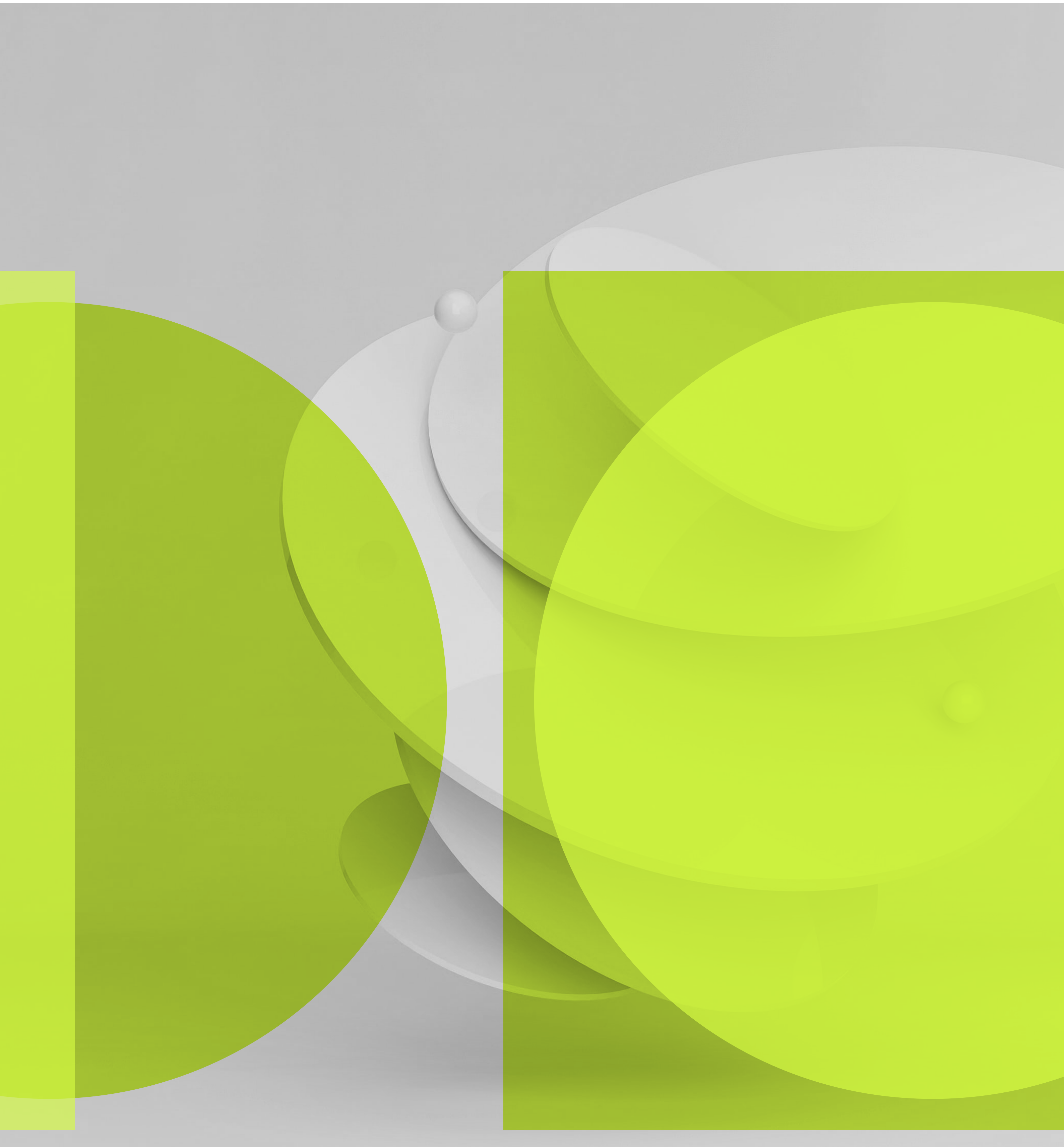
Mitigate the phishing threat



Visit: www.pgitl.com
Email: sales@pgitl.com

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT

Protection Group International Ltd
Registered in England & Wales, 07967865

Phishing is the number 1

Cause of data breaches and cyber-attacks

Source: DCMS Cyber Security Breaches Survey 2022

86% of malware

Is delivered using email

Source: 2022 Verizon Data Breach Investigations Report

40% of the attacks

Reported to the ICO in Q1 2022 were phishing attacks

Source: ICO Data Security Trends

Boost employee knowledge with tailored phishing awareness

The interactions people have with phishing emails provide threat actors with a foothold from which they can steal data or deploy an attack. These breaches can impact business operations by causing a loss of network functionality, degrading hardware functionality, data leaks, and significant reputational damage.

