# Security and Privacy

The world is a scary place, and everyone’ s out to get you.

Okay, maybe not, but that doesn’ t mean you want to flaunt all your secrets. Security (and privacy) is generally all about raising the bar for attackers. Find out what your threat model is, and then design your security mechanisms around that! If the threat model is the NSA or Mossad, you’ re *probably* going to have a bad time.

There are *many* ways to make your technical persona more secure. We’ ll touch on a lot of high-level things here, but this is a process, and educating yourself is one of the best things you can do. So:

### Follow the Right People

One of the best ways to improve your security know-how is to follow other people who are vocal about security. Some suggestions:

- @TroyHunt
- @SwiftOnSecurity
- @taviso
- @thegrugq
- @tqbf
- @mattblaze
- @moxie

See also this list for more suggestions.

### General Security Advice

Tech Solidarity has a pretty great list of do’ s and don’ ts for journalists that has a lot of sane advice, and is decently up-to-date. @thegrugq also has a good blog post on travel security advice that’ s worth reading. We’ ll repeat much of the advice from those sources here, plus some more. Also, get a USB data blocker, because USB is scary.

### Authentication

The very first thing you should do, if you haven’ t already, is download a password manager. Some good ones are:

- 1password
- KeePass
- BitWarden
- `pass`

If you’ re particularly paranoid, use one that encrypts the passwords locally on your computer, as opposed to storing them in plain-text at the server. Use it to generate passwords for all the web sites you care about right now. Then, switch on two-factor authentication, ideally with a FIDO/U2F dongle (a YubiKey for example, which has 20% off for students). TOTP (like Google Authenticator or Duo) will also work in a pinch, but doesn’ t protect against phishing. SMS is pretty much useless unless your threat model only includes random strangers picking up your password in transit.

Also, a note about paper keys. Often, services will give you a “backup key” that you can use as a second factor if you lose your real second factor (btw, always keep a backup dongle somewhere safe!). While you *can* stick those in your password managers, that means that should someone get access to your password manager, you’ re totally hosed (but maybe you’ re okay with that thread model). If you are truly paranoid, print out these paper keys, never store them digitally, and place them in a safe in the real world.

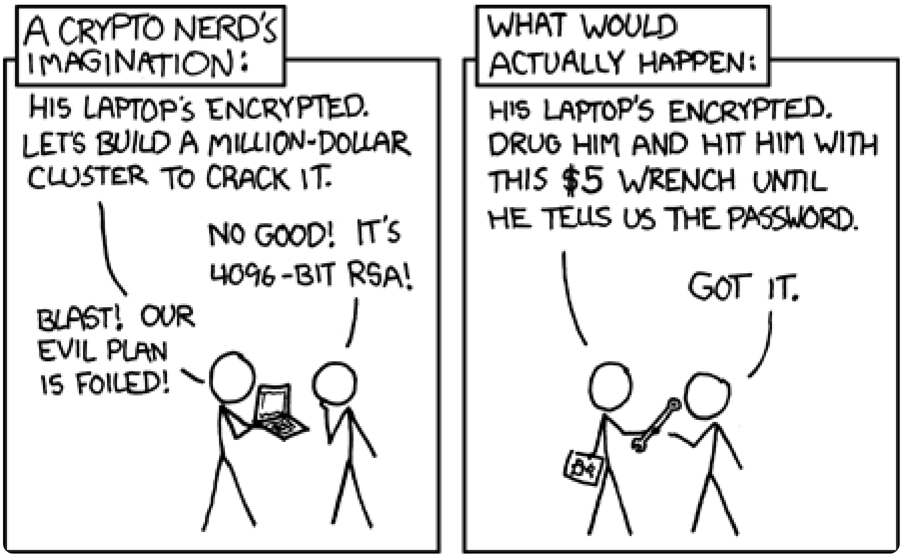
## Private Communication

Use Signal (setup instructions. Wire is fine too; WhatsApp is okay; don’ t use Telegram). Desktop messengers are pretty broken (partially due to usually relying on Electron, which is a huge trust stack).

