ABOUT US

Risk Crew is an elite London-based, information security governance, risk, compliance and testing consultancy. Experts in the cyber threat landscape, we excel in creating cost-effective controls and processes to meet these threats and comply with legislation, regulation and best commercial practices. We also put skin in the game and provide a 100% satisfaction guarantee on all our services. **Put us to work for you today.**

CONTACT US

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom
+44 (0) 203 653 1234
information@riskcrew.com
www.riskcrew.com

risk crew

SOCIAL ENGINEERING TESTING

Service

SERVICE

Real world attack simulations

Social engineering is the art of exploiting human nature to obtain unauthorised access to sensitive information, systems or facilities.

Risk Crew will design and deliver a series of customised social engineering exercises to test, measure and document your business' exposure to this real and critical threat. Simulated attacks will be based upon current threat vectors, methodologies and payloads. Attack sophistication, targets, objectives and timelines will be agreed in advance to ensure results serve your risk objectives.

"There is no technology that cannot be defeated by social engineering"

Frank Abagnale

METHODOLOGY

People, Process & Technology

Simulated attack methodologies shall be determined based upon your specific risk objectives, however, include attempts to identify and exploit vulnerabilities in your people, process and technology.

Attacks shall be designed based upon data collected in surveillance and through open source intelligence gathering techniques. A typical test is comprised of a combination of physical, remote or hybrid attacks which may include covert device placement, phishing, catfishing, telephone pretexting, smishing, vendor scams, road apples, piggy backing VoIP or RFID spoofing depending upon the stated objectives.

DELIVERABLE

Measurable results

The service results in a detailed report of our findings and recommendations to improve your defences against this type of attack. Report shall include all photographic, video and audio evidence collected during the attacks along with suggested key performance indicators for implementation to monitor and measure improvement. Risk Crew will also present the testing results in an interactive workshop with your stakeholders to ensure their understanding.