Compromised account

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Anyone, and the IT leads of an organization.

What to do when someone takes control of an email, social media or WhatsApp account, or an account on an internal system. The goal is to regain control, get the intruder out and keep them from using the account to deceive others.

Signs it is happening

- You cannot log in even though the password is correct.
- Login alerts from a device or place you do not recognize.
- Messages sent from your account that you did not write.
- Changes to the recovery email or phone number.
- Contacts telling you that “you” asked them for money or a code.

How serious it is

High	An administrator, finance or executive account; the organization's official account.
Medium	The account of a user with access to internal information.
Low	A personal account with no access to the organization's systems.

First hour

- [ ] **1.** If you still have access, change the password from a device you know is clean.
- [ ] **2.** Close all open sessions and unlink any devices you do not recognize.
- [ ] **3.** Turn on two-step verification, preferably with an app rather than SMS.
- [ ] **4.** Review and correct the recovery email and phone number.
- [ ] **5.** WhatsApp: reinstall the app and register your number again with the SMS code.
- [ ] **6.** Tell your contacts through another channel to ignore suspicious messages.

Preparation (before the incident)

- Use a different password for each service, with a password manager.
- Turn on two-step verification on all important accounts.
- On WhatsApp, turn on the two-step verification PIN.
- Never share a code you receive by SMS, not even with people you know.
- Store the recovery codes in a safe place.

Detection and Analysis

- Review the login history: date, device and location.
- Identify how they got in: phishing, reused password, shared code or malware.
- Review what the intruder did: messages sent, files downloaded, settings changed.
- Check whether the same password was used on other services.

Containment

- If you lost access, use the platform's official recovery process.
- Revoke the permissions of third-party applications you do not recognize.
- Remove forwarding rules, filters and automatic replies you did not create.
- Change the password on every service where you reused it.

Eradication

- Scan your devices with antivirus; if there is malware, the new password will leak too.
- Delete the fraudulent messages sent from the account, after saving them as evidence.
- Report to the platform any fake accounts impersonating you.

Recovery

- Confirm that only your devices have an active session.
- Let your contacts know you have recovered the account.
- Review the account's activity every week for a month.

Lessons Learned

- Identify the habit that allowed the access and fix it across all your accounts.
- In an organization, check whether other accounts share the same weakness.
- Share the case with your team or family so they can recognize the scam.

Evidence to preserve

- Screenshots of the login alerts and of the settings changes.
- Messages sent by the intruder.
- The email or message used to trick you, if there was one.
- Phone numbers or accounts that money was requested to be sent to.

What not to do

- Changing the password from a device that may be infected.
- Paying someone on social media who offers to “recover” the account: it is another scam.
- Sharing verification codes with someone claiming to be technical support.
- Creating a new account and abandoning the old one in the intruder's hands.

Who to notify

- Your contacts, through a channel other than the affected account.
- The IT department, if it is a work account.
- Your bank, if the account gave access to financial services.
- The Public Ministry (Ministerio Público), if third parties were scammed or extorted.
- cert.gt, at cert.gt/reportar, to receive guidance.

When to close the incident

- You have control of the account and of its recovery methods.
- Two-step verification is turned on.
- No sessions, applications or rules that are not yours remain.
- Your contacts have been notified.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).