

This is just the tip of the iceberg, there is so much more to learn :))

→ super super important

2 factor authentication

Secure Browsing

Secure file erasing

VPN

Malware

Phishing

Metadata

And much more..

read it with infomercial voice

If you are interested in knowing more of this you can check these sites

https → great!  
https://ssd.eff.org → websites  
https://securityinabox.org  
Umbrella App → Android App



So, WHAT ARE ALL THESE SECURITY THINGS!!!!

The slightly commented zine of  
**INFORMATION SECURITY**  
**FOR NON INFOSEC PEOPLE**

101

the maybe boring  
Before diving in technology, we prefer to introduce some basic premises:

NOTHING IS 100% SECURE  
#TheHorror!!!

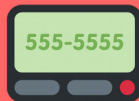


Sorry for the sensationalism...  
can't help it :)

Technology, as anything else made by humans is susceptible to be vulnerable. When someone says that "something is secure", it means "until today there is no evidence that something is compromised"

Technology changes, and  
**REALLY FAST**

See previous point  
What is super "secure" and advanced today, in a couple of years will be obsolete and easier to cheat



Talking about your accounts:

Use good passwords

10 characters passwords are gone forever, try something better like passphrases, like this example:

please don't use exactly this one

Omg this kind of password is way better

.....

Check these password habits

- Don't reuse passwords
- Review your security questions, they are easy to guess? Answers are in your social media? Try changing them by lies or passwords
- Also Secure your recovery accounts



we know this can be pretty hard, because of that we suggest

- Use a password manager

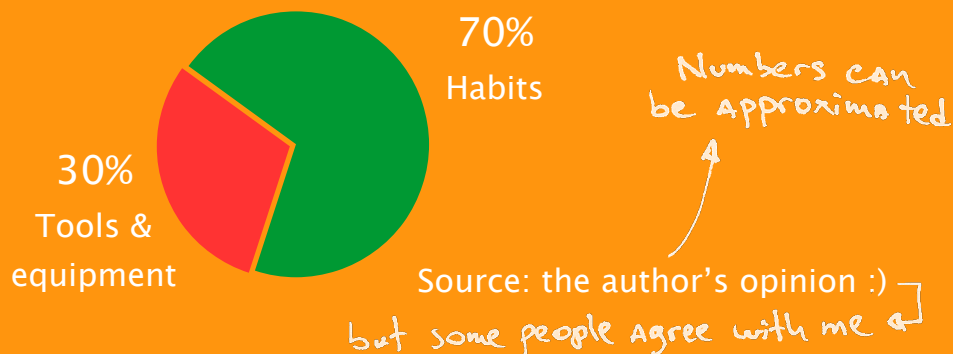
# The habit issue



As with the house example, it doesn't worth much having the best gear if we don't have the habit of closing all doors before leaving, this could be challenging at first but if you want to be more secure this "inconvenience" will pay off



For some people, a good security is about...



Now, imagine that your house have:



Maybe, just maybe

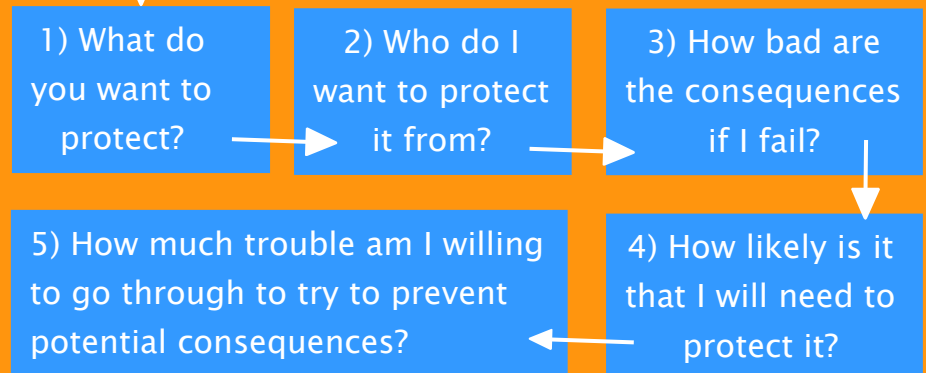
People will think you have more valuables than you actually have

It will be too expensive, uncomfortable and invasive

**You don't need all of this**

It could help if you build a threat model

It could be a little more complicated but to simplify, you can ask yourself



Source:



guide (EFF) <https://ssd.eff.org>

Now, with this knowledge you can decide if these strategies are fine within your threat model and include habits that you can build:

## Use the best encryption that you can

### Use HTTPS

 <https://example.com> 

Encrypt the communication between you and the sites you visit

### Encrypt your chats



When possible use Signal



If not, Whatsapp

The ability to transform a message so it only can be legible to those that you chose

Un encrypted *everyone CAN read it*

6Y#Kgiu  
7%0o9d\$ *WTF!! (encrypted)*

Un encrypted *when your friends read it*

## If you feel that sh... got real:

Use GPG for mail



Encrypt your files



Encrypt your computer



Filevault Mac



BitLocker Windows



LUKS Linux

With doubts on this?  
Just make some searches:



## A Chain is no stronger than its WEAKEST LINK



Imagine that you have a house with super fences and great locks, but you left the back door open or a key under the carpet



Your security could be "good" but a single vulnerability can compromise the entire system

Information security works in the same way.. i.e. You can protect your mail account with a great password, but your security questions are easy to guess? How protected is your recovery account?