

Social Engineering





What Is Social Engineering?

High Value Targets (HVTs), such as department heads, decision makers, those with access to company accounts and C-Suite staff are all much higher on a hackers list of targets than other organisation members.

For this reason, social engineers (hackers) spend huge amounts of time and energy researching these targets to find their potential weaknesses so they can exploit them in complex spear phishing campaigns.



Fully managed social engineering project

Using the information our social engineering team collate from various sources, we create fully managed spear phishing campaigns targeted at the agreed individuals or groups.

All areas of the campaign are managed by Phishing Tackle.



Bespoke reports and training

Once the campaign is complete and measured, Phishing Tackle will provide you with a suite of reports, detailing all interactions with our spear phishing emails and providing insights into potential threat blindspots.

We can then recommend a bespoke course of training for the individual or group to address their specific weaknesses in cyber awareness.



How can Phishing Tackle help?

All organisations have High Value Targets (HVTs). Social engineers find these users and exploit their weaknesses using emotional triggers.

Phishing Tackle's social engineering service uses our team of ethical social engineers to find the digital footprint of your HVTs. Whether it's from a list of users provided by you or those we've found and deemed to be threats using a black box approach.

Once we understand the threat they pose to your organisation, we launch authentic, targeted spear phishing attacks. Just like the bad guys.

Benefits

- ✓ Understand what threat your users pose to your organisation.
- ✓ Test your HVTs at the highest level possible.
- ✓ The next step up from Phishing Tackle's managed service.
- ✓ Relax knowing your users are trained to higher levels of security.
- ✓ Your users will understand their own digital footprint and how to reduce it.
- ✓ Highly targeted spear phishing campaigns from ethical social engineers.
- ✓ Full report detailing areas of weakness and what available data each user has online.
- ✓ Learn exactly what a social engineer knows about your organisation's HVTs.

Over 90% of all data breaches start due to a spear-phishing attack.

Understand the process of our Social Engineering Service



Target Acquisition

For any social engineering campaign to work effectively, it must first have a clear, defined target (or group of targets). These targets can be selected using two methods:

White box method - You provide Phishing Tackle with a specific user, or group of users, for our social engineering team to target.

Black box method - You authorise Phishing Tackle to actively seek out and select a user, or group of users, to be targeted during the campaign. Both methods provide valuable insights into your organisation's security and hybrid solutions can be formed as part of the bespoke service.



Forensic Research

With targets agreed, Phishing Tackle's social engineers adopt an offensive mindset, researching the targets digital footprint. Utilising a mixture of Open Source Intelligence (OSINT), social media and information gathered from various sources, we are able to build a profile of the target.



Emotional Triggers

At the heart of a successful social engineering attack is an emotional trigger. Something that is so enticing to the target they are compelled to click. Using the target profile, we are able to determine the emotional triggers most likely to cause the target to fall for a spear phishing attack, aiding the social engineers campaign.



Exploit the weakness then strengthen it

Phishing Tackle creates a bespoke strategic spear phishing campaign, laser focused on the agreed target(s). Up until this stage, we have acted in every way like a true social engineer, without any malicious intent. Once the campaign has run its course, we provide full and granular debrief reports, detailing all interactions and responses to the emails.

We then provide customised training courses designed specifically to strengthen any areas of weakness demonstrated by the targets.

Who are your high risk users?

Find out free at <https://phishingtackle.com/click-prone-test>