Cyber security training and simulated phishing

Contents

Cyber security threats continue to evolve at a rapid pace, becoming increasingly sophisticated. Among these, phishing emails are a particularly cunning form of attack that dupe staff into clicking dangerous links.

Therefore, ensuring your team is adequately trained to recognise phishing attacks is essential. This guide discusses cyber security training and the role of simulated phishing in enhancing your security posture.

1. The cyber security landscape

Cyber security is no longer merely a concern for IT departments; it's a critical business issue that impacts all levels of an organisation. The cost of data breaches is increasing in terms of financial loss, operational paralysis and damage to reputation.

With the continued digitalisation of businesses, the complexity and scale of cyber threats have expanded. And the now familiar 'work from home' policy has added a new attack surface.

Phishing remains one of the most prevalent forms of attack reported to the Information Commissioner's Office (ICO), according to its latest data*. It now accounts for **36.5%** of reported cyber incidents in the UK, closely followed by the previous leader, Ransomware (**31.2%**).

Specific sectors are prone to phishing, partly because they are seen as easy targets and partly because their information is regarded as more valuable.

Our analysis of ICO UK data shows five sectors regularly report phishing incidents. The table below is for the period Jan-Dec 2022.

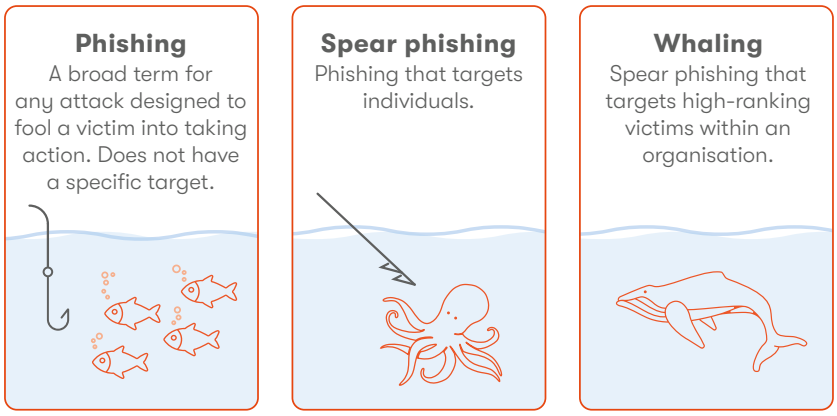
Sector	No. of phishing incidents	% of total phishing incidents
Education and childcare	575	22.2%
Charitable and voluntary	355	13.7%
Retail and manufacture	342	13.2%
Legal	255	9.9%
Health	242	9.3%

* ICO reported incidents, Jan-Dec 2022

> “...on average **35%** of staff will click a dangerous email link”

Source: KnowBe4

Broadly, there are three types of phishing attacks; basic phishing, spear phishing and whaling. An explanation of each is in the graphic below. Although the dominant phishing attack is email, smishing uses text messaging apps, and vishing uses voice calls to obtain sensitive data.



Criminals are also increasingly using AI in these attacks to add yet further sophistication, personalisation and scale to their outreach.

2. The importance of cyber security training

Cyber security is not solely about implementing sophisticated technical solutions; it’s also about creating a culture of awareness and vigilance.

Research indicates the majority of successful cyber-attacks are due to human error. Anywhere between **88%**-95%♦ of data incidents are due to human error**. Thus, continuous employee training is a key component of a robust cyber security strategy.

Cyber security training aims to equip employees with the knowledge to identify, manage, and prevent cyber threats. It involves:

- **Awareness:** Ensuring employees understand the types of threats and their implications.
- **Recognition:** Training employees to recognise signs of phishing attempts and other cyber attacks.
- **Response:** Equipping employees with the tools and knowledge to effectively deal with threats.
- **Reporting:** Encouraging employees to report suspected threats to the relevant person within an organisation.

KnowBe4, a phishing email training specialist, claims that, on average, **35% of staff will click a dangerous email link** on their first test. However, there is hope. After 6 months of training that figure drops to **16%**, and after 12 months it goes down to **4%**.

