

## Norm's Cyber Safety & Phishing Service

Norm's Cyber Safety Training and Phishing service is comprised of a standalone module of its Cyber Security as a Service (CSaaS) offering.

Over the past 12 months less than 10% of cyber-attacks observed globally made use of a system weakness. The vast majority exploited "the human factor": the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open and send money or data.

Norm's Cyber Safety Training and Phishing Service is built upon KnowBe4's platform which is integrated onto Norm's Security Operations Centre (SOC) and managed service. This service module focuses on the **People** element of norm's holistic trinity of cybersecurity - **People, Process and Technology**. Its purpose is simple:

- \* **Educate your staff to be cyber aware**
- \* **Continually Test your staff on their cyber awareness**
- \* **See the Results, continue the education and see the improvements**

The service provides regular, easy to consume, bite-sized security awareness training courses/tests combined with simulated phishing attacks to test ongoing awareness and compliance. The results are tracked and summarised in simple to understand reports, so you can see how your workforce are improving and becoming less susceptible to "opening the door" over time.

### Service Features

You will also gain access to Norm's managed service offering the following features:

- Access to the world's largest security awareness training & phishing platform providing access to
  - Extensive library of cyber awareness training programs
  - Automated management of cyber awareness training courses
  - Automated phishing campaigns
- Managed onboarding process including system integration support
  - Configure active directory integration to pull user lists and ensure that all current users are being phished.
  - Technical Support on hand to investigate and resolve email failures, if required.
  - Email Application integration for in-app "Phish-alert-button"
- Enrollment of your staff into a cyber training program with a defined syllabus and schedule
  - Customisable training campaigns to suit your needs to ensure that users are receiving relevant training
- Enrollment to a Norm managed phishing campaign providing regular simulated and targeted and focused phishing emails to your staff.
  - Customisable phishing campaigns to optimise the phishing emails to your staff.
- Norm's monthly summary made available via Board and Management report, detailing the outcome of each campaign. Real-time reporting available via Norm's portal.

## On-Boarding Process

Onboarding with the service will be managed through Norm's customer experience team who will arrange a Welcome call to provide a service introduction and onboarding assistance including:

- Enrolling your staff into cyber training and phishing platform using your staff's email addresses and domains provided.
  - Assistance with systems integration with Single Sign On (SSO), Active Directory and Email applications
  - Assistance with setting up whitelisting (norm will provide instructions, send test emails and perform problem diagnosis).
  - Assistance with internal enrolment communications
- Provide a 1-hour training session to demonstrate the core functionality of the platform including viewing results & modifying templates.
- Planning upcoming training courses & phishing campaigns for the upcoming 12 months with one training and phishing campaign for each month.
- Norm will assist with customisation requests for training and phishing campaigns
- Norm will set-up remedial training campaigns to provide additional training to users that fail a phishing test.
- Providing access to Norm's Visualiser platform

As part of the service deployment, our Customer Experience team will provide you with access to the Norm Visualiser. This Visualiser will provide you with an overview of all the performance of your staff's education and their resilience to the simulated phishing attacks.

## Integration Options

Enrolment to the service can be achieved through the following options:

- Staff Enrollment phase to be implemented through either Active Directory Integration or Import of a CSV file with Staff details including Name and email address\*
- Single Sign-On is applied for quick user access to the training platform. SSO Integration options include any SAML compliant SSO provider
- PAB (Phish Alert button) is available for Outlook (On-Premise), Office 365 Outlook.com mobile App and Gmail

\* Integration via Active Directory is the recommended route as this reduces your admin overhead as your staff population changes.

## Technical Requirements

The Cyber Safety Training and Phishing service supports the following clients:

### Cyber Training Platform

- Internet Browsers including
  - Microsoft Edge
  - Microsoft Internet Explorer
  - Chrome 54 and later (Linux, OS X and Windows)
  - Firefox
  - Apple Safari
- All Internet Browsers are required to have the following features and/or be enabled:
  - JavaScript Enabled
  - CSS3 Compliant
  - HTML5 Compliant

### Single Sign-On Technical Requirements

- Single Sign-On (SSO) integration with any SAML compliant SSO provider including:
  - Azure Active Directory
  - Bitium
  - Centrify
  - Google Suite (G Suite)
  - F5 Big-IP
  - Okta
  - OneLogin
  - PortalGuard
  - SecureAuth
  - Zoho

### Phishing Service Technical Requirements

- Outlook 2010, 2013, 2016 & Outlook for Office 365
- Microsoft Exchange 2013 & 2016
- Outlook on the web (Outlook.com)
- Outlook Mobile App (iOS and Android)

# No jargon, no compromise\*



## Service Availability

The service is managed within norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Customer Experience team operate Monday to Friday 9am to 5:30pm.

The Customer Experience and SOC teams will be on hand to provide technical advice and assistance on issues should this be required.

## Customer Responsibilities

- You will need to provide information on your Staff – either on a spreadsheet or Active Directory Integration (preferred)
- A list of domains covering all users email accounts e.g. client.co.uk, client.com, subsidiary.com
- Whitelisting of Norm's simulator Phishing server