Hutsix

Information Security Awareness Training with Phishing Simulator

Service Description G-Cloud 12

Overview

Hut Six's solution enables you to train, test and track your employees' security awareness to create a measurable, secure culture throughout your organisation.

TRAIN

Protect your company through measurable, bespoke, cloud-based information security awareness training that educates your staff effectively; changing behaviours through Hut Six's unique approach.

TEST

Hut Six's Phishing Simulator tests the efficacy of our training in the real world. The Phishing Simulator enables managers to "phish" their employees with their actual email address. Then, if/when the employees are caught out they are taken to on-the-spot training to help change their behaviour.

TRACK

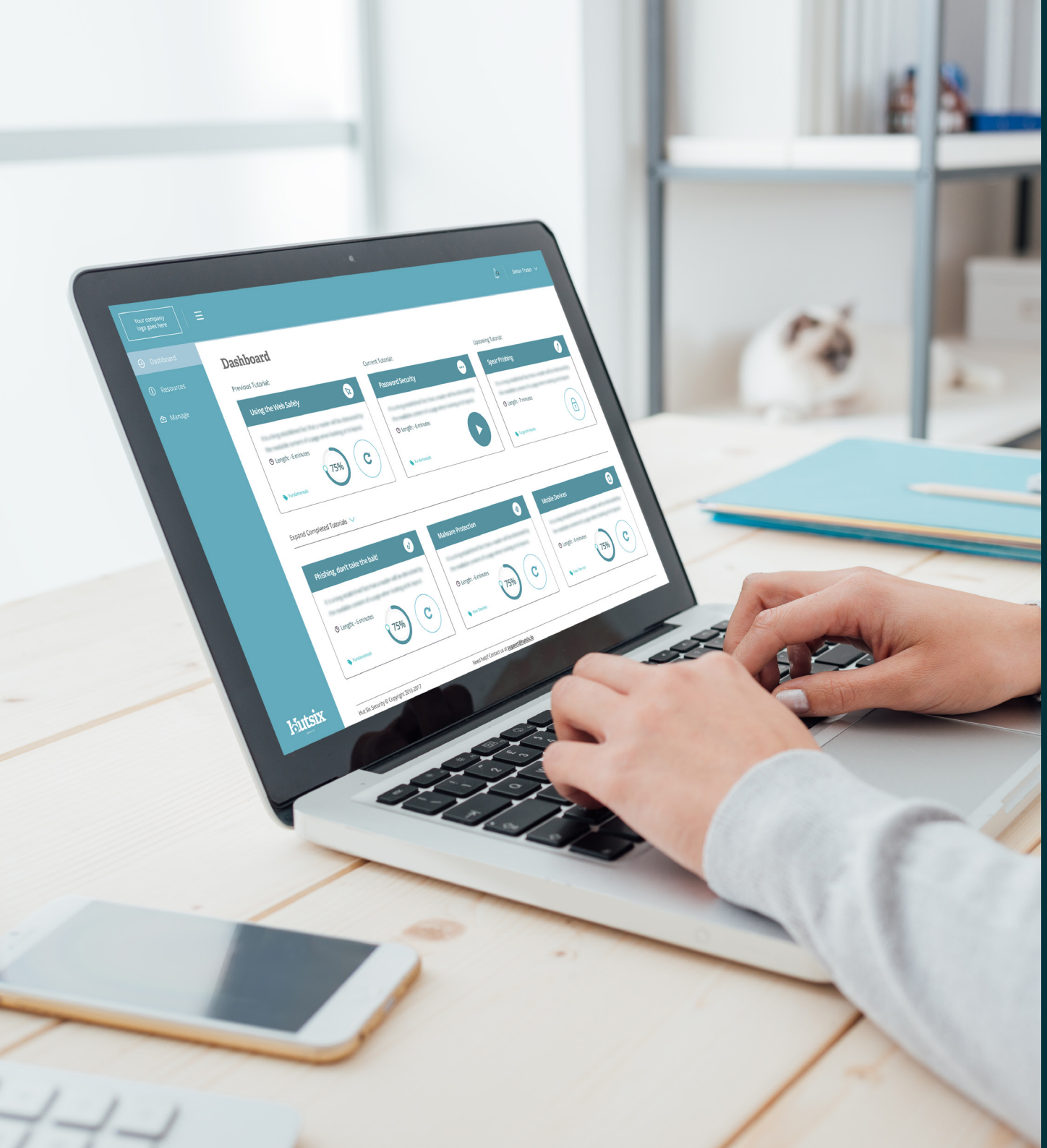
All responses to the interactive tutorials and phishing campaigns provide real-time actionable metrics on your organisation's security awareness campaign. This data is visualised via the management dashboard which enables you to track your employees' progress and effectively administer your awareness campaign.

