Passwords

Passwords are the ***show key*** key to everything in our lives; they give you access to bank accounts, emails, devices, everything. You know that saying "money makes the world go round"? Well, people can't hold on to their money if they don't have passwords to protect it, so passwords kind of make the world go round--maybe that's a stretch...

I wouldn't be able to be here today without these promos making my world go round, so here we go...

Promotional Spot

Let's start off with the basics! *When you register for a website, your password is put through a one-way algorithm called a hash-function* That way no one knows what your password is except you. The issue is when these services or websites *get pwned, or hacked*, it's common to find your username with your password's hash publicly available. Once a hacker or anyone else obtains these hashes, they can use tools like *John the Ripper, oclHashcat, and other tools to crack the hashes and retrieve the actual password*. I'll talk more about those tools shortly.

In 2014, there were several iCloud hacks that leaked the nudes of famous celebrities. This event was called 'The Fappening.' It turns out the hacker (or hackers) used a tool called *Elcomsoft Phone Password Breaker, or EPPB, a tool used by law enforcement and government agencies to access iCloud accounts, which by the way is sold publicly for as little as $80.* EPPB requires an iCloud user's username and password. It just so happened that there was another tool posted on GitHub called *iBrute, a password-hacking tool specifically created for getting iCloud credentials from just about anyone.* Using iBrute and EPPB together, someone could impersonate the victim and download a backup of that person's iPhone onto another device, which is very likely how this hack was accomplished. This isn't just an issue for individuals, passwords are how we protect medical data, any other sensitive data, and even company data--as a matter of fact, according to Ajit Gaddam at Enigma 2019, a security engineer for Visa, almost 80% of all data breaches resulted from weak or stolen password. How do we avoid this?

The first golden rule of passwords is to *use good, secure passwords for every website you visit*, making it harder to brute-force. What makes a good password? Glad you asked...Even highly targeted individuals don't always know. *The previous CEO of Sony, Michael Lynton, used sonyml3 as his domain account password,* no

wonder his emails were hacked and spread across the internet. There are also the passwords that were *exposed in the Ashley Madison hack*, the most common were *"123456", "12345", "password", "DEFAULT" "123456789", and "qwerty"*, *can we get much higher? A good password doesn't use dictionary terms, since brute-forcing attacks can guess word-based passwords extremely easily. If you are using the word red, try to replace the e with a 3, this is a very simple tip that can go a long way with longer passwords. You should be using both lower and uppercase letters, including symbols, numbers within the password, and making it as random as you possibly can. The longer the password the better, I'd recommend having at the very least 12 digits, and working your way up to the dozens if you can,* we'll cover how to do this easily and realistically, very soon.

The other golden rule is to *never use the same password twice.* Let's say *Adobe got hacked and your email and password are posted online. If your email account uses the same password that you used for Adobe, a person now has your email address, as well as the password to your account.* Giving them access to your email where they could possibly get access to other accounts. We will be discussing more ways to prevent this in the very next lesson.

Okay...so far this is pretty straightforward, use good passwords, and use different passwords. But how can you create several different passwords that are good, without losing track of them? Great question!

The first option is to write them down on a **** hold paper **** piece of paper. If you're going this route, NEVER write the password as is. Use things to help you remember, something cryptic. *Instead of writing gaming123 (which is your password), write timekiller +123, This way anyone who finds your list of passwords will have to do a lot of deciphering to figure them out.*

The second option (which is what I'd recommend) is using a password manager. Lots of people are aware of cloud-based password managers that sync your generated passwords instantly across your devices, like *LastPass, 1Password, Dashlane and all of these other services.* The way these work is you have an account that can be accessed using a *master password, giving you access to all of your passwords inside*. If you haven't already picked up how important that master password is, I'm going to be Gandalf and tell you... *(RECORD "PASSWORD"),* so pick a strong password. *Inside of this vault, all of the passwords for every service you use can be randomly generated by the service so you can use extremely secure passwords and not have to memorize them.* This is awesome on paper. **** Pun Intended, Hold up Paper with Passwords on it ****

However, these cloud-based password managers typically have three problems:

1) They are cloud-based and stored on the company's servers, so you don't own and control your database file. This is an enormous amount of trust to put in a company, especially when they are susceptible to attacks, *which have successfully happened in the past.*
2) They cost **** hold cash **** money, it's very rare to find a good option which is both unlimited and free.
3) Most of these services use proprietary software, meaning they are closed source, so nobody except the company can view the code and check it for bugs or backdoors. We want FOSS as previously discussed in section 1 of the course.

But, there are password managers that don't suffer these problems. The first one I would suggest is *KeePass, an open source password manager where you physically own an encrypted file with your passwords; the only way to access the passwords is by loading the file into a Keepass client.* Since the file is encrypted, *you can actually sync it using a cloud service like Google Drive, Dropbox, Nextcloud, or whatever you want to use; I made a guide on how to do this.* Even if someone got access to your cloud storage, they still wouldn't be able to load your passwords because it's an encrypted file. This is technically less secure than storing it entirely locally, but I would argue this is safer than using a cloud-based password manager.

