الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Cyber Security Guidelines

Securing Social Media Accounts

Public

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "Securing Social Media Accounts" - V 3.0 - in order to help agencies, understand and implement suitable controls to secure their social media identity.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "Securing Social Media Accounts".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

Document Control

Document Details	
Document ID	IAG-NGE-SSMA
Version	V 3.0
Classification & Type	Public
Abstract	This document is to help agencies understand and implement suitable controls to secure their social media identity.

Review / Approval

Department/Role	Reviewed/Approved	Version	Date
National Cyber Governance and Assurance Affairs		3.0	

Revision History

Version	Author(s)	Revision description	Date
1.0	MICT	Published V1.0 document	October 2015
2.0	MoTC	Branding Change (MICT to MOTC) + added controls for other or changed social media platforms	November 2016
2.1	MoTC	MoTC logo changed + Format Change	June 2018
3.0	NCSA	Branding Changed to NCSA + Updates on the Platforms Controls	December 2022
3.0	NCSA	Minor corrections	December 2023

LEGAL MANDATE(S)

Emiri decree No. (1) of the year 2021 regarding the establishment of National Cyber Security Agency, sets the mandate for the National Cyber Security Agency (hereinafter referred to as "NCSA"). The NCSA has the authority to supervise, regulate and protect the security of the National Critical Infrastructure via proposing and issuing policies and standards and ensuring compliance.

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

Table of Contents

1 Introduction

1.1 Context

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

2 Purpose, Scope, Usage and Targeted Audience

2.1 Purpose

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

2.2 Scope

All organizations in the State of Qatar having or planning to have social media presence.

2.3 Usage

This section describes when this document shall be used over the described scope.

2.4 Targeted Audience

This document is targeting employees who are managing and responsible for their organization's social media accounts.

Individuals may find this document helpful as well.

3 Key Definitions

Organizations/ Agencies	Refers to businesses operating in the State of Qatar with social media presence.

4 Understanding the Risks

Social media accounts of critical sector organizations, and any related accounts, pertaining to their projects or events, represent an ideal and logical target for our nation's adversaries, as social media persona (account), represents the virtual identity of the entity itself.

Further, since these accounts belong to critical sector organizations, they have a huge number of followers 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 to cause disruption or disconcert in the society,
- Legal implications,
- Blackmail

The risks may also apply to non-critical sector organizations, especially those that have large following.

5 General Recommendations

5.1 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:

1. Identify and define ownership for managing the social media accounts of the organization.
2. Define a process for approving the content to be published on the social media accounts.
3. Identify and assign responsibilities to an individual or a group of individuals, to manage the social media accounts of the organization.
4. Seeking consent from stakeholders prior disseminating information related to them.
5. Define procedures and specific criteria for the corporate social media accounts in terms of:
6. Who should the account follow or be influenced with etc.?
7. How should the information received from the follower network be re-posted or reshared?
8. Define hardware and software, which are authorized to manage the social media accounts.
9. Define procedures for incident handling and recovery plans in case of a breach or malicious attacks on the social media accounts.
10. Define procedures to ensure handover of social media accounts passwords, mobile numbers/devices/apps used to manage the social media accounts etc., to designated person in case when the concerned person is assigned different responsibilities, terminated, or leaves job.

5.2 Account creation and administration

To create and manage account ownership we recommend that organizations have:

1. A dedicated corporate email (usually used as the username), should be used to create, and maintain social media accounts. This email address should be a generic/nonspecific corporate email account for logging into social media networks. Individual corporate email addresses are easy to guess and decrease the security of social media accounts.
2. Each social media channel/account should be associated with a separate and unique corporate email. Example: The Username/Email/Password associated with corporate Twitter is different from the Username/Email/Password used on Facebook.
3. Do not use the same passwords for social media that you use to access company computing resources
4. Private emails and mobile numbers should not be used to manage and access a corporate social media account such as Twitter account or Facebook page
5. The social media account page should feature the communication department's approved logo and the profile text should include references that this account is "the official" account of the organization.
6. Organizations should define which organizations/agencies they may follow. E.g. Government agencies may follow other government agencies, verified accounts or trusted sources.
7. It is not recommended to follow individual users.

8. It is not recommended to access / re-post / re-tweet / share “unverified messages” with imbedded links and URLs.

5.3 Account Login

1. Configure social media accounts to use secure sessions (HTTPS) whenever possible. Facebook, Twitter, and others support this option. NCSA can help you configure your account to always use HTTPS
2. Login should only be from a dedicated corporate owned / managed device (PC or a mobile device)
3. Login should be from a trusted network, refrain from using public/open Wi-Fi networks like internet café’s, airports, etc.
4. Mobile devices linked to your corporate social media accounts should be adequately protected using biometrics, strong passwords. We recommend applying an extra layer of security by securing the apps with an additional PIN / password, which is different from the one used to access the device. This may be possible through use of certain third-party applications.
5. Disable the geo-location feature while posting or tweeting.

