PLAYBOOK

# Security Awareness & Phishing Simulation Playbook

Design a program, run multi-channel phishing simulations, measure effectiveness, handle repeat offenders, and report to leadership.

Published by
**Compliance Enablers LLP**

Last Updated
**March 2026**

Pages
**~10 pages**

# Introduction

Human error remains the leading cause of security incidents. According to industry research, over 80% of breaches involve a human element — whether clicking a phishing link, using weak credentials, misconfiguring a system, or falling for social engineering. Technology alone cannot solve this problem. Organizations need a deliberate, structured, and measurable security awareness program combined with realistic phishing simulations to build a resilient security culture.

This playbook provides everything you need to design, implement, measure, and continually improve a world-class security awareness and phishing simulation program.

# 1. Building the Business Case

## Why Security Awareness Matters

- **Regulatory requirements**: GDPR (Article 39), ISO 27001 (Annex A 6.3), NIST CSF (PR.AT), SOC 2 (CC1.4), HIPAA, PCI DSS — virtually every framework mandates security awareness training.
- **Risk reduction**: Organizations with mature awareness programs see up to 75% reduction in successful phishing attacks within the first year.
- **Insurance requirements**: Cyber insurers increasingly require evidence of awareness training and phishing simulations.
- **Client expectations**: Enterprise buyers routinely ask about awareness programs during due diligence and vendor assessments.
- **Incident cost reduction**: The average cost of a phishing-related breach is significantly higher when employees are not trained to recognize and report threats.

## Presenting to Leadership

Frame the business case around:

1. **Financial impact**: Cost of a breach (average $4.88M globally in 2024) vs. cost of an awareness program.
2. **Regulatory penalties**: Fines for non-compliance with training requirements.
3. **Insurance premiums**: Potential premium reductions with a documented program.
4. **Measurable outcomes**: Commit to tracking and reporting metrics (phish-prone percentage, report rates, response times).
5. **Competitor benchmarking**: Show how peers and competitors invest in awareness programs.

## Budget Considerations

A typical enterprise awareness program budget includes:

- Platform licensing (awareness training + phishing simulation).
- Content development or licensing (videos, modules, assessments).
- Internal staff time for program management.
- Incentive and gamification rewards.
- Third-party assessments (security culture surveys, external red team exercises).

# 2. Designing Your Awareness Program

## Program Structure

### Role-Based Content

Not all employees face the same risks. Tailor content by role:

| Audience | Focus Areas |
|---|---|
| All employees | Phishing recognition, password hygiene, social engineering, physical security, incident reporting, acceptable use |
| Developers | Secure coding practices, OWASP Top 10, dependency management, secrets management, code review |

| | |
|---|---|
| IT administrators | Privileged access management, secure configuration, patch management, logging and monitoring, incident response |
| Finance/ Accounts | Business email compromise (BEC), invoice fraud, wire transfer verification, payment security |
| HR | Data privacy, employee data handling, recruitment scams, social engineering targeting HR |
| Executives | CEO fraud/whale phishing, strategic risk awareness, privacy obligations, incident communication |
| Customer support | Social engineering via support channels, data verification procedures, escalation protocols |
| New hires | Onboarding security orientation, policy acknowledgment, initial phishing baseline |

**Content Delivery Methods**

Use a mix of delivery methods to maintain engagement:

- **Micro-learning modules** (3-5 minutes): Short, focused topics delivered monthly. High completion rates due to brevity.
- **Interactive e-learning courses** (15-30 minutes): Deeper dives on critical topics, delivered quarterly.
- **Video content**: Short, engaging videos covering real-world scenarios. Use storytelling and humor where appropriate.
- **Live sessions / webinars**: Quarterly town halls or workshops on trending threats. Enables Q&A and discussion.
- **Simulated attacks**: Phishing, vishing, smishing, and QR code simulations (covered in detail below).
- **Newsletters / alerts**: Monthly security newsletters with tips, threat intelligence summaries, and recognition of security champions.
- **Posters and digital signage**: Physical and digital reminders in office spaces.
- **Gamification**: Points, leaderboards, badges, and rewards for completing training and reporting simulations.
- **Tabletop exercises**: Scenario-based group exercises for incident response teams and leadership.

