WHAT TO DO IN A BREACH - SMB

there are various steps you can take to minimise the damage.

SCENARIO 1 | phishing link

Your business has an employee who responded to or opened a phishing link.

SCENARIO 2 | invoice fraud

Your business has been victimised by a fraudulent invoice.

SCENARIO 3 | spoofing

Your business recieved a call/text/email from an impersonated contact.

CyberSmartKiwis

ANY SUSPECTED BREACH

guidance for any suspected compromise

1 Isolate systems

- Disconnect compromised device from Wi-Fi/network
- Revoke active sessions/logins

2 Change credentials

- On any device that is suspected of compromise (Email accounts, Freezing cards, etc.)
- Run an in-depth AV scan on any suspected affected device

3 Notify | if applicable*

- Check the logs of the in-depth scan, and send results to:
- Management
- IT provider / MSP
- Legal/privacy contacts

4 Preserve evidence

- This matters for insurance, investigations, and law enforcement.
- Emails, Screenshots, Bank transaction records, Phone numbers used, etc.

5 Report the incident

- Privacy/data breach notifications may be mandatory
- Financial institutions may require immediate reporting
- Cyber insurance policies often have strict reporting timelines

6 Reach out for help

- If you are an ESET customer, you can reach out to your provider or us, Chillisoft for guidance and log collection.

CyberSmartKiwis

SCENARIO 1 – Phishing Link

If credentials were entered:

- Reset the password immediately
- Log out on signed-in devices
- Reset your 2FA/MFA
- Review mailbox forwarding rules
- Check for unauthorised logins from unknown devices

If malware may have downloaded:

- Disconnect devices from the network
- Run endpoint/antivirus scans
- Have a professional inspect and clear persistence mechanisms*

**Persistence mechanisms are when hackers allow access even after a reboot or deletion; this must be investigated and cleared.*

If email compromise occurred:

Attackers often:

- Create forwarding rules
- Hide emails
- Send from the mailbox
- Target finance staff

So make sure to check...

- Inbox rules
- Mailbox access
- Auth/app integrations
- Sent/deleted items

CyberSmartKiwis

SCENARIO 2 - Invoice Fraud

If payment *was* sent:

- Contact *your* bank
- Contact *recipient* bank
- Same-day reporting dramatically improves recovery chances
- Account freezing if possible, to conduct investigation

Validate all recent invoices:

- Look for any banking detail changes
- Validate recent/previous payment requests
- Check for unusual urgency in requests
- Any new/recent beneficiaries?
- Use verbal verification (i.e via a phone call). Never trust emailed banking changes alone

Notify vendors/customers:

Warn:

- Clients may receive fake invoices
- Your business identity may be abused

So make sure to check...

- Real mailbox compromise occurred
- Or simple spoofing/domain impersonation

CyberSmartKiwis

SCENARIO 3 – Spoofing

Verify identity independently:

- Hang up, call back using a known number
- Confirm through other channels (email, messages)
- Never rely on: Caller IDs (unless set by you), Email display names, SMS sender names (unless set by you)

Alert staff:

- Warn employees immediately of a spoofed identity, including:
- Reception
- Finance
- Customer service/Helpdesk
- Social engineering can be devestating

Review exposed information:

- Determine whether attackers obtained:
- Customer records
- Employee details
- MFA codes
- Password reset links
- Financial data

CyberSmartKiwis