

# Phishing Campaign

Assess security awareness, educate your workforce, and build lasting cyber resilience



**Simulated phishing attacks, targeted training, and actionable insights to build a resilient security culture.**

Our Phishing Campaign Service is a proactive security initiative designed to evaluate your organisation's resilience against phishing threats. Through realistic simulations and targeted awareness training, we help you understand how your employees respond to phishing tactics and strengthen your overall cyber defence posture.

## Why run a Phishing Campaign?

### Behavioural insight

Detailed metrics on user interactions - who clicked, who submitted data, who reported the attempt.

### Measure awareness

Measure awareness across departments and roles.

### Vigilant culture

Deliver targeted training to reduce future risk. Promote daily habits that prioritise security and reduce risk across your organisation.

## We're not testing people, we're training defenders



### Support and training

This campaign isn't designed to single out employees, it's about raising awareness and turning human error into human defence.



### Simulated phishing attacks

Simulated attacks are safely executed to mimic real-world phishing attempts.



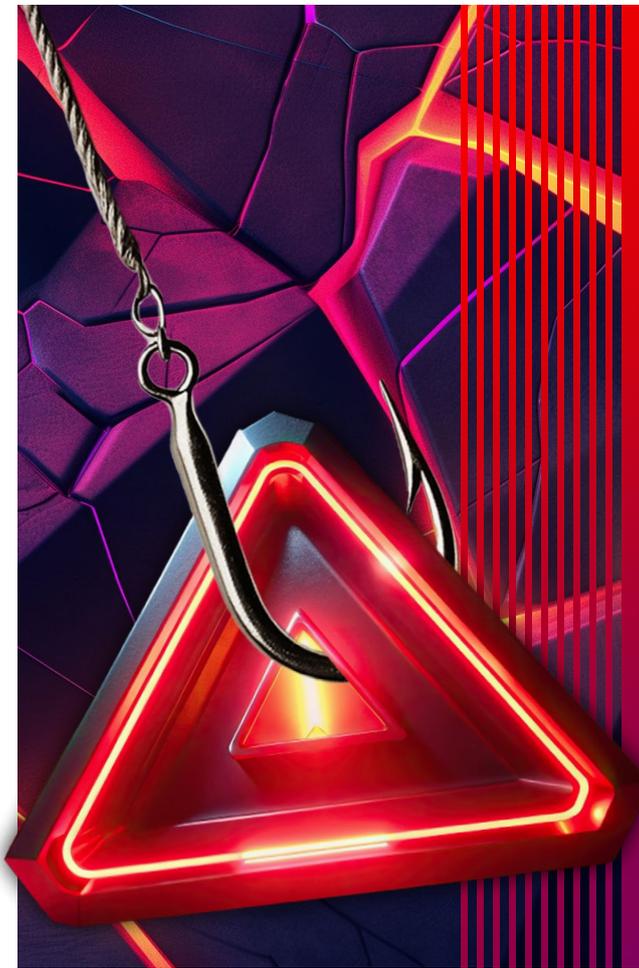
### Reduced risk of successful attacks

Simulations lower user susceptibility and strengthen frontline defences.



### Actionable intelligence

Clear recommendations to enhance user resilience and inform future security strategies.



## Our approach

### Strategic targeting

Campaigns are designed around roles, departments, and risk profiles.

### Controlled deployment

Simulated attacks are safely executed to mimic real-world phishing attempts.

### Phishing campaign report

Includes click rates, report rates, and data submission metrics.

### Security awareness training

Users who engage with phishing emails are enrolled in awareness training with engaging scenario based modules.

## Phishing remains one of the most effective attack vectors used by cybercriminals.

By simulating real-world phishing scenarios, organisations can uncover behavioural vulnerabilities, assess employee awareness, and take proactive steps to strengthen their human defences.



**Success is tracked through behavioural metrics** and post-training improvements.



**The focus is on education, not punishment.** Users are guided through training to improve future responses.



**Campaigns are designed to be low-impact** and run silently in the background.

## Contact us today

**Start building a culture of vigilance with targeted simulations and training.**