The Problem

Human error is the most prevalent cause of security breaches, with the four most common types of data breach being related to phishing (72%); viruses, spyware & malware (33%); social engineering (27%); and ransomware (17%).

Staff awareness and vigilance, alongside good technical defences, are now imperatives when securing organisations.

- Department for Culture Media & Sport, 2017



Train

The 12-month campaign consists of 26 interactive tutorials (each 5-10 minutes long) and covers all aspects of end user security including cyber and physical threats to your organisation's information.

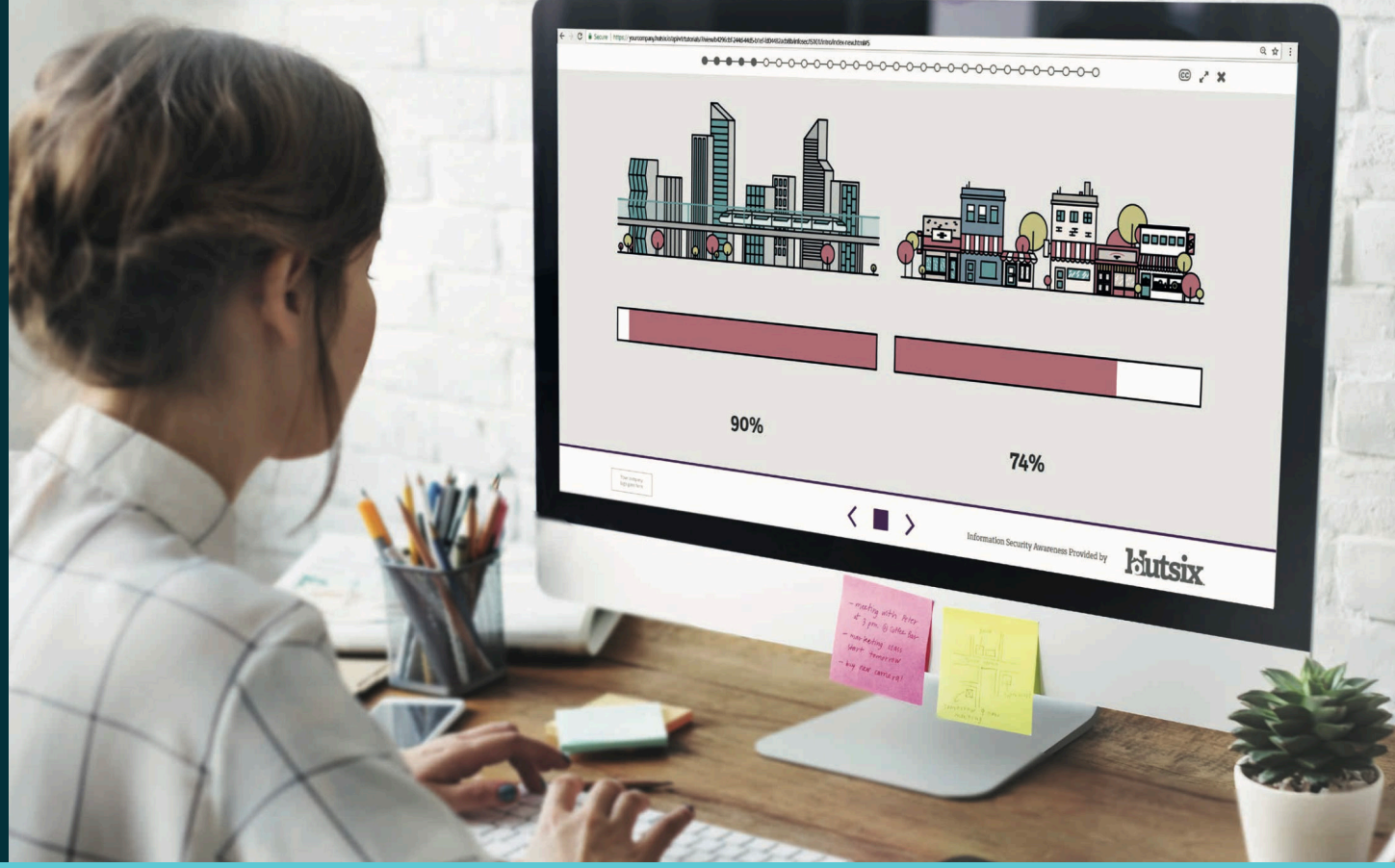
The tutorials are delivered via our cloud-based training platform in the web browser, as a Software as a Service (SaaS) model.

