Staying Cyber Safe on Social Media

We often see cyber security attacks on the news, but the reality is, cyber-attacks always happen when you least expect them. And when they happen, they happen quickly to anyone or any organization. We especially aren't always thinking about how our own social media accounts can leave us vulnerable to social engineering attacks. This week, the Education and Centre of Excellence is here to help you learn about cybersecurity vulnerabilities on social media and how to stay cyber safe!

What Makes You Vulnerable on Social Media?

- **Posting revealing information about your personal and professional life**- this can help threat actors gather data for social engineering attacks on you or your organization.
- **Keeping profiles public and accessible to everyone-** allowing anyone to have access to your profile makes it easier for threat actors to gather personal or company information from your profile.
- **Engaging with all content without vetting it first-** not vetting whether or not links are safe and reliable to click can lead to malware or ransomware attacks.
- **Using social media on public Wi-Fi hotspots-** public Wi-Fi is a common location for attackers to access your data and information. Attackers use public Wi-Fi networks to intercept data and inject malware into the connected devices.

Social Media Best Practices

- **Manage your privacy and security settings**- managing your privacy and security settings will help you control who sees and has access to your social media content.
- **Be aware of who follows your account**- only engage with people you know.
- **Be cautious of what you are posting**- am I releasing any private information about myself or my organization?
- **When in doubt, don't post it**- if you feel hesitant about posting certain information, keep it private.
- **Click links with caution**- social media accounts are regularly breached. Look out for language, content, or behaviour that is out of the norm.
- **Keep up to date on privacy policies**- be aware that privacy policies can change and keep up to date on how they impact you or your organization.

- **Use social media on a secure Wi-Fi network or personal cellular data**- only use hotspots or networks that are trusted, and password protected.
- **Enable multi-factor authentication (MFA)-** use MFA where possible, for your social media accounts.

Want to know more?

Social media is a great place for threat actors to gain information in order to engineer an attack that will specifically target and exploit you or your organization. That's why it is so important to follow our social media best practices so you can stay cyber safe. Tune in to the weeks to come to learn more about social engineering and other cyber threats! For more information, head over to the Knowledge Library on the Cyber Security Ontario Learning Portal.