PHISHING VULNERABILITY ASSESSMENT

WHAT IS PHISHING?

Phishing occurs when a scammer tries to trick people into giving away their/ their organisation's confidential information such as passwords, credit and bank card account details and financial information. They do this by pretending to be a legitimate contact and convincing a target to open a spam email, click on a dangerous link or go to a fake website.

When targeting a business, the scammer collects information about how an organisation's emails are presented and structured to make them look as authentic and believable as possible. Often the attacker will pretend to be a CEO or senior executive and send messages to employees further down the management chain asking them to transfer money or sensitive data. Alternatively, Whaling is a type of phishing attack that is aimed at top-level executives.

WHAT IS SOCIAL ENGINEERING?

Social engineering is the term used to describe various methods adopted to manipulate people into giving up sensitive information, such as pretending to know them using fake identification badges and conducting fictitious telephone calls.

WHY A PHISHING ASSESSMENT SHOULD BE TOP OF YOUR PRIORITY LIST

No matter how secure your company's networks are, they will still be vulnerable to human weakness. With phishing attacks being the most common form of cyber-attack, people need to know what to look out for when a potentially dangerous email lands in your or your employee's inbox.

HOW AWARE ARE YOUR EMPLOYEES?

We are not here to catch or ridicule anyone. Our process is to identify those employees that may require further training, and to bring the subject of phishing emails to the forefront of their consciousness, so when an email does land in their inbox or a telephone call received, they will know what to watch out for and when to say no.

OUR ASSESSMENT

PGI has developed a phishing vulnerability assessment with the purpose of measuring the current cyber awareness of the workforce, and delivering targeted training to reduce the organisation's risk of exposure to this type of attack.

PGI will conduct a bespoke test email phishing campaign, tailored to your organisation, based on:

- Open source research
- Our knowledge of your organisation
- The latest attacks targeted at your industry

This campaign can be carried out over a 4-week period with multiple emails.

Throughout the campaign the realism of these emails and the domain names used will vary to replicate the different abilities and skills used by attackers. Upon failing to identify a phishing email, staff will be presented with a short educational message such as a training video or webpage to help them identify and mitigate against that type of attack in the future.

METRICS AND FOLLOW-UP

PGI will actively monitor and report on the following metrics throughout the exercise:

- Opened phishing emails, and potentially malicious links clicked/ attachments downloaded.
- Geographical location of the user opening the email to identify access in non-typical locations.
- Out-of-date browsers and plugins, identifying potentially vulnerable users.
- Network endpoints vulnerable to data-exfiltration and firewall misconfiguration.
- Users who are subject to phishing emails but have failed to complete follow-up training.
- Reductions in the number of successful phishing emails.

At the end of the campaign, PGI's security experts will generate a comprehensive report based on the above which will provide an analysis of current cyber maturity, and produce recommendations to increase this.

By understanding your organisation's security posture, you can make informed decisions on effective investment in education and technology, as well as improving your organisation's level of security and awareness.

Unit 13/14 | Swallow Court | Sampford Peverell | Tiverton | EX16 7EJ | UK
Tel: +44 (0) 207 887 2699 Email: clientservices@pgitl.com Visit: www.pgitl.com