ISSUE
1
February
2023

Security Awareness Bulletin

In this issue

Creating Strong Passwords and Keeping Them Secure

CYBER-ATTACKS

are a growing threat to our online security and the security of the school. To enhance our collective secure practices and protect ourselves and the school from cyber-attacks, we must be proactive about password security.

Here are some best practices for creating strong passwords and keeping them secure.

By following these best practices, we can better protect ourselves and the school against cyber-attacks. Let's make security awareness a part of our daily practices and work together to stay informed and vigilant in the face of cyber threats.

If you have any questions or concerns regarding password security, reach out to IT Security at ITSecurity@smus.ca.

Together, we can keep our digital presence secure.

A strong password is your first line of defense, guard it like it's the crown jewels.

Length Matters

The longer the password, the harder it is to crack. Aim for a minimum length of 12 characters or more. Consider using a passphrase, a sequence of words that form a password, such as "mykidlovesawefulburgers" or "forthefirsttimeinforever". This type of passphrase is easy to remember, yet difficult to guess and provides stronger protection.

Mix it Up

Use a combination of uppercase and lowercase letters, numbers, and symbols to create a more secure password, for example “myk1d!0v3s@w3fulburg3rs”. Avoid using easily guessable information such as your name, birthdate, or address.

Store Passwords Securely

Store passwords in a secure password manager or encrypted file. Unsecured methods of storing passwords, such as writing them down on a piece of paper or saving them in an unencrypted file on a computer, make them vulnerable to theft or accidental exposure. A secure password manager, such as 1Password, Keeper, LastPass, uses encryption to protect passwords and stores them behind a master password, making it difficult for cybercriminals to access them. Password managers also generate strong, unique passwords for each of your online accounts and save them automatically, reducing the risk of password reuse and password fatigue.

Avoid Reuse

Don't reuse the same password across multiple accounts. If a cybercriminal gains access to one password, they could potentially access all of your accounts.

Regularly Change Passwords

Change your passwords regularly, at least every three to six months. This reduces the amount of time a cybercriminal has to access your accounts and sensitive information.

Don't Share Passwords

Sharing passwords is a dangerous practice that puts you, your online accounts, and the school's confidential data at risk. Never share passwords with anyone, even friends and family members. If you need to share access to an account, use alternative methods such as creating a new account or granting access through the account settings.

Enable Two-Factor Authentication

Whenever possible, enable two-factor authentication for an added layer of security. This requires a second form of authentication in addition to your password, such as a code sent to your phone or a biometric verification.

Be Cautious with Social Media and School Accounts

Social media and school accounts often contain sensitive information and should be protected with strong and unique passwords. Be cautious when logging into these accounts on public Wi-Fi or shared computers and regularly change your passwords to stay protected. Do not use your school account for personal social media account.

Watch Out for Phishing Attacks

Phishing attacks are a common method used by cybercriminals to steal passwords and other sensitive information. Be cautious when receiving unexpected emails or messages requesting personal information or login credentials, and never click on links or download attachments from unknown sources.