DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Guide for social media account protection and recovery

Risks and threats

Countermeasures

Facebook

Instagram

TikTok

WhatsApp

YouTube

Incident notification

TLP:CLEAR

Risks and threats

Social media accounts are exposed to various cyber risks and users should be aware of potential threats to protect their personal information and online presence. Here are some common cyber risks associated with social media accounts:

Account Takeover Attack (ATO): Cyber attackers can try to gain unauthorised access to your social media accounts by using stolen passwords or exploiting vulnerabilities. Once they gain control, they can steal your identity, post fake information or malicious content, or access sensitive information.

Phishing attacks: Phishing involves tricking users into providing sensitive information such as authentication, personal or financial data. Attackers manage to extract them from users by presenting various scenarios and pretexts, where the potential victim is encouraged to provide the data. Attackers make use of social engineering techniques and visual identity elements that have the role of providing a dose of trust and legitimacy to the action. An example would be clone sites, which look similar to the original but are accessible on a different domain. Users are contacted by email, sms, social media or chat platforms. The messages include malicious links designed to redirect the potential victim to fraudulent login pages controlled by the attackers and designed to capture their credentials.

Malware distribution: Cyber attackers can use social media platforms to distribute malware. This can happen through malicious links or attachments in messages or posts. Clicking on these links may install malware on your device.

Social Engineering: Cyber attackers can use social engineering techniques to manipulate users into revealing sensitive information. This could involve attackers masquerading as friends, acquaintances or trusted individuals to gain access to sensitive information.

Countermeasures

Securing your social media accounts is essential to keeping your personal information safe and preventing unauthorised access. Some tips:

Strong Passwords: Create strong passwords with a combination of uppercase and lowercase letters, numbers, and special characters. Avoid obvious passwords such as dates of birth or last names.

Two-Step Authentication (2FA): Enable two-step authentication for an extra layer of security. This involves providing a code generated on your mobile device or via email in addition to your password.

Regular password updates: Change passwords regularly and avoid using the same password for multiple accounts. The password must be unique for each account.

Reviewing your privacy settings: Regularly review and adjust your privacy settings to control who can see your information and who can interact with your content.

Avoiding suspicious links: Be wary of links and attachments received through messages or email. Do not access suspicious links or links from unknown sources.

Beware of phishing attempts: Be aware of possible phishing attempts and never provide personal information or login details following suspicious requests.

Regular app updates: Make sure your social media and related apps are updated to the latest version to benefit from the latest security options.

Check active sessions: Monitor active sessions and devices connected to your social media account. Disconnect unauthorised sessions.

Using a VPN: If you connect to your social media accounts on public networks, use a virtual private network (VPN) to secure your connection.

Avoiding Unofficial Apps: Download official applications of social media platforms and avoid using unofficial or dubious applications.

How you can recover your Facebook account

If you can no longer access your Facebook account, it is possible that someone has changed your access data and your account has been compromised. *What do you have to do*?

1. Enter the address https://www.facebook.com/login/identify
2. Enter the e-mail address you registered with or the phone number
3. Follow the on-screen steps to reset your account password

You can ask a friend for help. *What do you have to do?*

1. Ask your friend to search for your account
2. Log in to your account. On the right side you will see three dots (...)
3. Click on them and a menu will appear
4. From there choose **Get help or report**
5. Here you choose one of the options and follow the steps

Suspicious activity on your account

If you see any activity you don't recognise on your account, it's an indication that it may have been compromised and attackers have access to it. *If you notice changes:*

- Your name, birthday, email address or password suddenly changes
- Friend requests from your account are sent to people you don't know
- Messages you haven't written are sent from your account
- Posts you didn't create appear on your timeline

If you've discovered this kind of activity on your account, but you're still able to access your account, follow these steps:

1. Go to your Facebook profile and look for **Settings and Privacy**, then **Settings**
2. Tap **Password and Security** to see **Change Password**
3. Enter your current password, then enter a new password (minimum 6 characters, including letters, numbers and special characters)
4. It would be good to use more than 10 characters. A good password example: !1!k370g0707h3S34 (*I like to go to the Sea*)
5. Click **Change Password**

Check if your Facebook account has been hacked

How can you check if you have been hacked? Follow these steps to find out if someone else has logged into your Facebook account:

1. Go to your Facebook profile and look for **Settings and Privacy** then **Settings**
2. Tap on **Password and Security** to see **Where you've signed in** then **See all** (on mobile) and check if you recognise the devices that appear in the list
3. If you see a device you don't recognise, tap the device name, then tap **Select devices you want to disconnect from**
4. Tick the devices you want to disconnect, then click **Disconnect**

How to recover your Instagram account

If you have any doubts about your Instagram account or you can no longer log in to it, visit the official Instagram help centre page (https://www.instagram.com/hacked/) to start the recovery process. To identify your Instagram account, you need your **username, phone number or email address.**

Check if the email address associated with the account has been changed

If you received an email from **security@mail.instagram.com** notifying you that your email address has changed, you can cancel this change by selecting Secure Account in the message. If other information has been changed (password, username) and you can't change your email address, request a login link or a security code from Instagram.

Request a login link from Instagram

You can request a login link to your email address or phone number by following the steps below:

- On the sign-in screen, tap **Get help** for signing in
- Enter the username, email address, or phone number associated with your account, then click the Send the login link option. If you don't have access to the username, email address or phone number associated with your account, visit this page and follow the on-screen instructions. Complete **the captcha** verification to confirm that you are a real person, then click **Continue**
- Click on the login link in the email or text message (SMS) received and follow the instructions

Request a security code or support from Instagram:

If you are unable to recover your account using the login link, you can request assistance on a mobile device. Make sure you enter a secure email address that only you have access to. After submitting your request, you should receive an email from Instagram with the steps to follow. Learn more about what to do if you don't know your username.

