No jargon, no compromise*

*Reassuringly dull cyber security

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 CybSafe's platform which is integrated with 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:

- **Establish your staff's existing knowledge, confidence and risk perception levels**
- **Educate your staff with NCSC & CIISec certified content to strengthen their cyber resilience**
- **Provide personalised training, security advice and threat updates based upon each user's knowledge and confidence**
- **Test your staff on their cyber awareness through knowledge and confidence-based questions as well as simulated phishing emails**
- **Obtain tangible and quantifiable results, see what works and what doesn't, adapt and continue the education to see the improvements**

The service provides regular personalised, bite-sized security awareness training based upon data-driven analyse of each person's knowledge and confidence to provide a tailored training plan that fits their individual needs. As well as elevate your staff's cyber awareness and resilience, the service will further conduct further testing using simulated phishing attacks to test ongoing awareness and compliance.

The results are tracked and summarised in simple to understand reports. This enables you to see, how your staff's cyber knowledge and confidence is improving over time, what is working and what is not and how to adapt how your approach to ensure your workforce becoming less susceptible to "opening the door" over time.

Service Features

You will gain access to norm's managed service that will deliver the following features:

- Access to a people-focused security awareness training & phishing platform providing access to
    - Data-driven security awareness training platform providing tailored cyber awareness training courses
    - Extensive library of cyber awareness training courses, advice and news
    - NCSC & CIISec security certified content
    - Automated phishing campaigns
    - Reporting information looking beyond just click, report and completion rates. Using data-driven, behaviour analysis you'll get insight and visibility in a way that allows you to predict and manage human cyber risk
- Managed onboarding process including system integration support

- On-boarding planning session to discuss integration options and content needs
- Configure active directory or Single Sign-ON (SSO) integration to pull user lists and ensure that all current users are being trained and phished
- Technical Support on hand to investigate and resolve email failures, if required.

- Enrollment of your staff into a cyber training platform with per person onboarding questions to establish their current knowledge, awareness and confidence.
- Enrollment to a norm managed phishing campaign providing regular simulated, targeted and focused phishing emails to your staff.
- Access to norm's online visualiser dashboard where you will have full visibility of your organisation's cyber training and staff testing progress. Where the service has been purchased a part of a CSaaS contract, you will receive a monthly summary report within Board and Management report pack.

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 the 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
  - Assistance with setting up allow listing (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
- Initial user onboarding will take them through an initial knowledge and cultural assessment to baseline their awareness and attitude. The results of which are used to provide an individualised training program focused on their needs.
- 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.

* Integration via Active Directory or SSO 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 Internet Explorer 11
  - Microsoft Edge (current and last major version)
  - Mozilla Firewall (current and last major version)
  - Google Chrome (current and last major version)
  - Apple Safari (current and last major version)

- Mobile Internet Browsers including
  - Google Chrome
  - Apple Safari

Single Sign-On Technical Requirements

- Single Sign-On (SSO) integration with the following SSO providers:
  - Azure Active Directory
  - Office 365
  - Ping Identity
  - Okta
  - Google
  - Forgerock

If we don't currently support an SSO provider, we'll happily work with your organisations towards a solution - simply contact us to discuss what you need.

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 during UK business hours, Monday to Friday 9:00 to 17:30, excluding public holidays.

CybSafe routinely release updates during business hours operating a zero-downtime deployment policy. Where possible, we will conduct any significant maintenance requiring outage outside of business hours only after reasonable notice has been provided.

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

Customer Responsibilities

- The Customer will be required 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
- Set up allow listing of norm's simulated Phishing server.
- The Customer shall nominate an administrator internally for the norm Visualiser.
- The Customer shall be responsible for user administration within the norm Visualiser.