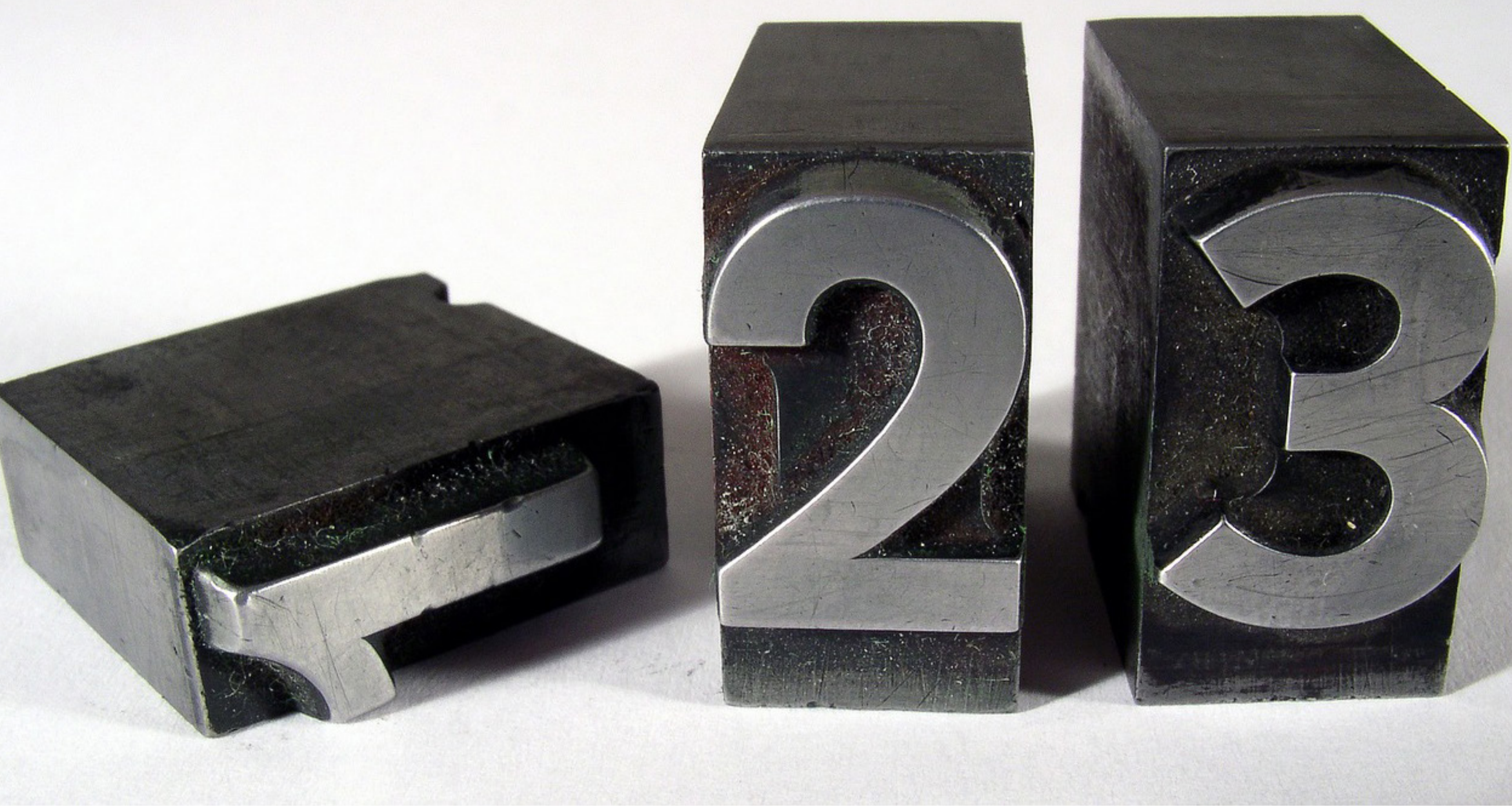
Protect • Comply • Thrive



Test – Educate – Assess

A three-step approach to mitigate the risk of phishing

www.itgovernance.co.uk

66% of professionals admit that employees are the weakest link in the company’s security strategy. 55% claim that their organisation suffered a security incident or data breach due to staff misconduct.

Managing Insider Risk through Training and Culture - Experian

The three fundamental domains of an effective cyber security strategy are: people, processes and technology.

Most organisations have invested heavily in technology to secure their valuable assets from cyber attacks. They have also implemented processes and procedures to meet compliance requirements and reduce the risk of cyber crime. Despite their efforts, they have still fallen victim to cyber attacks because they have missed an important, if not vital, component of cyber security strategy: **people**.

50% of the worst breaches in 2015 were caused by inadvertent human error.

Information Security Breaches Survey 2015 – PwC

Phishing: the sneaky threat

The most common type of cyber attack that targets employees is **phishing**, which is a fraudulent attempt to obtain sensitive information by impersonating a trustworthy entity and exploiting social engineering tactics.

Depending on the details of the attack, phishing is classified as:

Spear-phishing

Email-spoofing fraud specifically targeting your company.

Whaling

Spear-phishing attack targeting C-level esecutives or spoofing their email addresses to reach lower-level staff.

Vishing

Fraudulent phone calls urging the receiver to reveal sensitive information.

Smishing

Text messages urging the receiver to click on a link that instantly downloads malware on the device.

9 in 10 cyber attacks begin with email[1] because:

- Staff receive dozens of emails every day, and the more carefully phishing emails are crafted to look like legitimate ones, the higher the chance they will make it through the spam filter and into the inbox. Studies show that 1 in 3 recipients open the phishing email within an average 100 seconds[2].

