CHECKLIST · SCAMS & SECURITY

Your business email has been hacked: what to do in the first hour

Published 26 September 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/business-email-hacked-first-hour/

- [ ] **Call your bank now.** Ask it to check for suspicious activity and try to stop any payment sent to a fraudster.
- [ ] **Change the password from a trusted device.** Log in to the provider directly, not through an emailed reset link.
- [ ] **Sign out all sessions.** Use **Sign out of all sessions** in Microsoft 365, or in Google Workspace reset the password and then the sign-in cookies.
- [ ] **Turn on MFA and remove unknown methods.** Attackers may have added their own MFA methods and recovery details.
- [ ] **Delete unknown forwarding and inbox rules.** They keep sending your mail to the attacker after a password change.
- [ ] **Remove unknown delegates and connected apps.** Check mailbox permissions, OAuth apps and app passwords (in Microsoft 365 a password reset does not revoke app passwords).
- [ ] **Phone customers and suppliers.** Warn them about fake bank-detail changes and ask them to verify any change by phone.
- [ ] **Report through ReportCyber.** Keep the CIRS- reference number for your bank and insurer.
- [ ] **Call IDCARE if you qualify.** Businesses with 19 or fewer full-time equivalent staff get free recovery support on 1800 595 170 (weekdays); for a live incident call 1300 CYBER1 first.

- [ ] **Check whether the Privacy Act covers you.** If it does and personal information was exposed, you may need to notify the OAIC.

NOTES