Phishing Incident Report Updated

Summary:

Employees received emails impersonating HR and linking to a fake login page.
Credentials were harvested..

Identify:

Employee-reported emails triggered investigation.
SIEM flagged unusual access attempts..

Protect:

Email domain was blacklisted.
Affected accounts had credentials reset.
MFA was enforced..

Detect:

Patterns of malicious emails and behavior across users were flagged via advanced email gateway..

Respond:

All users were notified.
Malicious URLs were disabled, and impacted systems were reviewed..

Recover:

Compromised accounts secured.
Security awareness training was launched..

Reflections/Notes::

Regular phishing simulations and advanced filtering reduced risk.
Need to improve reporting process..