

I've Been Hacked: Business Recovery Checklist

A practical checklist for Microsoft 365, Google Workspace, staff accounts, websites, shared systems, customer data and incident records.

Before a breach: information to pull together

Keep this information somewhere safe and separate from the accounts or devices it describes. Do not write down passwords in this checklist.

Done	Item	Notes / account / date / case number
■	Business owner, manager and trusted IT support contact details	
■	Microsoft 365 or Google Workspace admin account holders	
■	Cyber insurance, bank, legal adviser and ICO contact routes	
■	Critical systems: email, website, finance, customer data and remote access	
■	Backup locations, retention periods and restore contact	
■	Staff communication route if email is not trusted	

If you think you have been hacked: follow this order

Stage	What to do	Record
1 Identify	Decide what appears affected: money, email, admin account, staff account, device, website, shared system or data.	Incident owner, affected service
2 Stop	Contact trusted IT support. Do not wipe devices, delete accounts or restore backups until evidence is preserved.	Containment action, time
3 Save	Start an incident log and preserve alerts, emails, screenshots, timelines, IPs, invoices and case numbers.	Evidence location
4 Secure	Secure administrator accounts, email, Microsoft 365 or Google Workspace, devices and remote access.	Admin accounts checked
5 Recover	Assess affected users, services and data, then restore safely from known-good backups.	Systems restored, tests passed

Stage	What to do	Record
6 Protect	Check insurer, ICO, legal and customer duties, then improve controls to reduce repeat risk.	Notifications, lessons learned

Evidence and recovery notes

Done	Item	Notes / account / date / case number
■	Incident log with date, time, person, action and result	
■	Screenshots and exported alerts from email, endpoint, firewall or cloud systems	
■	Suspicious emails with headers where possible	
■	Affected user list, devices, accounts, files and systems	
■	Bank, insurer, police, ICO, customer or supplier case numbers	

Useful UK links: NCSC hacked account guidance, Report Fraud, Have I Been Pwned and ICO breach guidance. Use official websites and avoid links in suspicious messages.