Staying Safe on Social Media

Social media platforms such as Facebook, Twitter, Instagram, Snapchat, and LinkedIn can be amazing resources. They allow us to meet, interact and share with people from all walks of life all around the world. However, all of this connectivity brings an inherent risk to all users (their friends, families, and employers too) of the platforms. In this communication we're going to cover what these dangers are and how to utilize these sites with a security-oriented approach.

Privacy

A common concern with social media is protecting your personal information. Potential dangers include:

- **Attacks Against You:** Cyber criminals can analyze your behavior on social media and leverage the information that's posted there to potentially gain access to your various online accounts. For example, they can likely guess the answers to your challenge questions that reset your passphrases if that information is readily available on social media. A criminal could also build a targeted phishing email against you—this is what's known as spear phishing attack using information shared on social media.
- **Attacks Against Marcus:** Criminals can use any sensitive information you post about Marcus against the organization. The best protection is to limit what's posted online. Privacy options provided by social media organizations give a thin layer of protection, but anything you post online, publicly or privately, is only as secure as the people you share that information with. The more friends you share with, the more likely that information will become public. You should assume that anything you post on social media can or will become public and a permanent part of the Internet.

Security

In addition to privacy concerns, here are some steps to help protect your social media accounts and online activities:

- **Login:** Protect each of your accounts with a strong, unique passphrase and do not share them with anyone else. Now many social media and email providers support multi-factor authentication (MFA). It's recommended to always enable multi-factor authentication when the service is provided.
- **Privacy Settings:** If you do use social media platforms, make sure to check your privacy settings to ensure you aren't sharing too much data with the social media company or other users. You may be surprised at how much data you're giving to companies when going through the Privacy Settings.

Email: You should always be cautious when reviewing email notifications that claim to come from social media sites. Fraudsters can easily create phishing messages that look like they're notifications from social media sites in order for you to click on a potentially malicious link or download an attachment with malware on it.

Final Notes

- **Oversharing on social media can lead to cyber criminals gaining access to your various online accounts**
- **Information you share online is only as secure as the people you share that information with.**
- **Review your privacy settings on the social media platforms that you frequent to ensure you aren't unknowingly sharing information or letting organizations collect your data without your consent.**

While social media platforms can be used to keep in contact with friends, family, and coworkers, it can also be leveraged by unscrupulous individuals or groups to build profiles against you and potentially compromise your various accounts. It's advisable to use caution when sharing personal information on social media as it could be used against you.