CAPACITY ENHANCEMENT GUIDE: SOCIAL MEDIA ACCOUNT PROTECTION

INTRODUCTION

The Cybersecurity and Infrastructure Security Agency (CISA) helps to secure the safety of the nation's critical assets, including the social media accounts of federal civilian executive branch (FCEB) agencies. Many federal agencies and other organizations use various social media platforms as a primary way to engage with the public. However, although these platforms provide a mechanism for rapid outreach, an organization's social media accounts, if compromised, can be used to spread false or sensitive information to a wide audience. A compromised social media account can:

- Damage the organization's reputation
- Disrupt operations
- Impose financial costs

The trusted nature of verified social media accounts—including those of large organizations or public figures— increases the likelihood that false stories posted by these accounts may be initially viewed as true. This guide provides recommendations to protect social media accounts and reduce the risk of unauthorized access on platforms such as Twitter, Facebook, and Instagram.

Audience and Scope

The technical measures described in this guidance focus on securing organization-run accounts, rather than those maintained by individuals. This guidance is intended primarily for federal agencies, but is applicable to state, local, tribal, and territorial governments as well as private-sector entities.

Constraints and Assumptions

This document includes the following constraints and assumptions:

- Due to varying services offered across social media providers, some recommendations may not apply to every organization's social media account(s).
- None of the recommendations in this product should be considered a formal endorsement from the United States government to procure or utilize any specific service.
- All recommendations are provided as-is.
- This guide assumes the audience has an understanding of authentication and social media platforms.

SOCIAL MEDIA ACCOUNT COMPROMISE IN THE NEWS

One prominent example of the widescale impact that can result from a social media breach is the 2013 breach of the Associated Press's Twitter account by the Syrian Electronic Army (SEA). (See Figure 1.)

After compromising the account, the SEA used it to send a tweet, claiming that two explosions occurred in the White House and injured President Barack Obama. The false tweet caused stock valuations to temporarily drop about 1%, resulting in over one hundred billion dollars of transient losses. https://www.cnbc.com/id/100646197

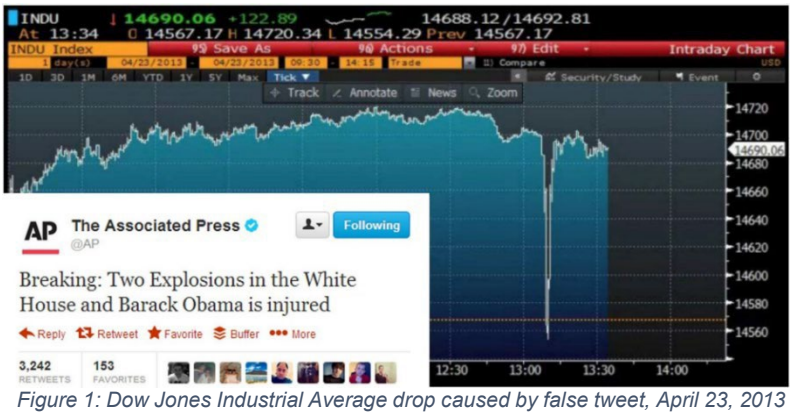

Figure 1: Dow Jones Industrial Average drop caused by false tweet, April 23, 2013

RECOMMENDATIONS

CISA recommends that federal agencies take the following actions—detailed in the sections below—to establish a baseline to secure their social media accounts from unauthorized access:

- Establish and Maintain a Social Media Policy
- Implement Credential Management
- Enforce Multi-Factor Authentication (MFA)
- Manage Account Privacy Settings
- Use Trusted Devices
- Vet Third-Party Vendors
- Maintain Situational Awareness of Cybersecurity Threats
- Establish an Incident Response Plan

Establish and Maintain a Social Media Policy

CISA urges organizations to establish a social media policy to govern how their personnel use the organization's social media accounts. This policy should mandate and detail measures described in this guide, including credential management, MFA, specified account privacy settings, and any other safeguards that the organization deems necessary to help protect social media accounts.

Organizations should distribute the social media policy to personnel and, if necessary, provide relevant training. Organizations should also review and update the policy at appropriate intervals.

Implement Credential Management

Organizations should take the following actions to secure the credentials used to access their social media accounts:

- Limit the number of employees that can access the organization's social media accounts.
- Use a "corporate account" feature if the social media platform provides it. Offered by various social media platforms, a corporate account allows an administrator to assign roles and access privileges to individual user accounts. This feature enhances security by:
    - Limiting the users that possess administrative control and
    - Ensuring that each user retains their own unique credentials for accessing the service.
- Ensure that administrator accounts enforce strong MFA. Examples of social media accounts providing this functionality include Facebook Business Suite, LinkedIn Company Pages, and Twitter TweetDeck.
- Ensure that employees' personal social media accounts remain separate from any of the organization's accounts. This action reduces the risk that third-party applications (apps) accessing the employee's personal account can gain undue access to any of the organization's accounts.
- Protect email accounts linked to the organization's social media accounts. Consider enrolling the linked email accounts in additional security services beyond MFA, such as services that may reduce risks from phishing attacks. Examples include:
    - Google's Advanced Protection Program, which adds a security key requirement for logins and additional protection against malware downloads.
    - Microsoft's Advanced Threat Protection service for Office 365 users, which adds various anti-phishing measures and options for security reports and automated incident response.
- Do not share credentials between employees.

