MARATHON PROFESSIONAL SERVICES

Phishing Mitigation Managed Service

PhishMe’s intelligence-driven solutions empower employees to be an active line of defence and source of attack intelligence by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats

In Q1 2016, the PhishMe Research team determined that ransomware now accounts for 50% of all phishing emails. As of the end of March, 93% of all phishing emails analysed contained encryption ransomware. And the number of phishing emails hit 6.3 million in the first quarter of this year, a 789% increase over the last quarter of 2015

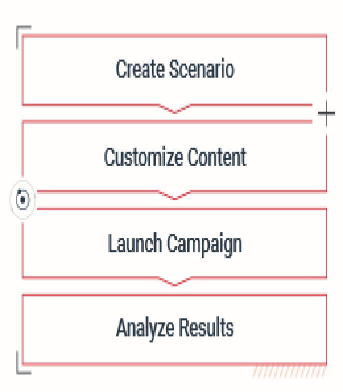
Changing Behaviour

PhishMe Simulator was designed to change employee behaviour and enable employees to recognize and report malicious phishing emails. The PhishMe methodology entails periodically sending employees real-life phishing scenarios that deliver hands-on experience with safe examples and on-the-spot education opportunities. The PhishMe attacks use examples and content focused on today’s greatest threats such as Business Email Compromise (BEC) and ransomware.

At a Glance

Key Benefits

- Reduce organizational susceptibility to phishing attacks by more than 95% through immersive training exercises
- Simulate the latest attack tactics with customizable scenario and training templates
- Employ differentiated learning techniques from a continuous library of multilingual content
- Validate program efficacy and identify areas of risk with detailed reporting



For more information speak with our **Managed Service Team** on 0208 329 1000
sales@marathon-ps.com

MARATHON
PROFESSIONAL SERVICES

Phishing Mitigation Managed Service

Real-World Phishing Simulations

PhishMe scenarios recreate a variety of such real-world attack techniques and escalate the latest and most critical phishing simulations as ‘Active Threats’ that include:

- Ransomware
- Business Email Compromise (BEC)
- Spear phishing attacks
- Social engineering attacks
- Malware and malicious attachments
- Drive-by attacks
- Advanced conversational phishing attacks

By leveraging phishing examples analysed as part of the PhishMe Intelligence service, PhishMe Simulator delivers the latest tricks and tactics being used in real-world phishing attacks.

Our Approach

- We will design and deliver regular and relevant phishing email attack campaigns
- Re-target offending employees or groups
- Provide comprehensive reporting to drive improved behaviours and education
- Totally independent and un-biased, ensuring maximum effectiveness

With over 20 million employees trained in 160 countries, PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% – preparing your last line of defence to recognize and resist phishing attempts.

At a Glance

Click Only: An email that urges the recipient to click on an embedded link.

Data Entry: An email with a link to a customized landing page that entices users to enter sensitive information

Attachment-based: An email with seemingly legitimate attachments in a variety of file formats.

Double Barrel: Patented technology that simulates conversational phishing techniques by sending two emails or an SMS and email – one benign and one containing a malicious element – to train users on this tactic used by APT groups.

Benchmarking: A patented feature to conduct an identical scenario and receive an additional report that provides an anonymous comparison of your results with other PhishMe customers or industry peers that ran the same scenario.

Highly Personalized: Simulate advanced social engineering tactics by using specific public, known details about email recipients gathered from internal and public sources

For more information speak with our **Managed Service Team** on 0208 329 1000
sales@marathon-ps.com

MARATHON
PROFESSIONAL SERVICES