Incident Report: Phishing Attack on Claims Portal

Date: June 3, 2025

At 09:13 AM, a phishing email impersonating a regional manager was sent to multiple staff members in the claims department.

One employee clicked a malicious link and entered their credentials into a spoofed login page.

By 10:00 AM, unusual login behavior was detected and flagged by our SIEM system. The Security Operations Center (SOC)

locked down the affected account and initiated containment protocols.

No customer data was exfiltrated. A post-incident review determined the user had not completed the latest phishing awareness training.

Recommendations:

- Immediate mandatory training for all employees
- Upgrade email filtering rules
- Conduct simulated phishing tests biweekly

Case closed: June 5, 2025