Tips to secure your computing devices and online accounts

Published 11/22/2023 by Giuseppe Aloisi

How many electronic devices do you have on your person, or in your household? Do you only have one, three, five, or maybe more? Whatever your answer may be, all these devices can pose a danger to yourself and your online accounts. As a student, you sometimes find yourself using your devices for work, school, and personal use. With this in mind, it is important to secure your devices and protect yourself so that you do not expose your personal accounts/information. Through this blogpost, we will explain how to keep your devices safe from criminals and threat actors.

Use Strong Passwords

Your accounts are only as safe as you let them be. Creating accounts with strong, and unique passwords can allow them to be extremely secure. When you are making a password, there are some basic requirements you should meet. Seneca Polytechnic has a set of password guidelines that can be extremely useful in securing your online presence. For more information on this please visit Password Rules.

Use a Password Manager

Password managers are a great tool to help you keep track of your passwords, there are a variety of online and local password managers you can use. These password managers range in capabilities, but most allow you to create complex passwords while also saving them in a secured database. There are some risks to using them, such as if you are using an online password manager they could have a data breach, or if you use a personal password manager on a USB and it gets stolen.

For more information, visit our Password Wiki

Use Two-factor Authentication (2FA)

While you are at Seneca, you may often find that whenever you try and log in you must receive a code from an authenticator app, or a text message. This is an example of Two-factor Authentication (2FA), and is encompassed by Multi-factor Authentication (MFA). Using a second form of authentication allows you to log in more securely and incorporates something you have on a device (MFA code such as Duo at Seneca) in addition

to something you know (A password).
The combination of a password and MFA on a device allows for more secure authentication and validation of the user's account.
There are a variety of applications that can aid authentication when logging in, some of the applications are Google Authentication, Microsoft Authenticator, 2FAS, and Duo.

We strongly recommend you do your own research and carefully pick a manager that you trust.

Avoid Public WIFI

When travelling you may find yourself connecting to a public Wi-Fi network. These networks are usually networks with no password, you can find these at the airport, coffee shop, or your local library. The reason why public Wi-Fi network is risky is that anyone can connect to them, and anyone can snoop on them. This can become an issue when you access your bank details over the network, or if you access some other private material. If you do choose to use a public network, make sure you use websites that have the lock in the top left of the address bar or make sure the website starts with https://. This means the connection is encrypted to the website.

Secure Physical Access to Your Device

While you may have a lot of digital security in place, such as strong passwords, 2FA, or a password manager, these can all be bypassed by accessing a device physically. When someone is able to access your device physically, they can do a variety of things such as install malware, steal data, or even just steal your device altogether. This is why it is important to have devices stored in a secure location or kept in your line of sight so that you can ensure a device is not tampered with.

Enable Device Encryption

Encrypting your devices is essential for safeguarding your sensitive information and protecting your privacy. In an increasingly digital world, where personal and professional data is stored on smartphones, laptops, and tablets, encryption serves as a crucial barrier against unauthorized access. It ensures that even if your device falls into the wrong hands or is compromised, the data remains inaccessible without the decryption key. By encrypting your devices, you shield your financial records, personal messages, login credentials, and other valuable data from prying eyes, hackers, and potential security breaches, ultimately providing peace of mind and enhanced security in our interconnected age.

Lock your Devices with a pin or passcode

Locking your devices with a PIN or passcode is a fundamental security measure that safeguards your personal information and privacy. In a world where smartphones and tablets contain a treasure trove of sensitive data, such as emails, photos, and financial details, a PIN or passcode acts as a vital first line of defense. It ensures that only authorized users can access your device, preventing unauthorized access in case it's lost or stolen. Without this protection, anyone can potentially access and misuse your personal information, putting your digital identity and assets at risk. Locking your devices is a simple yet effective way to fortify your digital security and maintain control over your sensitive data. When you leave your desk, consider locking your Windows or Mac device with the following shortcuts.

Windows: Windows key + L
Mac: Control + Command + Q