who have facial deformities to “protect them” and to make their platform look better.

- .Hiding videos of the abuse that the hong kong protesters are enduring.

- .Stealing peoples data and selling it to the chinese government.

- .supporting a potential pedophile ring by banning people who bring it to attention.



Tik Tok; lies, deception and protecting your family

Judging by all of those controversies, it's safe to say that you should be monitoring your kids on tik tok but the question then becomes: How?

You can follow [this guide](#) for parental controls.


We will be speaking about what a VPN is in the next section.



VPN-a virtual guardian

VPN stands for a virtual private network. VPNs create a private space that masks your searches and allows you to change your IP address to appear in other countries. This allows you to see content that is normally blocked in your country.

I would recommend [Express VPN](#) but any vpn can will do.



Valorant and why you still shouldn't trust companies.

Valorant is a game that is currently pretty big in the gaming community, but it has one big issue that many have brought up as an issue: the anti-cheat.

When you install valorant, you give it's anti-cheat access to ring 0. Ring 0 is essentially the main control hub of your system. If someone were to hack it's anti-cheat, they could potentially gain control over your entire system.

And the worst part is, people have already managed to hack into their anti-cheat.

The simple solution to this problem is to not install it.




Malvertising: why you should have a adblock

What is malvertising? Malvertising is a type of ad that a virus hides in. unlike the common idea that these ads don't exist in corporate run places (youtube, facebook, twitter, etc) they very much do. Google doesn't often vet advertisers and as such, all the thief has to do is stick a virus into a ad and your PC is toast.

You don't even need to open them to get infected. Some newer malvertisements can infect your computer by just appearing next to a video. This is why you should have adblock.

An adblock is a program that blocks ads from appearing (obviously). You can download one directly into your chrome browser or install it on your computer.



Miscellaneous cyber security myths and facts.

Myth: macs can't get viruses. They can but not often. Mac viruses can often be more aggressive than PC viruses due to the way macOS works.

Myth: iphones (or just phones) can't get viruses. Phones absolutely can get viruses (especially if they are jailbroken).

Myth: webcams are safe. This myth is incredibly false. A hacker can gain access to your webcam and mic in almost a heartbeat. (just unplug your webcam and mic or cover them)

Myth: hacking is super hard and complex. This myth is mostly propagated by TV shows. Most hackers dig through deleted files or try and use scams to lure people into giving their details.

Myth: A password can't protect you from hackers. This is probably the most dangerous myth here. There is actually no way to get around a password, so using a strong one can protect you more than any antivirus around.



Conclusion

Protecting your information and your family may seem hard to do in this day and age but I want to leave you with this: cyber security is 10% coding and 90% common sense. You don't need an antivirus or some form of hyper advanced coding knowledge to protect yourself; you just need to have basic common sense and to be informed. If you have a windows PC then you already have the best antivirus around: windows defender! Windows defender will notify you of strange things happening on your PC and will tell you about the files in zip files! Windows defender recognizes 90% of viruses out there and can get rid of them instantly!

Just remember; you should never be scared of the internet; just cautious.



Sources

Zoom:

<https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE>

<https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>

<https://www.lifewire.com/what-is-end-to-end-encryption-4028873>

<https://theintercept.com/2020/03/31/zoom-meeting-encryption/>

https://www.theregister.co.uk/2020/04/03/dont_use_zoom_if_privacy/

Tik Tok:

<https://www.scmagazine.com/home/security-news/privacy-compliance/tiktok-app-inherently-unsafe-and-a-privacy-risk/>

<https://meaww.com/tik-tok-growing-popular-lockdown-pedophiles-den-sexual-content-childrene-parents-safety-unsafe>



Sources 2

Valorant:

<https://dotesports.com/valorant/news/valorant-data-miner-leaks-new-rank-titles>

<https://arstechnica.com/gaming/2020/04/riot-addresses-kernel-level-driver-concerns-with-expanded-bug-bounties/>

<https://www.dexerto.com/opinion/richard-lewis-can-we-trust-valorants-anti-cheat-1355236>

<https://arstechnica.com/gaming/2020/04/ring-0-of-fire-does-riot-games-new-anti-cheat-measure-go-too-far/>

Malvertising:

<https://en.wikipedia.org/wiki/Malvertising>

<https://www.imperva.com/learn/application-security/malvertising/>

<https://www.cisecurity.org/blog/malvertising/>



Mentor

Mutahar: Owner and operator of the popular gaming YouTube channel SomeOrdinaryGamers that features Let's Plays, commentaries and reviews often of horror games and Creepypastas. His channel, subscribed to by more than 1.7 million, also features videos about the "Deep Web."

[Zoom app being banned](#)

[Valorant having Kernel level access to your PC](#)