5.4 Password Management

1. Always use strong and secure passwords to access social networks. The passwords should comply with the corporate password policy.
2. Change passwords frequently. Have different passwords for different accounts.
3. Never share your passwords with anybody.
4. Configure and use multi-factor authentication for social media accounts (if supported by the service). Generally, social media service providers support three types of second factor authentication. These include Text Message, Authenticator App, and the Security Key. Since, the “Security Key” is an out of band mechanism; it would provide better security as long as the “Security Key” is physically secured.

5.5 Information Sharing / Acceptable usage

1. Do not disclose any official information upon registration of social accounts.
2. Restrict employees from posting official and sensitive data or information over social networks.
3. Only authorized personnel should be allowed to operate corporate social media accounts.
4. 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.

5.6 Configure Privacy Settings

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

5.7 Monitoring

1. 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.
2. 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 users on usage of social media, active monitoring, and use of social media management solutions and / or any other compensating controls as deemed necessary.

3. Regularly monitor the access granted to authorized user accounts and revoke the access of employees who leave the organization (during employee termination procedure) or no longer have a business need to use social media.
4. Have a third-party individual/service, who is not responsible for content, continuously monitor social media accounts for unauthorized or unusual postings.
5. Evaluate usage of enterprise solutions that may support the organization in monitoring their social media channels; including monitoring for rogue, phishing, and dubious accounts that may be a potential threat for the organization's online reputation.

5.8 Third party Solutions

1. The organizations should consider using a social media management solution that may facilitate managing multiple social media accounts and channels through a single secure console.

5.9 Incidents: In case of suspicious activity

1. Please report to NCSA (**ncsoc@ncsa.gov.qa**) or call (**16555**) if you see any of the suspicious symptoms below:
   - 1.1 Automated likes, favorites, follows/un-follows or friend requests
   - 1.2 Private messages being posted to your friends (this can be hard to spot unless someone points it out to you)
   - 1.3 Unexpected email/push notifications from the social network, such as:
   - 1.4 Warning that your email address has been changed
   - 1.5 Warning that your account was accessed from an unknown location.
   - 1.6 Status updates/tweets that you didn't make
   - 1.7 Changes to the profile or pictures on the account.

5.10 Recovery Plan

1. Please liaise with NCSA if you need any help, support or guidance.
2. Collect all logs, traces, artifacts of malicious activity for investigation and possible legal requirements.
3. Immediately change account passwords.
4. Verify and change the password for the associated emails and backup emails
5. Verify the password recovery options set for the social media account; verify the alternative email address that has been set up.
6. Verify auto forward options if setup for the account and associated emails.
7. 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.

5.11 Security Awareness

1. 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.

6 Securing Most Common Social Networking Sites

6.1 Facebook

Account Management:

Facebook Business Page security relies on the Manager account security. Therefore, be aware of the following:

- 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.
- The security settings also let you enable log-in notifications and approvals, and view and edit your recognized devices and active sessions.
- Read and understand the Facebook Data Policy to understand what data is the Facebook app collecting about you https://www.facebook.com/policy.php

Password Policy

- It should be longer than 6 characters, unique to you, and difficult for others to guess.

How to enable 2FA

- Facebook provide three options on enabling two factor authentication security key, third party authenticator app and SMS code. Go to https://www.facebook.com/help/148233965247823 for details on how to enable two-factor authentication on Facebook

Security Tips

- Use a strong password.
- Use Facebook's extra security features.
- Make sure your email account(s) are secure.
- Log out of Facebook after you have finished your work.
- Run antivirus software on your computer:
- Think before you click or download anything.
- 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
- Update your accounts as per security tips and guideline of Facebook. You can find them at https://www.facebook.com/help/379220725465972

Privacy Tips:

- Disable others from posting in the account timeline, this can be done from (Timeline and Tagging) in settings
- Don't allow other accounts to tag the account in a photo before it's reviewed. This can be done from (Timeline and Tagging) in settings

Account Recovery

- The following links provide details and steps for account recovery https://www.facebook.com/help/231208473756221, https://www.facebook.com/help/105487009541643, and https://www.facebook.com/help/132243923516844
- If you believe the account was hacked go to https://www.facebook.com/help/1216349518398524/ for recovery details

6.2 X (former Twitter)

Account Management:

