



# MY LINKEDIN HAS BEEN HACKED. NOW WHAT?



A practical step-by-step recovery guide for personal profiles and company pages

This guide was written because it happened to someone we know. Their profile name was changed overnight. Their connections were being messaged with links they never sent. Their professional identity — years of building a network, a reputation and a presence — was stolen from under them.

We searched for a clear, practical guide and found very little. So we wrote one.

**Save this. Share it.** Hopefully you never need it.

## 1 FIRST: HOW DO YOU KNOW YOU HAVE BEEN HACKED?

The signs are not always obvious immediately. Look out for:



Your password no longer works



Your name, photo or profile information has been changed without your knowledge



Connections are messaging you asking about links or messages you never sent



You receive a LinkedIn email about a login from a device or location you do not recognise



Posts, comments or connection requests are appearing under your name that you did not create



LinkedIn has sent you a password change notification you did not initiate



You notice new connections in your network you never requested



**If any of these apply, act immediately. Every minute counts.**

## 2 ONE GROUND RULE BEFORE YOU DO ANYTHING



**Start recovery on a device, browser and network you have used to sign in to LinkedIn before.**

A familiar setup is more likely to be recognised and less likely to trigger extra verification.



**And critically: do not create a brand-new LinkedIn account to report the hacked one.**

Recovery always runs through your existing account.



**NEXT: SCENARIO A — YOU CAN STILL ACCESS YOUR ACCOUNT**

# YOU CAN STILL ACCESS YOUR ACCOUNT



If you are still logged in or can get back in immediately, move fast through these steps.



1

## Change your password right now

Go to Me icon > Settings and Privacy > Sign in and security > Change password. Tick 'Require all devices to sign in with new password' so the attacker is forced out of every active session. Make the new password long, random and unique to LinkedIn.



2

## Sign out every other device

Go to Settings and Privacy > Sign in and security > Where you're signed in. End all unrecognised sessions immediately.



3

## Check and secure your email address

Go to Settings and Privacy > Sign in and security > Email addresses. Make sure your email is still correct. Remove any unfamiliar email address straight away.



4

## Check your phone number

Go to Settings and Privacy > Account preferences > Phone numbers. Verify your number is still yours and remove any you do not recognise.



5

## Review your profile for unauthorised changes

Check your name, photo, headline, about section, experience, education and skills. Revert anything that has been changed.



6

## Check sent messages and connection requests

Review what was sent while the hacker had access so you can warn people clearly and specifically.



7

## Remove suspicious third-party app access

Go to Settings and Privacy > Data privacy > Other applications. Revoke access for anything unfamiliar or suspicious.



8

## Turn on two-factor authentication immediately

Go to Settings and Privacy > Sign in and security > Two-factor authentication. Use an authenticator app if possible.



**Move fast. The aim is to lock the attacker out before they make more changes.**



## Once you have done these 8 steps

- Warn any contacts who received suspicious links
- Post a clear status update if needed
- Keep screenshots of anything unusual for your records



**NEXT: SCENARIO B — YOU ARE LOCKED OUT COMPLETELY**



# YOU ARE LOCKED OUT COMPLETELY



If your email, password or both have been changed, stay calm. There is still a recovery path.

## 1 Try the password reset immediately

Go to the LinkedIn login page and click **Forgot Password**. Enter the email address associated with your account. Check your inbox and spam folder.

## 2 Try your secondary email address

If you ever added a secondary email to LinkedIn, use it to request the reset code or link.

## 3 Verify your identity

If you cannot access any linked email, submit the official **Report Unauthorized Account Access or Changes** form. Include your LinkedIn profile URL if you have it, explain clearly what changed, and be ready to provide a valid government-issued ID.

## 4 Submit one ticket only

Do not raise duplicate requests. Multiple tickets can slow the review process.

## 5 Contact LinkedInHelp on X

Message **@LinkedInHelp** to confirm your case is open. This does not replace the official form, but it can help.

## 6 Be patient but persistent

Support can take several days. Keep a record of every email, case number and step you take.



Official form to save

[www.linkedin.com/help/linkedin/answer/a1340402](https://www.linkedin.com/help/linkedin/answer/a1340402)

## WHAT TO DO ABOUT YOUR CONNECTIONS



### If you still have access

- Post a **status update** immediately
- Tell people not to click unusual messages or links
- Message close contacts directly if needed



### If you do not have access

- Contact key connections by email, phone or WhatsApp
- Ask a trusted connection to post a warning on your behalf
- Ask them to tag your profile name so people can find it



## DO NOT DO ANY OF THESE THINGS



Do not pay anyone to recover your account



Do not share a verification code with anyone



Do not create a new LinkedIn account



Do not use a public network or unfamiliar device during recovery



NEXT: ONCE YOU ARE BACK IN — YOUR SECURITY CHECKLIST



# DO NOT SKIP THIS CHECKLIST



Getting back into your account is only half the job.

## 1 YOUR SECURITY CHECKLIST

- ✓ Change your password to something long, unique and not used anywhere else
- ✓ Turn on two-factor authentication using an authenticator app
- ✓ Check every email address on the account and remove anything unfamiliar
- ✓ Verify your phone number is correct
- ✓ Sign out all other sessions via Where you're signed in
- ✓ Review third-party app connections and remove anything suspicious
- ✓ Go through your profile section by section and revert unauthorised changes
- ✓ Check sent messages and connection requests for anything the hacker sent
- ✓ Post a clear update to your network letting people know the account is secure
- ✓ Secure your email account too — change that password and enable 2FA there as well

## 2 FOR COMPANY PAGES



### If a super admin account has been hacked

Recover that personal profile first. Page access is restored with it.



### If you have been removed as an admin

Contact LinkedIn Help and provide proof of your association with the page — company email, registration documents or ownership evidence.



### If the page itself has been altered

Once access is restored, review the page name, logo, banner, description and posts made during the compromise period.



### Protect the page going forward

Keep admin access limited, review roles regularly and do not hand out super admin access unnecessarily.

## 3 HOW TO PROTECT YOURSELF GOING FORWARD

- ✓ Use a password manager
- ✓ Never click links in LinkedIn notification emails — go directly to linkedin.com instead
- ✓ Turn on two-factor authentication
- ✓ Check Where you're signed in periodically
- ✓ Keep a note of your profile URL somewhere outside LinkedIn

## 4 KEY LINKS TO SAVE NOW

- Report a compromised account: [www.linkedin.com/help/linkedin/answer/a1340402](https://www.linkedin.com/help/linkedin/answer/a1340402)
- Password reset: [www.linkedin.com/uas/request-password-reset](https://www.linkedin.com/uas/request-password-reset)
- LinkedIn Help Centre: [www.linkedin.com/help/linkedin](https://www.linkedin.com/help/linkedin)
- Support on X: @LinkedInHelp
- Where you're signed in: Settings and Privacy > Sign in and security > Where you're signed in
- Two-factor authentication: Settings and Privacy > Sign in and security > Two-factor authentication



This guide was produced by Innov8 Social.

We are a specialist maritime social media agency and we help businesses and professionals build and protect their LinkedIn presence.

Share this guide with anyone dealing with a compromised account.



Podcast: YouTube | Spotify



Blog: [innov8social.co.uk/socialmediablog](https://innov8social.co.uk/socialmediablog)

Making Maritime Marketing Social