Confirm your identity

If you request support for **an account that contains photos of you**, you'll be asked to record a video selfie of yourself turning your head in different directions to verify that you're a real person. After you send the video selfie, you will receive an email from Instagram to the email address you mentioned. This video clip will be used to confirm your identity.

If you submitted a support request for **an account that does not contain photos of you**, you should receive an automated email response from the Meta support team. You will need to provide the email address or phone number you signed up with and the type of device you used when you signed up.

If you can still sign in to your Instagram account:

If your account has been hacked, but you can still sign in to it, here are some things you can do to try to keep your account safe:

- Make sure the phone number and email address in your account settings are correct
- Change your password or send yourself a password reset email
- Enable two-factor authentication for added security
- Go to Manage Accounts and delete associated accounts you don't recognise
- Revoke access to any suspicious third-party apps

How to recover your TikTok account

If you notice any of the following suspicious behaviour, your account has most likely been compromised:

- Your account password or phone number have been changed
- Your account username or nickname have been changed
- Videos have been deleted or posted without your permission
- Messages you haven't written have been sent from your account

You must report the incident:

1. Tap **Profile** at the bottom right
2. **Tap the icon with 3 lines** on the top right
3. Tap **Settings & Privacy**
4. Tap **Report a problem**
5. Select a report topic

You can also follow these steps to secure your account:

Password change

- If you believe your account may have been compromised, change your password as soon as possible. Choose a password that is memorable for you, but difficult for other users to guess.
- Learn how to reset your TikTok password

Enable 2-step verification

- 2-step verification adds an extra layer of security to your account in case your password is compromised. It also helps you protect your account from unrecognised/unauthorised devices or third-party apps. Learn how to enable 2-step verification

Check the devices you're connected to

- You can view phones and other mobile devices that are currently using or have recently accessed your TikTok account. Learn how to access connected devices

Check for security alerts

- To review security alerts, go to TikTok app settings, tap **Security & sign-in**, then tap **Security alerts**

How you can recover your WhatsApp account

It's a good idea to let your friends and family know if you suspect someone else is using your WhatsApp account, as attackers could use the identity and trust generated by that account in conversations and groups. Keep in mind that WhatsApp is fully encrypted and messages are stored on your device, so if someone accesses your account from another device, **they can't read your previous conversations**.

Do not share the WhatsApp verification code received via SMS with anyone, not even friends or family members! Without this code, any user trying to verify your number will not be able to complete the verification process and will not be able to use your phone number on WhatsApp.

If someone fraudulently obtains your code and you lose access to your WhatsApp account, follow the instructions below to recover it:

- Sign in to WhatsApp with your phone number, then verify your number by entering the 6-digit code you receive via SMS
- After you enter the 6-digit code received via SMS, **the person using your account will be logged out automatically**
- You may also be asked to enter your code for two-step verification. If you don't know this code, the person who used your account probably enabled two-step verification
- **You have to wait 7 days before you can sign in without** the two-step verification code. Whether you know this verification code or not, the person who used your account is logged out the moment you enter the 6-digit code received via SMS

WhatsApp provides support to users, which is available on the phone, in the application, in the section WhatsApp > Settings > Help > Contact us or the official website of the application, in the section Contact us.

If your phone is lost or stolen, there's nothing WhatsApp support can do. It is not possible to deactivate your WhatsApp account, because there is no way to verify that you are the owner of the phone number associated with that account.

How to recover your YouTube account

Before taking action, it's important to double-check for signs that your channel has been compromised. Every YouTube channel is associated with at least one Google account. When a YouTube channel is compromised, it means that at least one of the Google accounts associated with the channel is also compromised.

If you notice any of the following activity in your Google Account, your Google Account may have been hacked or compromised:

- Changes you didn't make: Profile photo, descriptions, email settings, AdSense account association or the sent messages are different
- Uploaded videos that don't belong to you: someone posted videos from your Google Account. You may receive email notifications about these videos for inappropriate content penalties or warnings

To recover a compromised YouTube channel, you must first recover the compromised Google account associated with the YouTube channel. Three steps to recover your YouTube channel:

1. Recover and secure the compromised Google account associated with the YouTube channel
2. Immediately undo unwanted changes on the YouTube channel to avoid policy repercussions such as community guidelines or copyright warnings
3. Reduce the risk of unauthorised access to your Google account using security best practices for all associated channel users

Recover your Google Account

If you can still sign in to your Google account, it's important to update your password and secure Google account. If you can't sign in to your Google Account:

1. Follow these steps to recover your Google or Gmail account. You will be asked a few questions to confirm it is your account and answer them correctly. If you're having trouble, follow the tips to complete the account recovery steps
2. Reset your password when prompted. Choose a strong password that you haven't used before for this account. Learn how to create a strong password
3. Ask channel managers / owners to follow the same steps to secure their Google account

Incident notification

Reporting can be done through the online form on the website www.dnsc.ro, alerts@dnsc.ro or by calling 1911, which is the unique national emergency number dedicated to reporting cyber security incidents..

- If you received a **suspicious email**, send it to alerts@dnsc.ro or call 1911
- If you received a **suspicious text message**, report it via the online form on the website www.dnsc.ro, send it to alerts@dnsc.ro or call 1911
- If you have received suspicious phone calls, hang up, block the user and contact your phone provider.

This guide was produced by the following DNSC experts:

Mihai Rotariu, Daniel Abotezătoaei, Dan Andrieș, Mihaela Dan, Irina Nemoianu, Cristian Nistor