ZERODAYLAB®

Social Engineering: Criminal Tool of Choice

Social engineering has evolved quickly to be one of, if not the most effective tools in a cyber criminal's toolbox. Is your business truly prepared to protect against this ever-evolving threat?

63% **of breaches caused by data disclosure ***

54% **of cyber incidents caused by Phishing ***

Your Business's Number One Threat

Disclosure of data is by far the most common type of security incident reported to the ICO and phishing is still overwhelmingly the most common type of attack method used; both are intrinsically linked to Social Engineering.

The significance of social engineering continues to grow, driving more sophisticated and more successful phishing (email), vishing (phone), smishing (SMS) and physical attacks.

The Impact on Your Business

Attackers increasingly use psychology and predictable human behaviour to manipulate employees, either to carry out actions or divulge information that ultimately lead to;

- ⚠ Execution of malicious software
- ⚠ Theft of personal data
- ⚠ Hijacking of accounts
- ⚠ Processing of illegitimate payments
- ⚠ Significant operational disruption
- ⚠ Loss of revenue & damage to brand reputation
- ⚠ Potential for large fines

Find out how ZeroDayLab can help you combat the threat of Social Engineering

* https://ico.org.uk/action-weve-taken/data-security-incident-trends

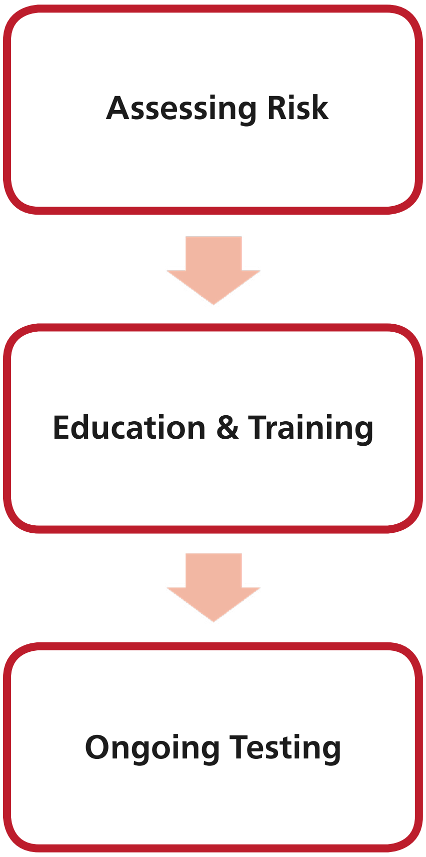
ZERODAYLAB®

Assessing Risk, Education & Training, and Testing

Social Engineers are increasingly combining sophisticated psychological techniques to manipulate predictable human behaviour, through pretexts that play on likability and empathy, and that build trust through authority and credibility. Building this trust is key to their success. Being able to identify when this is happening is even more key to protecting your business.

Empathy **Authority** **Credibility** **Likability**

How at risk are we? And how can I demonstrate return on investment? We are frequently asked these two questions. ZeroDayLab's approach to social engineering, including risk assessments, education & training, and ongoing testing will allow you to understand risk, drive cultural change and prove return on investment (ROI).



It is essential you gain a robust understanding of your cyber threats and direct efforts in the right areas. Only then can you put controls in place that are proportionate to your risk and that maximise ROI. ZeroDayLab is a world leader in identifying, quantifying and managing cyber risk, through services such as Threat Intelligence, Open Source Intelligence, Policy Reviews, and Social Engineering Resilience Programmes.

Our award-winning Education & Training is unique in the market, that drives behavioural change and reduces human error. We are proud to train some of the largest training providers in the world. Our Security Awareness courses are tailored to your business's threats and risks, whether that's by attack vector or business function. The result is engaging, high impact training that is targeted for maximum ROI.

Businesses need to regularly test their resilience to social engineering. This is partly so that you can measure improvements made as a result of your training but also because the threat is ever-evolving. ZeroDayLab carry out highly sophisticated simulations of cyber attack, using the most up to date techniques, to test your controls in a real-life setting. This could include phishing, vishing, smishing or physical attack scenarios.

To find out how we can help you protect your business from social engineering, contact us today on:

Tel: +44 (0)207 979 2067 Email: info@zerodaylab.com www.zerodaylab.com