

What to Do If Your Email Has Been Hacked: A Practical Guide

Email is the digital front door to your business – and if it gets compromised, the consequences can ripple far beyond your inbox.

This guide explains the practical steps you need to take immediately, and how to prevent future attacks.

Step 1: Regain Control – Immediately

Change Your Password

Change your password immediately. Choose a strong, unique password that you haven't used elsewhere. Don't just add a "1" to the end – go for a passphrase or use a password manager to generate something truly secure.

Contact us straight away – we can force a reset and help you regain access securely.

Locked Out? Take Action

If you've been locked out of your account or notice suspicious logins (e.g. sign-ins from unusual locations), act fast:

- Contact us
- Request an account reset and block further access if possible.

We can review Microsoft sign-in activity, force sign-outs, and apply conditional access to block further intrusion.

Step 2: Improve Your Security

Turn on Two-Factor Authentication (2FA)

This is the single biggest improvement you can make. 2FA means even if someone steals your password, they can't log in without access to your phone or authentication app. If you're using Microsoft 365, this should be turned on as standard - if it's not, we strongly recommend enabling it.

Use a Unique, Strong Password

One of the most common mistakes is reusing the same password across multiple accounts. If hackers get access to one, they often try it elsewhere — a method known as "credential stuffing." Use a password manager (like Keeper) to generate and store unique, strong passwords for each service.

Consider Additional Security Features

Advanced Email Threat Protection can block phishing and malware at source.

Step 3: Consider the Wider Impact

Was This Password Used Elsewhere?

If the same password was used on other services (e.g. LinkedIn, Dropbox, even Netflix), change those passwords too. Email accounts are often the gateway to resetting other logins – so this matters.

Check for Malware or Keyloggers

If a hacker gained access using a password that you're certain was private, it's possible your device is compromised. Run a full malware and antivirus scan, and consider:

Reinstalling a clean version of your operating system (if the compromise is severe)

Checking for persistent threats like keyloggers or remote access tools

Conclusion

Getting hacked can be stressful, but how you respond matters more. Taking swift action and improving your security setup can prevent far worse consequences including data theft, reputational damage, or unauthorised financial access.

Revision #2

Created 10 June 2025 08:31:51 by Doug

Updated 10 June 2025 08:41:10 by Doug