



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

PASSWORD MANAGEMENT

Mode of Delivery: Video

Objectives

At the end of this module, the learner should be able to:

- Create and use secure passwords
- Manage passwords securely
- Identify and avoid the use of bad passwords.

We use passwords in almost all facets of our lives across almost all our devices. On our phones and laptops/computers in the form of PINs, patterns, passcodes or passwords, and in some instances we use our fingerprints. We use PINs to access our money in ATMs, and our valuables in safes, as well as biometric information such as iris scanning, facial recognition or fingerprints to access locations that have limited access. Passwords are all around us and we use them more than we think we do.

Why should we manage our Passwords?

There are many challenges in securing passwords in this digital era. When the number of web services used by individuals is increasing year-over-year on one end, the number of cyber crimes is also skyrocketing on the other end.

Here are a few common threats to protecting our passwords:

1. Login spoofing is where a user is presented with a regular login prompt, which is actually a malicious program where once they enter their username and password the credentials are then relayed to an attacker.
2. Sniffing attack involves intercepting communication in order to capture personal information in transit.
3. Shoulder surfing attack involves obtaining sensitive information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder as they type it.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

4. Brute force attack consists of an attacker using trial-and-error to guess password combinations with the hope of eventually guessing the correct one.
5. Data breach and password leaks involves intentional or unintentional release of private/confidential information to an untrusted environment.

Why should we manage our Passwords?

What are some of the traditional ways in which we have managed our passwords?

1. Using simple, repetitive and easy to guess passwords such as pass123
2. Creating passwords that use identifiable pieces of information such as birthdays, IDs, e.t.c
3. Sharing passwords in emails, over text e.t.c
4. Writing down passwords in notebooks, sticky notes and post-its etc
5. Reusing the passwords across different web applications.
6. Frequently forgetting passwords and using the 'Forgotten Password' feature.

Best Practices

Use Password Managers

View a password manager as a book of your passwords, locked by a master key that only you know. Password managers not only store your passwords, they help you generate and save strong, unique passwords when you sign up to new websites. Firefox, Chrome, Safari and Internet Explorer all have built in password managers. But if you plan to use your passwords across devices, you probably should use one of these:

- 1 Password (Windows, Mac, iOS, Android)
- LastPass (iOS, Android; Chrome plugin works on Windows, Mac, Linux)
- KeePass (Linux, Windows, Mac, Android)



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Password managers come with both the free and paid options. Depending on the password manager, the free tier usually allows unlimited syncing across all your devices, auto filling and basic two-factor authentication (2FA). The paid tier offers options to encrypt online storage, safely share passwords and advanced 2FA capabilities.

And because many of the password managers in use have encrypted sync across devices, you can take your passwords 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 that is not accessible to hackers or malicious software. They can offer significant convenience while providing outstanding protection and ensuring that your information stays private.

Use Strong Passwords

Guidelines For Strong Passwords

1. Use a password length of at least eight characters, preferably 15 or more characters. A longer password is a more secure password.
2. Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.
3. Avoid passwords based on repetition, common dictionary words, letter or number sequences and other easily identifiable pieces of information such as your date of birth, your place of birth, year of birth, ID number etc.
4. Deliberately misspell a password. For example, Smith = Smyth = 5mYth



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

How to Generate Passwords

1. Use password managers to store and even generate passwords for you.
2. If possible, employ the use of passphrases instead of passwords. A passphrase involves the use of creating a phrase of many random words e.g 'Th15i5As7r0nGA4a5spRA5e' based on (thisisastrongpassphrase). Additionally, you can use sentences as passwords, if spaces are allowed. This site helps you generate secure passphrases.
3. Employ visual memory, create a grid of characters and choose your password at random and eventually muscle memory kicks in. While using visual memory, ensure you don't make it too obvious and into a keyboard sweep that's easy to figure out such as 1q2w3e4r5t

Additional Password Security Techniques

1. Update the security questions for your accounts. Always avoid using correct information e.g the answer to this question 'What's your mother's maiden name?' is publicly available.
2. Set up two-factor authentication for your accounts. Two-Factor authentication is a second layer of security that is used to protect an account or system. It increases the safety of online accounts by requiring two types of information from the user, such as a password or PIN, an email account, an ATM card or fingerprint, before the user can log in.
3. Test the strength of your password using an online testing tool to make sure it is strong.
4. Enable biometric authentication. Use facial recognition, iris scanning and fingerprint scanning on our devices where applicable.
5. Separate business and personal accounts and their passwords. This makes it easier to spot phishing mails and eases password management. Additionally, it compartmentalises attack, for example, if your personal email is compromised, the possibility of your work email being compromised is low.
6. Avoid password re-use. If a password is unknowingly compromised, the window of opportunity for the attacker to use the password is limited.
7. Do not write passwords down and leave them in obvious places such as on the desk or monitor.



COMMONWEALTH
of LEARNING

Teacher
Education

CYBERSECURITY TRAINING FOR TEACHERS (CTT)
