PRODUCT SHEET

Managed Security Service: Phishing Simulation Test

What is a Phishing Simulation Test?

In most security immune systems, the employee is the weakest link with approximately 90% of breaches caused by human error. Typically an employee has clicked on a suspicious email and provided their credentials, compromising not only their email account - but the whole integrity of their organisation. Critically, this triggers a 72-hour notification window to submit the breach to the ICO as part of GDPR, so businesses need to act quickly to avoid significant financial fines.

To assist in identifying an organisation's susceptibility to a phishing attack and aid prevention, GCI offers a Phishing Simulation Test. The Phishing Simulation is based on common phishing email scams that are regularly sent to organisations.

Key features

GCI's Phishing Simulation Test emulates a range of phishing attack types to help identify areas of weakness in an organisation's security posture, empowering users through awareness to strengthen internal defences.

Phishing Simulation Test

Targeting up to 100 users, GCI will send a selected phishing email template to employees to establish user behaviour and the likelihood of being fooled by a malicious threat actor. This consists of the following steps:

Step 1 - Approve temporary whitelisting on email infrastructure to enable mail delivery

Step 2 - Provide user list

Step 3 - Select phishing email template

Step 4 - Approve and send phishing test to users

Step 5 - Receive report and user education document

Phishing awareness documentation

This advises users on how to be diligent before opening a suspicious email and provides real-life examples of what to look out for.

Summary report

Provided on completion, the report will highlight the number of recipients who opened the simulated phishing email with actionable recommendations. Data includes:

- The number of emails sent and opened
- The number of users clicking links
- The number of attachments opened
- How many people reported the email

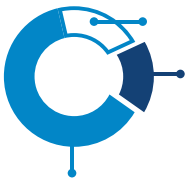
Business benefits

- **Identify risks** - Prevent data breaches as employees become well-versed in identifying phishing attacks.
- **Compliance** - Reduce the chance of any attacks that may result in the loss of company data and revenue.
- **User-education** - Boost employee's cyber-security awareness in a meaningful and controlled environment.
- **Threat reporting** - Understand business security risks and demonstrate return on investment.

IDENTIFY RISKS

COMPLIANCE

USER-EDUCATION



THREAT REPORTING

Why is GCI the security partner of choice?

We understand the compliance and security challenges that today's organisations face, having consulted on and supplied solutions for numerous businesses where this is paramount, including Government and Legal organisations. GCI's Managed Security Services portfolio is unique in the marketplace as our services are individually tailored to suit your requirements, leaving you confident that your infrastructure is in the reliable hands of a firm that truly understands your business. From mitigating security risks, implementing appropriate defence, and addressing GDPR and compliance, we provide a mature and truly end-to-end approach to security.

REQUEST A FREE CONSULTATION

If you would like to book a complimentary consultation or find out more about our solutions, please contact enquiries@gcicom.net, or call 0844 443 433.