E-mail is particularly problematic, even if PGP signed. It’ s not generally forward-secure, and the key-distribution problem is pretty severe. keybase.io helps, and is useful for a number of other reasons. Also, PGP keys are generally handled on desktop computers, which is one of the least secure computing environments. Relatedly, consider getting a Chromebook, or just work on a tablet with a keyboard.

## File Security

File security is hard, and operates on many level. What is it you’ re trying to secure against?


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

- Offline attacks (someone steals your laptop while it’ s off): turn on full disk encryption. (cryptsetup + LUKS on Linux, BitLocker on Windows, FileVault on macOS. Note that this won’ t help if the attacker *also* has you and really wants your secrets.
- Online attacks (someone has your laptop and it’ s on): use file encryption. There are two primary mechanisms for doing so
  - Encrypted filesystems: stacked filesystem encryption software encrypts files individually rather than having encrypted block devices. You can “mount” these filesystems by providing the decryption key, and then browse the files inside it freely. When you unmount it, those files are all unavailable. Modern solutions include gocryptfs and eCryptFS. More detailed comparisons can be found here and here
  - Encrypted files: encrypt individual files with symmetric encryption (see `gpg -c`) and a secret key. Or, like `pass`, also encrypt the key with your public key so only you can read it back later with your private key. Exact encryption settings matter a lot!
- Plausible deniability (what seems to be the problem officer?): usually lower performance, and easier to lose data. Hard to actually prove that it provides deniable encryption! See the discussion here, and then consider whether you may want to try VeraCrypt (the maintained fork of good ol’ TrueCrypt).
- Encrypted backups: use Tarsnap or Borgbase
  - Think about whether an attacker can delete your backups if they get a hold of your laptop!

## Internet Security & Privacy

The internet is a *very* scary place. Open WiFi networks are scary. Make sure you delete them afterwards, otherwise your phone will happily announce and re-connect to something with the same name later!

If you’ re ever on a network you don’ t trust, a VPN *may* be worthwhile, but keep in mind that you’ re trusting the VPN provider *a lot*. Do you really trust them more than your ISP? If you truly want a VPN, use a provider you’ re sure you trust, and you should probably pay for it. Or set up WireGuard for yourself – it’ s excellent!

There are also secure configuration settings for a lot of internet-enabled applications at cipherlist.eu. If you’ re particularly privacy-oriented, privacytools.io is also a good resource.

Some of you may wonder about Tor. Keep in mind that Tor is *not* particularly resistant to powerful global attackers, and is weak against traffic analysis attacks. It may be useful for hiding traffic on a small scale, but won’ t really buy you all that much in terms of privacy. You’ re better off using more secure services in the first place (Signal, TLS + certificate pinning, etc.).

## Web Security

So, you want to go on the Web too? Jeez, you’ re really pushing your luck here.

Install HTTPS Everywhere. SSL/TLS is critical, and it’ s *not* just about encryption, but also about being able to verify that you’ re talking to the right service in the first place! If you run your own web server, test it and test it again. TLS configuration can get hairy. HTTPS Everywhere will do its very best to never navigate you to HTTP sites when there’ s an alternative. That doesn’ t save you, but it helps. If you’ re truly paranoid, blacklist any SSL/TLS CAs that you don’ t absolutely need.

Install uBlock Origin. It is a wide-spectrum blocker that doesn’ t just stop ads, but all sorts of third-party communication a page may try to do. And inline scripts and such. If you’ re willing to spend some time on configuration to make things work, go to medium mode or even hard mode. Those *will* make some sites not work until you’ ve fiddled with the settings enough, but will also significantly improve your online security.

If you’ re using Firefox, enable Multi-Account Containers. Create separate containers for social networks, banking, shopping, etc. Firefox will keep the cookies and other state for each of the containers totally separate, so sites you visit in one container can’ t snoop on sensitive data from the others. In Google Chrome, you can use Chrome Profiles to achieve similar results.

Exercises

TODO

1. Encrypt a file using PGP
2. Use veracrypt to create a simple encrypted volume
3. Enable 2FA for your most data sensitive accounts i.e. GMail, Dropbox, Github, &c