- Read and understand X's Privacy Policy to understand what data Twitter is collecting from you and which information are they sharing or disclosing https://twitter.com/en/privacy
- Go to https://help.twitter.com/en/safety-and-security/account-security-tips for tips on how to secure you Twitter account

Password Policy

- Password length must be minimum 8-character length

How to enable 2FA

- Twitter provides three options on enabling two factor authentication security key, third party authenticator app and SMS code. Go to https://help.twitter.com/en/managing-your-account/two-factor-authentication for details and steps on how to enable two factor authentication on Twitter

Security Tips

- Use a strong password.
- Use login verification.
- Government organizations shall get their accounts validated and verified. You may verify your Twitter account by following instructions and filling up a form on Twitter (https://support.twitter.com/articles/20174631)
- Watch out for suspicious links, and always make sure you're on Twitter.com before you enter your login information.
- Never give / share your username and password with anybody.
- Use password reset protection to ensure that no one can infiltrate, and then lock you out of your Twitter account. Checking this option will require you to provide an email address or phone number whenever you try to change your password.

Privacy Tips:

- When you sign up for Twitter, you have the option to keep your tweets public (the default account setting) or to protect your tweets.
- Accounts with protected tweets require manual approval of each and every person who may view that account's tweets.
- Disable location data and tags from appearing with your tweets. To do so, go to **Settings and Privacy → Privacy and Safety → Location information** and uncheck **Add location information to my tweets**.
- Turn off the ability for other accounts to tag your Twitter account on photos from **Settings and privacy → Privacy and safety → Photo tagging**.

Account Recovery

- In case your account had been compromised, there are several steps need to be followed to recover the account: go to https://help.twitter.com/en/safety-and-security/twitter-account-compromised for instructions and details.

If you believe the account was hacked, go to https://help.twitter.com/en/safety-and-security/twitter-account-hacked for recovery details

6.3 Instagram

Account Management:

- Read and understand Instagram Data Policy to understand what data is Instagram collecting from you and which information are they sharing or disclosing (Generally or with Facebook) https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Policies%20and%20Reporting
- Read Facebook's (Platform Policy) at https://developers.facebook.com/terms?helpref=hc_fnav

Password Policy

- Password must be a combination of six or more letters, and never used before.

How to enable 2FA

- Instagram provides two options on enabling two factor authentication, third party authenticator app and SMS code. To enable online authenticator, go to https://help.instagram.com/1582474155197965 for details. Go to https://help.instagram.com/843785199163974 for enabling SMS code authentication.

Security Tips

- Pick a strong password.
- 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.
- Log out of Instagram when you have finished your work. Do not check the "Remember Me" box when logging in.
- Think before you authorize any third-party app.
- Update your accounts as per new security tips and guidelines of Instagram. You can find them at https://help.instagram.com/369001149843369[1]
- Government organizations shall get their accounts validated and verified. You may verify your Instagram account by following instructions and filling up a form on Instagram (https://help.instagram.com/854227311295302)[2]
- Never give / share your username and password with anybody.

Privacy Tips:

- Review tagged photos before they're posted to your profile. To do so, go to **Settings → Privacy → Posts** then enable **Manually Approve Tags**.
- Turn off your activity status so people can't see when you're online. To do so, go to **Settings → Privacy → Activity Status** then disable **Show Activity Status**

Account Recovery

- If your Instagram account is linked to your Facebook account, refer to the Facebook account recovery details above.
- If your Instagram account is not linked to your Facebook account, refer to the following link: https://help.instagram.com/149494825257596 with recovery instructions and details.

6.4 LinkedIn

Account Management:

- Update your accounts as per security tips and guidelines of LinkedIn https://www.linkedin.com/help/linkedin/answer/267/account-security-and-privacy-best-practices?lang=en.
- Read and understand the LinkedIn Privacy Policy https://www.linkedin.com/legal/privacy-policy, LinkedIn User Agreement https://www.linkedin.com/legal/user-agreement and if you are subscribing to LinkedIn Premium make sure to read the LinkedIn Subscription Agreement https://www.linkedin.com/legal/l/lsa.

Password Policy

It must contain at least six characters.

How to enable 2FA

LinkedIn provides two options on enabling two factor authentication, third party authenticator app and SMS code.

Go to https://www.linkedin.com/help/linkedin/answer/544 for details and steps to enable two factor authentications on LinkedIn

Security Tips

- Use a strong password.
- Make sure your email account(s) are secure.
- Log out of LinkedIn after you have finished your work.
- Run antivirus software on your device
- Check which devices can access to your LinkedIn, to do so go to **Account → Settings & Privacy → Sign in & Security → Devices that remembers your password**.
- Check Services you've connected to your LinkedIn account, to do so go to **Account → Settings & Privacy → Account Preferences → Partners & services**.
- Be wary of phishing cyber scams as they are very common on LinkedIn. Phishing messages are designed to look like coming from seemingly real people or companies. They'll often ask (or intimidate) you into clicking links, submitting your personal information or sending money.