- Review the list of authorized users and/or logons regularly in accordance with the organization's policy. During times of heightened sensitivity for the organization, review these lists more frequently.
- Monitor alerts for unauthorized logons, logoffs, permission changes, additions, deletions, or any unusual activity.
- Limit third-party app access to social media accounts. This action applies to both organization accounts as well as individual accounts that interact with or administer a social media page. Many third-party apps can request excessive privileges and may expose private information. Disallow or carefully restrict the number of apps permitted to post on the organization's behalf. To limit third-party- app access:
    - Develop a process to evaluate and approve third-party apps with access to social - media accounts. See National Institute of Standards and Technology's Special Publication 800-163 Rev. 1 Vetting the Security of Mobile Applications for detailed guidance.
    - Ensure that no unnecessary apps can access either organization accounts or individual accounts used on the organization's behalf. The organization's relevant IT policy should reinforce this control.
    - Review each third-party app's access privileges to verify that they comply with the social media policy and confirm whether the app should have access to the accounts.
- Secure any credentials used to interact with a social media service's application programming interface (API) such as API keys or tokens. Compromised API keys or tokens may allow malicious actors to impersonate authorized users during a login session without requiring usernames or passwords. For example, Twitter recommends encrypting tokens when storing them in databases, as well as storing session data either via secured (Hypertext Transfer Protocol Secure [HTTPS]-protected) cookies or through a web storage format that does not retain the data after immediate use. See Twitter's authentication best practices guide for details.
- Ensure passwords and tokens adhere to best practices for length and complexity. Maintain a policy that enforces changing passwords and tokens at set intervals. Do not share or write down credentials.
- Replace credentials immediately if there is any indication or suspicion that a password or secret token has been compromised.

Enforce Multi-Factor Authentication (MFA)

Use the MFA security feature for user logins to help protect social media accounts. MFA combines two or more distinct authentication factors to confirm an individual's identity, drawn from the following types: (1) something that is "known," such as a password; (2) something that is "possessed," such as a physical security key or authenticator app linked to a secondary device; and (3) something that a person "is," such as a distinguishing feature, e.g., a fingerprint or other biometric. CISA's Implementing Strong Authentication Capacity Enhancement Guide discusses MFA in further detail. Organizations can use either physical security
keys or authentication apps:

- Physical security keys protect against phishing attacks by providing a second, physical authentication factor that only allows the completion of the authentication process when a user is on the correct website. Thus, even if a user is tricked into supplying their password to a phishing website, attackers will be unable to access the account without the corresponding physical security key.
- Authentication apps display a code that the user must enter to log into a particular account.

This code regenerates in a short period of time, often 30 seconds. Although authentication apps can still be vulnerable to phishing attacks, they offer more protection than text or email message-based MFA.

Organizations should avoid using text and email message-based MFA methods when more robust forms are available. Text and email message-based MFA methods are vulnerable to phishing and subscriber identification module (SIM) swap attacks, although both options offer better protection than password- based, single-factor authentication. For example, Facebook, Twitter, and LinkedIn all allow MFA using an authenticator app, which can be enabled through their respective account settings.

Manage Account Privacy Settings

Limit the data that the platform and external parties can collect by using account privacy settings:

- Location settings. Limit the extent to which the social media website can track and share physical location unless a legitimate need exists to provide location data.
- Data and advertising. Limit extent to which information about the account is shared.

Use Trusted Devices

Ensure that only organization-issued computers and smartphones manage social media accounts. Take the following steps to secure these devices:

- Continuously monitor devices for any unusual activity.
- Control devices by using a mobile device management platform.
- Implement restrictive mobile application download permissions on the devices.
- Implement device tracking and locating functions, which can be used in the event of loss or theft.

Vet Third-Party Vendors

Some organizations use an external vendor to manage the organizations' social media accounts; however, such vendors may have weaknesses in their cybersecurity practices. When selecting a third-party vendor to manage a social media account, ensure that the vendor's security practices adhere to the organization's security policy. Codify this adherence in a service-level agreement (SLA) with the vendor, to gain assurance that the vendor takes cybersecurity seriously.

Maintain Situational Awareness of Cybersecurity Threats

Organizations should remain aware of cybersecurity threats against their social media accounts:

- Continuously monitor the organization's social media accounts for unusual behavior.
- Subscribe to notifications on emerging cybersecurity threats (e.g., CISA's National Cyber Awareness System publications, MITRE's Common Vulnerability and Exposures (CVEs), and the CERT Coordination Center's Vulnerability Notes).
- Create—and distribute to employees—a summary of the threats the organization faces (e.g., phishing, malware, ransomware) to help reinforce the role employees play in reducing cybersecurity risk.
- Explore communities of interest, which may include sector-specific information sharing and analysis centers, the Homeland Information Sharing Network, or other government and intelligence programs.
- Provide the social media account administrators relevant and situational security awareness training.

Establish an Incident Response Plan

Organizations should create, practice, and execute an incident response plan that includes:

- Expected actions to take in scenarios, such as unauthorized access or postings,

compromised devices, and the disclosure of private communications.
- Guidance on reporting an incident to CISA and other relevant authorities.
- Contact information for appropriate social media platforms should a breach occur.

The incident response plan should encompass the complete organization and not solely focus on IT. See CISA's Federal Government Cybersecurity Incident & Vulnerability Response Playbooks for detailed guidance.

Disclaimer

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

CONTACT INFO

For questions about this guidance and other CISA services available to federal agencies, please contact cyberliaison@cisa.dhs.gov.