Ministry of Information & Communications Technology

وزارة الاتصالات و تكنولوجيا المعلومات.

GUIDELINES FOR SECURING SOCIAL MEDIA ACCOUNTS

Version 1.0

Published October 2015

Document Control

Version:	1.0
Author:	Cyber Security Division - ictQATAR
Classification:	Public
Date of Issue:	October 2015

Contents

Introduction

Social networks / media is an organization's identity in the virtual world. This social identity is very much linked to its corporate public image and needs to be protected as much in the virtual world as in the real world. The social media account if not secured may open a floodgate to compromising and maligning your corporate public image.

This document provides mitigation advice and security controls to help reduce threats such as unauthorized access as well as steps to follow in order to retrieve a stolen account.

Objective

Provide necessary guidance to help organizations manage their social media accounts securely.

Scope

All organizations having social media presence.

Intended Audience

Staff authorized to manage and use the corporate social media accounts.

Legal Mandate

Article 14 of Decree Law No. 16 of 2014 setting the mandate of Ministry of Information and Communications Technology (hereinafter referred to as "ictQATAR") provides that ictQATAR has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (14) of Emiri Decree No. 27 of 2014 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

Article (15) of Emiri Decree No.27 of 2014 stipulates that the Ministry build and enable incident response framework and enhance capabilities to detect and analyze malicious content.

This Policy Document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

General Recommendations

Understand the Risks

Social media accounts related to government, semi government, national events represent an ideal and logical target for our nation's adversaries, as social media is seen as the virtual identity of the government.

Further being a government accounts, they have a huge following and the followers have implicit trust in them.

The risks associated with such social media profiles are:

- Leaking of confidential or inappropriate information
- Vandalism of content, spreading malicious content
- Legal implications
- Blackmail

Set up a Governance for Social Media

Define a policy for usage of social media in your organization.

On a minimum, the policy should include the following:

- Identify who in the organization is authorized to engage in social media on its behalf?
- Who controls and owns the information into a social networking site?
- What information are the stakeholders passing on to other people?
- Seeking consent from stakeholder prior disseminating information related to them.
- Explicit procedures on social media networking. Who would the corporate account follow or be influenced with etc How would information received from the follower network be broadcasted? i.e. re-shared or re-tweeted etc.
- Defined process for Incident handling / recovery plan in case of breach or malicious attacks.
- Hardware and software authorized to access the social media account from.

Account creation and administration

In order to create and manage account ownership it is recommended that we have:

- A dedicated corporate email (usually used as the username), should be used to create and maintain a social media accounts. This email address should be a generic/nonspecific enterprise email account for logging into social media networks. Individual enterprise email addresses are easy to guess and decrease the security of social media accounts.

- Each social media channel/account should be associated with a separate and unique corporate email. Example: the Username/Email associated with corporate twitter is different from the Username/Email used on Facebook
- Do not use the same passwords for social media that you use to access company computing resources
- Private emails should not to be used to manage and access a corporate social media account such as twitter account or Facebook page
- The social media account page should feature the communication department approved logo and the profile text should include references that this account is "the official" account of the organization.
- Organizations should define which organizations / agencies they may follow. E.g. Government agencies may follow other government agencies, verified accounts or trusted sources.
- It is not recommended to follow individual users.
- It is not recommended to access / re-post / re-tweet / share "unverified messages" with imbedded links and URLs.

Account Login

- Configure social media accounts to use secure sessions (HTTPS) whenever possible. Facebook, Twitter and others support this option. (Note: This is extremely important when connecting via public Wi-Fi networks). QCERT can help you configure your account to use HTTPS at all times
- Login should only be from a dedicated corporate owned / managed device (PC or Mobile device)
- Login should be from a trusted network, refrain from using public/open Wi-Fi networks like café's airports…etc unless using a corporate VPN to secure your session.
- If any mobile devices are linked to your corporate social media accounts, make sure that these devices are adequately protected.
- Disable the geo-location feature while posting or tweeting.

Password Management

- Always use strong and secure passwords to access social networks. The passwords should comply with the corporate password policy.
- Change passwords frequently. Have different passwords for different accounts.
- Use multi-factor authentication for social media accounts (if supported by the provider).

Information Sharing / Acceptable Usage

- Do not disclose any official information upon registrations of social accounts.
- Restrict employees from posting official and sensitive data or information over social networks.
- Only authorized personnel should be allowed to operate corporate social media accounts.
- Do not post any information that may be discriminatory, disparaging, defamatory or harassing comments regarding the organization or its employees or any third party in their electronic postings or publishing.

Configure Privacy Settings

- Review and revise as necessary the default privacy settings offered by the social media networking sites.