Privacy Tips:

- Only connect to people you know.
- Only allow your connections to follow and see your public updates. To do so, go to **Account → Settings & Privacy → Visibility → Visibility of your LinkedIn activity → Followers**
- Don't permit LinkedIn to show information from your profile to users of other services, to do so go to **Account → Settings & Privacy → Visibility → Visibility of your Profile and Network → Profile visibility off LinkedIn**
- Don't allow other accounts to mention or tag your account, this can be done from **Account → Settings & Privacy → Visibility → Visibility of your LinkedIn activity → Mentions or Tags**
- Don't submit any salary data on LinkedIn

Account Recovery

Contact LinkedIn Support to regain access to your account. You will be asked to upload a photo of your valid government issued ID card, driver's license, or passport.

More details can be found here:
https://www.linkedin.com/help/linkedin/answer/127580/verify-identity-to-recover-account-access?lang=en

The following link provides details and steps for compromised or hacked account reporting:
https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-compromised-account?lang=en

6.5 WhatsApp

Account Management:

Read the WhatsApp Terms of Service https://www.whatsapp.com/legal/terms-of-service , WhatsApp Privacy Policy https://www.whatsapp.com/legal/privacy-policy and the Intellectual Property Policy: Your Copyrights and Trademarks https://www.whatsapp.com/legal/ip-policy.

Go to https://www.whatsapp.com/security/ for tips on how to secure you WhatsApp account.

- **WhatsApp scams:** WhatsApp itself will never contact you through the app. Also, WhatsApp does not send emails about chats, voice messages, payment, changes, photos, or videos, unless you email their help and support to begin with. Anything offering a free subscription, claiming to be from WhatsApp or encouraging you to follow links in order to safeguard your account is definitely a scam and not to be trusted.
- **WhatsApp Web:**
    1. Although WhatsApp Web was designed to make life easier by accessing WhatsApp on your desktop, the service is prone to misuse. Just anybody who has access to your phone and WhatsApp application can initiate a web session, scan your WhatsApp security QR code and have complete access to your WhatsApp chats. This can be avoided by ensuring that you do not let anybody else have physical access to your phone. In case where you do need to share, make sure the application is locked with a PIN.
    2. Remember to log out of WhatsApp Web: The mirroring service makes life easier while working on PC. However, most users are unaware that they should ideally log out of WhatsApp Web on Google Chrome browser either from their mobile or the browser.
    3. WhatsApp Web should only be accessed from a dedicated corporate device

Password Policy

- No password

How to enable 2FA

To enable two-step verification by inserting a PIN when opening WhatsApp, do the following:

i. Open WhatsApp Settings.
ii. Tap **Account →Two-step verification →Enable**.
iii. Enter a six-digit PIN of your choice and confirm it.
iv. Provide an email address you can access or tap Skip if you don't want to add an email address. It is recommended to add an email address as this allows you to reset two-step verification and helps safeguard your account.
v. Tap Next.
vi. Confirm the email address and tap Save or Done.

Security Tips

- 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.
- Don't share your WhatsApp SMS verification code with others, not even friends or family.
- **Encryption:**

i. First, make sure that WhatsApp has access to your camera. You may have already allowed this when you installed WhatsApp, but if you did not, it is an easy setting in your Applications area of your phone.
ii. Next, open a conversation with your contact in WhatsApp and then select the person's name at the top of the conversation. This will open the contact window for that person. Near the bottom of that screen, you will see a setting for Encryption.
iii. Tap on the encryption field, and you will be presented with a screen that displays a QR code as well as a 60-digit decimal code that represents the contents of that QR code.
iv. At the bottom of the QR code screen, there is a link that will enable you to scan your friend's code, and they can do the same for your code. This is why you need to allow camera access in WhatsApp, even if only temporarily.
v. Deactivate the access to the camera when done.

Privacy Tips:

Block WhatsApp photos from appearing in photo roll: You could restrict your WhatsApp photos from appearing in photo roll.

i. iPhone: Go to your phone's Settings menu, then 'Privacy', 'Photos', and deselect WhatsApp from the list of apps whose images are fed into the photo stream.
ii. Android: Using a file explorer app like ES File Explorer, find WhatsApp's 'Images' and 'Videos' folders. Create a file within each called '.nomedia'. That will stop Android's Gallery from scanning the folder.

