How to Measure the Success of Security Awareness Training

and what each metric means

Phishing Click Rate

What it means:

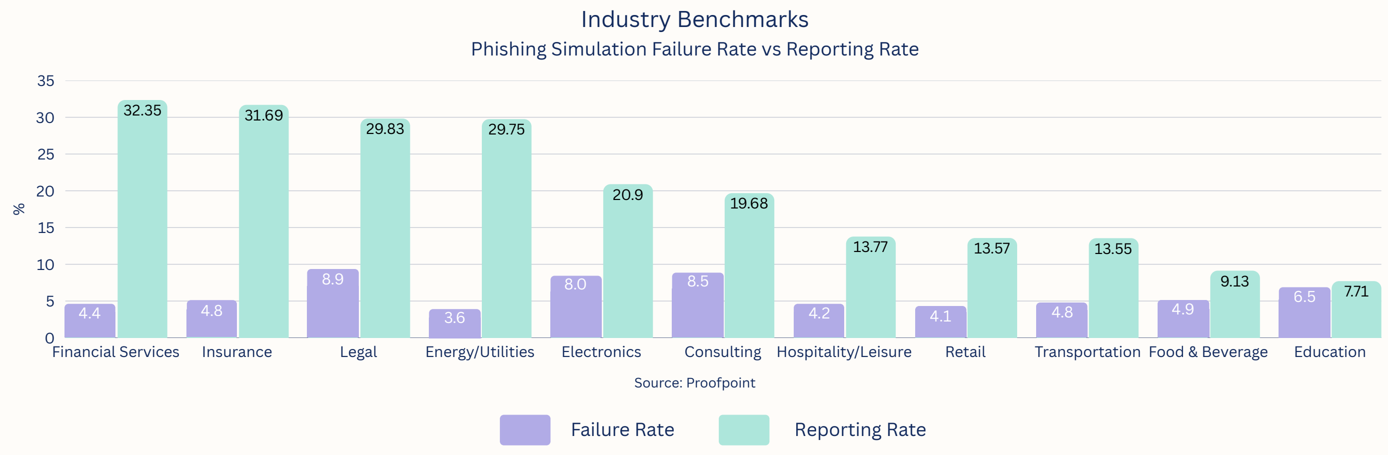
Decreased click rate

People are less likely to fall for scams.

Increased click rate means people are more likely to fall for scams.

This is still **one of the strongest indicators** of organizational risk. If phishing click rates decrease, risk decreases. If click rates rise, it signals a need for additional support or targeted coaching.

Many organizations average between **5% and 10% click rates** depending on industry and company size. The closer to zero, the better.



Reporting Rate

Reporting rate measures how many employees actively identify and report suspicious emails.

A growing reporting rate usually means employees are becoming more confident and engaged. **This is important because early reporting helps stop attacks before they spread.**

Note: A decreased reporting rate could also mean users are getting better at differentiating legitimate emails from scams.

What it means:

Increased report rate

People are more actively identifying scams so IT can stop them before they get to other users.

Decreased report rate could mean fewer people are actively identifying scams.

Training Completion Rate

What it means:

100% completion rate

All of your users are informed which is great for compliance and insurance audits.

A training completion rate of less than 100% means not all users are fully informed which could be a risk to your security and a red flag for insurance audits.

Training completion demonstrates participation and supports compliance requirements.

Users who repeatedly avoid training often become the highest-risk group inside the organization. This metric also matters for:

- Cyber insurance requirements
- Regulatory audits
- Internal policy compliance

High-Risk Users

Every organization has **users who require additional attention**. These might include:

- Frequent phishing clickers
- Employees with privileged access
- Users who repeatedly miss training
- Employees handling sensitive financial data

Identifying high-risk users early and determining ways to encourage participation helps reduce overall organizational exposure.

What it means:

Users to watch

Users are a risk to your security, which is especially bad if it's users most likely to be targeted.

Executives & Leadership

New Employees

Time to Complete Training

What it means:

Shorter time to completion

Your employees are staying up to date on their training which which helps with insurance audits and keeps security top of mind.

Employees are far more likely to engage with training when it is:

- **Short**
- **Relevant**
- **Easy to complete**
- **Practical**

Tracking how quickly users complete training indicates whether your training is engaging, relevant, and easy to consume. Faster completion often means users are staying current on emerging threats rather than falling behind.

Check out Security Awareness Training Best Practices