A Complete Guide of Password

by Ruchir Shah

https://theruchirshah.github.io/Pass-Check/

Index

1 - What is a password ?
2 - How to Choose a Password ?
3 - Password Management
4 - Password Attacks?
5 - Tips and Warnings
6 - Reference Links

https://theruchirshah.github.io/Pass-Check/

by Ruchir Shah

1 - What is a Passsword ?

A **Password** is a word, phrase, or string of characters intended to differentiate an authorized user or process (for the purpose of permitting access) from an unauthorized user, or put another way a password is used to prove person's identity, or authorize access to a resource. It's strongly implied that a password is secret. A password is usually paired with a username or other mechanism to provide authentication.

The password is nothing new. In fact, it has been around for centuries. Way before Google, Twitter and Netflix were prompting you to create a secure code with a funky username, the Roman military reportedly used passwords as a way to distinguish friend from foe.

Basically it was a simple way to protect information. Fast forward a few thousand years. The literary history of the password also includes the classic tale **"Ali Baba and the Forty Thieves"** invented in the 18th century by the French Orientalist Antoine Galland. Used in the tale to open a magically sealed cave, the invocation **"Open, Sesame!"** enjoys broad currency as a catchphrase today, not only in other literary, cinematic and television adaptations of the tale itself, but in many other contexts as well.

2 - How to Choose a Password ?

2.1 - Password components

Before choosing or creating a new password first understand the components of a good password. Including all of the following components in your password will make it very difficult for someone to crack it.

- Use both upper- and lower - case letters
- Numbers
- Symbols
- At least 12 characters
- Not easily decipherable as a real word or phrase upon first glance

2.2 - Avoid These things for passwords.

- Pet, family, or friend names.
- Words/phrases that are too common
- Personal information (your phone number)
- Don't use birthdays, house number in passwords.
- Don't use common words in your password.

2.3 - Pick a main word or phrase that stands out to you. You most likely have several words, a phrase (an album or a song), or something similar that stands out to you for some reason.

- For example, you might pick the name of a song from a specific album, or your favorite phrase from a specific book.

- Make sure that you don't pick a word or phrase that people know you like. (favorite movie, actor, character)

2.4 - Add an abbreviation for your password's service.

For example, if the password is for your work email, you might add "work email" (or "wrk_ml") to the end of the password. This way, you can use the same base password for most services without repeating the exact password anywhere.

- It's important not to repeat your password more than once.
- don't use your Facebook password for your Twitter, etc.

2.5 - Create variations of your password.

While adding an abbreviation to the end of your password will help you remember a specific service's password.

- If you replaced any letters with numbers, you might switch back to using letters and use numbers for different letters in the password.
- For Hello World **"H311oW0rlD"** would become **"h@ll0xoR1d"**

3 - Password Management

Today, a person may have dozens, or even more, personal passwords to manage. In organizations, this number may be even higher, and also include embedded passwords within applications. The sheer number of passwords to manage generally means that, when left to humans, password practices are inadequately followed. Poor password creates opportunities for and hacker exploits.

Password Managers are software applications that enforce best practices for generating and securing passwords (such as by using encryption). By using a master password/key, the user can prompt the password manager to automatically pull the correct password from a database and authenticate into a system/software via form filling. Password managers can be cloud or browser-based, software or app.

A password manager is a program that houses all your passwords, as well as other information, in one convenient location with one master password. The benefits to using a password manager are:

- A password manager will do the work of creating/storing the complicated passwords you need to help protect your online accounts.
- You need to remember only the master password. That single password will give you access to all of your others.
- Many password managers offer the extra layer of protection of two-factor authentication. As a result, each time you attempt to log in to your password manager, a unique, one-time verification code is sent to your mobile phone. To complete the log-in process, you must enter the verification code, in addition to your username and password.

Some best Password Managers

1. LastPass - www.lastpass.com
2. Dashlane - www.dashlane.com
3. Bitwarden - www.bitwarden.com
4. LogmeOnce - www.logmeonce.com
5. 1password - www.1password.com
6. Password Boss - www.passwordboss.com
7. NordPass - wwwnordpass.com

4 - Password Management

Attackers and malware covet passwords, which allow them to access the desired resource, steal data and identities, and wreak havoc. The combination of poor password practices by users, inadequate password security controls, and automated password cracking hacker tools increase the risk of password theft or exposure. Here are some common credential exploit tactics:

4.1 - Brute force attacks

Repeatedly testing a password, potentially generating millions of random guesses per second, with combinations of characters (numbers, letters, and symbols) until one matches. The more mathematically complex a password, the more difficult to crack.

4.2 - Dictionary attacks

Generating password guesses based on words in a dictionary of any language.

4.3 - Pass-the-Hash (PtH) attacks

In PtH attacks, an attacker doesn't need to decrypt the hash to obtain a plain text password, once captured, the hash can be passed through for access to lateral systems. A hacker could elevate privileges simply by stealing RDP credentials from a privileged user during an RDP session.

4.4 - Pass-the-Ticket (PtT) and Golden Ticket attacks

While similar to PtH, these involve copying Kerberos tickets and passing them on for lateral access across systems. A Golden Ticket attack is a variation of Pass-the-Ticket, involving theft of the krbtgt account on a domain controller, which encrypts ticket-granting tickets (TGT).

4.5 - Shoulder surfing

This attack method involves observing passwords (either electronic or hard copy) as they are being entered.

4.6 - Social engineering password attacks

These attacks, such as phishing and spear phishing, involve tricking people into revealing information that can be used to gain access.

- By implementing password best practices, such as via an automated tool, these attacks can be largely deflected or mitigated.

5 - Tips & Warnings

Tips -

- You need to memorize your password.
- If you say the letters or numbers to yourself as you type them you will begin to get a rhythm.
- You might combine several of these methods and still come up with a truly memorable yet very strong passphrase.
- The most secure passwords contain lowercase letters, capital letters, numbers, and symbols. Make a standard of holding down shift for the first four characters, or characters three through seven, or whatever you like. You won't have to stop and remember.
- When coming up with a mnemonic sentence, try to make the sentence funny or relevant to yourself. That way you will find it easier to remember the sentence and the password.
- like **“T&nw8Br@c”** and make phrase like this to remember **“tom and newton won 8 books in running at club”**

Warnings -

- Do not use any of the passwords that are shown as examples on this site! (abc123, iloveyou, etc) Someone might see this too, and might guess yours. Make up your own!
- Do not use any number that is a matter of record, such as phone, address, and Social Security numbers.
- Make sure you're not reusing passwords. It may be tempting to only use one or two passwords for all of your logins, but you should have different passwords for everything.
- Don’t use your birth date in your password.
- Don’t share your password with anyone.

- Don’t email your password.
- Don’t type your password when using the internet on a network you don’t trust.
- Dont use other persons device.
- Pet, family, or friend names.
- Words/phrases that are too common
- Personal information (your phone number)
- Don’t use birthdays, house number in passwords.
- Don’t use common words in your password.

6 - Reference Links

Ruchir Shah

Website - www.ruchir-website.vercel.app

Blog - www.ruchir-blog.netlify.app

Twitter - www.twitter.com/theruchirshah

Github - www.github.com/TheRuchirShah

Linkedin - www.linkedin.com/in/theruchirshah

A Complete Guide of Password

by Ruchir Shah

https://theruchirshah.github.io/Pass-Check/