Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Use of personal social media in the workplace

February 2023

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 systems. You can even be placing your online identity and that of your co-workers at risk.

What to consider when joining social media applications

- Research the social media platform you want to join or use, including review of publicly available information
- Take time to understand the platform's privacy, data collection and data use policies, their requirements for permissions, and their terms and conditions of using the application to know what data will be accessed and where it will be stored or transmitted
- Understand the ownership, control or influence, and data residency—the vendors and owners of the platform are subject to the laws of their region, which could impact the security and privacy of users
- Know which features and elements of your devices can be accessed by the app, such as your camera, microphone, location, and contacts list

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 your organization's Internet usage and social media policies are read, understood, and adhered to, especially by users who have publishing rights
- Limit the number of users in your organization who have administrator or publishing rights to corporate social media
- Ensure all authorized users have separate accounts, with unique credentials, when publishing content.
- Seek final approval before publishing any content or making a post to official accounts
- Publish content using only trusted and approved applications and devices
- Secure corporate devices with multi-factor authentication (MFA) and strong passwords or passphrases
- Keep web browsers, operating systems, devices, and applications patched and up-to-date

AWARENESS SERIES

Cat. No. D97-1/00-066-2023E-PDF
ISBN 978-0-660-47410-6

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:

Unintentional loss of data

Think before posting work-related material to a personal social media account. Whether you share the physical location of your place of work, or make 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.

Malware and viruses

Threat actors can deploy malware 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 cyber security attacks on your organization's devices and network. Be wary of clicking on anything suspicious when using your personal accounts in the workplace. If you suspect you may have been compromised contact your 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 publicly available information that can ultimately be used in well-crafted social engineering scams. Threat actors can use this information to imitate you and send targeted emails containing malware to colleagues in your organization. If the recipient is fooled into opening the email and any attachments, it can lead to malware infecting their device and corporate networks.

For more information on spear-phishing, see ITSAP.00.100 Spotting Malicious E-mail Messages.

How to reduce risks when using personal social media in the workplace

- Use a unique passphrase or password for each of your accounts
- Seek approval before posting work-related information on a personal account
- Limit the use of tracking or location services in social media applications.
- Enforce MFA on all devices and accounts when available
- Accept friend, follower or contact requests only from people you know
- Be wary of posts containing unusual language or content
- Use caution when clicking on shortened URLs; they could direct you to a malicious site
- Avoid revealing private information on personal accounts like your home address or phone number; the more you share, the easier it is for a threat actor to steal your identity
- Review privacy settings to control who sees what
- Sign 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.

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