# Case study: Phishing attack

**Scenario: A medium-sized Practice had a phishing attack which compromised their email system.**

#### Immediate Response:

* On a Tuesday afternoon, the practice manager received an unusual email request from what appeared to be a trusted supplier. On clicking the link, the practice manager unknowingly provided login credentials, resulting in the email system being compromised. The IT team was notified immediately after the manager noticed suspicious activity, including unauthorised emails being sent from their account.

#### Incident Response Activated:

* The practice manager, activated the BCP. IT immediately locked down the compromised email account and began an investigation into the extent of the breach. The privacy officer was alerted.

#### Assessment and Documentation:

* IT established that the email breach allowed unauthorised access to sensitive communications, including patient referrals and appointment details. A rapid risk assessment was conducted, revealing that multiple patients’ information, including appointment histories and referrals, might have been exposed. The team discovered that the breach potentially involved phishing for further information from patients.

####  Immediate Notification:

* OPC and the Police were notified of the breach. A well thought through Comms plan was executed.
* Patients were informed about the phishing attack and warned not to click on any suspicious links received via email. Staff were briefed on the incident and instructed on additional security measures.

#### Evaluation of Risks and Impacts:

* The IT team worked to identify the source of the breach and the extent of compromised data. A detailed privacy impact assessment indicated moderate to high risks due to the nature of the emails accessed and patients with potentially compromised information were given immediate attention. The practice continued with manual workarounds to ensure that patients could still be seen.

#### Notification of Impacted Individuals:

* Affected patients were contacted via secure channels, and a dedicated helpline was established to answer questions and provide support. Information on how to protect themselves from potential identity theft was also provided.

#### Recovery and Mitigation:

* The compromised email system was secured, and multi-factor authentication was implemented to prevent future incidents. The practice conducted cybersecurity awareness training for all staff, emphasising the importance of vigilance in email communication.

#### Ongoing Management and Review:

* The incident prompted a review of all digital communication policies. Lessons learned highlighted the importance of early detection and response to phishing attempts. The practice decided to implement regular cybersecurity drills and review their BCP to ensure readiness for future incidents.