Audits

The very last thing we're going to talk about in section 4 is auditing. It is one of the most important things that you can do in this course, so don't take it lightly!

Don't take this message lightly either...

Promotional Spot

When we think of auditing, we think of inspections, uneasiness, error-finding, and unfortunately...that's what it is. But, auditing is very important. Your privacy and security etiquette is going to change over time. Either you're going to slowly start slacking off, or you're going to want to continually improve your habits. Additionally, technology is always evolving, so things that worked when you started may need to change. *For example, when two-factor authentication was being popularized, it was mostly used with email and phone numbers, which as we discussed in section 3, are susceptible to attacks. Now, many services implement apps that handle 2-factor authentication offline with OTP, something you all should be utilizing.* Changes like this happen constantly, and it's important for you to keep up with news related to these topics. Whether it's through *Reddit, a news source, us, make sure you're continually keeping up-to-date. We have surveillance reports uploaded every week offered as a video and a podcast if you want an easy way to keep up with news.*

In order to make sure you're always protected, you will need to self-evaluate your privacy and security habits. I broke up auditing into different steps to help you out. Premium users can refer to the checklist.

1) *Check haveibeenpwned and search for your personal information through startpage or searx.me for hacks and leaks of your personal information.* If anything has been compromised, you need to make sure you secure your account by changing your password and ideally the email associated with the password. *Go back to lesson 2.4 and 3.4 for more instructions on what to do in this scenario.*

2) *Check for updates on every device you own, and every piece of software on that device. We covered why this is important in lesson 3.2.*

3) Run antimalware scans on your devices that have a higher risk of infection. This will be most desktop operating systems, even Linux. *Malware was covered in lesson 3.12.*

4) Update all of your passwords, at least for your most sensitive accounts. Sometimes hacks and leaks aren't publicized, so someone may have access to an account without your knowledge. Additionally, continually changing your passwords will make it difficult for somebody to brute force their way into your accounts using computational power. *I covered these topics in lesson 3.4 and 3.5.*

5) *Check up on your phone's settings, apps, and app settings. Make sure no recent apps you downloaded have unnecessary permissions.* Shopping apps don't need your microphone, and calculators don't need your location. *Go to lesson 3.3 for more details.*

6) Delete unneeded files, photos, programs, and apps. *What I tend to find is I'll try a few apps and forget to delete them, and the audit will catch these, as well as any settings for new apps I haven't configured yet. Refer to the minimalism lesson in 2.2 to re-cover this.* Don't forget to clear your temporary files like history, cache, and cookies as well.

7) *Try to ask a friend to dig up information on you online.* If they find more than you'd like, you need to ask them where they got the information so you can remove or falsify it. You can also do this yourself if you don't have any friends ** long pause ** that don't want to do it for you.

8) This is your decision, the other things we covered I recommend you always check up on, but you may have different priorities and things to look at. Section 5 will talk about physical security and privacy, and some of you may have things in there you want to audit. I'd encourage you to find what's important for your personal interests, priorities, and threat models and add them to your list of items to consistently check up on. Expand as need be.

Like I said before, auditing is an extremely important part of increasing your digital privacy and security. You can configure everything properly in January as a New Year's resolution, but in six months you can be completely vulnerable. Stay on top of things! I recommend you set aside a day every week, other week, month, or every other month to sit down and audit yourself. The frequency is your decision and where you draw your convenience line.

Queue Outro Promos

I wish you luck! Thank you for watching this lesson and I will see you in the finale of section 4, where we recap everything we covered.