Users are alerted via email to new, outstanding or overdue tutorials and can access the training from links within the email or via their organisation's bespoke portal (yourorganisation.hutsix.io). Here, they can take their next tutorial, review previously completed tutorials and manage their account. It is designed to allow users to quickly take their next tutorial, minimising the amount of time required to complete the training. The tutorials are accessible within supported web browsers and can be taken anywhere with an internet connection and device.

Our Approach

The Hut Six approach has been designed with reference to modern behavioural science principles, particularly within eLearning educational campaigns.

We emphasis three core aspects to replace traditional corporate training:



FREQUENT

Information security tutorials delivered every two weeks maintain security at the forefront of employee minds, whilst keeping the content fresh and relevant.

ENGAGING

The interactive elements woven into the tutorials not only educate your employees, but provide metrics to assess, track and improve their performance throughout the campaign.

CONCISE

Five-minute tutorials taken once every two weeks fit seamlessly into your routine and provide consistent training without detracting from employee productivity.

SECURITY FATIGUE

In order to maintain continual user engagement and the success of the campaign, it is necessary to subvert the stereotype of monotonous, unengaging and time consuming corporate training.

Often the reason employees do not follow security policies, is not because they aren't aware of them, but because of security fatigue from a multitude of poorly communicated measures.

To overcome this, Hut Six's format of delivery has been designed to take into account the various influencers that affect end user actions.

Technical, social, economic, professional and personal arguments for secure behaviour all play a part in convincing people to change their behaviour.

UNIVERSAL MESSAGE

One of the biggest challenges information security campaigns face is addressing all the varying grades of employees with one message that speaks to everyone.

Traditionally there has been "a lowest common denominator" approach resulting in a condescending narrative to most users.

Hut Six overcomes this challenge by basing the majority of its material in real-world case studies. As such, technical specialists are kept engaged whilst the less technical still absorb the baseline message.

ONGOING CAMPAIGN

Once the year's course is complete, Hut Six delivers Refresher Tutorials to their trained users focussing on simulated attacks, current events in security and interactive questions in order to avoid rehashing past materials.

This is designed to be an adaptive process responding to threats posed to, and weaknesses within, the organisation.

CUSTOMISATION

Seemingly arbitrary or vague security policies are one of the core causes of insecure behaviour. To combat this, Hut Six's training always explains the reasoning behind security policies and are tailored to closely match your organisation's specific policies. This provides users with accurate and definite actions they can take as opposed to generalised guidelines. Hut Six also incorporates their client's corporate branding into the training in order to carry the authority of 3rd party expertise whilst building an internally recognised secure culture.

