USE OF PERSONAL SOCIAL MEDIA IN THE WORKPLACE

MARCH 2019 **ITSAP.00.066**

SOCIAL MEDIA IN THE WORKPLACE

Social media gives you the power to connect with others effortlessly and share information instantly. Since these services and platforms have become so integrated and integral to daily online activities, many employers allow employees to use personal social media accounts at work. However, when you use personal social media at work, you can be providing threat actors easy and obvious entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk.

RISKS OF USING PERSONAL SOCIAL MEDIA ACCOUNTS IN THE WORKPLACE

Whether you share images on Facebook, tweet or post content to your LinkedIn page, your activity can reveal a lot of information about you or your organization which can then be exploited. Some risks include:

MALWARE AND VIRUSES

Cyber threat actors can introduce malware (which can include viruses, trojans and worms) to a device or network through social media. By clicking on a shortened URL, photo, or advertisement, you can be opening the door to serious cybersecurity attacks on your organization's devices and network. Be wary of clicking on anything suspicious when using your personal accounts in the work place. If you suspect you may have been compromised contact you IT security team.

SOCIAL ENGINEERING

The more information you reveal on social media, the greater the possibility of you becoming a target for a threat actor. Be aware that what you share and post becomes publically available information that can ultimately be used in well-crafted social engineering scams. Cyber threat actors can use this information to imitate you and send targeted emails containing malware to colleagues in your organization. If they are fooled into opening the email and any attachments, it can lead to malware infecting their computers and corporate networks.

For more information on spear-phishing, read CCCS's *ITSAP.00.100 Spotting Malicious E-mail Messages.*

UNINTENTIONAL LOSS OF DATA

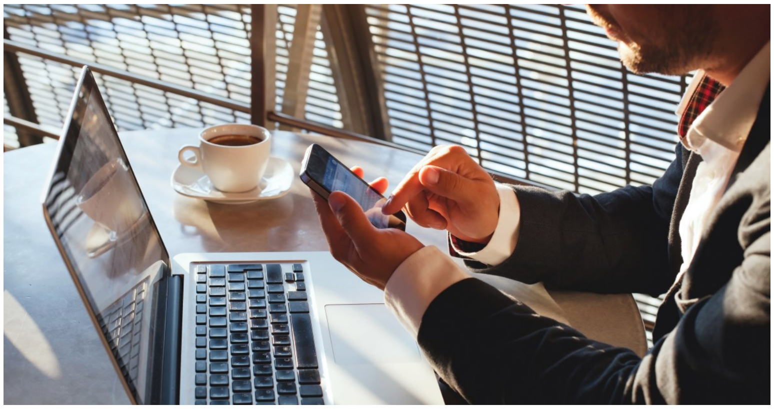
It is important to think before posting work-related material to a personal social media account. Whether it is sharing the physical location of your place of work, or making what may seem like an innocent post about a project you completed, you may be unintentionally helping threat actors gather information about your organization. Even with the highest privacy and security settings your personal social media account can be compromised by a threat actor, not only can they gain access to your personal data, but they can also gather data about any of the work contacts you may have. This can help them build a clearer picture of your organizational structure.

THE RISKS OF USING PERSONAL SOCIAL MEDIA AT WORK ARE REDUCED BY:

- Using a unique, and lengthy passphrase or password (if supported by the website or application) for each of your accounts
- Seeking approval before posting work-related information on a personal account
- Limiting the use of tracking or location services in social media apps
- Using two-factor authentication when available
- Only accepting friend, follower or contact requests from people you know
- Being wary of posts containing unusual language or content
- Using caution when clicking on shortened URLs; They could direct you to a malicious site
- Avoiding revealing private information on personal accounts. (e.g., home address, birthdate or SIN); The more you share, the easier it is for a threat actor to steal your identity
- Periodically reviewing privacy settings to control who sees what
- Signing out or log off when you're done using your accounts

Even if you take all these precautions always notify your IT security team immediately if you notice abnormalities or if you suspect your account has been compromised.

It is also important to note that when you identify your place of work in your profile and share your opinions and views on social media, you and your organization's reputation can be impacted. Negative comments or poor online behaviour by you can lead to unwanted attention for both you and your workplace.



CONSIDERATIONS WHEN USING CORPORATE SOCIAL MEDIA ACCOUNTS

If you manage or maintain a corporate social media account, consider the following guidance to help reduce the chance of the account being compromised.

- Ensure that the organization's internet usage and social media policies are read and understood by all who have publishing rights
- Limit the number of people who have administrator or publishing rights to the corporate account
- Seek final approval before publishing any content or making a post to official accounts
- Publish content using only trusted applications and devices
- Enable password protection on corporate mobile devices
- Keep web browsers, operating systems, and apps up-to-date

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**