TLP:WHITE

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Security Considerations When Using Social Media in Your Organization

MANAGEMENT

TLP:WHITE

Canada

FOREWORD

This document is an unclassified publication issued under the authority of the Head of the Canadian Centre for Cyber Security.

EFFECTIVE DATE

This publication takes effect on January 3, 2022.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	January 3, 2022

Cat. No. D97-4/10-066-2022E-PDF
ISBN 978-0-660-41585-7

OVERVIEW

The rapidly changing social media environment reveals new risks and challenges. All stakeholders should be informed of the changing threat environment and the security measures required to safeguard their social media activities.

This document discusses common social media threats and recommends security and privacy protection measures that your organization can implement to safeguard users, processes, and technologies involved in creating and publishing posts online.

TABLE OF CONTENTS

1 INTRODUCTION

This document recommends security measures that your organization can implement to safeguard users, processes, and technologies involved in creating and publishing posts online.

Social media has changed the way Canadians communicate, stay in touch, and build new relationships. Canadians are spending more time online, and organizations use social media tools to engage with their customers and users. Increasingly, businesses are working with social marketing management tools to execute their digital marketing strategies. Government of Canada (GC) departments also use social media channels to connect with Canadians and promote government programs and services.

Malicious actors target social media assets to launch destructive cyber attacks. For example, nation-state actors use social media as surveillance tools, and they create fake profiles to influence public discourse. There is a need to pay attention to the security risks associated with social networking applications. To protect yourself and your organization's social media activities, you should consider a multi-faceted approach to security by implementing various security controls.

2 COMMON SOCIAL MEDIA THREATS

Your social media activities can expose your business and users to several types of threats. Below, we have included some examples of typical threats:

- **Phishing attacks:** Threat actors use phishing attacks to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. When users are not aware of how to protect their social media accounts against phishing, threat actors can use these techniques to steal access credentials and take control of target accounts. Compromised accounts can be used to distribute malicious spam messages or commit financial fraud online. Threat actors can also post malicious messages (replies) as phishing lures to target account owners or followers.
  - **Spear phishing:** Threat actors target specific individuals by sending personalized messages that may include details such as their interests, recent online activities, or purchases.
- **Malware attacks:** Threat actors can distribute malware programs through social media posts. Hijacked social media accounts can be used to distribute malware to unsuspecting users. Your users or social media followers may click on URL links which may redirect to websites hosting malware or ransomware.
  - **Ransomware:** A type of malware that denies a user's access to files or systems until a sum of money is paid. When ransomware infects a device, it either locks the screen or encrypts the files. Ransomware can also use a network to spread to other connected devices.
- **Disinformation campaigns:** Disinformation campaigns are intentional efforts to spread false information on social media. Through targeted campaigns, threat actors can spread false messages to promote a particular narrative for financial gain or achieve their desired outcome.
- **Insider threats:** Employees or close contacts who have authorized access to social media systems can post messages intentionally to cause harm to an organization. Employees can also accidentally inflict damage on your organization's social media profile.
- **Human errors:** An employee could mistakenly leak access credentials to a social media account and cause considerable damage to an organization. Messages posted online containing typos may also convey negative impressions about an organization's brand. Poorly implemented social media profiles can also expose users and businesses to unintended privacy risks.
- **Brand impersonation and typo-squatting**: Brand impersonation can occur when a threat actor creates fake accounts to mimic or steal an organization's identity online. Typo-squatting attacks exploit typing errors that users may make when typing a URL, redirecting users to fake websites. Typically, the goal of these attacks is to defraud users or steal information. In more sophisticated attacks, this technique can be paired with social engineering to gain privileged access to backend resources.
- **Identity theft or account takeover attacks:** Hacktivists or threat actors can take over social media accounts to promote their agenda or distribute malware. Some recent campaigns involved hackers using malicious applications with false messaging to trick users and gaining access to their social media profiles.

- **Vulnerabilities within platforms and third-party applications:** Unknown and known vulnerabilities in software tools, publishing tools, and vendor applications can expose social media accounts to additional risks. Threat actors may exploit these flaws to launch more sophisticated attacks.
- **Reconnaissance attacks:** Threat actors can retrieve information on employees, company projects, and corporate tools from social media posts, job listings, news releases, and other online activities. Information collected from these sources can give valuable insights and be used to launch highly targeted intrusion attacks.
- **Inference attacks**: Threat actors can infer sensitive user information by gathering user posts or online activities. The inferred data can then be weaponized to target users.

