BOXPHISH

Practical Advice For Your Cyber Awareness Training Programme

1. Define your why

Before implementing an ongoing cyber security awareness training programme, it is important to consider your why and then communicate this internally. Gone are the days where a training programme was implemented for compliance or regulation reasons. The current stats on “successful” cyber-attacks cannot be ignored.

1. 95% of successful cyber-attacks are a result of human error
2. 74% of cyber-attacks start in the inbox
3. The education sector is the 2nd most targeted sector for Ransomware with the average cost ransom demand now over £165,000

The threat from cyber criminals is here to stay and the human element needs to be considered, indefinitely, end user education and awareness should make up a key part of your defence posture.
Considerations for your why

1. Protect your technology and digital assets from cyber criminals
2. Demonstrate to all your stakeholders that you take data and cyber seriously and you ensure you have the correct measures in place to reduce your risk
3. Keep your people safe from cybercrime, identify, mitigation and reporting are key to remaining safe and educating end users with practical advice will really support this

2. Positioning is key

When communicating an ongoing cyber training programme to end users the positioning is key, try stay clear from terminology such as workplace learning, the goal for a programme is to want your end users to take the time to complete the modules because they see value in it, not because they are prompted or asked to.

A good way of increasing end user buy in is taking into consideration the best practise on spotting scams, setting strong passwords, and working remotely safely can have as much of a positive impact on their personal life as they can on the work life, this should not be ignored – skills for life is a good way to position this.

Net-Ctrl

Practical Advice For Your Cyber Awareness Training Programme

3. Assign an Executive Sponsor

Even with best efforts from both your internal IT team and your Cyber Security Awareness Training Vendor it is always good practise to assign an executive sponsor that is the internal voice of the programme. A quarterly reminder of the importance or a bulletin on recent attacks in your sector or region can help to reinforce and renew engagement of the programme.

4. Provide clarity

We do not want to shock an end user, upfront communication is key, send internal communication before the first course assignment, any reputable Security Awareness Training provider can help with this. Consider including in the communication when the first course can be expected and what it will look like can be useful to include.

Decide whether you want to as part of the initial positioning communicate that both testing (simulated attacks) and regular, bite sized training is part of the programme. Remember regular testing is not designed to “trap your end users” it is to provide insights to you on where high-risk areas are in your ecosystem, this could be sites, departments, or users.

5. Make it easy for your end users

When selecting a Cyber Security Awareness Platform, ensure that courses can be delivered via email, ideally single sign on (SSO) would be an inherent feature and reminders are enabled to remove any barriers to take the programme

BOXPHISH

Practical Advice For Your Cyber Awareness Training Programme

7. Consistency is key

"For changes to be of any true value they've got to be lasting and consistent"

Delivering a consistent and regular programme is so important for many reasons:

1. You can educate on real time threats
2. The best practise remains front and centre of mind
3. Behaviour changes only happen when a regular cadence is adopted, simply put there is a high risk of people forgetting to adopt good practise if not regularly "nudged" to do so

Before investing a cyber security awareness platform, consider, are we purchasing a tool kit or a platform that provides an outcome? If a tool kit, do you have internal resources to ensure the programme can be delivered month in month out.

We hope the tips within this document provide value to anyone looking to embark on educating their users how to stay safe in their digital lives. Should you have any questions or want to explore how Boxphish may be able to help please contact hello@boxphish.com

68% increase in Phishing on Edu in last 12 months

30% of Edu sites have been infected with **Malware**

14% of global Phishing is aimed at Office 365 account takeovers

Edu considered **high profile** due to media exposure

More than **35%** of leaders think their site will suffer a cyber breach in the next **12 months**

Over **90%** of Cyber Attacks involve Staff Error

Net-Ctrl