Phishing awareness: introductory module, simulated attack, and practice exercise

Format	Microlearning module + live simulated-phishing platform event + untimed practice exercise
Duration	Introductory module: 4–5 minutes. Simulation: delivered live, unannounced. Exercise: self-paced.
Voiceover	None — on-screen text only.

1. Introductory module

Short block, 4–5 minutes. Opens the course and sets the principles every later simulation builds on. No branching — a linear sequence of 4 screens.

Screen	On-screen text	Interaction	Dev notes
1	**An attack looks like an ordinary email — not a "suspicious" one.** Modern phishing has no obvious typos or odd formatting. It looks like a message from a coworker, a vendor, or a manager. The job is not to spot "obviously suspicious" — it's to check specific signals.	Tap/click "Next" to advance. No quiz element.	Single static screen. Pair with a plain, realistic inbox screenshot (placeholder) — no dramatized "red flag" styling.

Screen	On-screen text	Interaction	Dev notes
2	**Three questions before you act:** 1. Was I expecting this message? An unexpected request is already a reason to pause. 2. Does the sender match who they claim to be? Check the domain, not just the display name. 3. Is the message manufacturing urgency? "Do this immediately, or else…" is a pressure tactic, regardless of how plausible the context sounds.	Three items reveal one at a time on click/tap, or all at once on scroll — developer's choice; no branching.	These 3 questions are the throughline for the whole course — reuse this exact wording in the simulation feedback screen.
3	**Pausing is the single most effective action.** On average, only 21 seconds pass between opening an email and clicking. That's enough time to catch yourself — if you've practiced stopping and checking instead of acting on autopilot.	Static screen. Optional: animate a simple countdown/timer motif to visualize the 21 seconds.	Stat can be pulled into a pull-quote/highlight treatment (use the accent mark sparingly on "21 seconds").
4	**Reporting is not admitting a mistake.** Even after clicking or entering data, reporting to the security team immediately cuts the damage sharply. The course explicitly removes the stigma of "reporting means I broke something" — reporting is the correct action, full stop.	Tap/click "Start course" to exit the module.	This message must land before the employee ever meets a live simulation — it's the reason "Report Phishing" is framed as a win later, not a fallback.

2. Simulated phishing alert — ”Urgent request from a manager”

Not a branching storyboard screen — this is the real format of the simulated-attack platform: an email lands in the employee's inbox during normal work hours, unannounced. Employee action → immediate system response. Context is industry-neutral, recognizable in any workplace.

Field	Content
From	[employee's actual manager's name], sender address visually similar to the real one but not an exact match (e.g. one substituted character)
Subject	Urgent
Body	"I'm in a meeting and can't talk. I urgently need you to buy 5 gift cards, $100 each, for partners — I'll pay you back today. Send me the card codes here as soon as you buy them, I don't have much time."

Outcome logic

Employee receives the email (no warning)

↓

Clicks the link / replies intending to comply
→ Reveal screen, same click

Clicks "Report phishing"
→ Confirmation screen

Ignores the email
→ No in-moment feedback

Path	On-screen text	Dev notes
Clicks link / replies	**This was a training simulation.** What should have raised a flag: • The sender's address differed from the real one by one character. • The request manufactured urgency ("I don't have much time," "can't talk"). • The request was atypical for this manager (personally buying gift cards). • There was no chance to verify through an independent channel before acting. What to do instead: message the manager on a different channel (call, or a separate message — not a reply in the same email thread) and confirm the request is genuinely theirs.	Reveal screen fires instantly on the same click that would have completed the phishing action (30–60 sec read). Reuse the "three questions" wording from Screen 2 of the intro module where it maps to a flag.
Reports phishing	Correct — this was a training simulation, and you caught it. +1 to your team's counter.	Team-level scoreboard increment, visible to the employee. Positive, low-key confirmation — no fanfare/gamified badge animation per brand tone.
Ignores	No message is shown to the employee.	Logged as "not recognized" server-side only. No individual notification — avoids a surveillance feel for inaction. Rolls into aggregate HR/security analytics only, never surfaced to the individual employee.

3. Practical exercise — spot the phish

Part of the training module. Employees practice attention to detail in a safe environment, self-paced, no timer, before ever facing an unpredictable live simulation.

Setup 8–10 emails/messages shown one at a time (real screenshots or constructed examples). Employee marks each "safe" or "suspicious," own pace, no timer, no pass/fail threshold.

Example cards

#	Card content	Correct answer	Why
1	Email from "IT Department" asking you to confirm your password via a link, sent at 11:47 PM.	Suspicious	Unusual send time; password request.
2	Routine email from a coworker with an attachment the employee was expecting after a meeting.	Safe	Expected sender, expected content.
3	"You've won a gift certificate" message from an unknown address.	Suspicious	Unknown sender; unsolicited prize.
4	Automated calendar reminder for a meeting that's genuinely on the employee's schedule.	Safe	Verifiable against the employee's own calendar.

Summary screen Number of correct answers, plus 1–2 cards the employee got wrong with a brief explanation. Tone: calm review, not a score judgment — no pass/fail language, no "Try again."