Monitoring

- Limit corporate social media account access to an authorized employee in order to control the content distribution over social networks. This could be the Public relation officer (PRO), official spokesperson, etc.
- In case where more than one person has access to the corporate social media account, internal procedures should be defined to regulate this activity, this should include training user on usage of social media, active monitoring, and use of social media management solutions and / or any other compensating controls as deemed necessary.
- Regularly monitor the access granted to authorized user accounts and revoke the access of employees who leave the organization or no longer have a business need to use social media.
- Have a third party individual, who is not responsible for content, continuously monitor social media accounts for unauthorized or unusual postings.

Third Party Solutions

- The organizations should consider usage of a social media management solution.

Incidents: In case of any suspicious activity

- Please report to QCERT (incidents@qcert.org) or call (+974 4493 3408) if you see any of the suspicious symptoms below:
    - Automated likes, favorites, follows/un-follows or friend requests
    - Private messages being posted to your friends (this can be hard to spot unless someone points it out to you)
    - Unexpected email/push notifications from the social network, such as:
    - Warning that your email address has been changed

- Warning that your account was accessed from an unknown location.
- Status updates/tweets that you didn't make
- Changes to the profile or pictures on the account.

Recovery Plan

- Collect all logs, traces, artifacts of malicious activity for investigation and possible legal requirements.
- Immediately change account passwords.
- Verify and change the password for the associated emails and back up emails
- Verify the password recovery options set for the social media account; verify the alternative email address that has been setup.
- Verify auto forward options if any setup for the account and associated emails.
- Visit the applications page of the social network and remove any apps you do not recognize. If the account continues to behave erratically, we recommend you revoke access to all applications.

Security Awareness

- Employees managing and / or maintaining the organization's social media accounts shall be sensitized and educated on information security. They should be made aware of prevalent threats such as Phishing and social engineering.

Securing Most Common Social Networking Sites

Facebook:

a. Ensure you're using a secure connection whenever one is available, click Security in the left pane of Facebook's Account Settings and make sure Secure Browsing is enabled.
b. The security settings also let you enable log-in notifications and approvals, and view and edit your recognized devices and active sessions.
c. **Security Tips:**
    i. Protect your password.
    ii. Use Facebook's extra security features.
    iii. Make sure your email account(s) are secure.

iv. Logout of Facebook when you use a computer you share with other people. If you forget, you can logout remotely.
v. Run anti-virus software on your computer:
vi. Think before you click or download anything.

d. Enable **'Login Approvals'** from the 'Account Security' section of the account settings page. Follow the link - https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920
e. Update your accounts as per new security tips and guideline of facebook. You can find them at https://www.facebook.com/help/379220725465972

Twitter:

a. When you sign up for Twitter, you have the option to keep your Tweets public (the default account setting) or to protect your Tweets.
b. Accounts with protected Tweets require manual approval of each and every person who may view that account's Tweets.
c. **Security Tips:**
   i. Use a strong password.
   ii. Use login verification.
   iii. Government organizations shall get their account validated and verified. Q-CERT can help you in this.
   iv. Watch out for suspicious links, and always make sure you're on Twitter.com before you enter your login information.
   v. Never give your username and password out to untrusted third parties.
d. **Using SMS text message login verification:** To set up SMS text message login verification:
   i. Go to your Security and privacy settings on twitter.com and select the option to Verify login requests.
   ii. When prompted, click Okay, send me a message.
   iii. If you receive our verification message, click Yes. (Note: you'll have to enter your password).
   iv. You can generate a backup code by selecting the option to Get backup code. Write down, print, or take a screenshot of this backup code; this will help you access your account if you lose your phone or change your phone number.
e. Update and follow the best practices mentioned by Twitter regularly. You can find them at https://support.twitter.com/articles/76036

Instagram:

a. **Security Tips:**
   i. Pick a strong password.
   ii. Make sure your email account is secure. Change the passwords for all of your email accounts and make sure that no two are the same.
   iii. Logout of Instagram when you use a computer or phone you share with other people. Don't check the "Remember Me" box when logging in from a public computer.
   iv. Think before you authorize any third-party app.

b. Update your accounts as per new security tips and guidelines of Instagram. You can find them at https://help.instagram.com/369001149843369

LinkedIn:

a. **Security Tips:**
   i. Change your password regularly.
   ii. Sign out of your account after you use a publicly shared computer.
   iii. Manage your account information and privacy settings from the Profile and Account sections of your Privacy & Settings page.
   iv. Keep your antivirus software up to date.
   v. Don't put your email address, home address or phone number in your profile's Summary.
   vi. Only connect to people you know and trust, or those you have trustworthy common connections with.
   vii. Consider turning two-step verification on for your account.
   viii. Be informed about reporting inappropriate content or safety concerns.

b. Update your accounts as per new security tips and guidelines of LinkedIn, https://help.linkedin.com/app/answers/detail/a_id/267/~/account-security-and-privacy---best-practices