The Importance of Password Managers and MFA Codes for Seneca Polytechnic Students and Employees

Published 10/9/2024 by Giuseppe Aloisi

In our modern digital landscape, where technology revolves around every aspect of our lives, from academic pursuits to financial transactions, protecting our personal data has become paramount. One of the most potent strategies to fortify your online security is combining a password manager and Multi-Factor Authentication (MFA) codes. This article aims to acknowledge the significance of these tools and offer accessible options to facilitate your journey toward enhanced digital safety.

Why Use a Password Manager?

1. Keeps Your Passwords Safe

A password manager securely stores all your passwords in one place. This means you won't have to remember dozens of complex passwords, reducing the temptation to reuse simple ones.

2. Generates Strong Passwords

Password managers can create strong, unique passwords for each of your accounts. This makes it much harder for hackers to gain access.

3. Prevents Password Reuse

Reusing the same password across multiple sites is a big security risk. If one account gets hacked, all your other accounts are vulnerable. A password manager helps you avoid this by encouraging unique passwords for every login.

4. The numbers don't lie

- **13%** of Americans use the same password for every account.
- **59%** of US adults use birthdays or names in their passwords.
- **30%** of internet users have experienced a data breach due to a weak password.
- **Two-thirds of Americans and Canadians** use the same password across multiple

accounts.

Source:

MFA Codes: An Extra Layer of Security

MFA adds steps to the login process, making it much harder for someone to access your accounts. Here's how it works:

1. **Enter Your Password**: You log in as usual.

2. **Receive a Code**: A temporary code is sent to your phone or email.

3. **Access Granted**: You enter the code to complete your login.

Even if someone knows your password, they can't access your account without the MFA code.

Keep Your MFA Codes Private

MFA codes are time-sensitive and should only be shared with the intended service. Never share these codes with anyone, as doing so could compromise your account security.

Tips for Keeping Your Passwords and MFA Codes Secure

1. **Use Unique Passwords**: Always use different passwords for different accounts. A password manager makes this easy.

2. **Enable MFA**: Whenever possible, turn on MFA for your accounts. It adds an extra layer of security.

3. **Keep Codes Private**: Never share your MFA codes. Treat them like your passwords.

4. **Regularly Update Passwords**: Change your passwords periodically, especially for sensitive accounts.

5. **Be Wary of Phishing Attempts**: Don't click on suspicious links or share your information without verifying the source.

Available Password Managers

Here are some user-friendly password manager options to consider:

*Seneca won't provide support and they shall be used at the user's discretion

Online Password Managers - accessible your password vault anywhere on the Internet with secure access

LastPass	**Features**: Easy to use, available on multiple devices, and offers a free version. **Pros**: Automatic password generation and secure sharing options.
1Password	**Features**: Intuitive interface with strong security features. **Pros**: Great for families and teams; includes a password vault.
Bitwarden	**Features**: Open-source and free to use, with premium options available. **Pros**: Transparent security practices and easy to navigate.

Offline Password Managers - saved offline, your password vault and security are only accessible to those with physical access to the password vault.

KeePass	**Features**: A free, open-source option that stores passwords locally. **Pros**: Does not require an internet connection, making it very secure. - Available on your Seneca laptop company portal
Password Safe	**Features**: Simple and effective, this program allows you to store your passwords offline. **Pros**: Easy to set up and use for those who prefer keeping their data private.