DIGITAL DETECTIVE

Business Cyber Incident Checklist

Containment and preservation actions after suspected compromise.

Contain while preserving

Stop active harm where necessary, but avoid deleting accounts, reimaging systems or clearing logs before relevant evidence is preserved.

Create an incident log

Record times, alerts, affected users, systems, communications, containment actions and decision-makers.

Preserve key records

Retain identity, email, endpoint, firewall, VPN, cloud, application and transaction logs. Coordinate with legal advisers, insurers and service providers.

Quick checklist

	Action
	Record the first known indicator and time
	Preserve alerts, logs and suspicious messages
	Reset credentials through a clean trusted system
	Revoke malicious sessions and tokens
	Notify bank/provider where funds are at risk
	Do not delete compromised accounts before preservation

Important: This guide is general information and does not replace matter-specific legal advice or forensic direction. Do not send original evidence through ordinary email or messaging applications unless secure transfer arrangements have been agreed.