**Learning Tech**

Pretend you were just teleported into the year 2020 from a time when computers did not exist. How would you explain to such a person what computers are and what they would need to learn in order to become an IT master?

What are your tech goals?

Privacy / security / mastery of the tech I use / functionality that comes with being a power user

This is a list of files I can reference. Write down instructions for things:

Windows command s

mac os commands

linux commands

**Torrents and Trackers:**

[P2P paper](https://www.cambridge.org/core/services/aop-cambridge-core/content/view/2F379FE0CB50DF502F0075119FD3E060)

[Private Tracker List](https://hdvinnie.github.io/Private-Trackers-Spreadsheet/)

[Private Tracker img](https://uploadir.com/u/khd576y4)

[/PTG Tracker manifesto](https://pastebin.com/thLgSkNE)

[Private Trackers Wiki](https://wiki.installgentoo.com/index.php/Private_trackers)

**IT First Principles:**

**Networking: How does the internet work?**

* Packets and data
* Hardware (infrastructure / backbone)
* Hosts/clients
* Networking
* Security / encryption

**Hardware: How do computers work?**

* Software / OS and programs
* Mobile devices are just smaller computers
* Computer architecture / 1s and 0s

**Programming: What is programming?**

* Layers of programming languages
* Assembler / compilers
* Specializations of programming
* Web apps
* Fundamental concepts of programming that can be learned in any language
* How to learn new languages quickly once you know one

**Who are the major players in the IT field?:** (aka the biggest threats to your privacy/security)

government agencies: the five eyes and others?

tech companies: Google, Apple, amazon, facebook, microsoft, ibm, intel, telecommunications companies, eastern companies (huawei and others)

rogue hackers: the dark net and grey hats

**Social Media**

You can browse social media, but you cannot have an account.

You don’t need a Facebook, Instagram, Twitter, Snapchat etc. These apps are designed to keep you plugged into a toxic culture. They are an integral part of brainwashing.

Social media is a good way to study human nature in a particular context, but a good scientist has to be completely detached from his experiment, otherwise he risks tainting the experiments with his own bias.

IoT and “smart” everything is an extension of this. These are just more ways to keep track of you, to monitor what you’re doing and what you say and how you act and what you think. If you are going to use these devices, only use them in a secure sandbox environment and never depend on them.

<http://www.linuxfromscratch.org/>

**Cybersecurity Business:**

My cybersecurity business is going to teach a handful of very high value clients to become experts at IT so they can protect themselves. The moment you try to port something so complex as privacy and security in the modern world to the masses, you are going to dilute the quality of the product until it becomes a generic, half-baked version of what it could be. Don’t waste your time making security solutions approachable to the masses, focus on creating a product for the big head portion of the market. The people with the highest amount of disposable income who are willing to pay as much as necessary to become as secure as possible.

**Tagline:** Cyberspace is the wild west. Make sure you come prepared.

Consulting sessions consist of the degree to which you are willing to sacrifice ease of use with security/privacy, plus an overview of the kind of lifestyle changes you would need to make in order to become secure.

Consider two products, a premium product that does everything for you, and a regular product that gives you all the information to do this yourself. The easiest way to create a top tier quality product for high profile clients is to create a minimal version for the masses

**Target Audiences:**

* Technically minded people
* People concerned about hackers, cyber criminals malware and viruses
* If you want to share information anonymously
* If you want to keep communication and personal information private
* Interest in technology and the Internet
* Security professionals
* Students studying IT or security
* Freedom fighters
* Political or religious dissidents
* Journalists
* Businessmen or women where security, privacy and anonymity matters
* High profile individuals
* people concerned about government and corporate spying
* Whistle blowers
* Anonymous bloggers
* Anyone who has an interest in security, privacy & anonymity

**The ratio between privacy and anonymity:**

* Privacy: you have an identity and you share it with an individual(s)
* Anonymity: your identity is completely anonymous
* Pseudonymity: eg. Satoshi Nakamoto

**Protect what you value:** Ask yourself,

* What is most confidential?
* What can’t you afford to lose?
* What is irreplaceable?
* What would cause the most damage?
* What might impact your reputation?

**Example of security assets:**

* Photos
* Credit card details
* Bank account details
* Personal identifiable information (full name, address, phone number, SSN)
* Account information: fb, linkedin, amazon, paypal
* Primary email
* Bitcoin wallet / cryptocurrency
* Browser history
* Secret files
* Password information
* Financial records

Make clients apply to the program. The upsell is exclusive, and we can only accept a handful of clients per month because it’s a lot of work. You have to be chosen to have the privilege to pay us to protect you.

**ZenGuard is about creating digital nomads who make the complexity of cyberspace approachable to common people.**

**Cryptocurrencies**

* **using ai to locate crypto arbitrage opportunities**
* Crypto trading bots/scripts
* Cryptocurrency mining
* Best cryptos to cloud mine
* Find out all the problems with bitcoin and invest in the cryptocurrencies that provide solutions (Bitcoin scaling issues)
* **Why does bitcoin have a limited amount**
* **BIPs:** Bitcoin improvements proposals
  + Bip148, bip91, bip100
* Rootstock: smart contracts on the bitcoin network

**Learn to operate a computer without using the GUI**

**Security and privacy has ceased to become cool. Make it cool again.**

They have no online presence yet they seem to have complete mastery over technology.

**An OS that can run on any device. Highly compartmentalized / individualized / customizable. Barebones with very few weaknesses to exploit and scales in complexity depending on your needs.**

The easiest way to secure your social media is to not have any social media at all.

**Secure your digital brain.**

**Secure your access to the internet.**

**Secure your private network.**

**other books like Data and Goliath**

“Threat modeling” posts:

* government agencies
* blackhat hackers
* stalkers
* Parents
* Social media
* big tech

People are not as concerned about their privacy as they should be. Would you be angry or upset if you found out someone could record sound and video on your phone any time they want?

how does google control how you search and what comes up when you search?

How does google track what you search and give you a biased search?

The easiest way to be secure online is to be anonymous. Keep your digital life and your real life completely separate

100% security is non existent but you can make yourself less of a target and make it too much of a hassle to be hacked

You may have bought the phone but whoever hacked it is the one who actually owns it. Since we are so attached to our phones, whoever has hacked your phone also owns a very important and precious part of you. This is why you should get to a point where you don’t even need a cellphone to function in the world.

Privacy is related to the notion of free will. Just like people who are free to say what they want and test their ideas in a public forum have the ability to think freely and explore new ideas, our right to privacy gives us the freedom to act as we please without fear of shame or consequences. So long as we are not hurting anyone else, we should be free to do whatever we want.

you may trust your own government to keep you safe but do you trust every government in the world? they have all invested heavily in making sure they have access to your data. Russia and China are spying on the American people. American allies are too.

Is there a way to use signal without using your phone number?

pidgin messenger