Hide 'last seen' timestamp: You can disable or restrict who sees your 'last seen' time in WhatsApp's 'Profile'; 'Privacy' menu, in Android, iOS, Windows or Blackberry. Be aware though, if you turn it off, you won't be able to see other users' 'last seen' times either.

Restrict access to profile picture: If your WhatsApp sharing is public, anyone you've ever spoken to – even if you've just replied to an unwanted message – can download your pic from your WhatsApp profile and, using Google Image search, very quickly find out more about you. Set profile picture sharing to "contacts only" in the Privacy menu. For corporate accounts, the profile image should be the corporate logo.

Be careful what you talk about: Don't send personal information if you can possibly avoid it – addresses, phone numbers, email addresses – and never send your bank, QID or credit card details, or your passport or other identification details as it can be very dangerous in case the mobile was lost/stolen or account was compromised.

You can set a timer as to when the messages will start disappearing after they have been read by the recipient.

Account Recovery

- Deactivate WhatsApp if you lost your phone. WhatsApp recommends that you immediately activate WhatsApp with the same phone number on a different phone, with a replacement SIM card. Only one number on one device can use the app at a time, so by doing so, you can instantly block it from being used on your old phone. If that is not possible, WhatsApp can deactivate your account.

Find more details and instructions here: https://faq.whatsapp.com/general/account-and-profile/lost-and-stolen-phones/?lang=en

6.6 Snapchat

Account Management:

- Read and understand the Snapchat Privacy Policy https://snap.com/en-US/privacy/privacy-policy.
- Go to https://support.snapchat.com/en-US/article/safety-tips-resources for tips on how to secure your Snapchat account

Password Policy

At least 8 characters long, and don't include personal information, like name, username, phone number, or birthday. Include a mix of numbers, symbols, and capital and lowercase letters in your password.

How to enable 2FA

To enable 2FA, follow the steps below:

i. Open Snapchat on your device.
ii. Tap the Ghost icon at the top of the screen.
iii. Tap the Cog icon to open the Settings menu.
iv. Scroll down and select Login Verification.
v. Tap Continue.
vi. Choose to verify via Text or an Authentication App.
vii. Enter the verification code supplied via Text or through an Authentication App.

Security Tips

- Use a strong password.
- Use 2FA login verification.
- Make sure your email account(s) are secure.
- Log out of Snapchat after you have finished your work.
- Run antivirus software on your device

Privacy Tips:

Keep your Snaps and Stories friends-only: Snapchat sets your account options to friends-only by default. This means only people you have added as a friend that have added you back can send you Snaps or view your own. We strongly recommend keeping it that way, so you always know who is viewing what you create. Don't change your settings to 'everyone,' as that means literally anyone with a Snapchat account can send you messages or see your Stories.

Make sure you know (read: really know) who is on your friends list. If another user tries to add you as a friend, check whether you know who they are before accepting the friend request. If the username of the person who added you does not appear to be anyone you know, it could be a spambot, or an overly curious stranger who has no reason to learn about your life via Snapchat. It is best to ignore these requests.

If you don't want it to be permanent, don't Chat or Snap it: Snapchat content expires after a set time, and Snapchat should also notify you if someone screenshots one of your Snaps or Chats. But don't let that fool you into complacency – your Snaps can definitely be saved (and shared) for posterity without your knowledge.

Snapchat Live: If you ever try to submit something to a "Snapchat Live" story — the collection of stories Snapchat creates for events, holidays, locations or various other reasons — keep in mind that it has the potential to be viewed by everyone if it is selected. Therefore, before trying to submit something, make sure you are comfortable with that.

If someone is making you uncomfortable, you can block that Snapchatter and leave any group chat. Click here to learn about Snapchat's abuse reporting: https://support.snapchat.com/en-GB/a/report-abuse-in-app

- Choose who can contact you directly with Snaps, Chats, calls, etc.
- Customize who can view your location or preferably turn on Ghost Mode to go off the grid.
- Choose who can use your Cameos selfie in two-person Cameos.
- Choose who can see you in Quick Add, a feature that appears around Snapchat which makes it easier to add friends.

Account Recovery

- If you believe the account was compromised or hacked, go to: https://support.snapchat.com/en-GB/i-need-help?start=5145405817880576 and https://support.snapchat.com/en-GB/a/hacked-howto for recovery details

6.7 Tumblr

Account Management:

Read and understand the Tumblr Privacy Policy: https://www.tumblr.com/privacy/en and Tumblr's Terms of Service: https://www.tumblr.com/policy/en/terms-of-service

Password Policy

It should be at least 8 characters, and not recognized as weak password.