Our research appears to confirm those figure. We surveyed 520 people and asked if they had ever clicked a dangerous email link at work. **21.7%** of respondents said Yes, but **10.2%** were not sure.

5 red flags of a phishing email

1. Message is from a public email domain
No legitimate organisation will send emails from an address that ends ‘@gmail.com’.

2. The email domain is misspelt
Check the email address carefully - is it ‘@microsoft.com’ or ‘@micrasoft.com’?

3. The email is poorly written
Spelling errors and poor grammar are a big clue. Scammers aren’t very good at writing.

4. It has suspicious attachments or links
Phishing emails contain a payload. Infected attachments or a link to a bogus website. Be cautious before you click unsolicited emails.

5. The message creates a sense of urgency
Scams push you to act now. Criminals know we’ll drop everything if it seems our boss is making an urgent request.

** Stanford University ‘Psychology of Human Error’, 2022
♦ IBM Cyber Security Intelligence Index Report, June 2022

3. The role of simulated phishing

Simulated phishing is an effective way to measure the effectiveness of cyber security training and to reinforce lessons learned. Mock phishing emails are sent to assess employees' ability to recognise and manage such threats.

Benefits of simulated phishing include:

- **Real-world experience:** It provides a safe environment for employees to gain first-hand experience of phishing attempts.
- **Identification of vulnerabilities:** It helps identify areas of vulnerability and tailor training accordingly.
- **Behavioural change:** Regular simulations promote a state of continuous vigilance and encourage secure behaviours.

Chart II - Phishing tests at work

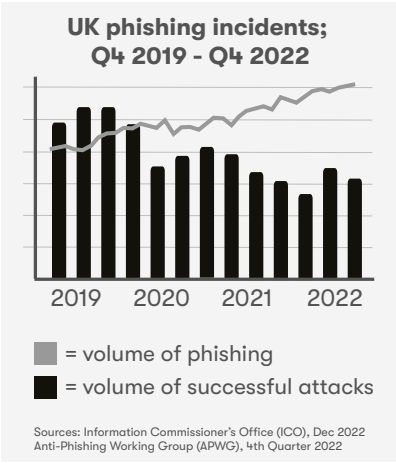
4. Implementing a simulated phishing program

The design of a simulated phishing program should reflect the complexity and variety of real-world phishing attacks. It should consider the following:

- **Frequency:** Regular simulations increase vigilance and help maintain awareness.
- **Variety:** Using different phishing scenarios reflects the diverse tactics attackers employ.
- **Progressive difficulty:** The complexity of the simulations should increase over time to challenge and improve skills.
- **Feedback:** Constructive feedback should be provided to staff, highlighting areas of success and those needing improvement.

We asked 497 people if their company sent fake phishing emails to test staff. **39% said No** (see Chart II). One reason companies don't do phishing tests is that it can be time-consuming - especially the post-test training.

Chart III - Positive future



5. Conclusion

Employees remain one of the most critical elements of cyber security. **Human error accounts for 88-95% of data incidents**. Regular cyber security training and simulated phishing exercises can **reduce dangerous clicks from 35% to 4% after a year**.

Managing the testing and training of staff can be a burden on over-stretched IT departments. This may be why **39%** of organisations don't do it. SMEs should consider outsourcing this effective barrier.

But it's not all doom and gloom. Our research shows that although the volume of phishing attacks has increased♠ in the last three years, the number of successful♥ attacks is falling (see Chart III). Possibly due to **45%** of organisations adopting phish training exercises.♣

♠ Anti-Phishing Working Group (APWG), 4th Quarter 2022
♥ Information Commissioner's Office (ICO), Dec 2022
♣ OryxAlign, July 2023

OryxAlign
Bury House
31 Bury Street
London EC3A 5AR

T: +44 (0)207 605 7890
E: hello@oryxalign.com
W: www.oryxalign.com

For some good advice on Cyber Security Training and Simulated Phishing Tests you can book a 45-minute consultation or email hello@oryxalign.com.

OryxAlign brings people and technology in parallel to drive better, faster outcomes. By listening closely, adjusting along the way and delivering to the highest standards, we create true alignment between your ambitions and the technology you need to reach them.

First published 13 July 2023