How to run phishing simulations

Best Practices

The best phishing simulation programs don't just check a compliance box.

Phishing simulations should:

- Change behavior
- Reinforce reporting habits
- Reduce real-world risk
- Stay easy to manage at scale

Make simulations realistic

If your phishing emails are painfully obvious, users aren't learning anything useful. It's like an NFL team practicing for the Superbowl with a high school football team.

Simulations should reflect modern simulations:

1. Polished
2. Personalized
3. Realistic scenarios based on the person's role

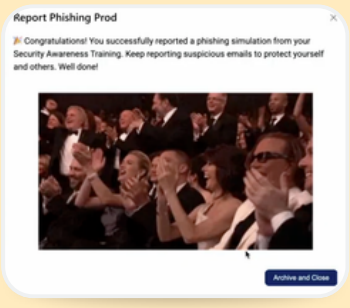
Positive Reinforcement > Punishment

Nobody learns effectively after getting slapped with a 20-minute training video.

What Works Better:

- Show users what they missed
- Explain why it mattered
- Keep feedback short and relevant
- Reward users for reporting suspicious emails

Positive reinforcement builds habits.
Punishment creates shame and resentment.

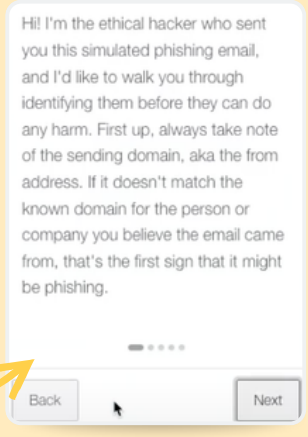


When you report a simulation

You should receive a message that instantly celebrates your good work – like a GIF!

When you click a simulation

You should receive an instant walkthrough of the email you clicked to learn how you could've spotted that it was a phish. This will better prepare you to spot the next phish in your inbox.



Phishing simulations you should send

- Software notifications (e.g. Unusual login activity)
- File sharing alerts
- Vendor invoices
- Package delivery notices
- Password expiration alerts
- Internal IT notices

Phishing simulations you shouldn't send

- Anything related to pay and employment (e.g. raises or layoffs)
- Imitating a government agency (e.g. The IRS or law enforcement)
- Health and medical scares
- Emergency or crisis notifications
- Tragedy charity exploitation (e.g. recent attacks or disasters)

Don't Send "Soul Crushing" Simulations

Realistic ≠ cruel.

Use Fresh, Relevant Templates

Reusing phishing templates with consistently similar content and formats makes simulations predictable. Users stop analyzing the email and start recognizing the test.

Use varied, up-to-date templates that reflect current phishing trends.

Find the Goldilocks frequency

Ideal frequency:
1–2 times per month

Too few simulations = users forget what to look for.
Too many simulations = users get fatigued and tune out.

Measure More Than Click Rates

A strong program tracks:

- Click rates
- Report rates
- Reporting speed
- Improvement over time

Fewer clicks + More reports = Better security

Fewer clicks by themselves are good, but not great. You also want to be aware of any malicious activity in your users inbox, because if they're not reporting it, you don't know what's floating around in your ecosystem.

Automate Delivery & Allowlisting

If phishing emails don't reach inboxes, the program fails before it starts. Your IT department should automate allowlisting and delivery wherever possible.

Manual allowlisting & campaign management:

- Takes time
- Breaks easily
- Creates inconsistent delivery

Check out Security Awareness Training Best Practices

Powered by PHIN