3 PROTECTIVE MEASURES

To protect against online threats and reduce the likelihood of malicious activity impacting your organization's social media accounts, we recommend that you continuously monitor and assess risks. As a part of your risk management activities, you should review your organization's social media processes, identify potential risks, and implement appropriate security measures to address those risks and safeguard your data.

You should consider the following security measures:

- Secure provisioning;
- Secure publishing; and
- Incident response and recovery.

3.1 SECURE PROVISIONING

Secure provisioning refers to governance activities and foundational building blocks that you can implement to secure your social media processes. These activities set the right tone for your employees and provide a secure framework to guide the initial steps within your social media program.

3.1.1 SOCIAL MEDIA POLICY

Your social media policy establishes the requirements and sets standards on how your organization will use social media. Your policy should address the following aspects:

- Provide direction on how your organization plans to conduct its interactions online;
- Set principles on acceptable use cases for staff and business interactions;
- Define consequences for misuse of social media in the organization;
- Define corporate data classification types that can or cannot be shared through social media channels;
- Mandate that all employees should be formally trained on their behavioural expectations and the details of the policy document;
- Mandate the need for regular awareness training specifically for those directly involved with social media content publishing; and
- Set standards for engaging with outsourced service vendors such as content marketing or online marketing teams.

3.1.2 SOCIAL MEDIA PLATFORM(S)

Selecting a social media platform and managing associated accounts should be a continuous risk assessment decision. Your organization should evaluate its social media goals and ensure that these platform(s) can support those goals. Before selecting a social media platform, you should review the platform's security and privacy features. Some of the features to look for include the following examples:

- Supports secure network communication technologies, such as Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), Secure Shell (SSH), for web and mobile application communications;
  - Uses valid, verified, and trusted Certificate Authority (CA) signed certificates; and
  - Does not use obsolete algorithms and protocols (platform supports TLS 1.2 or higher).
- Supports secure authentication mechanisms such as strong passwords, multi-factor authentication (MFA), and Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA);
- Supports separate user accounts for multi-user management social media accounts;
- Supports a role-based user access model to manage user authentication and permissions;
- Supports the detection of new or suspicious authentication activity on user accounts;
- Supports user privacy and customization of privacy settings; and
- Possesses a dedicated support desk or security team available to address incidents.

3.1.3 ACCESS MANAGEMENT

To enforce policy requirements and protect against identity theft, you should ensure that you are properly managing access to organizational social media accounts. All accounts should conform with your policies on user accounts and credential management. If available, we recommend that you use MFA.

You should review all access and authorization rights regularly and remove access for terminated employees. Also, ensure third-party permissions are carefully reviewed and secured. To safeguard access and data, your organization should implement appropriate monitoring protections.

Consider the following tips for additional security:

- Use strong and unique passphrases or passwords for each social media account;
- Avoid sharing credentials;
  - Users should have individual accounts with the appropriate permissions granted as needed for their roles;
- Disable authentication services that are not in use, such as application programming interface (API) access; and
- Decommission social media accounts that are no longer in use and archive related posts.

For more guidance on access management, see the following related publications:

- *ITSAP.10.094 Managing and Controlling Administrative Publications* [1][1];
- *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication* [2]; and

[1] Numbers in square brackets reference resources cited in the Supporting Content section of this document.

- *ITSP.30.031 v3 User Authentication Guidance for Information Technology Systems* [3].

3.1.4 SECURE APPLICATIONS AND SYSTEMS

You can implement the following recommendations to ensure proper cyber hygiene for all social media systems, devices, and software applications used for publishing social media posts:

- Ensure only approved devices (i.e. devices defined in your mobile device deployment model) are used for social media interaction;
- Update systems and devices regularly and install software patches as soon as they are available;
- Install anti-malware prevention and detection solutions;
- Implement device hardening controls to tighten permissions and restrict access from these devices to critical systems on your corporate network; and
- Ensure staff use a virtual private network (VPN) or similar technologies when accessing social media accounts over public or untrusted Wi-Fi networks.

For more on securing your devices at home and on the corporate network, refer to the following publications:

- *ITSAP.00.007 Cyber Security at Home and in The Office: Secure Your Devices, Computers, and Networks* [4];
- *ITSAP.10.096 How Updates Secure Your Devices* [5];
- *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi* [6]; and
- *ITSAP.80.101 Virtual Private Networks* [7].

