



## In this issue

Security Knowledge Test

Are you up to date on your security know-how? Put your security smarts to the test!

Welcome to this month's security bulletin! In this edition, test your knowledge on various security topics that we have covered in the past. So, if you have been keeping up with previous security bulletins, you should be well-prepared to answer the questions that we have in store for you. Don't worry if you haven't read all the previous bulletins, you can find them on the SMUS IT Intranet page. We hope that you find this month's security bulletin both informative and fun!

**1. What is the recommended minimum length for a password?**

- a. 1 character
- b. 2 characters
- c. 12 characters
- d. 1,000 characters

**2. Which of the following should be avoided when creating a password?**

- a. Three key ingredients from your favourite recipe mixed with numbers and special characters
- b. A long catchy phrase from your favourite movie or book, mixed with numbers and special characters
- c. A long word combined with the translated word from another language, mixed with numbers and characters
- d. Easily guessable information such as your name, birthdate, address, or short simple words

**3. How should passwords be stored securely?**

- a. Storing them in a secure password manager or encrypted file
- b. In your sock drawer
- c. In a clear plastic bag on your desk
- d. Sharing them with your arch-nemesis

**4. Why should you avoid reusing the same password across multiple accounts?**

- a. Cybercriminals get bored seeing the repeating password repeatedly
- b. It makes it easier for cybercriminals to access all your accounts
- c. It makes it harder for your friends to guess your password
- d. It increases the risk of password fatigue

**5. What is two-factor authentication?**

- a. Using two different passwords
- b. Using two different usernames
- c. A second form of authentication in addition to your password
- d. A fancy way of saying "double secret password"

**6. What is phishing?**

- a. A type of fishing where you try to catch a computer
- b. An activity where you send emails to your pet fish
- c. A type of cyber-attack where an attacker attempts to trick you into providing sensitive information by posing as a trustworthy entity
- d. It is a tangy-tasting fish recipe

**7. How can you recognize a phishing email?**

- a. The email has misspelled words, grammatical errors, and a sense of urgency to prompt you to act quickly
- b. It includes a photo of a prince offering you a share of his wealth
- c. The email is written in a language you don't understand, such as Klingon
- d. By requesting your nearest post office to check the email

**8. How can you protect yourself from phishing attacks?**

- a. Only use your computer while wearing a tinfoil hat
- b. Never use the internet on a Tuesday
- c. Look for suspicious emails, be wary of links, check the sender's email address, and keep your software up to date
- d. Don't stay too close to fishers when they cast a fishing line with an attached hook

**9. What is the simplest way to keep your devices and software updated?**

- a. Enable automatic updating on all your devices
- b. Check for updates manually every day
- c. Sacrifice your password to the tech gods
- d. Placing your device under a pillow so tooth fairy can take care of it

**10. Why is it important to enable multi-factor authentication (MFA) for your personal email or financial accounts?**

- a. It is a fun challenge to enter a code every time you log in
- b. You can impress your friends with your high-tech security measures
- c. MFA is the single most crucial step you can take to secure any online account
- a. So you can get a secret way to access a secret club of tech geeks

**11. If you have any questions or concerns regarding security, who you gonna call?**

- a. The Avengers
- b. Batman
- c. Ghostbusters
- d. IT Security at ITSecurity@smus.ca