Executive Summary

User received a suspicious email with a link to a fake login page. Credentials may have been exposed.

Timeline

Timestamp	Action
2025-08-18 09:00	User reported suspicious email
2025-08-18 09:10	Security team notified
2025-08-18 09:20	Analyzed email headers and URL
2025-08-18 09:30	Isolated the affected endpoint
2025-08-18 09:40	Reset compromised account password
2025-08-18 09:50	Blocked sender and malicious domain
2025-08-18 10:00	Notified management

Impact Analysis

One employee account compromised. No system-wide breach detected.

Remediation Steps

Blocked the sender, reset the user’s password, enabled MFA.

Lessons Learned

Users need more phishing awareness training. Enable advanced email filtering.

Phishing Checklist

- ☑ Verify email headers
- ☑ Check URL on VirusTotal
- ☑ Identify affected users
- ☑ Block malicious domain
- ☑ Report to management

Post-Mortem

The phishing email exposed gaps in user awareness and email filtering. Immediate actions included isolating the endpoint, resetting the password, and blocking the sender. Future improvements: implement advanced phishing protection, conduct regular security awareness training, and maintain clear incident response procedures to prevent similar incidents.