**Frequency**

| Activity | Frequency |
|---|---|
| Micro-learning modules | Monthly |
| In-depth e-learning courses | Quarterly |
| Phishing simulations | Monthly |
| Multi-channel simulations (SMS, voice, QR) | Quarterly |
| Security newsletter | Monthly |
| Live sessions / town halls | Quarterly |
| Security culture survey | Annually |
| Tabletop exercises | Semi-annually |
| New hire onboarding training | Within first week of employment |

# 3. Phishing Simulation Strategy

## Starting a Simulation Program

**Phase 1: Baseline (Month 1)**

- Send a moderate-difficulty phishing simulation to all employees (no prior warning).
- Measure baseline click rate, credential submission rate, and report rate.
- Do not name and shame — use results only for program planning.
- Common baseline click rates for untrained organizations: 25-35%.

**Phase 2: Foundation (Months 2-4)**

- Begin monthly simulations at low to moderate difficulty.

- Launch awareness training addressing the most common failure points from the baseline.
- Communicate transparently: "We are running simulations to help everyone improve."
- Introduce the phishing report button (email plugin for one-click reporting).

**Phase 3: Escalation (Months 5-8)**

- Increase difficulty progressively: more targeted, more realistic, more varied.
- Introduce spear-phishing simulations targeting specific departments.
- Add multi-channel attacks: SMS phishing (smishing), voice phishing (vishing), QR code phishing (quishing).
- Recognize and reward employees who consistently report simulations.

**Phase 4: Advanced (Months 9-12)**

- Use highly realistic scenarios: impersonating internal executives, mimicking actual vendor communications, leveraging current events.
- Combine techniques: email + phone follow-up, QR code in a physical document.
- Conduct red team exercises for high-risk departments (finance, IT, executives).
- Target click rate goal: below 5%.

### Multi-Channel Simulation Types

| Channel | Description | Example Scenario |
|---|---|---|
| Email phishing | Traditional deceptive emails with malicious links or attachments | Fake password reset from IT, fake invoice from a vendor, fake package delivery notification |
| Spear phishing | Targeted emails using personal/organizational information | CEO requesting urgent wire transfer, HR sending "updated benefits enrollment" |
| SMS phishing (Smishing) | Deceptive text messages with malicious links | Fake delivery notification, fake MFA verification request, fake IT support message |
| Voice phishing (Vishing) | Phone calls impersonating trusted entities | IT helpdesk requesting password reset, vendor requesting payment details |
| QR code phishing (Quishing) | Malicious QR codes placed in emails or physical locations | Fake Wi-Fi setup instructions, fake parking payment QR code, fake document access QR |
| USB drop | Planted USB devices to test physical security awareness | Labeled USB drives left in common areas (lobby, parking lot, break room) |

### Difficulty Progression Matrix

| Level | Indicators | Typical Click Rate |
|---|---|---|
| Easy | Obvious spelling errors, unknown sender, generic greeting, mismatched URL clearly visible | 10-15% |
| Moderate | Branded template, plausible sender, mild urgency, URL similar to legitimate domain | 15-25% |
| Hard | Highly realistic branding, known sender name (spoofed), strong urgency or authority, convincing pretext | 25-40% |
| Expert | Personalized content from research, mimics actual business processes, multi-channel, compromised look-alike domain | 30-50%+ |

## 4. Measuring Effectiveness

### Key Metrics

#### Primary Metrics

| Metric | Definition | Target |
|---|---|---|
| Phish-Prone Percentage | Percentage of employees who click or interact with simulated phishing | Below 5% within 12 months |
| Report Rate | Percentage of employees who correctly report simulated phishing via the report button | Above 70% within 12 months |
| Time-to-Report | Average time between simulation delivery and first employee report | Under 5 minutes |

| | | |
|---|---|---|
| Credential Submission Rate | Percentage of employees who not only click but enter credentials on a phishing page | Below 1% within 12 months |
| Training Completion Rate | Percentage of employees completing assigned awareness training on time | Above 95% |

### Secondary Metrics

| Metric | Definition | Purpose |
|---|---|---|
| Repeat Offenders | Employees who fail 3+ consecutive simulations | Identify individuals needing additional intervention |
| Department Click Rates | Click rates broken down by department | Identify high-risk departments for targeted training |
| Improvement Over Time | Month-over-month or quarter-over-quarter click rate trend | Demonstrate program ROI |
| Real Threat Reporting | Number of real phishing attempts reported by employees | Measure behavioral change in actual threat scenarios |
| Security Culture Score | Composite score from security culture assessment survey | Track cultural shift toward security mindfulness |