3.1.5 LEGAL AND PRIVACY CONSIDERATIONS

Using social media exposes your organization to legal and privacy risks. Some industry sectors may have data residency requirements they must adhere to. Before using social media, you should ensure you understand the associated legal and privacy implications on your operations. For example, what data is stored (e.g. posts, views, logins, tracking data), who owns the data on your account, where your data is stored, (i.e. geographical location where data are stored, including transient data or backups).

Canada has privacy legislation such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which restricts how data can be collected, used, or disclosed, in certain circumstances, by social media companies. However, users can give consent to these companies to collect, use, or share their information. Pay close attention to the terms of use agreements and the privacy notice statements to ensure you are aware of what you are agreeing to. You should familiarize yourself with platform-specific tools and customizable privacy features that you can use to improve your account's privacy. Finally, continuously review these services for updates and take advantage of new tools that you can use to reduce your risk of exposure.

3.2 SECURE PUBLISHING

This section outlines some best practices for publishing and safeguarding your social media posts.

3.2.1 PUBLISHING PROCEDURES

Your organization may have dedicated teams responsible for community engagement, content marketing, and public relations. These teams may involve several individuals who have direct access to your organization's social media accounts. It is essential to implement processes to ensure that all content is reviewed and authorized before it is posted.

You should consider the following actions:

- Implementing a workflow process to approve posts and ensure some level of consistency with published content;
- Reviewing and approving all updated content and updates;
- Ensuring you have permission to use, reproduce, or publish third-party or copyrighted content;
- Involving your legal department in the content approval process as required;
- Enabling access and activity logs to capture details of the review process; and
- Sanitizing documents, images, or video content to remove associated metadata before posting publicly.

3.2.2 THIRD-PARTY ACCESS

Often, third parties play significant roles in creating and publishing social media content. For example, you may be working with a digital marketing agency to execute your online marketing strategy. To do this, they are granted administrative access to the organization's social media account to be able to post content as needed. When a third party is granted administrative or privileged access, you must ensure that access is tightly controlled. Security and user-conduct expectations should be defined as part of the contract engagement terms. Password and user behaviour policies that apply to in-house employees must also be extended to the agency to ensure consistency. Threat actors are known to target the weakest links in the supply chain; even if your organization is not the direct target of a cyber attack, you may be affected if one of your vendors or suppliers is compromised.

When reviewing third-party applications, consider the following actions:

- Identify third-party applications that have access to your social media data;
- Validate permissions for applications that need to retain access;
- Delete or remove unwanted applications or disable permissions you would like revoked; and
- Implement monitoring to alert you whenever a third-party application accesses your account.

3.2.3 EDUCATION AND TRAINING

Training is vital for all users involved in the publishing process. Users need to be informed of acceptable use policies and their responsibilities. Specifically, for systems or accounts that require multi-user access, individual account holders should be educated on the possible risks. Your organization should have routine training sessions (e.g. conducted annually) for all employees. Train employees to use tools and procedures to remove metadata details such as usernames, geographical location, device model and other details from posts. Users should be required to sign a terms of use agreement. Also, due to

the frequent changes to these social media platforms, you should review all recent updates. New features that enhance desired privacy settings or those that may impact user privacy are some examples to watch out for.

3.3 INCIDENT RESPONSE AND RECOVERY

Incidents do occur. To minimize the impact of an incident, you should have response and recovery plans to guide staff on how to handle issues.

3.3.1 INCIDENT RESPONSE PLAN

Document your incident response plan to reflect potential outcomes, such as someone posting an unapproved message or hijacking an account to cause harm. The document should outline recommended actions required to appropriately respond to different incidents. Most social media platforms have their abuse-contact information on their website. Non-compliance with PIPEDA legislation, unauthorized intentional or accidental access or disclosure of personal information when using social media may be considered a privacy breach and should be reported to your organization's privacy management office and the Office of the Privacy Commissioner of Canada.

By reviewing, testing, and updating your response plan, you can ensure the effectiveness of your plans and procedures. You can use scenario-based tabletop exercises to analyze steps in your response plan. You should apply any lessons learned from these tabletop exercises by updating the plans.

