Cyber Vigilance
We've got your back...

Datasheet
Cyber Awareness & Phishing

Cyber Vigilance’s Cyber Awareness & Phishing Service is a foundational element of our 'People’ pillar of Cyber Security Managed Services.

Service Overview

There is a growing threat to your organisation and employees; 91% of successful data breaches start with a spear-phishing attack. On top of this, showing that you have a cyber aware workforce is becoming increasingly important for compliance. For example, under 8.2.2 for ISO27001, “All employees of the organisation should receive appropriate awareness training and regular updates on organisational policies and procedures, as relevant for their job function”.

Cyber Vigilance’s Managed Cyber Security Services 'People' pillar focuses on creating a cyber security-aware workforce through bespoke managed simulated phishing and awareness training. This service is built upon KnowBe4, the world’s largest security awareness training platform.

The purpose of this service is to:

- Educate staff to be cyber aware and create a “human firewall” for your organisation.
- Maintain and improve awareness via continuous phishing simulation and education.
- Provide ongoing visibility of test and risk scores to see improvement over time.
- Show your organisation takes security seriously and improves your reputation with customers, suppliers, and regulatory bodies.

Cyber Vigilance
We've got your back...

Datasheet
Cyber Awareness & Phishing

Service Features

Managed Browser-based Training - Interactive training gives your users a better learning experience. Your users can choose the language they're most comfortable with for the entire training interface, helping deliver a more immersive training experience. This service gives you access to the world's most extensive training library, including National Cyber Security Centre (NCSC) approved content. Surveys are conducted after training to ensure the training remains relevant to your users. This service can also train specific groups or employees with role-based training and other speciality courses.

Managed Simulated Phishing – Put what your users have learnt into practice. You'll receive at least one phishing campaign a month, of which your organisation's unique requirements can determine the frequency. This service tracks how your users react to phishing emails and calculates an organisation-wide risk score.

Remedial Training – Users who click on a suspicious link in a simulated phishing campaign can be enrolled on a remedial training campaign to help reaffirm them of the red flags missed.

Assessments - Find out where your users are in both security knowledge and security culture to help establish baseline security metrics.

Custom Experience – Our service gives you the option to add branded custom content to the training modules. You can add your organisation's branding elements including your logo, custom graphics, and corporate colours to tailor any messaging you want to deliver to your users.

Phish Alert Button - Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis and deletes the email from the user's inbox to prevent future exposure.

Support – The Cyber Vigilance team are here to assist you, whenever it is required. Our team will also help with the onboarding process, getting you up and running as quickly as possible.

Reporting - Reporting on your organisation's risk scores, phish-prone percentage, and riskiest users so you can manage your human risk. This will be included in your monthly report but also can be provided ad-hoc.

Datasheet
Cyber Awareness & Phishing

Onboarding Process

Cyber Vigilance will provide support throughout the onboarding process to ensure the service meets your organisation's requirements.

Firstly, our team will arrange a welcome call to discuss your needs, such as training content and simulated phishing campaigns.

Your users will need to be enrolled onto the platform either by Active Directory (preferred) or CSV file, including username and emails. Whitelisting of the platform will also be required since simulated phishing emails will be sent to your users. Whitelisting the mail servers will also ensure that training-related notifications will reach your users.

Your company logo and branding can be added to the platform, including your organisation's business hours, to ensure phishing emails are only sent when you would like them to.

We will conduct an initial simulated phishing campaign. The purpose of this preliminary test campaign is to:

- Ensure that you have whitelisted correctly and that the emails pass through your spam filters and firewall protection.
- Ensure that clicks and other phishing test failures are tracked in your account.

This will show your organisation's initial phish-prone percentage. Consider the initial phish-prone percentage as your starting point. Cyber Vigilance uses this initial phish-prone percentage to measure the success of your security awareness training plan.

How The Service Works

Once your users have been enrolled, and the first simulated phishing campaign is completed, we will conduct a comprehensive baseline training campaign covering various topics.

Ongoing training and phishing will then be carried out, which includes:

- At least one phishing email per month to all users and targeted phishing emails to high-risk departments and users. Users who click a phishing email will be added to a group for remedial training.
- Conducting remedial training campaigns and targeted training.
- Train specific groups or employees with role-based training and other speciality courses.
- To keep your users aware and ready to defend against the latest phishing and social engineering scams, we can set up a campaign to send 'Scam of the Week' emails for your users.
- Provide all users with a "Phish Alert" button to allow them to report suspicious emails easily.
- All users will be enrolled on a baseline training campaign twice a year to ensure knowledge is retained throughout the year. Any new employees will be automatically enrolled on a baseline training campaign.
- Cyber Vigilance will observe risk scores from the simulated phishing campaigns to ensure the service is effective.

Cyber Vigilance
We've got your back...

Datasheet
Cyber Awareness & Phishing

Customer Responsibilities

- The customer will be required to provide information on your staff – either in a CSV file or via Active Directory Integration (preferred), which includes the user email address.
- Inform Cyber Vigilance of new employees, so they can be enrolled on the baseline training campaign and so any appropriate billing adjustments can be made.
- Provide a list of domains covering all users email accounts (e.g. customer.co.uk, customer.com, subsidiary.com).
- Whitelisting of the platform mail servers.
- Ensure users are completing training.
- Installation of 'Phish Alert Button'.
- Ensure user count does not exceed purchased licenses. Additional license can be purchased where required.