Physical Social Engineering & Red Teaming

THE ANTISOCIAL ENGINEER
An Ultima Company

What is Physical Social Engineering?

The fake IT guy - this is where a hacker shows up at your workplace pretending to be an IT technician, there to check a computer, server, printer or other network device. Many smart devices automatically 'cry for help' when they need maintenance, which gives these kinds of attacks plausibility.

Tailgating - tailgating is where an unauthorised person follows an authorised person into a secure area. This happens naturally when multiple people pass through doors. The person at the front swipes an ID card or taps in a code and the person behind follows through the open door, entering the area without having presented any kind of identification.

How aware are your employees and security teams of the risks of a physical social engineering attack? Are they ready and equipped to avoid them? Do you have an effective training program in place?

What to Expect

Our social engineering assessments simulate realistic attacks that reflect the risks posed to your organisation. We conduct an extensive online examination to gather data that will later be used to explore common attack vectors, such as phishing and malicious onsite access.

No two assessments are the same and our priority is meeting the requirements of our clients. You will be in total control, every step of the way.

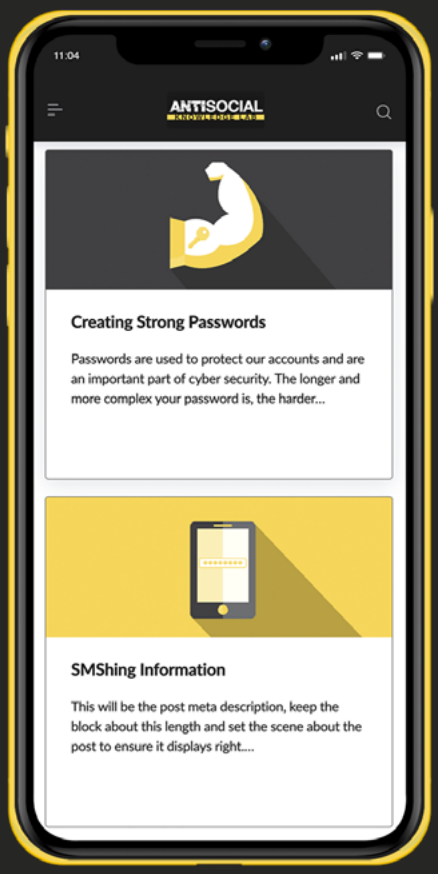
This is our most intensive assessment that aims to give an organisation a real insight into their security defences.

- IN-DEPTH RECONNAISSANCE
- PHISHING/SPEAR PHISHING
- AUDITING
- DEVICES
- USER PROFILING
- VISHING
- COMPLEX FRAUD SCENARIOS
- TAILGATING
- IMPERSONATION
- DISTRACTION TECHNIQUES
- DUMPSTER DIVING
- LOCK PICKING
- SMSHING
- WIRELESS NETWORK
- ROGUE NETWORK
- RFID KEY CLONING