3.3.2 MONITORING

Your organization may implement social feed monitoring to detect fraudulent corporate brand mentions and address potential incidents. Monitoring can help you detect threats such as impersonation and disinformation attacks early.

Successfully implementing brand monitoring can be challenging due to possible higher rates of false-positive alarms; however, with fine-tuned detection rules and proper coordination among community engagement teams, this can be extremely valuable. Many platforms offer basic abuse reporting features, while some enable administrative account holders to flag imposter activities for swift takedown action.

To monitor authentication-related attacks, you may consider setting up notifications for successful authentication with new devices or when account permissions change. For advanced use-cases, monitoring can be implemented to identify successful federated authentication events if an account is used to login to other web applications. This may help identify account policy violations or identity theft incidents.

3.3.3 AUDITING AND LOGGING

The success of a monitoring program is heavily dependent on the capabilities of its auditing and logging infrastructure. Implementing processes to capture, store, and provide accurate user activity logs provides visibility into malicious use and helps support incident investigations. By default, most social media platforms offer basic audit logging features to their users. You should understand the capabilities and the constraints of a default set-up and determine if it is sufficient to meet your needs. Retention policies, retrieval procedures, and service response times for custom requests should be given careful considerations. For specific use cases, you can engage the social media platform to explore the potential for advanced logging capabilities or support for off-platform storage.

3.3.4 PARTNERSHIPS

You should develop partnerships with relevant stakeholders before an incident occurs. Use their public contact information to reach out and inquire about their participation in your tabletop exercises. Most would be willing to support you.
When dealing with an incident, contact all relevant agencies as required – social media, local law enforcement and specialized agencies such as the Canadian Anti-Fraud Centre. You can also report these incidents to our Contact Centre for tracking purposes.

Your organization may want to invest in cyber security insurance if you determine it to be beneficial to your organization. Your policy may add an additional layer of protection and may also provide your organization with incident response expertise in the event of a ransomware attack.

For more information on recommended actions when dealing with an incident, refer to our guidance on *Social Media Account Impersonation* [8].

4 SUMMARY

The social media threat landscape is evolving. Users and organizations need to stay informed of new threats that may target their social media activities online. There are various safeguards and strategies that your organization and stakeholders can use to protect your social media platforms. You should implement protective measures such as secure provisioning of your devices and incident response and recovery techniques. Companies must pay attention to the changing business risk environment and ensure they have security controls, such as those listed above, to address potential gaps.

4.1 CONTACT INFORMATION

For more information on implementing this guidance, email or phone our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
API	Application programming interface
CA	Certification authority
CAPTCHA	Completely Automated Public Turing test to tell Computer and Humans Apart
GC	Government of Canada
HTTPS	Hypertext Transfer Protocol Secure
MFA	Multi-factor authentication
PIPEDA	Personal Information Protection and Electronic Documents Act
SSH	Secure Shell
StatsCan	Statistics Canada
TLS	Transport Layer Security
VPN	Virtual private network

5.2 GLOSSARY

Term	Definition
Authentication	The process of verifying an identity claimed by or for a system entity.
Multi-factor authentication	A form of user authentication that requires two or more different ways (factors) of verifying a claimed identity. The three most commonly recognized factors are: (1) something you know (e.g. a password), (2) something you have (e.g. a physical authentication token), and (3) something you are (e.g. a biometric).
PIPEDA	The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private-sector organizations.
Virtual Private Network	A private communications network usually used within a company, or by several different companies or organizations to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

5.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSAP.10.094 Managing and Controlling Administrative Privileges*. July 2020.

Number	Reference
2	Canadian Centre for Cyber Security. *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*. June 2020.
3	Canadian Centre for Cyber Security. *ITSP.30.031 v3 User Authentication Guidance for Information Technology Systems*. April 2018.
4	Canadian Centre for Cyber Security. *ITSAP.00.007 Cyber Security at Home and in the Office: Secure Your Devices, Computers, and Networks*. October 2020.
5	Canadian Centre for Cyber Security. *ITSAP.10.096 How Updates Secure Your Device*. February 2020.
6	Canadian Centre for Cyber Security. *ITSAP.80.009 Protecting Your Organization While Using Wi-Fi*. October 2020.
7	Canadian Centre for Cyber Security. *ITSAP.80.101 Virtual Private Networks*. October 2019.
8	Canadian Centre for Cyber Security. *Social Media Account Impersonation.*