USE IT MATE

The Phishing Response Plan

Exactly what to do the second a staff member clicks a malicious link.

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

Panic is the hacker's best friend.

Real Estate agencies are targeted by phishing emails every single day. Eventually, an exhausted Property Manager or Sales Agent is going to accidentally click a fake "View Microsoft Document" link and enter their password. When that happens, you have a 3-minute window before the hacker gets into your system and starts intercepting trust account invoices.

If someone clicks a bad link, follow this exact 3-step emergency protocol.

Store the completed checklist with employee records.

Step 1: Isolate the Machine (Do NOT turn it off)

Do not reboot the computer. Rebooting can trigger ransomware to start encrypting files faster. Instead, immediately disconnect it from the internet. Unplug the Ethernet cable, or turn off the Wi-Fi on the laptop. This severs the hacker's connection to your device.

Step 2: The "Kill Switch" (Revoke Sessions)

Using a completely different computer or your phone, the agency administrator must log into the Microsoft 365 Admin Portal.

1. Reset the compromised employee's password immediately.
2. Click the critical "Sign out of all sessions" button. This instantly boots the hacker out of the employee's Outlook and SharePoint, even if they are currently logged in.

Step 3: Hunt for "The Hidden Forward"

Hackers know you will eventually change the password. Before you do, their first move is to set up a hidden email rule in the background. They create a rule that says: "If an email contains the word 'Invoice' or 'BSB', secretly forward a copy to [Hacker's Email Address] and delete the original."

• You must open Outlook on the web, go to Settings > Mail > Rules, and delete any suspicious forwarding rules the hacker left behind.