USE IT MATE

Phishing Incident Response Plan

Author: Jasson Borgueta, Technical Lead — Use IT Mate (Bundaberg & Wide Bay)
support@useitmate.com

The Golden Rule: Speed beats everything.

When a staff member accidentally clicks a malicious link and enters their Microsoft 365 or Google Workspace password, hackers don't wait. They immediately log in, set up hidden email forwarding rules, and start emailing your clients with fake bank details.

If an employee reports clicking a bad link, execute this 5-step lockdown immediately.

Store the completed checklist with employee records.

Step 1: Isolate the Device (Minute 1)

- Do not turn the computer off. Instead, instantly sever its connection to the internet to stop malicious software from spreading to your server or cloud drive.
- Action: Unplug the physical Ethernet cable from the laptop/PC.
- Action: Turn off the Wi-Fi on the device.

Step 2: The Global Kill Switch (Minute 2)

Changing a password does not kick a hacker out if they are already logged in. You must kill their active session.

- Action: Log into your Microsoft 365 or Google Workspace Admin Center.
- Action: Locate the compromised user.
- Action: Click "Sign out of all sessions" (This forces every device connected to that account offline instantly).

Step 3: The Hard Reset (Minute 3)

Now that the hacker is kicked out, lock the door so they cannot get back in.

- Action: Reset the compromised user's password to a complex, temporary passphrase (e.g., BlueMonkey$492!).
- Action: Verify that Multi-Factor Authentication (MFA) is strictly enforced on the account.

Step 4: The Forwarding Rule Audit (Minute 4)

Hackers almost always create hidden rules to hide their tracks. If you skip this step, they will still intercept your emails even after you lock them out.

- Action: Log into the user's webmail inbox.
- Action: Go to Settings > Rules / Forwarding.
- Action: Delete any suspicious rules (e.g., "Forward all emails containing the word 'Invoice' to an external Gmail address" or "Move all replies to the RSS Subscriptions folder").

Step 5: The "All Clear" Scan (Minute 5)

Before allowing the staff member back online, ensure the local machine isn't infected with keylogging malware.

- Action: Run a full, deep antivirus/anti-malware scan on the isolated device. Do not reconnect it to the office Wi-Fi until the scan returns 100% clean.

Do you have a "Global Kill Switch"?

If you are reading this and realize you do not have Admin access to instantly sign out your staff, your business is highly vulnerable.

Traditional IT setups often lack centralized control, meaning a single compromised laptop can take down your entire agency.

My team at Use IT Mate specializes in building "Zero Gravity" Microsoft Cloud environments for local QLD businesses.

We centralize your security so you can lock down devices, wipe data remotely, and control access with a single click.

Visit useitmate.com or email us directly (support@useitmate.com) to authorize the fix today.