A ONE-PAGE TOOL

The Awareness Programme Scorecard

Whether your phishing programme is reducing risk or just generating a completion percentage.

Bhavin G Patel · C|CISO · CISSP-ISSAP · CISM

Most awareness programmes measure attendance. Attendance is not behaviour, and behaviour is the only thing that changes an outcome. Score yours honestly against the six things below. Anything scoring low is where the risk still lives, regardless of how good the completion rate looks.

The six measures that matter

Measure	Why it beats the usual number	Current
Click rate over time, same difficulty	Only meaningful if difficulty is held constant. A falling rate against easier tests measures nothing.	
Report rate	More important than click rate. A workforce that reports fast gives you detection you cannot buy. This is the number to optimise.	
Time to first report	Minutes matter. The first report is what lets you pull the campaign before it spreads.	
Repeat clickers	A small group usually accounts for most clicks. Naming the group as a management problem rather than a training one is what moves it.	
Credential submission rate	Clicking is human. Entering a password is the failure that matters. Track it separately.	
Reports of real phishing	The programme's actual output. Simulations are practice; this is the game.	

What actually moved the number

1. **Make reporting one click and instant.** If reporting is harder than deleting, people delete. This single change usually does more than any content.
2. **Thank every report, including the wrong ones.** A person who reports a legitimate email and gets a friendly reply reports again. One who gets corrected does not.
3. **Stop punishing clicks.** Shame produces silence, and silence is worse than a click, because the click you know about is one you can contain.
4. **Match the simulation to real threat.** Generic templates train people to spot generic templates. Use what is actually arriving in your environment.
5. **Fix the systemic causes.** If a supplier really does send unexpected invoice links, that is a process problem, and training people to distrust it is asking them to fight their own job.

6 **Target the repeat group personally.** A conversation with the person and their manager beats another module every time.

Signals your programme is theatre

Signal	What it actually means
Completion rate is the headline metric	You are reporting attendance, not risk
Click rate improves but report rate is flat	People learned to ignore, not to raise
Difficulty was quietly reduced this year	The trend line is measuring your test design
Nobody reports real phishing	Either the channel is broken or people fear using it
The same people click every time and nothing changes	It has been treated as a training gap, not a management one

THE HONEST BASELINE

Publish the starting number before you improve it, including the bad one. A programme that starts at 70% and reaches 8% is a story. A programme that only reports its current figure invites the question of what it was before, and the hesitation answers it.

ONE CAUTION ON TARGETS

Driving click rate to zero is not the goal and is not achievable. A determined, well-researched attack will beat almost anyone on a bad day. Build the programme so that a click is survivable — strong MFA, fast reporting, quick containment — rather than betting the outcome on nobody ever clicking.

Companion to: “How I Took Phishing Click Rates From 70% to 8%” at cybersecleader.com. Adapt freely inside your organisation with attribution retained. Not legal or HR advice; check your own obligations before measuring individuals.