

NextGrid Technologies — Email Hacked? 7-Step Incident Response

What to do in first 30 minutes when email sends spam at 3am | Updated: 25 July 2026 | For SA SMEs 5-50 staff | Secure Score 42% → 85%

NextGrid Technologies • Microsoft 365 Authorized • Lenovo 360 Authorized 2026 • POPIA Ready • For SA SMEs 5-50 staff • Pretoria on-site, remote SA • +27 76 948 9154

This is the exact checklist we use on R950 Health Checks. Average 4.2 critical issues found. Same-day fix R2,290. No lock-in. Call +27 76 948 9154.

Immediate Actions (First 30 minutes)

1. Change password + revoke sessions

From another device (not hacked PC), change password, revoke all sessions in M365 > My Account > Sign-out everywhere. Do this first before attacker creates persistence.

2. Enable MFA number matching

Enforce immediately in Entra ID, block legacy auth via Conditional Access. Number matching stops MFA fatigue bypass.

3. Check Inbox rules

Hackers create hidden rule forwarding to external Gmail / outlook.com. M365 > Outlook > Rules – Delete ALL unknown rules. We find this in 18% of audits.

4. Check Sent Items

Look for invoices sent with new banking details — warn recipients by phone immediately. Check for auto-forward to external.

5. Check OAuth apps consented

M365 > Enterprise Apps > User consented apps — Revoke Mail.ReadWrite, Mail.Send from unknown apps (EvilProxy creates OAuth persistence).

6. Reset finance team + check banking details

If finance mailbox hacked, verify ALL supplier bank details changes in last 14 days via known phone numbers. Call suppliers.

7. Notify per POPIA if needed

If personal data (ID numbers, bank details, health data) exfiltrated, notify clients + Information Regulator within 72h. We provide template + evidence pack for insurer.

Our monitoring – catches this in 2 minutes

Our 24/7 monitoring catches rule creation, impossible travel, mass file deletion, inbox rule creation in 2 min. WhatsApp +27 76 948 9154 — avg response <15 min business hours. Included in R290 M365 package + managed IT.

What R950 Check does for this