- The email’s malicious content doesn’t expire regardless of how long it sits in the inbox, granting cyber criminals the longest window possible for their attack to succeed.

- Other than fooling inattentive users into revealing sensitive information through social engineering tactics, phishing emails can also deliver malware and ransomware via malicious links or attachments, multiplying their chances of success.

Although technology and processes can protect your company from a wide variety of advanced cyber attacks, when it comes to basic threats like phishing, it’s all in the hands of your staff. Their behaviour cannot be controlled, but a **staff awareness programme** can influence them to be more secure and reduce cyber risks.

60% of organisations experienced a phishing attack in 2015.
30% of these organisations experienced phishing attacks every day.

State of Cybersecurity – ISACA

> "The human factor is critical when creating cybersecurity capability, and education based on practical guidance is key to reducing the related business risks."
>
> *Christos Dimitriadis, chair of ISACA's board of directors*

Staff awareness programme

A staff awareness programme should be an integral part of your security strategy. Carried out during the induction process for new members, it should also be regularly rolled out to the whole staff and whenever staff-related security incidents occur.

Phishing attack, and spear-phishing campaigns in particular, target specific members of your organisation, usually those with access to payrolls, bank accounts and confidential data.

> 72% of large organisations and 63% of small businesses provide ongoing security awareness training to their staff.
>
> *Information Security Breaches Survey 2015 – PwC*

Before carrying out a phishing awareness course, it's beneficial to assess your staff's resistance to phishing attack, to assess which areas are weaker and need a deeper training.

IT Governance's ethical hackers will help you reduce your phishing exposure by testing and assessing your staff's vulnerability to phishing attacks.

CONTINUAL SECURITY IMPROVEMENT

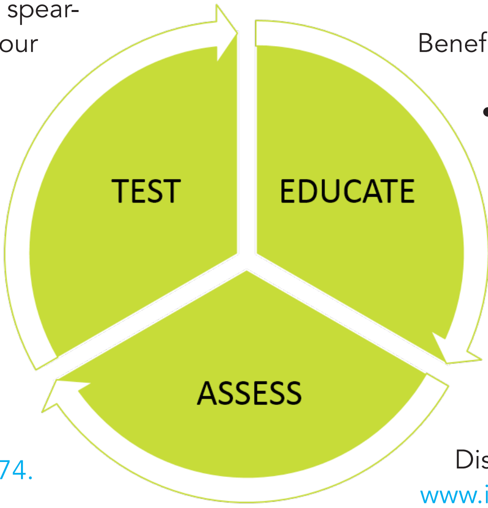
We have developed a three-step approach to help you mitigate the risk of a phishing attack. Based on testing and training, it represents the ideal process to keep your staff on top of existing and newly found phishing threats.

Test

IT Governance's **Simulated Phishing Attack** will establish whether your employees are vulnerable to phishing emails, enabling you to take remedial action to improve your cyber security posture. Following a scoping discussion with you, our Certified Ethical Hackers (CEHs) will simulate a mock spear-phishing attack, which will identify your 'high-risk' employees – those who represent a vulnerability to your security system.

After the test, you will be given an executive summary of the results, which will be the baseline for assessing the effectiveness of the staff awareness course in the next phase.

Discover more at www.itgovernance.co.uk/shop/p-1574.aspx.



Educate

The **Phishing Staff Awareness E-learning** course will help your staff understand how phishing attacks (and its variants) work, the tactics that cyber criminals employ to lure inattentive users, and how to spot and avoid a phishing campaign.

Benefits of the e-learning course:

- Delivered online, so staff can access it anytime from anywhere with an Internet connection;
- Staff can start and stop the training as they wish and based on their workload to minimise business disruption;
- Monitor your staff's progress with the administration dashboard.

Discover more at www.itgovernance.co.uk/shop/p-1690.aspx.

> 54% of employees tested with the Simulated Phishing Attack failed the test. They clicked through the masked malicious link within a few seconds of receiving the mock spear-phishing email.

Assess

After a successful first run of the Phishing Staff Awareness course, we suggest repeating the Simulated Phishing Attack test to assess any improvement. By repeating the phishing simulation, you will identify staff who no longer represent a risk and staff who need to improve their knowledge of phishing and still represent a risk.

When appointing an external provider of technical services, it is important that you choose a trusted supplier who can most effectively meet your requirements.

Call us on **+44 (0) 845 070 1750** or email **servicecentre@itgovernance.co.uk** for further requirements.

Why choose us?

IT Governance is a professional consultancy and technical services firm that provides a comprehensive range of information security resources, audits and testing to help organisations of all sizes contain and minimise information security risks.

- IT Governance is a CREST member and has been verified as meeting the high standards mandated by CREST. Clients can rest assured that work will be carried out to rigorous standards by qualified and knowledgeable individuals.
- Our simulations and penetration testing are conducted by penetration testers who have been awarded the Certified Ethical Hacker (CEH) certification.
- Our deep technical knowledge and expertise deliver insight and advice that is not available from off-the-shelf technical solutions.
- Our compelling e-learning portfolio is designed to train your staff to understand your security procedures and meet compliance requirements, like the ISO 27001 standard, the PCI DSS and the DPA. More at itgovernance.co.uk/itg-elearning.aspx

Our credentials and corporate certificates:

[1] Mimecast
[2] Verizon

IT Governance Ltd
Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA, United Kingdom

t: + 44 (0) 845 070 1750
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

@ITGovernance
/it-governance
/ITGovernanceLtd