SOUNDNETWORKS
soundnetworks.net

PHISHING AWARENESS

POWERED BY: THINK MARBLE

WHAT IS PHISHING?

Phishing emails are fraudulent attempts to steal information or infect the computer you are using with malware. An important way to protect yourself is to learn how to recognise a phishing email attempt.

Those easiest to spot pretend to come from sites, services or companies that you don't recognise nor have accounts with.

Harder to identify emails appear to come from well-known organisations that you may have an account with. They often ask for a range of information, from usernames and passwords, to credit card numbers or other useful information.

The most sophisticated attempts will utilise personal information, lending them much more credibility.

HOW DO CRIMINALS STEAL INFORMATION?

In order for internet criminals to successfully 'phish' your information, they would usually direct you to a fake website that resembles the original.

This is often done by providing a 'link' within the phishing email that they want you to click. The fake site would then prompt you to enter additional data.

91% OF SUCCESSFUL DATA BREACHES STARTED WITH A PHISHING ATTACK

HOW CAN THINKMARBLE HELP?

We have partnered with the world's most popular integrated platform for Cyber Security awareness training combined with simulated email phishing attacks, with over 14,000 customers.

If you are serious about protecting your business from an almost inevitable hacker attack, this is something you need to do today.

SERVICE FEATURES

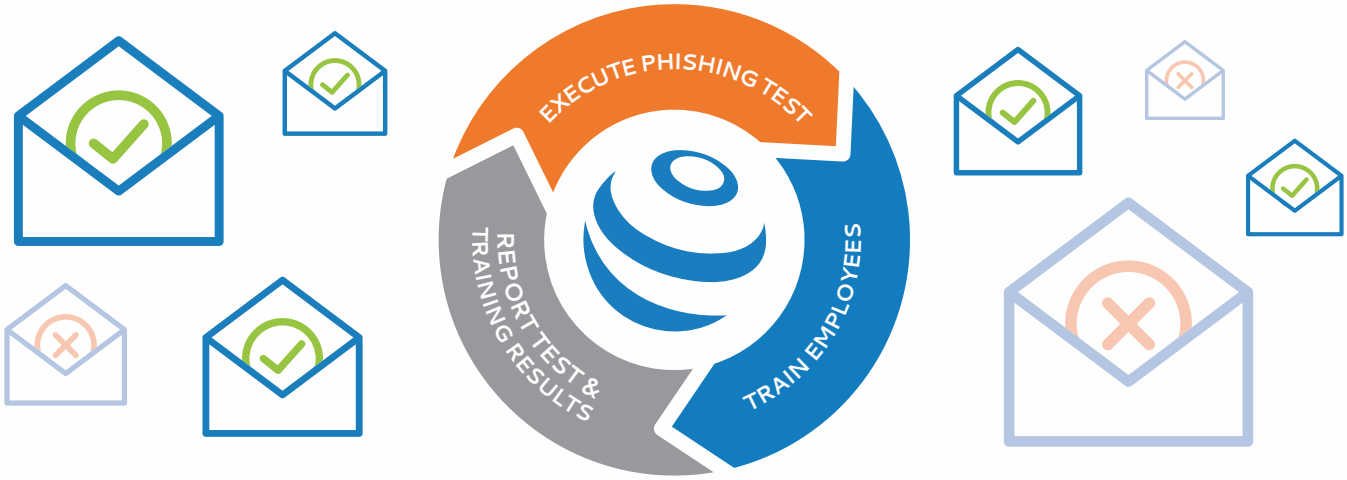
- Engaging awareness materials and resources
- Templates mimic prolific phishing attacks
- Bespoke communications and phishing templates
- Whale & Spear phishing assessments
- 10,000 existing customers
- World's most popular simulated phishing platform

SERVICE BENEFITS

- ☑ Train employees in a positive and encouraging manner
- ☑ Analysis of risk level and weak spots within your organisation
- ☑ Learners able to identify and mitigate phishing attacks effectively
- ☑ Comprehensive audit trail to assist in compliance of standards
- ☑ Full online fun and engaging training material
- ☑ Monitor improvements and quantify campaign effectiveness
- ☑ Promote a measurable improvement
- ☑ Heightened awareness of phishing attacks

networks@soundm.com | 01225 701650 | www.soundnetworks.net

PHISHING AWARENESS



1 BASELINE SCOPING

An initial scope discussion will provide a baseline understanding of the phishing awareness within your organisation, and the key performance indicators required. This will enable us to create an appropriate campaign plan and schedule.

We will leverage existing resources such as existing suppliers, corporate contacts, and internal departments to provide realistic looking emails.

2 CREATING THE CAMPAIGN

Following on from the scoping discussions, we will craft tailored, targeted, and authentic looking emails that purport to be from recognised sources. This is the same approach taken by phishing attackers.

These emails will attempt to entice users to click links to associated websites. They will have a similar appearance to their genuine counterparts, but will solely be used to try and capture user credentials.

3 GONE PHISHING

Our analysts will start the campaign according to the agreed schedule and frequency. This will usually take between four and six weeks. The users on your recipient list will then start receiving emails. The progress of the campaign is then tracked by our analysts with staged reporting. Review discussions will be completed as necessary.

4 REPORTING & RECOMMENDATIONS

We will produce a series of reports for you that will break down how your staff are interacting with the campaign. These will comprise:

- **Weekly Reports:**
  Information provided includes the number of emails sent, delivered and clicked (including number of clicks).
- **Final Report:**
  This comprehensive report allows you to highlight specific areas in your organisation which would benefit from further training.

networks@soundm.com | 01225 701650 | www.soundnetworks.net