THE ANTISOCIAL ENGINEER
An Ultima Company

Learn More

theantisocialengineer.com
ultima.com



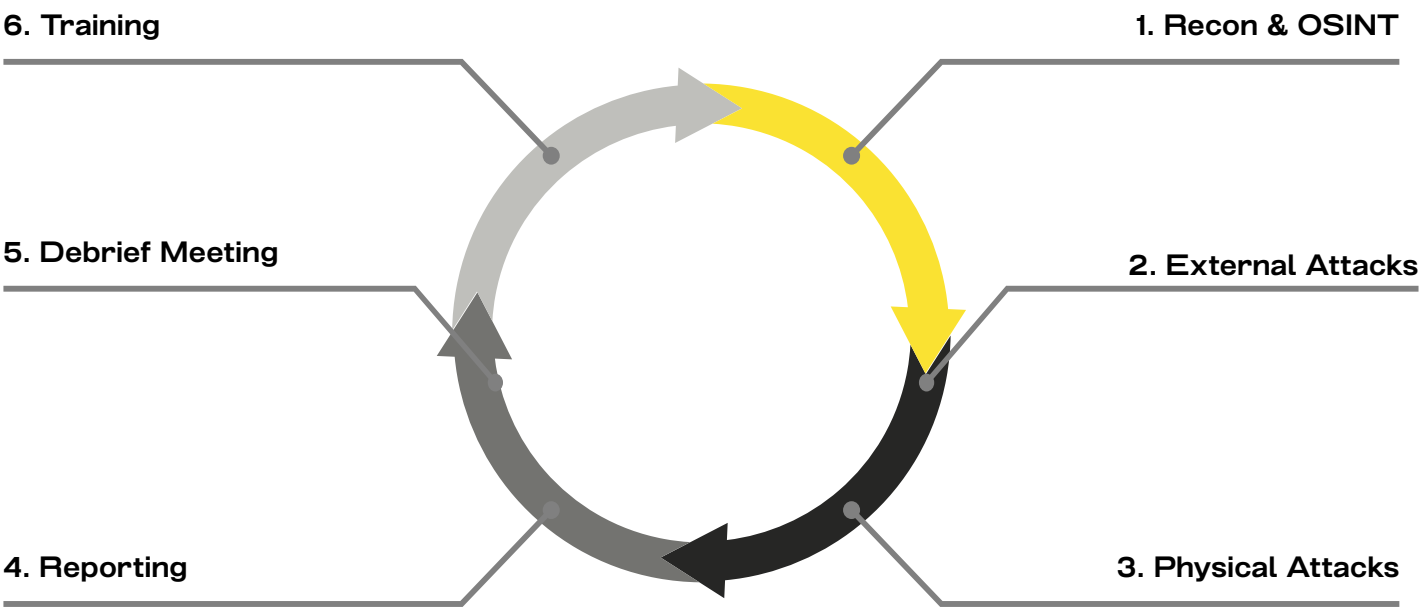
Deliverables

We provide in-depth, comprehensive reports authored by our principal consultant and social engineering expert. Our reports stand out from the crowd and offer breakdowns on remediation, findings discovered during the assessment and technical reporting. Raw data can be provided in CSV, XLSX and JSON format to facilitate further analysis.

It is vital after the test that the report is able to portray every piece of information discovered in a clear, concise manner. All reporting is dispatched using secure, encrypted transfer mechanisms.

GATHERING EVIDENCE THROUGHOUT
As we conduct our Social Engineering Assessments, we collate all aspects of the information gathered. Starting with the data we find from online OSINT, manuscripts, recordings of phone calls and photographic evidence of the physical engagement are all transferred in technical appendices to the report. All evidence gathered is transferred, so your

Our Process



THE ANTISOCIAL ENGINEER®
An Ultima Company

Learn More

theantisocialengineer.com
ultima.com

Legal Processes

ENGAGEMENT PROCESS
We set up an initial meeting to discuss the requirements of the planned assessment and scope of works, and put in place an agreement prior to commencement of the engagement. Safe transfer of files is then arranged between organisations, always prioritising your data handling requirements.

SCOPING
With every new customer we work on a 'scoping' document that will ensure we work using only agreed methods. We use our experience in social engineering to ensure the client is always in control at every step of the journey.

OFF-BOARDING PROCESS
A technical debrief will be available and is included as standard following delivery of the report, explaining key findings and potential business risks of any issues found. This will include suggested priorities for the customer to take action against. We delete sensitive data after 14 days.

CUSTOMER RESPONSIBILITIES
This service has elements that involve The AntiSocial Engineer's consultant(s) alempting to gain 'perceived' unauthorised physical access to buildings and offices. Therefore, it is the customer's responsibility to ensure that in the event that a consultant is successfully challenged they are able to demonstrate (via both a valid letter of authority and personnel contact details for the duration of the exercise) good reason for their activities.

The AntiSocial Engineer: Capabilities

ANTIPHISH
STOP · THINK · PROTECT

AntiPhish Phishing Prevention combines educational phishing campaigns with a realistic experience.

ANTISOCIAL
KNOWLEDGE LAB

A combination of eLearning, printed assets, communications, technical knowledge transfer sessions and educational offerings.

ANTISOCIAL
BLOCKLIST

AntiSocial Blocklist can tell if domains are likely to be used for social engineering - before an attack.

STAFF VETTED TO BS7858, GDPR AND INDUSTRY BEST PRACTICES ADHERED TO.
We do everything we can to keep your people and data secure.

ABOUT ULTIMA
Ultima offers over 30 years of world class technical expertise to UK businesses. We specialise in providing solutions, end to end managed services, in-house development and innovation in today's business critical areas of Cloud, Security and Digital Workspace. Our acquisition of The AntiSocial Engineer in 2022 supports our purpose and mission to deliver on reputational and revenue growth for our clients.