SURVEILLANCE SELF-DEFENSE

SECURITY STARTER PACK SUMMARY PRESENTATION

ATTRIBUTION

Everything in these slides, except on passwords, is a summary from the EFF's "Security Starter Pack," as part of their fantastic Surveillance Self-Defense program, which also includes information on:

- attending protests both in the US and internationally
- how to delete data securely
- protecting yourself from malware

I'm able to adapt and share this content with explicit permission from the EFF. I license this summary similarly.

SECURITY IS A PROCESS, NOT A PURCHASE: OVERVIEW

1. No tool will entirely protect you from surveillance or hacking.
2. You should not trust any person or organization that tries to make that claim.
3. More important than any tool or product is getting into the habit of thinking about how your privacy can be compromised.

https://ssd.eff.org/en/playlist/want-security-starter-pack#choosing-your-tools

SECURITY IS A PROCESS, NOT A PURCHASE: TOOLS

Remember: no tool is perfect, but some are better than others. Whatever you use, here is what's important:

1. Research it, whether online or with friends who know the subject. Focus less on quantity of information than how much you can trust where it comes from.

2. Keep whatever you use updated, because that often means security updates.

https://ssd.eff.org/en/playlist/want-security-starter-pack#choosing-your-tools

PROTECTING YOURSELF ON SOCIAL NETWORKS

Check on the following:

1. Do you use your real name, or give real answer to security questions? Do you need to?
2. Is there enough information online for someone to impersonate you? Does anyone know enough about you to look up answers to your security questions?
3. Do you know who can see what in your online profiles?
4. Have you opted out of whatever you can, both with the website itself and with your friends?

Exercise 1: with people you trust but who aren't your friends on a social network, compares notes about what is visible and what can be learned.

Exercise 2: search for "<social network name> opt out" and check whether you've changed your settings.

Exercise 3: let your friends know that you don't want to be tagged or named in certain things.

https://ssd.eff.org/en/playlist/want-security-starter-pack#protecting-yourself-social-networks

INTRODUCTION TO THREAT MODELING

1. **What** do you want to protect?
2. **Who** do you want to protect it from?
3. **How likely** is it that you will need to protect it?
4. **How bad** are the consequences if you fail?
5. **How much** trouble are you willing to go through in order to try to prevent those?

Exercise: go through these steps for one thing or kind of thing you care about.

https://ssd.eff.org/en/playlist/want-security-starter-pack#introduction-threat-modeling

COMMUNICATING WITH OTHERS

1. The most secure way to communicate is in-person.
2. The second most is using end-to-end encryption.
3. Even encryption won’t protect your metadata, which is often still enough to reveal who you are, who you’re with, where, when, and why.

Exercise: sending a secret message in writing.

https://ssd.eff.org/en/playlist/want-security-starter-pack#communicating-others

CREATING STRONG PASSWORDS, BUT UPDATED

1. Never use the same password for more than one website that you care about (email, bank account).
2. Make your passwords at least 10 characters, because computers are powerful enough to guess anything smaller.
3. Ignore the “four common random words” advice; that is too easy to compute now.
4. When you make your own password, instead use acronyms of something that only makes sense to you: “WIw7,mstmsritt”= “When I was seven, my sister threw my stuffed rabbit in the toilet”
5. Use a password manager like 1Password or LastPass, which now allows you to sync passwords across devices for free.

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

SHORTEST POSSIBLE STORY

1. Use a password manager.
2. Use Signal for end-to-end encryption of text messages and phone calls.
3. Make a plan for if someone were to start trying to track your internet activity.
4. Make sure your phone and computer are always secure: locked up or hidden when they aren’t on you, and password-protected at all times.