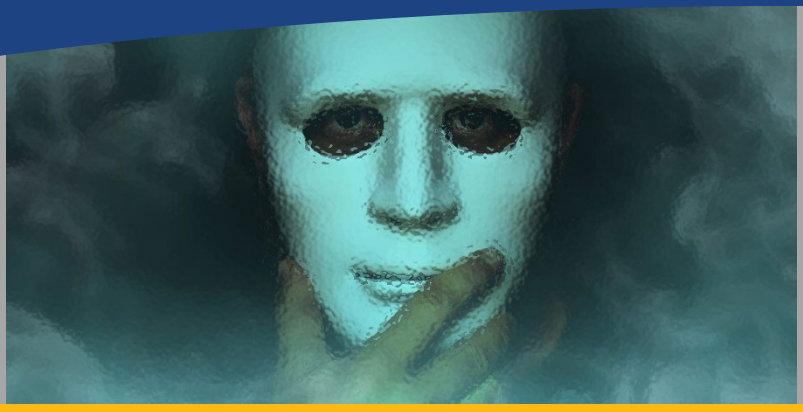
ISSUE
5
June
2023

Security Awareness Bulletin



In this issue

Be Cautious, They're Pretentious.

In an era where digital communications have permeated every aspect of our lives, the risk of cyberattacks, particularly social engineering, has drastically increased. Social engineering, by design, manipulates human trust to acquire confidential information. It is vital for us to be aware of these tactics and know how to safeguard ourselves. This bulletin will illustrate some examples of social engineering and provide guidelines to avert these threats.

What is Social Engineering?

Social engineering exploits human psychology, using manipulation to trick individuals into divulging sensitive information or granting access to secure systems. The attacker usually masquerades as a trusted entity, making their deceit even more potent.

Examples of Social Engineering Attacks

1. **Phishing**: An attacker sends an email impersonating a reputable company (like a bank) asking for your login credentials or convincing you to download a malicious attachment. For instance, you could receive an email that appears to be from your bank, warning you about a suspicious transaction and asking you to confirm your account details.
2. **Baiting**: Here, the attacker offers a lure (like free music or movie downloads) that, once downloaded or clicked on, infects your computer with malware. For example, a pop-up window could suddenly appear on your screen, promising free access to a popular software if you just download a particular file.
3. **Pretexting**: The cybercriminal poses as someone who legitimately needs data from you to perform a critical task. They might pretend to be a school IT staff member asking for your login details to perform a necessary system update. At SMUS, we will never ask you for your password.
4. **Quid Pro Quo**: The attacker offers a service in return for your information or access. This could look like someone offering to install a piece of software or to fix a non-existent problem on your computer in return for your password.
5. **Tailgating**: In this case, an unauthorized person physically follows an authorized person into a secured area. This might occur if someone unfamiliar holds the door open for you and enters a secure staff area without scanning their own access card.

Recognizing Social Engineering Attacks

To protect ourselves, we must learn to spot potential threats. Signs of a social engineering attack may include:

- Urgency: Attackers often create a sense of urgency, pressuring you to act quickly to avoid negative consequences.
- Generic greetings: Phishing emails may start with a vague "Dear User" instead of your actual name.
- Spelling and grammar mistakes: Cybercriminals often overlook these details, resulting in errors within their deceptive messages.
- Suspicious attachments or links: Be cautious of unexpected or unknown attachments or links, especially within unsolicited emails.

Protective Measures Against Social Engineering

Staying protected requires a proactive approach. There are several precautions we can all take to fortify our defenses against social engineering attacks. By incorporating the following measures into our daily routines, we can significantly reduce our vulnerability and ensure the security of our information and systems:

- **Double-Check**: Always authenticate the source. If a message seems suspicious, even if it appears to come from a known contact, confirm with them through another method before taking any action.
- **Think Before You Click**: Be wary of links or attachments from unfamiliar senders. Be especially careful with messages that attempt to rush you into action.
- **Keep Software Up-to-date**: Regular software updates often contain vital security enhancements that protect you from known threats.
- **Use Robust Passwords**: Employ long, strong, unique passwords for all of your accounts to enhance your security profile.
- **Limit Personal Information Sharing**: Authentic organizations typically do not request sensitive information via email. Even on the phone, be cautious about divulging personal details unless you initiated the call and are confident in the legitimacy of the recipient.
- **Regular Training**: Engage in ongoing security awareness training to stay informed about evolving threats. SMUS will be introducing online training in the Fall 2023.

Reporting Potential Social Engineering Attacks

Should you encounter a suspected social engineering attempt, avoid engagement and immediately report the incident to our IT department for analysis. Please provide as much detail as possible without further interaction with the suspected entity.

A collective, informed approach to social engineering threats is the best defense we have. Stay vigilant, stay safe, and let us protect our school community together.

Stay Informed, Stay Safe

Our commitment is to ensure a secure digital landscape for all. We encourage all faculty and staff to remain alert and promptly report any suspicious behavior.

Answers to Issue 4 Security Knowledge Test Questions

Are you ready for the moment of truth? It's time to unveil the answers to the thought-provoking questions from our previous bulletin. We hope you had an exhilarating time testing your security knowledge and now it's time to see how well you did. Whether you aced the quiz or stumbled upon a few surprises, we commend you for your dedication to staying informed and secure.

1. What is the recommended minimum length for a password?
   c. 12 characters
2. Which of the following should be avoided when creating a password?
   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
4. Why should you avoid reusing the same password across multiple accounts?
   b. It makes it easier for cybercriminals to access all your accounts
5. What is two-factor authentication?
   c. A second form of authentication in addition to your password
6. What is phishing?
   c. A type of cyber-attack where an attacker attempts to trick you into providing sensitive information by posing as a trustworthy entity
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
8. How can you protect yourself from phishing attacks?
   c. Look for suspicious emails, be wary of links, check the sender's email address, and keep your software up to date
9. What is the simplest way to keep your devices and software updated?
   a. Enable automatic updating on all your devices
10. Why is it important to enable multi-factor authentication (MFA) for your personal email or financial accounts?
    c. MFA is the single most crucial step you can take to secure any online account
11. If you have any questions or concerns regarding security, who you gonna call?
    d. IT Security at ITSecurity@smus.ca