How to Secure Social Media Accounts (CSB20-08)

The most popular social media platforms have billions of users, and the number keeps getting bigger every year. These are initially for sharing, entertainment and communication. Now, enterprises see them as valid advertising tools and users have built careers out of sharing content. Also, other applications are using major social media accounts to validate user identify – you can sign up for different apps and games just using Facebook or Twitter account. And employers now routinely check prospective employees on social media, using it as a type of character check.

SECURITY RISKS

Mine personal information – social media accounts can lead to shopping accounts or even have banking information

Gain access to corporate networks – hackers could compromise enterprise networks if your social media is linked to your work email

Steal identity – one account can be used to register on another site

Blackmail user and friends – hackers can use sensitive information to harass the victim and even their list of friends

HOW TO SECURE

- Close the accounts that you're not using. Forgotten social media accounts may be compromised without being noticed. Hackers can leverage these and access other accounts linked to it, like your email.
- Check what apps are connected to your social media. Do you use Facebook or Google to sign in for any other applications? Assess if this type of access is necessary.
- Practice good password hygiene. Use different passwords for your social media accounts, and also make sure each password is complex and unusual. Enabling 2FA for all your accounts can prevent unauthorized parties from accessing your accounts.
- Keep your mobile apps updated. Make sure you have the latest version of the platform you're using. Security patches protect you from the newest known threats.
- Use a unique email for your social media accounts. If possible, create a whole new email specifically for social media accounts so that if you are compromised, the hackers won't have access to any valuable information.

FOR CORPORATE SOCIAL MEDIA ACCOUNTS:

- Monitor your social media regularly—keep an eye on what's happening on all your social media platforms.
- Limit access to only the necessary people—the fewer people with access, the better. This makes it easier to control the posts and avoid any deliberate sabotage.

- Separate what is personal and what is professional—you don't want to accidentally post something personal on a corporate account.
- Audit which tools have access to your accounts—regulate tools that help with posting since they might be vulnerable to attacks.
- Be aware of the latest security solutions—some platforms might be moving away from passwords soon, or they may be implementing a new security feature that you may want to implement.
- Like all users, practice good password hygiene and also implement strict policies about patching and updating.

REFERENCE

- https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/best-practices-how-to-secure-your-social-media-accounts; and
- https://itms.pnp.gov.ph/main/storage/2020/02/socmed.pdf