### Calculating ROI

**Awareness Program ROI** = (Estimated breach cost x Reduction in phishing susceptibility) - Program cost

Example:

- Estimated annual phishing breach cost exposure: $500,000
- Phish-prone percentage reduced from 30% to 5% (83% reduction)
- Estimated risk reduction value: $500,000 x 0.83 = $415,000
- Annual program cost: $50,000
- ROI: ($415,000 - $50,000) / $50,000 = 730%

## 5. Handling Repeat Offenders

A small percentage of employees will consistently fail simulations. Handle this constructively, not punitively.

### Intervention Framework

| Failure Count | Intervention |
|---|---|
| 1st failure | Immediate educational feedback (landing page with explanation). Assign targeted micro-learning module. |
| 2nd failure | One-on-one coaching session with security team. Assign additional training module. Manager notified. |
| 3rd failure | Mandatory in-depth training session. Risk documented. Increased simulation frequency for this individual. |
| 4th failure | Escalation to HR and management. Formal discussion about security responsibilities. Consider access restrictions. |
| Persistent failure | Role-based access review — reduce access to sensitive systems. Ongoing monitoring. Include in performance review discussion. |

### Important Principles

- **Never publicly shame employees**: This destroys trust and discourages reporting.
- **Focus on education, not punishment**: The goal is behavior change, not discipline.
- **Consider the individual**: Some employees may need different learning formats (visual, hands-on, one-on-one).
- **Document interventions**: Maintain records of all training and coaching for compliance evidence.
- **Recognize improvement**: When a repeat offender starts reporting correctly, acknowledge the change.

## 6. Security Culture Assessment

A security-aware employee is not the same as a security-cultured employee. Awareness is knowledge; culture is behavior and attitude. Measure both.

### The Seven Dimensions of Security Culture

1. **Attitudes**: How employees feel about security (positive, negative, indifferent).
2. **Behaviors**: What employees actually do day-to-day regarding security practices.
3. **Cognition**: How well employees understand security threats, policies, and their role.
4. **Communication**: How effectively security information flows within the organization.
5. **Compliance**: The extent to which employees follow security policies and procedures.
6. **Norms**: What employees perceive as normal security behavior among their peers.
7. **Responsibility**: Whether employees feel personal ownership for security outcomes.

### Measuring Security Culture

- **Annual survey**: Distribute a validated security culture survey covering all seven dimensions. Benchmark against industry peers.
- **Behavioral observation**: Monitor actual behaviors — clean desk adherence, badge tailgating, document handling.
- **Simulation results**: Phishing simulation data reflects actual behavioral patterns.
- **Incident data**: Types and frequency of human-caused incidents indicate cultural maturity.
- **Focus groups**: Conduct qualitative focus groups to understand attitudes and perceptions.

## 7. Reporting to Leadership

### Monthly Report Elements

- Phishing simulation results (click rate, report rate, credential submission rate).
- Training completion rates.
- Trend charts showing improvement over time.
- Notable incidents related to human factors.
- Upcoming activities for the next month.

### Quarterly Report Elements

- All monthly elements plus:
- Department-level performance comparison.
- Repeat offender trends and interventions.
- Multi-channel simulation results.
- Budget utilization.
- Program recommendations and adjustments.

### Annual Report Elements

- All quarterly elements plus:
- Security culture survey results and year-over-year comparison.
- ROI calculation.
- Benchmarking against industry peers.
- Strategic recommendations for the following year.
- Program maturity assessment.