How to enable 2FA

To enable 2FA, follow the steps below:

i. Click "Settings" under the Account menu at the top of the Dashboard.
ii. In the Security section, enable "Two-factor Authentication."
iii. Enter your phone number.
iv. Now decide whether you would like to receive the code via text or through an authenticator app.
v. Follow the steps laid out in the Settings page. More details can be found here: https://tumblr.zendesk.com/hc/en-us/articles/226270148-Two-factor-authentication

Security Tips

- Use a strong password.
- Make sure your email account(s) are secure.
- Don't share your passwords even with people you trust.
- Always log out of your session once you have finished your work.
- Check which apps are connected to your account from Account → Apps
- Report SPAM
    a. From posts on the web: From the dashboard or a search results page, click the share menu (paper airplane) at the bottom of the post, and click "Report."
    b. From blogs on the web: Report an entire blog by hovering over the blog's avatar, clicking the little person silhouette, and clicking "Flag this blog".
    c. From messages in the app or on the web: Tap or click "Mark as spam" under the spammer's first message. Note that "Mark as spam" won't appear if it's somebody you follow, or somebody you've already had a conversation with.
    d. From fan mail on the web: From the inbox, click the three dots at the bottom of a spam message and choose "Report."
    e. If you do not have access to a computer now, you can use a mobile browser's desktop view to report spam following the steps listed above. To get to the desktop view in iOS, open Safari and visit tumblr.com, log in, tap the share icon (little box with an arrow) at the bottom of the screen, and tap the gray "Request Desktop Site" button. On Android, open Internet or Chrome and visit tumblr.com, log in, tap the three dots icon in the top right-hand corner of the screen, and check the "Desktop View" box.
- Generate backup codes to get back into your Tumblr account, in case you don't have access to your phone for some reason. Here's how to get them:
    i. Go to your Account Settings on web.

ii. In the Security section, click on the "Generate backup codes" button (note that you'll need to have two-factor authentication enabled in order to see this option).
iii. Enter your account password when prompted and you'll get 10 backup codes.

Privacy Tips:

Tumblr does not allow private blogs. But Tumblr offers you to make a secondary blog, which you can restrict access to. To create a secondary blog go to: https://tumblr.zendesk.com/hc/en-us/articles/226340308-Secondary-blogs for instructions.

Account Recovery

If you believe your Tumblr account was compromised or hacked, go to: https://tumblr.zendesk.com/hc/en-us/articles/226176987-Compromised-accounts for recovery details.

6.8 YouTube / Google

Account Management:

Google account controls access to YouTube social media platform plus Gmail and many sites and apps you are visiting/using; so, its security configurations must be in place. Read and understand Google Policies https://policies.google.com/privacy?hl=en-US, YouTube's Terms of Service https://www.youtube.com/static?template=terms and the Community Guideline https://www.youtube.com/intl/en_us/howyoutubeworks/policies/community-guidelines/

Make sure you are using the latest version of your browser. Learn how to update Google Chrome from here https://support.google.com/chrome/answer/95414.

Password Policy

- The password can consist of at least 8 characters. It can be any combination of letters, numbers, and symbols (ASCII-standard characters only). Accents and accented characters are not supported.
- You can't use a password that:
- Is particularly weak. Example: "password123"
- Has been used before on the account
- Starts or ends with a blank space

How to enable 2FA

Google gives several options for enabling two-factor authentication through one of the following:

i. Google prompts
ii. Verification code from a text message or call
iii. Google Authenticator or other verification code apps
iv. Backup Codes
v. Security Keys

To enable 2FA with any of the above, go to: https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome

Security Tips

- Use a strong password.
- Use 2FA login verification.
- Log out of your account after you have finished your work.
- Run antivirus software on your device
- Take the Google Security Checkup. This step-by-step tool gives you personalized and actionable recommendations to help strengthen the security of your Google Account.
- Install only essential apps and browser extensions on devices that have access to sensitive information. Avoid installing unknown apps or apps from unknown sources to protect your device and personal info. Here is the link to know how: https://support.google.com/chromebook/answer/2589434 .
- Frequently check your backup contact methods. This is what Google will use should you get locked out of your account to verify you're the account owner.

- Check and review the devices that were used to access your account. To do so, go to https://myaccount.google.com/security and you will see a list of your devices.