While spam filters and other technical mitigations will limit user exposure to these phishing campaigns, they are still becoming more sophisticated and harder to spot, so they may slip through the digital filters. The most effective way to protect your business from phishing attacks is to ensure your employees are cyber-aware and remain vigilant. We recommend conducting phishing vulnerability assessments so all your employees know what to do if they are the recipient of a phishing scam and keep your company safe in the event of an attempted breach. This way, you can help strengthen any vulnerabilities within your workforce before it's too late.

What is a phishing vulnerability assessment?

Understanding how phishing works and what to look for will make a big difference in how your workforce handles any suspicious email.

OUR ASSESSMENT IS DESIGNED TO:

- Identify vulnerable areas in your workforce and demonstrate how to best to deal with emails that may be malicious.
- Deliver tailored assessments for your organisation's requirements and typically includes a controlled phishing campaign and post-assessment report.
- Provide aftercare that will include a training about phishing threats for any employee who clicks a link or downloads a file.

A generic phishing vulnerability assessment engagement with our team may look like:

1

We meet with you to understand your concerns/challenges

2

We recommend a certain approach

3

We conduct a detailed scoping call where we discuss the details that will form the basis of the campaign materials

4

We send phishing emails, as discussed, to the selected employees or the whole workforce

5

You whitelist the domain we will be sending from

6

We agree dates and timings

7

We collect data and produce a detailed report that will enable you to see which areas need to be addressed

8

Employees who click links will be provided with educational material

9

You may wish to repeat this process regularly for the whole organisation or with just the departments/ areas that need further assistance

Assessment package options

		BASIC	TAILORED	BESPOKE
Content	The content used for your campaign emails and landing pages.	We use basic email templates, landing pages and PGI's generic phishing domain URL.	To better simulate a phishing email, our consultants can work with you to customise a message to fit the context of your organisation.	We work with you to develop content for emails and landing pages that is specific to your organisation, to show the breadth of the social engineering tactics threat actors use.
Campaign monitoring	We monitor the interactions with the campaign as it is happening for a set period.	7 DAYS	14 DAYS	14 DAYS
Pre-engagement scoping call	We take the time to understand your organisation's risk profile and appetite so we can recommend an appropriate solution.	✓	✓	✓
E-learning	Employees who click a malicious link and/or input their credentials will be provided with an e-learning module to help them identify phishing emails in future.	✓	✓	✓
Campaign reporting	We produce a post-campaign report to help you understand the awareness level of your workforce.	✓	✓	✓
Custom domain	We will register domains that look similar to those that your organisation uses to deliver these campaigns, so at a quick glance can appear to be the same.	✕	✓	✓
Employee credential audit	When an employee enters their credentials, we can record this so you can compare again best practice standards or your organisation's internal password policy.	✕	✕	✓

Benefits of conducting phishing vulnerability assessments

Identify the risks

Gain an understanding of your employees' current awareness of phishing and social engineering threats, as well as identifying where the gaps are, and which areas of the business need further training.

Gain more control over your business

While you can control the technology being used in the workplace, it is not as easy to control the actions of employees; informed employees create a safer digital environment, so it's important they stay vigilant.

Educate on common threats

Phishing campaigns can open organisations up to a range of threats, primarily that of malware. By educating your workforce you decrease the likelihood of a phishing campaign being successful.

Mitigate the risk of a data breach or operational disruption

Educating your workforce about the dangers of phishing emails, and how to spot them, will strengthen your cyber security and reinforce your digital defences.

Why choose PGI's experts over an off the shelf phishing assessment?

Tailored assessments

We provide a full spectrum of phishing vulnerability assessments, including end-to-end support.

We understand wider digital risk

We have experience helping clients understand and mitigate all forms of digital risk, so we can help you take a holistic approach to managing them.

Practical and affordable

Our solutions are proportionate and focused to your needs, not a blanket approach.

A flexible approach

We know the cyber threat is constantly evolving, so our team work to your business requirements, ensuring your digital security is resilient.

Vendor-neutral advice

We are vendor-neutral, so we will always act in your best interests when assessing your risks and offering a solution.

About PGI

We are an internationally acclaimed team of digital threat experts and thought leaders. Our mission is to protect organisations and nations from cyber threat and online harm.

We work at the cutting-edge of threat detection, continually scanning the horizon for next-generation risks. Using technology to support human insight, our experts build long-range resilience for clients.