Using and Managing Passwords

Brought to you by Assemble You.

It's time to work on YOU. So, sit back and listen to practical, actionable advice to secure yourself.

Today we are discussing using and managing passwords.

Your house often contains the most valuable possessions you own. Family heirlooms, pictures of your family, jewelry, and whatever else. Would you leave the front door open to allow anyone to walk in and take those valuable items? What about if you knew thieves were prowling? Would you lock up then?

People go to great lengths to protect their homes. They have neighbors open and close the curtains and turn lights on and off while they vacation. Buying locks, motion-sensitive lights and alarm systems, and intimidating guard dogs.

So, why are we so willing to forego this level of security online? Where we do our banking. Where we shop for things. Where we have some of our most confidential conversations. 123456 is the most popular password on the internet. 123456!! According to Schneider Downs, it's used by 103 million people. And it can be compromised in less than a second.

Even Meta CEO Mark Zuckerberg has fallen prey to his own lazy password maintenance. Around 80% of people reuse their passwords across sites, and Zuckerberg proved to be no different when his Twitter account was hacked in 2018. Zuckerberg had been a victim of a LinkedIn data breach. The weak password he used across social media - *dadada* - had been compromised and used to access his profiles.

Perhaps when the threat is non-physical, we feel less pressure to protect ourselves - "what we can't see won't hurt us" type of thing. Make no mistake, this is a grave error.

Thankfully though, through just a little bit of diligence and effort, we can go a considerable distance to ensuring we're protected.

Hackers don't have to guess your password manually. They use different methods and tools to automate the entire process and discover the actual password. This is why we must use a secure password - one that's lengthy and complex.

Passwords are low-hanging fruit for hackers, as password attacks are more straightforward than other attacks. To conduct them, hackers use different methods - let's look at some of them.

The first method - **phishing** - is the most common example of what we call a social engineering attack.

Using a spoofed email address, a hacker sends you an email. The email body is intended to trick you into providing personal information, such as a credit card or social security number.

The email might even ask you to reset your password by clicking on a link. Via this link, you're redirected to a fake website, a replica of an actual company, such as a bank. The moment you enter your credentials, they are captured by the hacker in the background. Recent data on Hosting Tribunal shows that 52% of organizations had been compromised this way.

Next up is the **brute-force** attack.
Using specialized tools, hackers use every possible combination of allowable characters. That includes lowercase and uppercase letters, numbers, and special characters. The tool will run and attempt to create a password, and it will continue to run until it finds the correct combination. Such a tool makes thousands of guesses per second to speed up the process.

A subset of the brute-force attack is the **dictionary** attack.
Remember the '123456' password? Earlier, we mentioned that it takes less than one second to break this password. Hackers use "dictionaries," which, as you'd imagine, are lists of millions of words. They run the dictionary entries against a website to detect the passwords within seconds. But the dictionary in these types of attacks isn't limited to single words - it can also be a collection of previously leaked passwords or keyphrases. Given that it appears first alphanumerically and is incredibly popular, 123456 will be guessed immediately.

So, if it's not your bank account, is it still a big deal if your details are compromised? YES. Suppose somebody got ahold of your Facebook or Instagram password. They log on and change the password, the registered mobile number, and the address. Your long friend list and your extensive gallery of photos are gone. You've now lost access to the account, and the chances are you won't get it back.

Protecting Yourself
So, how do we prevent that? How do we safeguard ourselves? Here are several tips that we can use to secure our passwords.

The first tip is to **stop sharing your passwords**.

Using social engineering techniques, a hacker might pretend to be from the technical support team and ask you to share your password. Never share it.

Passwords are like house keys, except when you get the house keys back, you don't need to change the locks. When somebody appears to have finished with your password, they still know it. Effectively, they still have the keys until you change the locks. And if you give the wrong person your keys, they'll get inside and change the lock themselves.

The second critical tip is to **avoid repeating passwords**.
We should always use different passwords for different websites. Multiple points of security ensure that if one is compromised, we are still safe with the others. Most users, just for the sake of convenience, use the same password across websites. The problem is that most of us aren't aware if our passwords from one website have been breached, so we're careless. Therefore, it is critical to use different passwords on different websites. You can check whether you've been compromised by typing your email address into Have I Been Pwned?. If so, ensure you update your passwords immediately.

You should also be using **two-factor authentication.**
In most cases, hackers are after user credentials, which they later use to exfiltrate and steal information. Even if hackers get your credentials, they still require a PIN, One-time Password, or even a smart card with two-factor authentication.

You should be aiming to **use complex passwords that avoid using dictionary words, names, places, or birth dates**. Short passwords and passwords made from actual words can often be cracked within minutes. You can actually check the time it takes to break a password on PasswordMonster, though we recommend NOT checking your own **real** password there. But, let's test a random single word, in this case, a name - 'JOSEPH.' As per PasswordMonster, it would take **less than a second** to crack this password. Let's consider another password, 'JCRJSW,' which is random but the same length. It would take PasswordMonster about **24 days** to crack. If we extended it to 'JCRJSW1100', it would take **17 centuries** to break! So, the strength of your password depends on its length and how random it is. A good rule of thumb for a great password is to aim for a total of 16 letters, numbers, and special characters.

The final tip is about the **use of password managers**.
When we create complex, lengthy passwords, we have difficulty remembering them. For the sake of convenience, some of us write the password on a piece of paper or in a diary. That's bad practice. Anyone who gets their hands on the piece of paper or diary has

access to the passwords as well. It's also too easy to lose those things. We should use a password manager to resolve this situation, such as LastPass. We not only get to save all our passwords, but we also lock the password manager with a master password. Instead of remembering 20 passwords, we need to remember the master password.

Password managers also allow us to copy the password and paste it into the password field if a website allows it. This prevents us from typing the password, which can be captured if a keylogger is installed on the system. Since we are not typing the password, the keylogger does not detect the password.

Additionally, when we need to generate a complex password, we can use a password manager, which can generate a long, complex password for us to use.

So, that's a lot of information to digest. But now is always the best time to take action.

That's all for today. Thanks for listening, and remember: keep building the best you.

Reading List

- [Video] watch how a PRO Hacker Hack and Crack Passwords!
- [Video] This is How Hackers Crack Passwords!
- [Video] Generating Rainbow Tables With RainbowCrack
- [Article] Impressive Password Statistics to Know in 2021
- [Article] What Are The Most Common Passwords of 2021?