Email Disaster Recovery Guide

What to do immediately when your business email is hacked, compromised, or completely broken. Follow

■ **CRITICAL:** If your email is compromised RIGHT NOW, jump directly to Phase 1. Do not read the introduction first. Every minute of delay gives attackers more time.

ABOUT THIS GUIDE

This guide was created by TechWokx Ghana based on real email compromise incidents experienced by hotels, NGOs, and SMEs across Ghana. It covers the exact steps our engineers follow when a client calls with a compromised business email account. Keep this document saved offline so it is available even if your email is down.

73% of breaches start from email	**15 min Response window before major damage**	**■0 Earned from emails that go to spam**	**5 steps To secure access in first 15 minutes**

■ PHASE 1 — IMMEDIATE RESPONSE (First 15 Minutes)

1 Change Your Admin Password — Right Now

Go to your email provider admin console (Google Workspace: admin.google.com / Zoho: mail.zoho.com / Microsoft: admin.microsoft.com). Change the master administrator password immediately. Use a minimum 16 characters including uppercase, lowercase, numbers and symbols. Do NOT use any password you have used before on any account.

2 Enable Two-Factor Authentication (2FA)

Go to Security Settings and enable 2FA on the admin account immediately. Use Google Authenticator or Authy — NOT SMS verification if possible, as SIM cards can be hijacked. This single step blocks 99% of future unauthorised access attempts.

3 Terminate All Active Sessions

In your admin console, find Security → Active Sessions or Device Management. Look for any unfamiliar devices, locations, or IP addresses. Click "Sign out all other sessions" or revoke access to all devices except the one you are currently using.

4 Find and Delete Suspicious Email Forwarding Rules

Go to Gmail/Zoho/Outlook settings → Filters and Forwarding. Attackers commonly create forwarding rules to silently copy all your emails to an external address. Delete any rules you did not create yourself. Also check for auto-delete or auto-archive rules.

5 Scan for Hidden Inbox Rules

In addition to forwarding rules, check for inbox rules that hide attacker activity — rules that mark emails as read, move them to obscure folders, or delete them before you see them. Check every existing rule and remove anything you did not create.

■ PHASE 2 — CONTAINMENT (First Hour)

6 Force Password Reset for ALL Staff

In your admin console, force a password reset for every single staff account — not just the compromised one. Notify each staff member by PHONE, not by email (which may still be compromised). Instruct them to choose a strong, unique password they have never used elsewhere.

7 Review and Remove Unauthorised User Accounts

Go to Admin → Users and look for any accounts you do not recognise. Pay attention to accounts created recently. Look for accounts with unusual names, missing profile information, or administrative privileges you did not assign. Suspend or delete any suspicious accounts immediately.

8

Revoke ALL Former Staff Access — No Exceptions

If any former employee still has an active email account or access to shared drives, suspend or delete their account right now. Also check aliases, distribution lists, and group mailboxes — former staff are frequently left in these even after their main account is deleted.

9

Audit and Revoke Third-Party App Permissions

Go to Security → Third-Party Apps or API Access. Review every application with access to your email system. Revoke access for any application you do not recognise or no longer use. Attackers often maintain persistent access through connected apps even after password changes.

10

Verify Your DNS Records Are Unchanged

Log into your domain registrar immediately and check your DNS records. Verify that MX records (email routing), SPF, DKIM, and DMARC records are exactly as you configured them. Attackers sometimes modify DNS to intercept email or enable impersonation. If anything looks different, restore it immediately and contact your registrar.

■ PHASE 3 — RECOVERY & COMMUNICATION (First 24 Hours)

11

Assess What Data Was Accessed or Exfiltrated

Review your email access logs (Admin Console → Reports → Email Log Search). Identify which accounts were accessed, which folders were opened, and whether any emails or attachments were downloaded or forwarded. Document every finding — you will need this for notifying clients and for insurance purposes.

12

Notify Affected Clients and Partners

If any client data, financial information, or sensitive correspondence was potentially exposed, notify those clients immediately — by phone first, then follow up by email. Be direct and transparent: tell them what happened, what may have been accessed, and what you have done. Clients respect honesty far more than silence. Hiding a breach makes it catastrophically worse.

13

Change Passwords on ALL Linked Accounts

Your business email is the master key to dozens of other accounts — banking notifications, accounting software, CRM, cloud storage, social media, and domain registrar. Change the passwords on every account that uses the compromised email address for login or password recovery. Do this before attackers use email access to reset those accounts.

14

Report the Incident to Your Email Provider

File a support ticket or call your email provider (Google, Zoho, Microsoft) to report the compromise. They have forensic tools that can help identify the source, restore deleted emails, and flag the attacker's IP address. They may also have additional recovery options not available in self-service.

15

Enable Complete Audit Logging Going Forward

Enable full activity audit logging in your admin console if it is not already active. This records every login, every email sent, every setting changed, and every file accessed. Review logs at least monthly. This is your early warning system for any future suspicious activity.

■ PREVENTION CHECKLIST — Never Let This Happen Again

■	Use a custom domain email address — not Gmail or Yahoo for business communications	/1
■	Configure SPF, DKIM, and DMARC records on your business domain	/1
■	Enable two-factor authentication (2FA) on all admin and staff accounts	/1
■	Remove ex-staff email access on their last working day — not days or weeks later	/1
■	Review active login sessions and connected apps every month	/1
■	Never share admin credentials with staff — use delegated admin roles	/1
■	Use a password manager — never reuse passwords across accounts	/1
■	Back up critical emails and attachments monthly to a separate, offline location	/1
■	Train staff to recognise phishing emails before they click suspicious links	/1
■	Conduct an annual email security audit — contact TechWokx Ghana for a free assessment	/1

■ EMERGENCY CONTACTS & SUPPORT RESOURCES

Provider	Emergency Action	Contact
TechWokx Ghana (Emergency IT Support)	Call for immediate remote assistance with email breaches and IT emergencies	WhatsApp: +233 555 087 407 hello@techwokx.online
Google Workspace	Admin Console → Support → Start Chat Or call Google Workspace Support	admin.google.com support.google.com/a
Microsoft 365	Admin Center → Support → New Request Available 24/7 for business plans	admin.microsoft.com support.microsoft.com
Zoho Mail	Help Centre → Submit Ticket Or use live chat on Zoho site	mail.zoho.com help.zoho.com

Your Domain Registrar	Login and verify/lock DNS records Enable domain lock to prevent transfer	Your registrar login panel

■ Need Emergency IT Support Right Now?

TechWokx Ghana provides emergency remote IT support for businesses in Ghana and internationally. We can audit your email setup, respond to active breaches, fix security gaps, and implement all the prevention steps in this guide. WhatsApp: +233 555 087 407 | hello@techwokx.online | techwokx.online Free email risk audit available at techwokx.online — know your risk before something breaks.