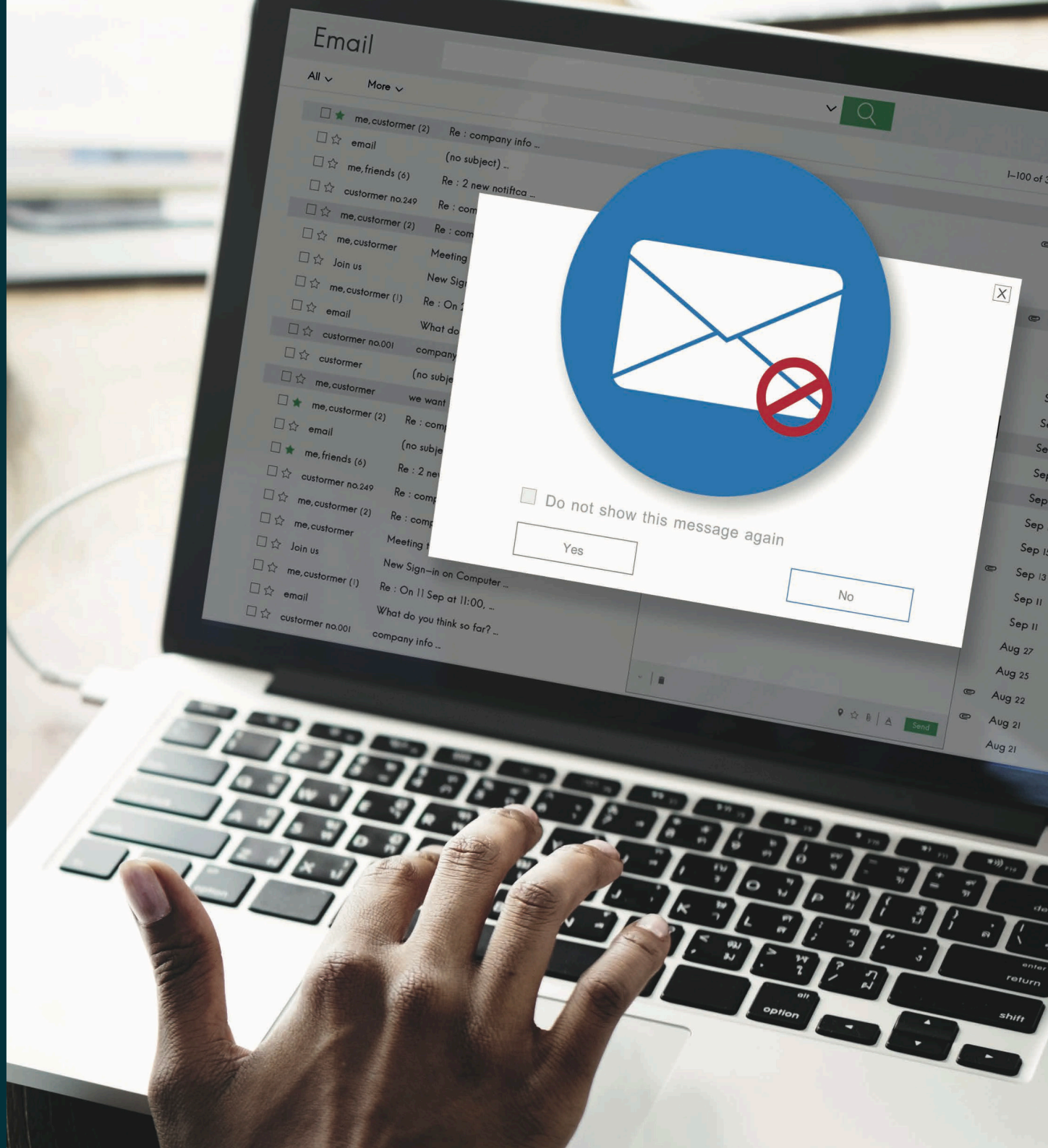
Entirely bespoke modules with custom content are available on request at additional cost.

Test

Hut Six's Phishing Simulator enables customers to create unique simulated phishing campaigns tailored to the needs of their organisations. These fake phishing emails look and read like an ordinary phishing email, however, once a user has fallen for the scam they are routed directly to on-the-spot training.

The training explains what the user did wrong, and what to watch out for next time.

The data that is gathered by performing these simulated attacks can be very valuable. Users and departments who are the most vulnerable to phishing attacks can be identified, as well as which types of phishing attacks are particularly effective against the organisation. This gives IT teams the information they need to target their training efforts and help users in particular need of additional training.



SCHEDULE YOUR CAMPAIGN

Select the duration of the campaign and the times of day the phishing emails will be sent to your employees. Our system will then randomise delivery across your workforce.

CRAFT YOUR EMAILS

Choose from our range of phishing templates and customise them with images and branding to have the greatest impact for your particular organisation. Include attachments and links to gather more data.

