

PHISHING & SECURITY AWARENESS TRAINING.



A single click can undo every other control — awareness training only works when it changes behavior under pressure, not just completion rates on a slide deck.

- SIMULATED PHISHING
- CLICK & REPORT RATES
- JUST-IN-TIME COACHING
- REPEAT-CLICKER PROGRAMS

01 THE MECHANISM



Simulated Phishing Campaigns

Realistic, unannounced phishing emails go out to employees on a recurring schedule, measuring **who clicks, who enters credentials, and who reports** — without real-world consequence.



Just-in-Time Coaching

An employee who clicks gets immediate, specific feedback tied to the exact email they fell for, **delivered at the moment of failure** — not a generic annual module months later.



Behavioral Metrics

Click rate, report rate, and time-to-report are tracked per campaign and per employee, **replacing “percent who finished the training video”** as the real signal.

02 THE FLOW

The Trained Response REPORTED

- 1 An employee receives a suspicious email and recognizes red flags from recent simulated phishing training.
- 2 They report the email through the built-in “Report Phishing” button instead of clicking or replying.
- 3 Security teams see the report within minutes, and if it's a real threat, **can block it organization-wide before others act on it.**

The Untrained Response CLICKED

- 1 An employee receives the same suspicious email but has no recent frame of reference for what a phishing attempt looks like.
- 2 They click the link or enter credentials, treating the message as routine business communication.
- 3 The compromise isn't discovered until **downstream systems show signs of misuse**, often days or weeks later.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Recurring Simulated Campaigns	Sends realistic phishing tests on an ongoing schedule, not a single annual event, so recognition skills stay current.
Just-in-Time Coaching	Delivers specific, immediate feedback tied to the exact simulation an employee failed, at the moment of failure.
Report-Rate Culture	Makes reporting a suspicious email as easy and normalized as deleting one, turning employees into a detection layer.
Repeat-Offender Programs	Targets additional coaching and manager visibility at the small percentage of users who fail consistently, rather than treating everyone identically.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Annual Compliance Training Video	No	Measures completion, not whether an employee can recognize or resist a real phishing attempt months later.
Simulations Without Follow-Up Coaching	No	Identifies who clicked but does nothing to change behavior before the next campaign.
Punitive-Only Response to Clicks	No	Discourages honest reporting, so employees hide mistakes instead of surfacing real compromises quickly.
Technical Filtering Alone	No	Stops known bad senders and links but cannot catch a well-crafted message that reaches the inbox regardless.
Recurring Simulation + Just-in-Time Coaching + Normalized Reporting	Yes	Builds recognition skills continuously and gives security teams early signal on real threats.

PHISHING & AWARENESS TRAINING.

SIMULATE · MEASURE · COACH

05 PROGRAM OPERATIONS

Click rate alone is a vanity metric.

A low click rate paired with a low report rate can just mean employees are silently deleting suspicious emails, not detecting them.

Report rate matters as much as click rate.

A high report rate gives security teams early warning on real campaigns targeting the organization, not just a training scorecard.

Fear-based programs suppress the exact signal they need.

Employees who expect punishment for clicking are less likely to self-report a real mistake.

Training must reflect current attacker tactics, not last year's templates.

Simulations that don't evolve stop measuring anything relevant to actual risk.

06 CONTROL MAPPING

NIST SP 800-50

Framework for building and maintaining an information security awareness and training program.

SANS AWARENESS MATURITY MODEL

A five-level maturity model for benchmarking a program's progress from compliance toward measurable behavior change.

PCI DSS

Requires a formal awareness program for all personnel with access to cardholder data environments.

ISO/IEC 27001 (ANNEX A)

Requires appropriate awareness education and training as part of an information security management system.

07 WHAT THIS DOES NOT SOLVE

Sophisticated, Novel Pretexts

Even well-trained employees can be deceived by an attack that **doesn't resemble anything in prior simulations.**

Technical Control Gaps

Awareness training changes human behavior; it **does nothing to fix missing email authentication or filtering.**

Compromised Accounts Acting Internally

A trained employee can still be fooled by a message from a **colleague's genuinely hijacked account.**

One-Time Culture Shifts

A single strong quarter of metrics doesn't guarantee the next campaign — **sustained investment is required, not a one-time push.**

08 MYTHS VS. REALITY

MYTH "A single annual training satisfies the requirement."	REALITY Recognition skills decay quickly without reinforcement; most frameworks now expect ongoing, recurring simulation, not a once-a-year module.
MYTH "Punishing employees who click reduces risk."	REALITY Punitive responses drive underreporting, which removes the early-warning signal security teams depend on most.
MYTH "A low click rate means the program is working."	REALITY Without a rising report rate alongside it, a falling click rate can just mean employees are getting better at silently ignoring email altogether.
MYTH "Technical employees don't need phishing training."	REALITY Technical staff are frequently targeted specifically because their accounts carry elevated access.
MYTH "One template style covers the threat."	REALITY Effective programs vary pretext, urgency, and delivery channel, since real attackers do the same.

09 SPEAK THE PROGRAM — KEY TERMS

SIMULATED PHISHING CAMPAIGN

A controlled, realistic phishing email sent to employees to **measure and train recognition without real risk.**

CLICK RATE

The percentage of recipients who **interact with a simulated phishing link or attachment.**

REPORT RATE

The percentage of recipients who **flag a suspicious email through the proper channel**, whether simulated or real.

JUST-IN-TIME TRAINING

Immediate, targeted coaching delivered **at the moment an employee fails a simulation**, tied to that specific mistake.

REPEAT CLICKER

An employee who fails multiple consecutive simulations, typically **flagged for additional coaching or manager involvement.**

SECURITY CHAMPION

An employee outside the security team given extra training and visibility to **reinforce awareness within their own department.**

SOURCES: NIST SP 800-50 · SANS AWARENESS MATURITY MODEL · PCI DSS · ISO/IEC 27001

PHISHING & SECURITY AWARENESS TRAINING · FIELD REFERENCE