SOC Playbook: Customer Phishing

1. Incident Overview

ID: PB-008
Severity: Medium (High if large customer base, financial loss, or brand impact)

Description:
A Customer Phishing incident occurs when attackers impersonate the organization to deceive customers into revealing credentials, financial details, or personal information via fraudulent emails, websites, or messages.

Log Sources:

- Customer reports (email, web forms, social media)
- Phishing intelligence feeds (PhishTank, Safe Browsing)
- Email security gateways
- Web proxy and DNS logs
- Brand monitoring tools
- SOC and CERT notifications

2. Phase 1: Preparation & Detection

Trigger:

- Customer complaints about suspicious emails or websites
- Detection of look-alike or typosquatted domains
- Alerts from phishing repositories or CERTs

- Abnormal referrer traffic to legitimate websites
- Social media or public reports of fraud

Initial Readiness Actions:

- Maintain an inventory of legitimate company domains
- Deploy SPF, DKIM, and DMARC on all email domains
- Prepare customer phishing warning pages
- Maintain takedown contact lists (hosting providers, registrars, ISPs)
- Monitor cybersquatted domains and brand abuse
- Define 24/7 customer reporting channels (security@ email, web forms)

---

3. Phase 2: Analysis & Investigation

Phishing Analysis:

- Identify phishing vector (email, SMS, website, social media)
- Analyze phishing URLs, domains, and hosting infrastructure
- Capture phishing pages and emails with timestamps
- Review source code to identify data exfiltration methods
- Identify credential drop locations (email, API, messaging bots)

Context & Threat Assessment:

- Assess scope of customer exposure
- Determine if credentials or financial data were stolen

- Identify reuse of legitimate branding or website resources
- Evaluate reputational and regulatory impact

Coordination:

- Engage SOC, Brand Protection, Legal, and PR teams
- Notify decision-makers for takedown authorization
- Share IOCs with external partners and CERTs

---

4. Phase 3: Containment & Neutralization

Customer Protection:

- Block phishing URLs via browsers and security vendors
- Submit phishing URLs to browser blacklists and anti-phishing platforms
- Report fraudulent emails to spam-reporting services

Communication Actions:

- Publish customer phishing warning page
- Notify customers through official channels if required
- Reinforce awareness that credentials are never requested via email

Operational Containment:

- Monitor web logs for suspicious referral traffic
- Prevent reuse of stolen credentials by enforcing MFA (where applicable)

---

5. Phase 4: Eradication & Recovery

Phishing Takedown:

- Contact hosting providers to remove phishing pages
- Engage domain registrars for domain suspension
- Disable fraudulent email accounts receiving stolen data
- Request takedown of redirection services

Recovery Actions:

- Verify phishing sites and emails are fully removed
- Continue monitoring for reappearance
- Remove warning pages once the threat is neutralized

---

6. Phase 5: Post-Incident Activity

Root Cause & Impact Analysis:

- Identify how attackers impersonated the brand
- Assess customer impact and financial loss
- Evaluate response time and takedown efficiency

Improvements:

- Improve domain and brand monitoring
- Enhance customer awareness campaigns
- Update takedown contact lists and procedures

- Strengthen email authentication policies

Documentation & Closure:

- Prepare a phishing incident report
- Document timelines, actions, and IOCs
- Review coordination effectiveness

---

7. Escalation Criteria

Escalate to senior management, legal teams, or regulators if:

- Large numbers of customers are impacted
- Financial fraud or identity theft is confirmed
- Media or reputational damage is likely
- Regulatory notification is required
- Phishing campaign is persistent or targeted