TARGET USER GROUPS

Target different users and groups with attacks tailored to their behaviours and performance in past training. Adapt these groups as the campaign progresses to comprehensively train your organisation

CREATING A SIMULATED ATTACK

A simulated phishing attack consists of three pieces of content that are configured for each attack: an email template, a webpage designed to extract personal information from the users, and an on-the-spot training module highlighting where the errant user went wrong.

The managers of your security awareness campaign will be able to configure these settings and work with the Hut Six team to identify the best form of simulated attacks to test your user base.

The platform has the flexibility to vary which user groups are involved in the phishing campaign; which types of phishing attack are used; how many emails and type of attack are sent to each user; and the range of dates/times in which the emails are sent.

Once planned and activated, the campaign will automatically execute on the chosen dates.

EMAIL TEMPLATING

Email templates can be selected from a range of custom templates, with the potential to design your own bespoke spear-phishing emails.

These templates mirror the most effective phishing tactics employed in real-world attacks with customisable attachments, images, HTML and user information, such as the user's name and email address.

A preview panel demonstrates how the email will look once sent.

ON-THE-SPOT-TRAINING

If a user is caught out by a simulated phishing attack, they are automatically taken to a tutorial designed specifically for that simulated attack.

The tutorial will explain how the user could have spotted that it was a phishing email/web-page.

If a user successfully navigates the phishing emails they are congratulated at the end of the campaign, reinforcing that positive behaviour and clarifying exactly why they were right or showing the indicators they might not have identified.

PHISHING WEB-PAGE

The phishing web-page is an optional part of the simulated attack. It tests if the target is willing to divulge personal information to a potential attacker.

Users would reach this page after clicking on a link in the phishing email. The web-page would then present them with a form to gather the information.

For example, a simulated attack may consist of an email purporting to be from the Human Resources department, asking the user to update their personal details. The web-page would then include a form containing inputs for the user's name, address, date of birth and national insurance number; everything needed to steal their identity.

This data would not be stored or transmitted; the only information sent would be the acknowledgment that the user had completed the form.

The webpage itself will be based off a series of in-house custom designed templates. The template would allow the colours, text and images featured to be changed.

Track

At Hut Six we believe that unmeasured or untested training is a wasted investment, as such we include our Learning Management System (LMS) with our training, so managers can track the progress of departments, teams and individuals throughout the course.

Our analytics provide intelligence on the weakest topics and areas of your business, providing you with actionable metrics of where to apply to your security efforts.

As the course progresses, departments or teams can be given specific training on areas they previously performed poorly on. This enables your organisation to take an adaptive and risk-based approach to your information assurance.

LEARNING MANAGEMENT SYSTEM

The LMS collects and stores a large amount of data that is used in the generation of valuable insights into the security awareness at all levels within the organisation.

The progress of users throughout the course, the answers to the interactive questions and tasks, their responses to the phishing simulator attempts, and total use time, are all monitored.

