Personal Security

or, how to **not** get hacked for fun and profit

@balex

Step 0.

Disconnect your computer from the internet, shut it off, seal it in a lead safe, and bury that safe 20 feet underground.

But seriously, no device will ever be 100% secure, no matter how hard we try. The best we can do is take every precaution we can to make it more difficult to break into.

Problem 0/1: Passwords

- weak passwords (qwerty, admin, name of your dog, etc.)
  - easy to crack or guess
- password reuse or patterns across different sites
  - if your password gets leaked for one site, it’s easy to get into the others accounts you have
  - check haveibeenpwned.com to see if your info has leaked
- no multi-factor authentication
  - allows people to login if they get your username and password, they don’t have to verify anything else

Step 0. (actually)

USE A PASSWORD MANAGER! Password managers make it easy to:

- generate secure passwords
- make unique passwords for every site (and remember them later!)
- use two/multi-factor authentication (more on that soon)

Step 0. (actually)

One of my favorite password managers is 1Password. I pay for a subscription, but they also have a free tier. They also have:

- apps for Mac, Windows, iOS, and Android (plus fingerprint locking if your device supports it)
- browser extensions for Chrome/Chromium/Brave, Firefox
- syncing across devices

Step 0. (actually)

“But Alex, I don’t want to have my passwords hosted by someone else/I only use open source software/I don’t want to pay!”

Then you should use BitWarden! It’s free (as in food and in thought), open source, and you can host it locally on your own machine or in your own cloud storage service! It also has clients on literally every platform (including the command line!)

Step 1

Turn on 2 Factor Authentication (2FA)/Multi-Factor Authentication (MFA) for every account you can! This means that anyone trying to log into your account will also need a code, or security key, or link, or something else to get in. That way if your password somehow gets leaked, you will still be able to deny attempts to log in.

// 1Password has a built in 2FA service, and it will tell you what sites have 2FA/MFA available to use :)

Step 1

There are many types of 2FA/MFA (listed in rough order of how secure they are):

- security keys like SoloKey (open source!!), YubiKey
- authenticator apps like Duo, Google Authenticator, etc.
- Google and Facebook (among others) will require you to approve your logins with a check box on another device
- emailing 2FA/MFA codes or a live link you must click
- texting/calling with 2FA/MFA codes (yuck)

Step 1

A company texting/calling you with security codes is bad.
It is *very* easy for an attacker to spoof your phone number/SIM card.

If there are better alternatives (authenticator app/ security key), use that instead- I’m begging you. Only use the text/call option if there are no other options. It’s better than no 2FA/MFA, but not by much.

//Unfortunately, a lot of banks only have this option :(

Problem 2: Physical

Humans are the weakest link (in terms of security). You can have all of the authentication you want, on top of 64-character long passwords, but if you leave your laptop unlocked, then an attacker can just skip over all of that.

Step 2

Enable a password on all your devices, and have it require the password as soon as the screen is locked.

Nowadays, we have our banking information, personal addresses and contact information, health information, grades, and more available on all of our devices. Enabling a password on everything you own makes sure that it’s more difficult to access this information.

Step 2

If you want to be even a little more paranoid like me, then **encrypt the hard drive on your laptop**! If your hard drive isn't encrypted, then if someone gets a hold of your hard drive (with or without the rest of the laptop), they can still access all your files even without your normal computer password.

//Also, if you use Linux and don't have an encrypted hard drive, it's pretty easy to bypass your root password and login to your computer using GRUB.

Step 2

Lock your computer/phone if you step away from it- even if it’s only for a minute.

While most of the time this just prevents your friends from sending stupid messages from your accounts, if an attacker were trying to access your computer, leaving your computer open for even a few minutes is enough to give them a way in.

//You should probably just take your devices with you/put them away when you step away in the first place :)

Problem 3: Oversharing

The rise of social media has led to a lot of oversharing, and a lot of information being posted online that can be used against you.

People can use this information to guess passwords or worse, to answer security questions that allow them to then reset your password.

Step 3

Be very careful with the information that you post online.

Parents names, your old high school, pet names, teachers names, etc. are all common security questions. They’re also plastered all over Facebook.

To be super secure, treat security questions like passwords - don’t use real answers. Make up answers specifically for security questions (or even per website) that people can’t guess from your personal information.

Step 3

Don’t post:

- Information about when/where you will be travelling (beforehand)
  - Then people know your home will be empty/unguarded during that time!
- Photos of boarding passes, house keys, credit cards, or any other personally identifiable information
  - Boarding pass barcodes embed lots of fun information in them, see @mangopdf’s recent story

Miscellaneous Advice

~ Check your Google, Facebook, Netflix, Spotify, Hulu, etc. for current logins, and remove any logins you don't recognize
~ Check all the emails you've ever used on Have I Been Pwned (haveibeenpwned.com)
~ Split up all of your login info: use a different service for password management than you do for 2FA/MFA
  - When you can, only save passwords (no email/username) in your password manager entries

That’s all :)

If you want to know anything else about security (personal or otherwise), just ask in the Discord or send us an email at contact@isss.io