There is a step-up from KeePass, and it's called *Master Password. Master Password doesn't do any syncing, backups, and doesn't require internet to function, similar to Keepass. The difference is Master Password uses algorithmically generated passwords from the username you pick, along with a password and title you give the entry.* This means you can access the information anywhere, assuming you remember exactly the correct information. I do personally feel more comfortable with something like Keepass, where I control a physical file, but Master Password is undoubtedly more secure, and quite honestly an ingenious idea, although more complex.

Now, there is one major downside to password managers: you're putting all of your eggs in one basket. If someone gets into your database, they have access to everything. Here are a couple things you can do to protect yourself and make your password manager an even stronger solution.

1) *Make multiple databases with different passwords for different uses. You can separate schooling, from entertainment, from your personal life, one compromise won't jeopardize everything else.*
2) The second thing you can do is to memorize a second password that you can append at the end of passwords within your vault. *Let's say you remember the password 'lemurs.' You can randomly generate your secure passwords in the password manager, but when you use it online, you add 'lemurs' to the end of the random passwords. This way, even if someone*

breaks into your password manager, they still can't get into the accounts because they don't know to add 'lemurs' to the end of each password.

I also want to point out the importance of frequently changing your passwords, since even your secure passwords can be pwned without your knowledge. *I would recommend you reserve a day every given time period to sit down, and update your passwords.* This ties in with doing consistent audits on yourself, a topic we will discuss in section 4 of the course.

Alright, now you know how to create strong passwords and manage them properly. Sadly, only 12% of Americans in 2016 used a password manager, so please spread how and why your friends and family should use them. Now,what happens when you don't need a traditional password, maybe a device uses fingerprints, patterns or other biometrics. What should you do?

Biometrics, at least today, are almost always *less secure than a password,* since biometric technology isn't advanced enough to fully verify if somebody is who they say they are. *Apple's touch ID has been cracked, FaceID has been cracked, most biometric methods on Android have been cracked, and most other forms of identification like voice authentication just aren't advanced enough. Additionally, Police in Florida recently tried to get access to a person's dead body to unlock the person's cell phone with a fingerprint. Police in Michigan 3D-printed a murder victim's fingerprint to gain access to a device, and someone you know could easily unlock your phone while you're asleep. Face ID means someone just holds a device to your face, I mean seriously?*

Let's not forget that biometrics can be very invasive privacy-wise. On top of all of this, there are legal differences between biometric passwords and physical passwords.

In the US, courts have ruled that a passcode is classified as *"knowledge"*. *Because of the Fifth Amendment, there are constitutional protections against being forced to surrender your passcode to law enforcement* But, biometrics are not classified as "knowledge", therefore you can be forced to legally unlock your devices. This is the US though, and different countries have different laws. For example, in Canada, if you are a citizen, *you must hand over your passwords as part of the law. For more information on these laws in other countries, the Privacytools.io website has a great list.*

No matter what, I'd recommend disabling all biometric passwords when going to *airports, crossing the border, attending protests,* or any other situation with lots of law enforcement, since these are major areas where people are unfairly searched. If you use biometrics on a mobile device, you can leave it enabled and

simply reboot your device before going to a high risk or high guarded area, since a reboot will require a password. Alternatively, Apple recently introduced a feature in iOS 11 where if you click your power button 5 times, it will automatically lock you out of your phone and require a password to unlock it. This was created for the exact scenario we're discussing.

Another form of verification is ALP, or Android lock patterns. In short, avoid these. *At the passwords-con conference in 2015, researchers reported that people often used the first letter of their first name, and that people tended to use the dots in the middle and not in the 4 corners. On top of this, security researchers at the US Naval Academy and the University of Maryland Baltimore County published a study showing an observer can visually pick up and then reproduce an Android unlock pattern with relative ease.* About two of every three observers successfully recreated a pattern from five or six feet away after a single viewing.

Okay...that was all a ton of information, and I hope you kept up, but there are a few more things that you should know before we finish this lesson, let's quickly go through them.

First, use a password. This seems like a no-brainer, *yet consumer reports found that over one third of Americans don't have protection on their mobile devices.*

Second, *don't remember passwords inside your browser or allow your browser to manage them.* If anyone gets into your system, your browser won't ask for any additional verification to use those passwords, which is a security concern.

Third, never leave your system unlocked for any reason, even for a minute. *When you walk away from your computer--sign out. On Windows and most Linux distros, just click Windows Key + L, it's that simple.*

The very last topic is security questions. *These are those questions you get when signing up for a website to verify who you are.* We have been taught since we were small children to always be honest. The problem in being honest with security questions is lots of them are ridiculously easy to guess, even for a random stranger. Luckily, there's a simple solution to this: we're going to lie, by not just putting fake information, random information. You know that password manager I told you to start using? *You should create a password for every security question, so that no one can guess them, and there's no personal information being given. Save it in your password manager, and that's where you go if you ever need to access the answer to your security question.*

Queue Outro Promos

That is going to wrap up what you need to know about passwords. It is a very simple topic, but can really expand when you start getting into the nitty gritty. In the next lesson, we will talk about *two factor authentication,* which I would argue is just as important as having a strong password, so make sure to watch that as well. I'll see you there and thank you for watching.