## 8. Sample Annual Calendar

| Month | Training Activity | Simulation Activity |
|---|---|---|
| January | Annual security refresher course (all employees) | Moderate email phish: fake IT password reset |
| February | Social engineering awareness module | Hard email phish: fake vendor invoice |
| March | Data privacy and GDPR module | Easy email phish: fake delivery notification + SMS phish |

| | | |
|---|---|---|
| April | Secure remote working module | Moderate email phish: fake HR benefits update |
| May | Business email compromise (BEC) module for finance | Hard spear phish targeting finance: fake CEO wire request |
| June | Physical security and clean desk module | Moderate email phish + QR code quish in office poster |
| July | Password hygiene and MFA module | Easy email phish: fake social media alert |
| August | Incident reporting procedures module | Hard email phish: fake internal system notification |
| September | Secure coding practices (developers only) | Moderate email phish + vishing targeting IT helpdesk |
| October | Cybersecurity Awareness Month campaign | Multi-channel campaign: email + SMS + voice over 4 weeks |
| November | Third-party risk and supply chain awareness | Hard spear phish: fake vendor breach notification |
| December | Year-in-review and security culture survey | Expert-level holiday-themed phishing campaign |

# 9. Sample Metrics Dashboard

## Executive Summary View

```
+--------------------------------------------------------------------+
|  SECURITY AWARENESS PROGRAM DASHBOARD - Q1 2026                    |
+--------------------------------------------------------------------+
|                                                                    |
|  Phish-Prone %     Report Rate       Avg Time-to-Report           |
|  4.2% (target <5%) 72% (target >70%) 3.8 min (target <5 min)     |
|  [DOWN from 6.1%]  [UP from 65%]     [DOWN from 5.2 min]         |
|                                                                    |
|  Training Completion    Credential Submission    Repeat Offenders  |
|  97%                    0.8%                     12 employees      |
|  (target >95%)          (target <1%)             (down from 18)    |
|                                                                    |
+--------------------------------------------------------------------+
|  DEPARTMENT CLICK RATES                                            |
|  Engineering:   2.1%  | Finance:       3.5%  | Marketing: 5.8%   |
|  Sales:         6.2%  | Operations:    4.1%  | HR:        3.9%   |
|  Customer Svc:  7.1%  | Executive:     2.8%  | IT:        1.5%   |
+--------------------------------------------------------------------+
|  TREND (12 MONTHS)                                                 |
|  Click Rate:  30% -> 18% -> 12% -> 8% -> 6.1% -> 4.2%            |
|  Report Rate: 15% -> 30% -> 45% -> 55% -> 65% -> 72%             |
+--------------------------------------------------------------------+
```

## Department Drill-Down View

For each department, track:

- Monthly click rates over 12 months.

- Most effective simulation types (which topics generate the most clicks).
- Training completion rate.
- Number of repeat offenders.
- Real phishing reports submitted.
- Recommended focus areas for next quarter.

## 10. Program Maturity Model

### Level 1: Non-Existent

- No formal awareness program.
- No phishing simulations.
- Training is ad hoc or compliance-only (annual checkbox).

### Level 2: Initial

- Basic annual compliance training deployed.
- Occasional phishing simulations (1-2 per year).
- No metrics tracking beyond completion rates.

### Level 3: Developing

- Monthly phishing simulations with progressive difficulty.
- Quarterly training on varied topics.
- Click rates and report rates tracked.
- Phishing report button deployed.

### Level 4: Established

- Role-based training program with monthly content.
- Multi-channel simulations (email, SMS, voice, QR).
- Comprehensive metrics dashboard reported to leadership.
- Repeat offender intervention program active.
- Security culture survey conducted annually.

### Level 5: Optimized

- Security is embedded in organizational culture.
- Employees are active defenders — high report rates, low click rates.
- Real-time threat intelligence feeds into simulation scenarios.
- Continuous improvement driven by data analysis.
- Program benchmarked against industry peers.
- Recognized as a competitive differentiator.

## Conclusion

A security awareness and phishing simulation program is not a one-time project but a continuous discipline. The organizations that achieve the strongest security cultures are those that invest consistently, measure rigorously, communicate transparently, and treat every employee as a potential security champion rather than a liability.

Start with a baseline, set clear targets, deliver engaging content, simulate realistic threats, measure everything, and iterate. Within 12 months, you will see measurable improvement in your human risk metrics — and more importantly, you will build an organization where employees actively defend against threats rather than passively falling for them.

*This resource is provided by Compliance Enablers — the unified GRC platform with 27 modules, 261+ compliance frameworks, and built-in security awareness training. Learn more at complianceenablers.com*

## Ready to Transform Your Compliance Program?

27 modules • 261+ frameworks • 157 templates • 40+ integrations • AI-powered • From $999/yr

Schedule a Demo

Start Free Trial