Cyber Threat
End-User Action Plan

mother technologies

Action Plan: Immediate Steps if You Suspect a Cyberattack

No business is immune to cyber threats — having a clear response plan can minimise damage and protect your data. Here's what to do, step by step.

If You Think Your PC Might Have Been Compromised

Step 1

Shut Down your Computer Immediately

- If your machine doesn't shut down normally, it may be that a malicious infection is preventing it from doing so.
- If that's the case, perform a hard shutdown by holding down the power button until the machine shuts down.

Step 2

Report the Incident Internally

- Speed is of the essence.
- Don't delay in reporting the incident to your manager or internal IT team.

Step 3

Report the Incident to Mother

- Unless your internal policies instruct otherwise, call us.
- Mother needs to speak with you directly to understand the incident and take appropriate action.
- Do not use email, apps, or the Client Portal to report it.
- Phone us and **clearly state** that you are reporting a cyber threat.
- Mother has an internal protocol to deal with potential cyber threats.

If You Think Your Mobile Device Might Have Been Compromised

- Unless jailbroken, mobile devices—especially iPhones—are generally more secure than PCs.
- However, your credentials could still be stolen, potentially compromising access to other services and your corporate network.

Step 1

Reboot the Device

- Rebooting your phone or tablet interrupts running processes and flushes the memory.

Step 2

Disable WiFi and Mobile Data on your Device

- Once your device has rebooted, disable WiFi and mobile data to prevent further Internet communications.
- You will still be able to make and receive calls.

Step 3

Report the Incident Internally

- Speed is of the essence.
- Don't delay in reporting the incident to your manager or internal IT team.

Step 4

Report the Incident to Mother

- Unless your internal policies instruct otherwise, call us.
- Mother needs to speak with you directly to understand the incident and take appropriate action.
- Do not use email, apps, or the Client Portal to report it.
- Phone us and **clearly state** that you are reporting a cyber threat.
- Mother has an internal protocol to deal with potential cyber threats.

Ransomware Attack

- An attack might not always present as a prompt for payment.
- Are you unable to login or access your device?
- Are files missing or have they unexpectedly moved?
- Are files requesting a password or code in order to open them?
- Have filenames been replaced with random characters or unusual extensions? (e.g., .locked, .xyz, .encrypted).

Step 1

Shut Down your Computer Immediately

- If your machine doesn't shut down normally, it may be that a malicious infection is preventing it from doing so. If that's the case, perform a hard shutdown by holding down
- the power button until the machine shuts down.

Step 2

Report the Incident Internally

- Speed is of the essence.
- Don't delay in reporting the incident to your manager or internal IT team.
- Your internal IT team should:
  - Disconnect your network from the internet ("pull the plug").
  - Shut down all systems.

Step 3

Report the Incident to Mother

- Unless your internal policies instruct otherwise, call us.
- Mother needs to speak with you directly to understand the incident and take appropriate action.
- Do not use email, apps, or the Client Portal to report it.
- Phone us and **clearly state** that you are reporting a cyber threat.
- Mother has an internal protocol to deal with potential cyber threats.

Key Points to Remember

- Act fast to minimise damage during cybersecurity incidents.
- Shut down affected systems immediately if you're unsure what to do.
- Report the incident to Mother without delay.
- Mistakes happen — what matters is a swift and effective response.
- Mother's team understands your systems, allowing for quicker identification and resolution.
- We follow established protocols and maintain clear communication to contain and manage threats efficiently.