

Phishing Simulation

A phishing test is a safe, fake phishing email you send your own staff to see how they respond. Here is what it is, what to measure and the one habit that makes it work.

WHAT IT IS

A phishing test, also called a phishing simulation, is a controlled fake phishing message sent to your own employees with permission. It measures how people respond and teaches safer habits, and no real attacker is involved. It matters because phishing is the leading way attackers break in, so the people who receive the email are part of the defence.

WHY IT MATTERS

About 60%

Of initial intrusions in the EU start with phishing, the leading vector.

ENISA Threat Landscape, 2025

21 seconds

Median time to click a phishing link after opening the email, under a minute to data entry.

Verizon DBIR, 2024

20%

Of users reported the phish in simulations, the metric that warns everyone.

Verizon DBIR, 2024

WHAT HAPPENED

In April 2021 the UK operator West Midlands Trains emailed about 2,500 staff a fake bonus to thank them for their pandemic work, with a link to claim it. Anyone who clicked learned it was a phishing test. The rail union called it a cynical stunt, a reminder that the lure matters as much as the test. (CNBC, 2021)

RED FLAGS TO WATCH FOR

The warning signs in a real phish are the same ones a good simulation teaches you to notice.

- Urgency or a deadline, a reward or threat that supposedly cannot wait.
- A request to click a link or open a file to claim or confirm something.
- A login page that arrives by email and asks for your password.
- An unusual channel or sender, a bonus or delivery you were not expecting.

THE ONE RULE THAT STOPS IT

When a message pressures you to click, log in or pay, stop and report it with your report button before you act.

THEN BUILD THE HABIT AROUND IT

- Make reporting one tap on every device, and thank the people who use it.
- Coach anyone who clicks, never punish or name them.

- Run simulations regularly and vary the difficulty and the channel.
- Put MFA and email filtering behind the people, so one click is not a breach.

MYTHS AND FACTS

MYTH

A low click rate means we are safe.

FACT

Click rate never reaches zero and drops if you just send easier emails. Report rate and time to report show real resilience.

MYTH

People who click should be punished.

FACT

Punishment makes staff hide mistakes and report less. The UK NCSC says coach clickers and reward reporters instead.

MYTH

One test a year is enough.

FACT

A single test is a snapshot, not training. Behaviour changes only when simulations run regularly and pair with feedback.

THE LEGAL DUTY

Security awareness training is a legal duty under NIS2 Article 21(2)(g), in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based security awareness and phishing-simulation training built around reporting, not blame. Read the full guide at the link below.

[Read the Full Article →](#)