

WEEK 3: PASSWORD MANAGEMENT

Welcome to the third week of this training. My name is Malusi Faith and I will be your instructor throughout the week. In this video, we will look at password management and we will have a brief overview over the best password management techniques available.

Why Do We Need Passwords?

Before we even delve into password management, why do we even need passwords in the first place? We use passwords in all facets of life. We need passwords in the form of pins, passcodes, patterns and even fingerprints in order to access private locations, private information, money and even valuable items in safes.

Why Should We Manage Passwords?

So, what exactly do we mean when we talk about managing our passwords? What does it involve and why do we even need to manage these passwords? As we are all aware, we live in a heavily digitized time and we need passwords to access increasingly private and sensitive information. So, password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords, as much as they can in order to prevent unauthorized access.

Common Threats Facing Passwords

If we don't manage our passwords securely, they face the risk of being stolen by malicious individuals. Common threats facing our passwords include login spoofing, which is where a user is presented with the regular login prompt, which is actually a malicious program where once they enter their details, which is their user name and their password, this information is then relayed to the attacker.

Secondly, we have sniffing attack, which involves intercepting credentials or communication in order to steal credentials as they are in transit. Third, we have shoulder surfing, which involves obtaining sensitive information, such as pin numbers, ATM numbers, passwords, and other confidential data by looking over the victim's shoulder as they type it on their screen. Fourth, we have the brute-force attack, which consists of an attacker using trial and error to guess password combination with the hopes of eventually finding the correct password.

And finally, we have the data breach or password leak, which involves intentional or unintentional release of private or confidential data to an untrusted environment or to the public domain. All of these threats create an opportunity for attackers to steal user passwords and have unlimited access to your information. This information could be sensitive and critical. It could be your student records, payroll information, financial information of your employees and so on and so forth.

Traditional Password Management

Before we move on to the best practices available, what are some of the typical or traditional methods that individuals and businesses use to manage their passwords? One, we have the use of simple, repetitive, and easy to guess passwords. Two, individuals may create passwords that use identifiable pieces of information, such as their birthdays, their ID numbers, their places of birth, where they live and so on and so forth. Three, individuals and businesses often share passwords through texts, spreadsheets, post-its, sticky notes, and many other ways.

Fourth, individuals may write down passwords on sticky notes and post them on their monitors or on their desks in order to easily remember them. Fifth, individuals and businesses are prone to re-using the same passwords over and over across different or rather multiple websites. And finally, because of how often or how frequently we need passwords, individuals may forget their passwords frequently and may need to use the forgot password option in order to create their passwords all over again.

Best Practices

Hackers are equipped with very advanced tools and techniques that enable them to steal passwords and credentials. So, what best practices can we employ in order to secure our passwords? We're going to begin with password managers. A password manager is a software application that is designed to store and manage online credentials. View a password manager as a book of your passwords, lock to the master key or phrase that only you know or rather have access to. Password managers not only help you store online credentials, they can help you generate and save strong unique passwords every time you sign up to a new website.

Firefox, Chrome, Safari and Internet Explorers are all browsers that have inbuilt password managers but if you plan to use your passwords across your devices, you should probably employ the use of third-party password managers such as OnePass, Keepass and LastPass. Password managers come with both the free and the premium option, depending on the password manager, the free tier usually allows

unlimited syncing across all your devices, auto-filling of your passwords and usernames and basic two factor authentication.

We will look at two factor authentication later. The paid tier offers options to encrypt online storage, safely share passwords with your coworkers or with your students and advanced two factor authentication capability. And because many of the password managers in use have encrypted synchronization across devices, you can take your password with you anywhere even on your phone. Password managers are designed to provide you with access to all of your passwords in an encrypted format, across all your devices in a manner that is not accessible to hackers or even malicious software. Additionally, they can offer a significant convenience while providing outstanding protection and ensuring that your information stays private and safe. Another best practice is to use strong passwords. Earlier, we had looked at the brute-forcing attack. The stronger the password is the more difficult it is to crack using brute-forcing software or technique.

So how exactly do we go about creating strong passwords? One, always use a password length of more than eight characters. The longer the password is, the more secure it is. Two, learn to make your passwords complex. Always include a mix of uppercase and lowercase letters, different numbers as well as different symbols. Avoid passwords that are based on repetition, common dictionary words, letters or number sequences and other easily identifiable pieces of information that may relate to you. These pieces of information include your date of birth, your place of birth, where you live, where you frequent, your best friend, your dog's name and so on and so forth. And finally, you can deliberately misspell a password. You can equally generate strong passwords without having to go through the mental gymnastics of coming up with a strong yet easy to remember password. You can one, use password managers to generate the passwords for you every time you sign up to a new website.

Two, you can employ the use of passphrases instead of passwords. A passphrase usually involves the use of creating a phrase of many random words. Additionally, you can use sentences even with the spaces as passwords. The easier the sentence it is for you to remember, the easier and stronger it is at the same time. Finally, you can employ visual memory. This involves creating a grid of characters and choosing your passwords at random and eventually muscle memory will kick in every time you have to sign up to a new website. While using visual memory, ensure that you don't want to make it too obvious and into a keyboard safe that is easy to be cracked. For example, a very common password that employs visual memory is a use of the first line of your keyboard from Q all the way to P. While this password appears very strong, it is very easy to crack using brute-forcing software.

Additional Password Security Techniques

Now that we have looked at using strong passwords as well as password managers, what other additional password management techniques exist? One, always learn to update the security questions for your accounts. For example, the answer to the question, what is your mother's maiden name is used a lot in security questions. And while this information is in the public domain, it may be used to impersonate you and eventually change your passwords. Two, set up two-factor authentication, two-factor authentication is a second layer of security that is used to protect an account or a system. It increases the safety of online accounts by requiring two types of information from the user. You may enter your passwords but using two factor authentication after entering your password, it may require you to enter a security code or a pin number.

Three, test the strength of your passwords using online testing tools to make sure they're strong enough before you actually decide to use them. Four, use and enable biometric authentication. Biometric authentication relies on the unique biological characteristics of an individual in order to verify their identity. Biometric authentication comes in the form of fingerprint scanning, facial recognition as well as iris scanning. You can use these techniques in order to secure your devices. Always learn to separate your personal and business accounts, as well as the passwords used to access all of these accounts. This makes it easier to spot phishing emails, as well as manage these passwords. Additionally, it compartmentalizes attack. For example, if your personal email is compromised, it is very difficult for the probability of your work email being compromised is low. Another best practice is to always avoid passwords re-use. Use one password for one account. If a password is unknowingly compromised, the window of opportunity a hacker has to use this password is very limited. Once a hacker has access to a password that you have used across many websites and accounts, it is very easy for them to get as much information as they can from you. Finally, do not write passwords down and leave them in very obvious places such as on your desk or even on your monitor. This brings us to the end of this video. In this video, we have learned about the need of password management, and we have seen the best practices available, which include both a password manager and creating strong passwords. Next, we will look at how to identify a bad password.