tdmgroup
we make IT possible

Phishing Attack Simulator Service

Strengthen your business against the next cyber attack

The TDM Group Phishing Attack Simulator service works as a positive and proactive security awareness system to help staff safeguard your company's infrastructure and data.

Protecting corporate assets from a rising tide of malicious emails

While your employees are undoubtedly your most valuable resource, they are also a magnet for cyber attacks. Scammers and spammers have become experts at tricking your team by masquerading as legitimate business contacts. Spoofing – the forgery of an email header to look reassuringly familiar – is surprisingly easy.

Cyber criminals have become experts in obtaining sensitive and significant business information. They use techniques ranging from generalised phishing to customised spear-phishing scams that incorporate convincing personal details, to going after the 'big fish' by targeting high profile senior executives in so-called whaling attacks.

Phishing - using your employees to compromise your network

Phishing involves using psychological manipulation to steal user data, including login credentials and credit card numbers. Masquerading as trusted entities, attackers dupe their victims into opening an email or message. Clicking a malicious link then activates malware, freezes the system as part of a ransomware attack or discloses sensitive information.

Phishing frequently provides a foothold in corporate or governmental networks, to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. The consequences range from severe financial losses to reputational and brand damage.

Email phishing is a numbers game

For a phishing campaign to be successful, it's enough to trick a small percentage of targeted recipients. Cyber criminals go to great lengths to mimic the corporate identity of legitimate emails, using apparently genuine phrasing, typefaces, logos and signatures. They will try to create a sense of urgency to encourage recipients to let down their guard: an email may threaten account expiration or – ironically! –alert them to bogus activity on their account.

Links inside messages resemble their authentic counterparts and a cursory glance may not always spot misspelled domain names or extra subdomains.

IT'S TIME TO FIGHT BACK!

TDM Group will help you reinforce your email defences, and assess how quickly employees can spot a suspicious email and figure out whether it is genuine.

Cyber Security Testing Campaigns

We will be testing your employees' digital security awareness and susceptibility to social engineering tactics, as well as their resistance to phishing, credential harvesting or malware attacks, by periodically emulating basic and advanced phishing attacks. This will help them to identify real-world scams and keep them alert with six customised testing campaigns throughout the year.

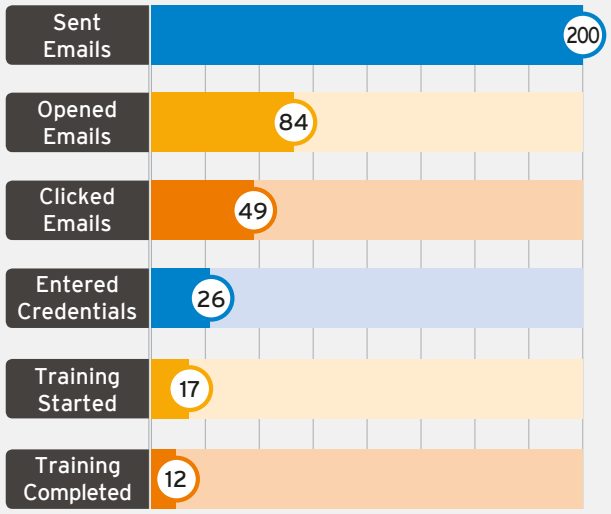
Effective Security Awareness Training

Anyone failing the assessment will be provided with on-the-spot security awareness training. The training modules are designed to educate staff about specific threats such as suspicious emails, credential harvesting, password strength and regulatory compliance, all in an informative and engaging way.

Comprehensive and Automated Reporting

You'll receive reports on results by department, group or individual users, as preferred. These reports equip you with insights into individual performance and an understanding of just how resilient – or not – your business is in the face of increasingly sophisticated attacks.

The discovery phase of a TDM Group phishing attack simulator campaign identifies and quantifies employees' readiness to interact with bogus emails.



Contact us for email user security training

0808 129 22 99 | hello@tdmgroup.net | www.tdmgroup.net