🛡️ Phishing Incident Report

Report Title: Simulated Phishing Incident – August 2025
Prepared By: [Sudeep Kumar Gupta]
Date: 20 August 2025
Classification: Internal – Confidential
Version: 1.0

📋 1. Executive Summary

On **15 August 2025**, a **simulated phishing email** was conducted as part of the organization's security awareness program. The campaign was designed to evaluate employee susceptibility to phishing attempts and measure the effectiveness of current email security controls and training programs.
A total of **150 employees** were targeted with a crafted phishing email imitating a trusted internal IT notification. The phishing message requested users to log in to a fake portal to resolve a pending IT issue. The objective was to simulate a credential-harvesting scenario.

- **24 users (16%) clicked the phishing link**
- **7 users (4.6%) entered credentials**
- No actual credentials were harvested or stored
- Results will inform further training and technical mitigation measures

---

🕒 2. Incident Timeline

Date & Time (UTC)	Event
15 Aug 2025 – 09:00	Simulated phishing campaign launched by internal red team
15 Aug 2025 – 09:03	First user clicked the phishing link
15 Aug 2025 – 10:15	Phishing email reported by a vigilant employee via phishing report button
15 Aug 2025 – 11:00	Email campaign flagged and analyzed by Security Operations Center (SOC)
15 Aug 2025 – 11:30	All campaign emails recalled from inboxes

Date & Time (UTC)	Event
16 Aug 2025 – 12:00	Credentials submitted to fake portal reviewed – confirmed to be simulated only
17 Aug 2025 – 09:00	Awareness follow-up emails sent to users who interacted with the phishing message
20 Aug 2025 – 09:00	Report finalized and submitted to executive team

---

🧠 3. Technical Details

- **Type of phishing**: Credential harvesting (simulated)
- **Phishing vector**: Email (via internal simulation tool)
- **Email Subject**: " ⚠️ IT Alert: Secure Your Account Now"
- **Sender Name**: “IT Support”
- **Sender Address**: it.alerts@fakecorp.com
- **Payload**: Link to simulated phishing landing page mimicking internal login portal

---

📉 4. Impact Assessment

- **No real credentials compromised**
- **7 users** submitted credentials to a controlled environment
- The test exposed a **medium level of user susceptibility**
- Detection was quick: First report received within **1 hour**
- Email security tools allowed delivery due to intentional configuration for simulation

---

🔧 5. Mitigation & Response Steps

✅ Immediate Actions

- Recalled phishing emails
- Monitored credential submission on the fake portal
- Logged and reviewed affected users
- Communicated with users who clicked or submitted credentials

✅ Long-Term Recommendations

- Enhance user awareness training (monthly micro-trainings)
- Conduct targeted follow-up training for users who clicked or submitted credentials
- Consider technical safeguards:
  - Enable email banner warnings for external senders
  - Expand MFA adoption and monitoring for unusual logins
- Schedule quarterly phishing simulations for trend analysis

📈 6. Lessons Learned

- Positive reporting culture is developing (early report from user)
- Some users still vulnerable to convincing phishing messages
- Training needs reinforcement, especially on verifying sender and checking URLs

---

📌 7. Conclusion

The simulated phishing test successfully identified a moderate level of risk and highlighted specific user groups that need additional security training. No actual breach occurred. The test met its objectives and will be used to guide future awareness and technical security improvements.

Submitted by:
[Sudeep Kumar Gupta]
Security Operations Team
[Genisys Global]
Date: 20 August 2025