ideal Your strategic Healthcare IT Partner

Security Awareness Training and Simulated Phishing Managed Service

The use of phishing emails to propagate malware and ransomware is on the increase, primarily due to the high success rates they yield. Traditional perimeter technical controls are no longer effective in isolation to protect organisations from these types of attacks.

Alongside more effective perimeter and endpoint technical controls, Ideal believe that the more effective way to protect your organisation is to create a human firewall by educating your staff and raising general awareness on how to spot potential phishing threats and how they should be handled.

Building an effective human firewall

Our phishing awareness service takes a structured approach over a twelve-month period to help your organisation become more resistant to attacks delivered by email. Providing phishing testing combined with security awareness training provides ongoing improvements to securing your businesses.

The traditional approach of using technology to protect your organisation from email delivered attacks no longer works. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

The best way to protect your organisation is to create a human firewall by educating your staff and raising general awareness in relation to the origin of an email and how it should be handled.

The Managed Service from Ideal takes a structured approach over a 3 month, six month or twelve-month period to help your organisation become more resistant to attacks delivered by email. To do this we offer:

- *Baseline Testing:* we provide baseline testing to assess the Phish-prone™ percentage of your users through a simulated phishing attack.
- *Train Your Users*: on-demand, interactive, engaging training with common traps, live demos and new scenario-based 'Danger Zone' exercises
- *Phish Your Users:* fully automated simulated phishing attacks, personalised to your Trust by Ideal
- *See the Results:* enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management

Providing phishing testing combined with security awareness training provides ongoing improvements to securing your businesses.

With our managed phishing testing and user awareness service, organisations can identify their exposure to phishing, offer relevant awareness training and measure its effectiveness with ongoing testing and training.

ideal Your strategic Healthcare IT Partner

The system demonstrates ROI

Helping our customers train their employees to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks dramatically reduces the number of security breaches. The combination of web-based training and frequent simulated phishing attacks really works.

A structured approach

Our phishing awareness services operates over a three month, six month or 12-month period, helping your organisation to become more resistant to attacks delivered by email. Initially we offer baseline testing to assess how phish-prone your organisation is to this type of threat sector.

Once we have established your baseline, we work closely with you to offer on-demand, interactive and engaging training. In parallel, we agree tailored simulated phishing attacks which are relevant to your Trust and manage this process seamlessly from testing, through testing and retesting.

We provide monthly metrics detailing the results of the campaigns as well as improvements in security awareness giving visible evidence of the value of the training to your organisation.

Service introduction

Ideal provides phishing exposure and awareness training which is designed to be a sustained phishing campaign inclusive of training modules for a 3, 6 or twelve-month period. The solution comprises emails to be sent monthly or bimonthly basis, metrics following every campaign (including openers, link-clickers, PDF-downloaders, data-inputters and overall phishing click percentages) and targeted training that will reduce your overall risk through user awareness.

Don't think that we need the below at this stage, below is an example of a standard engagement:

Stage 1 Deliverables:

- On-boarding, including user importing and defining logical user groups
- Set up test for SMTP whitelisting
- Initial quarterly planning
- Agree training enforcement & modules to be associated with clickers for each campaign
- Define campaign in systems and start the process

Stage 2 Deliverables:

- Monthly phishing exposure risk report
- Monthly awareness training report (who's started /not started/completed the training)
- Quarterly user update for starters/leavers
- Define 1 new phishing template per month
- Define 1 new landing page template per month

Get in touch:

Tel: 01483 453 508/0113 360 7550
Email: info@idealts.co.uk
Web: www.idealts.co.uk

ideal Your strategic Healthcare IT Partner