Privacy Tips:

- Remove account access for any non-essential apps to better protect sensitive information.
    1. Manage apps with access to your account and learn more about the risks.
    2. Turn off access for apps that use less secure sign-in technology.
- To check if someone else has access to your account, sign into your Gmail account and scroll to the bottom of the page, click on **Last account activity** at the end of that line, click **Details** to see when, how and where your account is being used. If you suspect any suspicious activity, click on the button labeled **Sign out of all other Gmail web sessions** and immediately change your password.
- Set & check permissions on your YouTube channel, you can invite someone else to manage your YouTube channel without giving access to your Google Account. Invite someone to access their channel as a:
    1. Manager: Can add or remove others and edit channel details.
    2. Editor: Can edit all channel details.
    3. Viewer: Can view (but not edit) all channel details.
    4. Viewer (limited): Can view (but not edit) all channel details except revenue information.

To do so, visit: https://support.google.com/youtube/answer/9481328.

Account Recovery

If you believe the account was compromised or hacked, go to:
https://support.google.com/accounts/answer/7299973 and
https://support.google.com/accounts/answer/6294825 for recovery details and tips.

6.9 Telegram

Account Management:

- Read the Telegram Terms of Service: https://telegram.org/tos, and Telegram Privacy Policy: https://telegram.org/privacy.
- Telegram -*nowadays*- is considered as cryptocurrency scammers heaven and must be treated with caution.

Password Policy

- No password required

How to enable 2FA

To enable two-factor verification by inserting a PIN or Password when opening Telegram, do the following:

1. Open the Telegram app.
2. Tap "**Settings**" in the bottom right corner of the screen.
3. Select "**Privacy and Security**".
4. Near the top of the screen, tap "**Two-Step Verification**".
5. Choose "**Set Additional Password**".
6. Enter a password and confirm it by re-entering it.
7. Now tap "**Create Password**".
8. Enter a password hint, then select **Continue**.
9. Enter the email address you want to use to recover a forgotten password. Then select **Continue**.
10. You'll receive a verification code at your email address. Enter the code to authenticate your email.

Security Tips

- Don’t share your Telegram SMS verification code with others, not even friends or family.
- End-to-end encryption is not the default configuration in Telegram chat. To have an end-to-end encryption chat, you will need to launch a “**Secret Chat**” which can be enabled by going to the profile of the contact you want to start encrypted chat with, tap on options, then choose and confirm the “**Start Secret Chat**” option.

Privacy Tips:

Try not to share your information with all Telegram users, here are a few privacy configurations tips which you can change from **Settings ➔ Privacy and Security:**

1. Set “Who can see my phone number” to Nobody.
2. Set “Who can find me by my number” to Contacts.
3. Set “Who can see my timestamp” to Nobody.
4. Set “Who can see my profile photo” to My Contacts.
5. Set “Who can call me” to My Contacts.
6. Set “Who can add a link to my account when forwarding my messages” to My Contacts.

7. Set “Groups & Channels → Who can add me” to My Contacts.

Account Recovery

Deactivate Telegram if you lost your phone. Telegram recommends that you immediately activate Telegram with the same phone number on a different phone, with a replacement SIM card. Only one number on one device can use the app at a time, so by doing this, you can instantly block it from being used on your old phone.

If that’s not possible, you can contact Telegram support or use a third-party app, you will need to provide some personal information such as name and email.

6.10 Signal

Account Management:

Signal private messaging chats are end-to-end encrypted by default and the application is built in the sense of carrying sensitive and classified messages and information.

Signal private messaging app is an open source software that tries to minimize the amount of data stored on Signal servers https://signal.org/blog/signal-profiles-beta/, https://signal.org/bigbrother/eastern-virginia-grand-jury/

Read the Signal Terms of Service and Privacy Policy https://signal.org/legal/#terms-of-service and their contact discovery https://signal.org/blog/contact-discovery/.

Password Policy

- No password required

How to enable 2FA

To enable two-factor verification by inserting a PIN or Password when opening Signal, do the following:

i. Tap on your profile icon at the top-left corner and then choose Privacy.
ii. Scroll to the bottom and enable Registration Lock.
iii. If you don't remember your PIN, then you can simply tap on Change your PIN and create a new one. You can create at least a 4-digit or a maximum 20-digit PIN
iv. Signal does not support Authenticator apps or offer any backup codes.
v. If you forget your PIN and have no access to your old device, then you will have to wait 7 days for the Registration Lock to expire. Only after that, you will be able to log in to Signal and create a new PIN.

