Incident Response Report: Simulated Phishing Incident

Executive Summary

On August 20, 2025, the company's email security gateway detected a phishing attack targeting multiple employees. The email impersonated a trusted business partner and contained malicious links designed to capture user credentials. The security team quickly identified the threat, quarantined the malicious emails, and launched an incident response process. Impact analysis showed no evidence of unauthorized data access. Swift containment and remediation activities mitigated further risk. This report documents the timeline, findings, mitigation steps, and recommendations for enhanced organizational security posture.

Incident Description and Timeline

An attacker sent a carefully crafted phishing email from an external IP address. Despite existing email filters, the message reached employee inboxes because it used familiar language and logos to increase credibility.

Date & Time	**Activity**	**Description**
2025-08-20 09:15 AM	Email Gateway Alert	Suspicious phishing email flagged by gateway.
2025-08-20 09:30 AM	Incident Response Team Notified	Team alerted, investigation launched.

2025-08-20 09:45 AM	Email Quarantine	Malicious emails blocked and quarantined.
2025-08-20 10:00 AM	User Communication	Employees warned not to interact with email.
2025-08-20 11:00 AM	Credential Reset Initiated	Password resets initiated for affected users.
2025-08-20 01:00 PM	URL Blacklisting	Firewall and web filters blocked phishing URLs.
2025-08-20 03:00 PM	Log and System Review	Reviewed logs, no further compromise found.
2025-08-20 05:00 PM	Incident Containment Confirmed	Incident formally declared contained.

Analysis and Key Findings

- The phishing email successfully bypassed some filters due to social engineering elements.
- No successful credential theft was detected, but several users had clicked the link, warranting proactive credential resets.
- The attacker used a previously unknown phishing URL, which required manual blacklisting.
- Monitoring showed no lateral movement or additional network intrusions.

Mitigation Steps and Recommendations

- Enhance Email Filtering: Update spam and phishing rules with signatures and heuristics aligned to recent tactics.
- User Training: Schedule company-wide phishing awareness training focused on spear-phishing and social engineering.
- Enable Multi-Factor Authentication (MFA): Enforce MFA across all accounts to limit impact of stolen credentials.
- Incident Playbook Update: Incorporate lessons learned to improve phishing detection and response processes.
- Continuous Monitoring: Increase monitoring on email systems and endpoints for early anomaly detection.
- Password Reset Automation: Improve systems to automatically flag and initiate credential resets when risky activity is detected.

Incident Response Process Flowchart

```
Detection
   ↓
Containment
   ↓
Recovery
```

1. Detection: The email security gateway detects phishing.
2. Containment: Email quarantined, URLs blacklisted, affected accounts isolated.
3. Recovery: Credential resets initiated, system logs reviewed, training rolled out.