Phishing Incident Report

Date of Incident: 14-01-2026
System Affected: Employee email account

What Happened

An employee received a phishing email that appeared to be from a trusted site. The employee clicked the link in the email and entered their login information. As a result, the attacker gained unauthorized access to the employee's email account.

Impact

The employee's email account was compromised. There was a risk that an attacker gained unauthorized access to company information.

Root Cause

The root cause of the incident was a phishing email and a lack of user awareness in identifying spam emails.

Actions Taken

The employee's account password was reset immediately.
The account was logged out from all sessions.
The IT team reviewed the account activity.
The phishing email was reported and blocked.

Prevention

Conduct phishing awareness training for all employees.
Use Multi-Factor Authentication (MFA).
Remind employees not to click unknown links.
Improve email filtering rules.

Conclusion

The incident was caused by a phishing email and limited user awareness. Immediate actions were taken to secure the account and prevent future risks.