Security Tips

- Don't share your Signal Private messaging app SMS verification code with others, not even friends or family.
- Enable Screen Lock to restrict your messages from unauthorized access.
- Set a PIN for reinstallation, backup restore, and identity verification

Privacy Tips:

- Disable **Contact Joined Signal** Notification
- Custom Notification to get a notification with the name of the sender without any message.
- You can blur faces on Signal before sharing images
- You can set a timer as to when the messages will start disappearing after they have been read by the recipient.
- Block Screenshots.
- Relay Calls so that your IP address is not revealed to your contacts.
- Create a Local Backup
- Verify Contacts to avoid the possibility of man in the middle attack, and to do so follow these steps:

i. Open the contact's profile you want to verify
ii. Scroll down and open "View safety number"
iii. Tap on the QR code and scan the QR code from the device of the other contact

Alternatively:

i. Open the contact's profile you want to verify
ii. Scroll down and open "View safety number"
iii. Tap on the "share" button to send your safety number to another user
iv. Compare and verify the safety numbers.

Account Recovery

If you lost your phone number, then there is nothing that can be done with Signal.

Signal developed Secure Value Recovery which keeps your social graph unknown to Signal servers. If you lost or switched your mobile device your PIN can recover your profile, settings, contacts, and the accounts you've blocked, but A PIN is not a chat backup. Your message history is not linked to a PIN and a PIN cannot be used to recover lost chat history. More details here: https://signal.org/blog/secure-value-recovery/.

6.11 TikTok

Account Management:

TikTok security concerns largely center on the fact that TikTok is a Chinese company and the Chinese laws enforce companies in China to share information with the government of China.

Read and understand TikTok's Privacy Policy to understand what data is TikTok collecting from you and which information are they sharing or disclosing https://www.tiktok.com/legal/privacy-policy?lang=en and Terms of Service https://www.tiktok.com/legal/terms-of-service?lang=en.

Go to https://www.tiktok.com/safety/en/privacy-and-security-on-tiktok/ to know more about TikTok privacy and security features

Password Policy

Password should be between 8 and 20 characters with letters, numbers, and special symbols.

How to enable 2FA

To enable 2FA, follow the following steps:

i. Go to Your Profile.
ii. Tap on the three lines symbol to open your settings.
iii. Tap Security and Login.
iv. Change 2-step verification from off to on.
v. Choose either the SMS* or E-mail option for the verification code to be sent.

Security Tips

- Ensure that your TikTok account is private. To do so, go to your profile **Settings** → **Privacy and Safety** and look for the **Discoverability** heading, then turn on the Private Account option.
- you can turn off the **Suggest your account to others** option from **Discoverability** as above. Turning this setting off will stop your account from being recommended to other users and will prevent other people from finding your account via search engines.
- Avoid opening TikTok links outside the app
- Log out of TikTok when you have finished your work.
- Check mobile devices that are currently using or have recently accessed your TikTok account. To do so, go to **Privacy and safety** → **Manage my account** → **Security** → **Your Devices**.
- Be careful of what you choose to post. And that your videos don't contain personal information like address signs or national IDs.
- Enable security alerts to ensure that you are alerted when your account displays any suspicious account action. To do so, go to your profile then tap on the three lines menu then choose **Security** where you can find and enable **Security Alerts**

Privacy Tips:

- Read TikTok's Safety Tips: https://www.tiktok.com/creators/creator-portal/en-us/community-guidelines-and-safety/safety-tips/
- Limit the amount of information you share on the app
- Limit other users' interaction with your videos. To do so, go to **Privacy → Safety →** then set **Allow your videos to be downloaded** to **off,** set **Who can send you direct message** to **friends** and set **Who can Duet with your Videos** to **Only me**
- Turn off Ad Authorization. To do so, go to your profile **Settings → Privacy** and look for the **Personalization and Data** heading, then turn off the **Ad authorization**.

Account Recovery:

1. Visit this link for details on compromised accounts: https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked, contact TikTok Support if you believe your account is hacked.

7 Compliance and Enforcement

7.1 Compliance and Enforcement

This guideline is published to help organizations better understand the risks to their social media identities and how to manage the risks associated with a social media account.

The guideline complements National Information Assurance Standard and the National Data Classification Policy.

8 Annexes

8.1 Acronyms

NCSA	National Cyber Security Agency
2FA	Two Factor Authentication.
QR Code	Quick Response code.
PIN	Personal Identification Number.
ASCII	American Standard Code for Information Interchange.
SMS	Short Message Service.
IP	Internet Protocol.

8.2 References

Emiri Decree No 1 of year 2021

President of National Cyber Security Agency (NCSA) Decision No 3 of year 2022

8.3 List of Figures

No Figures

8.4 Reporting Incidents to NCSA

Agencies that are experiencing a DDoS attack may report an incident to NCSA in one of the following ways:

Call NCSA Hotline at 16555 (24 x 7 service)

Email NCSA at ncsoc@ncsa.gov.qa

Agencies may also find the following guidelines useful to prepare themselves to face an attack / incident.

Guidelines for Incident Management – Pre-requisite Measures