Phishing Simulation – Data Sheet

Phishing and spear phishing emails present a constant threat to organisations of all sizes. Email remains the primary vehicle for the delivery of ransomware and research by the SANS Institute has shown that 95% of breaches start with a phishing attack. It is therefore unsurprising that over 75% of organisations reported being victims of phishing attacks in 2016, with attacks becoming more sophisticated. Examples include targeted phishing, spear phishing, 'whaling' (which is aimed at phishing senior executives) and 'imposter emails' (emails purporting to be from an executive requesting the transfer of funds). It is therefore important to include phishing awareness in your employee security training.

Awareness training is best achieved through explanation and demonstration. Phishing simulation helps achieve this by targeting your employees or specific functions with highly credible email phishing campaigns with the aim of raising awareness of the risks and improving knowledge of what to do when a suspicious email arrives. The Voyager Phishing Simulation service helps educate your employees and raise their phishing awareness whilst also enabling you to measure employee susceptibility to social engineering attacks.

What we do

Based on our knowledge of your working practices and objectives, we'll build and suggest various customised phishing emails and landing page designs to deliver a realistic attack. A single campaign typically uses a combination of customised email templates, which become more sophisticated over the period of the campaign. We can build email templates and landing pages based on major corporate brands, or using your own branding, or that of your major customers or suppliers. You'll be asked to review and approve all email and landing page designs and templates before the campaign is launched.

Username and password harvesting is our commonest and most effective phishing awareness campaign. When delivering a credential harvesting campaign, phishing emails are sent to agreed targets purporting to be from the IT Department or a well-known service provider, such as a major bank or cloud storage provider. The email will include a 'phishing lure' encouraging targets to follow an embedded hyperlink.

What we do

When the targets click on the hyperlink they are redirected to a matching landing page hosted on our servers on which they are directed to enter their domain username and password in order to access the file or benefit. Once a target has entered their username and password they are redirected to a tailored phishing awareness education page on our website. This is branded with your corporate logo and can be as detailed as you consider appropriate. The education page typically covers:

- An explanation that the user has been phished.
- Reasons why the campaign is being run.
- An explanation of what phishing is.
- Guidance on how to avoid falling victim to phishing and what they did wrong/should have looked for on this occasion.

Furthermore, we collect statistics including the numbers of emails sent, the number of recipients that clicked the hyperlink, and the number of recipients who submitted their username and password. This information is formulated in to a report and delivered to the project stakeholders.

About Voyager

Voyager Networks is an IT Solutions business delivering a range of innovative solutions to its many clients across a wide range of public and private organisations. Solutions can be provided on-premise, from a data centre or in a hybrid environment to best suit business needs. Additionally, working in partnership with a number of finance houses, we can provide both Capex and flexible Opex purchasing models.

In summary we make complex networking and communication technologies simple to deploy and support – IT MADE SIMPLE.