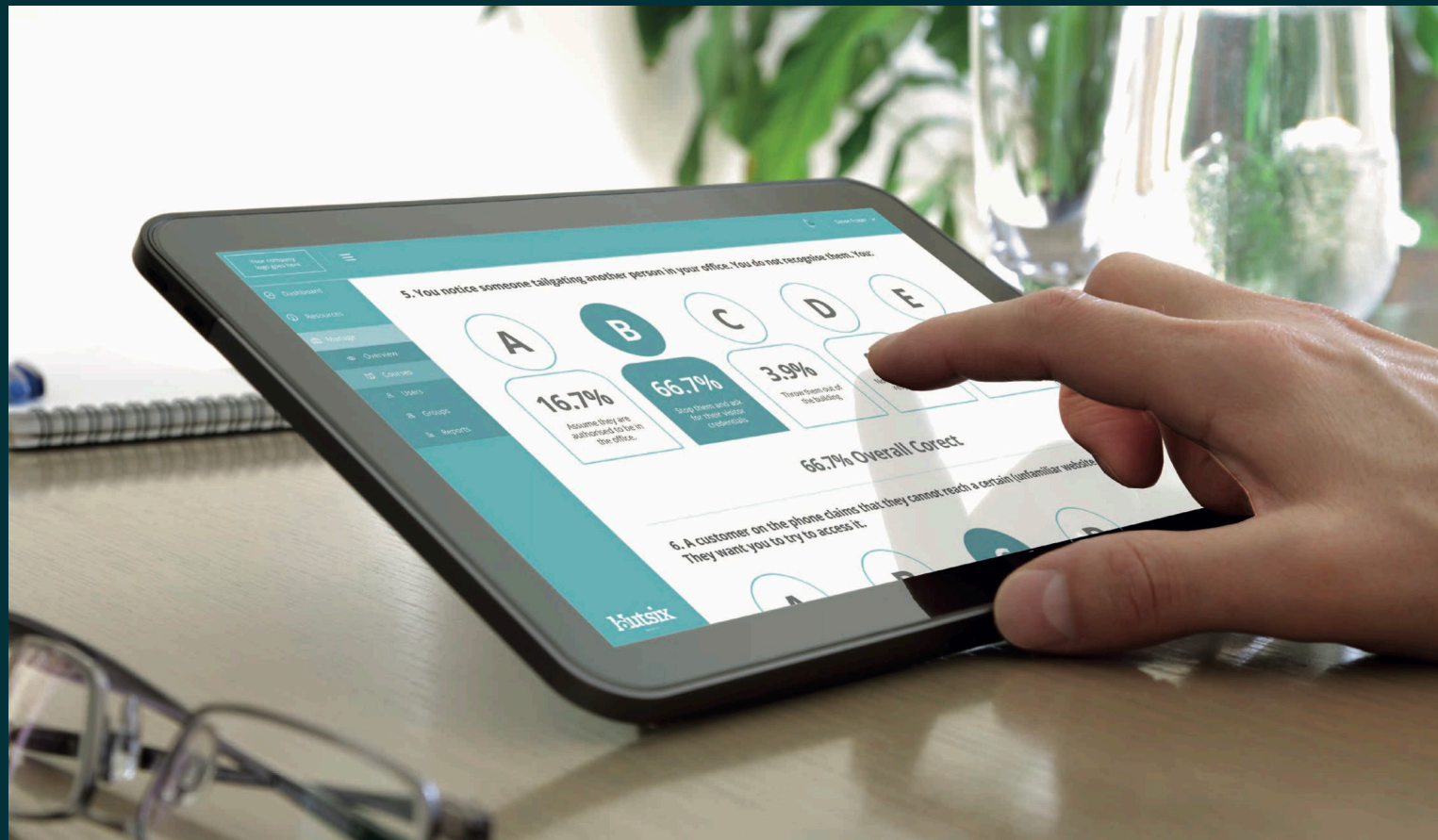
The phishing simulator tracks every stage of a phishing attack. Recording whether the users read the email, engage with the content, follow the links, open the attachments or submit data to simulated malicious web-pages.

All of this information is aggregated across the LMS to compare which forms of phishing attacks your organisation is most vulnerable to, and who is at the most risk.

The analytics are oriented around your organisation's structure, and can reveal vital information at every level. The system tracks the performance of groups of users, as well as the individual.

This allows you to see broad trends across departments and teams, as well as ensuring that struggling individuals are identified and given the help they need.

A notification system automatically brings these areas to the attention of management either through a weekly report email or directly in the dashboard. For example, if staff in Finance are performing worse than the rest of the company in the phishing exercises, this will be flagged and extra attention can be given to those users to ensure they understand how to detect phishing emails.



Supported Systems

	Internet Explorer 11	Google Chrome (Latest 2 Versions)	Mozilla Firefox (Latest 2 Versions)	Microsoft Edge	Safari
Windows 7	✓	✓	✓		
Windows 8/8.1	✓	✓	✓		
Windows 10	✓	✓	✓	✓	
Android 6+		✓			
Windows 7/8/8.1/10 with JAWS and/or NVDA Screen Readers	✓	✓	✓	✓	
MacOS 10.13+		✓	✓		✓
iPhone/iPad iOS 10+					✓

Hutsix

Platfform, 11 Devon Place,
Newport, NP20 4NW

Contact us today on: 0330 223 0182
or visit us at hutsix.io