Phishing, Vishing & Smishing (Social Engineering)

Employees are your frontline defence against the threats you and your organisation face. Whether it is voice, email, text or face-to-face, a successful social engineering attack can lead to an immediate compromise of your business. At NCC Group, we offer a suite of services to identify your susceptibility, improve your resilience and measure your improvement.

The consequences of a successful social engineering attack could be catastrophic, and it won't just be your bottom line that suffers - it will also be your reputation.

In 2022 83% of breaches used phishing as the attack vector. But phishing isn't the only threat. Attackers will use any and all means of social engineering to further their goals.

NCC Group offers two categories when carrying out social engineering assessments: Measurement and Improvement. We run assessments to measure your current exposure to different types of social engineering attacks and improvement packages to measurably reduce your organisation's susceptibility to such attacks.

All NCC Group social engineering engagements are run by our dedicated social engineering security consultants.

Services

Phishing:
Email-based attacks that target password capture, malicious file attachments, browser exploits and data exposure.

Vishing:
Call-based attacks exploiting caller ID spoofing, policy review, multi-factor authentication bypass and other data exposure.

Smishing:
Text-based attacks that target password capture, multi-factor authentication bypass and other data exposure.

Determine your current susceptibility to social engineering attacks through simulation.

Improve your staffs awareness and resilience to modern social engineering attacks.

Demonstrate your organisation's improvement through measurable output from assessments.

Phishing

It can take as little as 1 minute 29 seconds for an organisation to be breached by a phishing attack, with over 22 per cent of employees falling victim. But can you tell the difference between a legitimate email and a phishing email? What about your employees? Do you think they would be able to spot a phishing attack? Knowing how to spot the signs is vital.

The hoax websites used by cyber criminals are a lot more sophisticated than in previous years, so it is not surprising that more people are getting caught out.

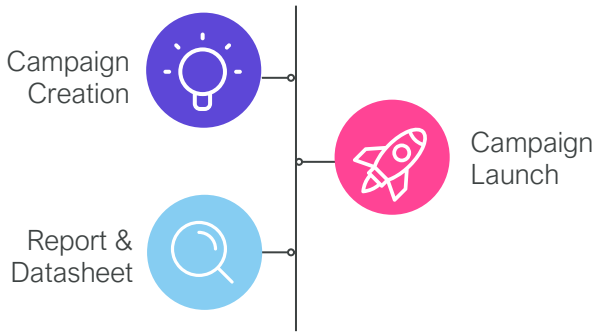
Furthermore, our own research suggests that such websites are becoming a lot harder to spot with some 70% of employees at large organisations unable to tell a legitimate website from a phishing site.

Our campaigns are custom built with you to ensure we replicate your threat actor's capabilities. Whether they are simplistic "spam" or advanced targeted attacks, the campaign will be designed simulate your threats.

Single Campaign

Single campaigns are run to understand your current susceptibility to email-based social engineering attacks. The output of this assessment provides you with comprehensive details of where precisely in your organisation you are most vulnerable.

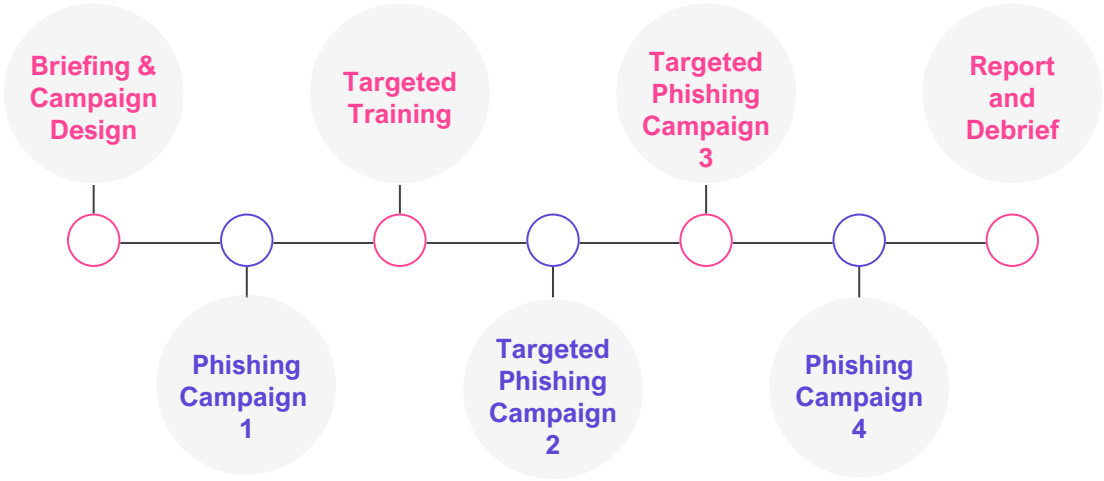
Each assessment includes a report with identified vulnerabilities, recommendations and details of the campaign. A datasheet is also provided with a time stamped account of every significant action carried out, from campaign launch to password capture / attachment opened.



Phishing Improvement Package

Improvement packages are custom scoped to each organisation. They consist of a number of phishing campaigns and training workshop that gradually increase in complexity to take your staff from “general spam” phishing emails to advanced, targeted attacks. Throughout this package you are provided with reports and datasheets to measure your staffs overall improvement against phishing attacks.

The data collected from each campaign is used in the design of the next. This ensures business areas that require additional support are supported and campaigns are appropriate to improve your staffs awareness. This service allows you to outsource your phishing solution and training. Regular reporting and datasheets will keep you updated on you organisations current susceptibility to email-based social engineering attacks.



Vishing

Whilst people are becoming more aware of email-based social engineering attacks, they are far less familiar with those that take place over the phone.

There are substantially fewer protections against vishing attacks in comparison to phishing, and where spoofing email addresses is unlikely to succeed, spoofing phone numbers is trivial.

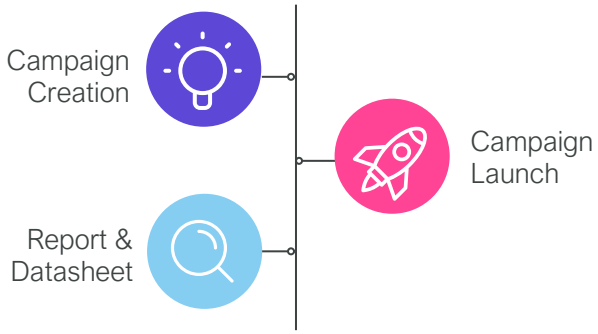
Attackers will use vishing to extract information from staff members and lead them to malicious websites where malicious software can be downloaded. Vishing is also a preferred method for bypassing multi-factor authentication. Targeting staff members using a combination of call and email attacks means attackers can create dynamic scenarios to increase their success in bypassing your security controls.

Basic Vishing

A basic vishing assessment targets your staff to determine how they handle call-based attacks. Specific objectives can be specified, or exploratory calls can be made to determine what sort of information an attacker may be able to acquire.

This service includes scenario design, client specified objectives and call ID spoofing (region dependent).

Each assessment includes a report with identified vulnerabilities, recommendations, details of the campaign and call logs.



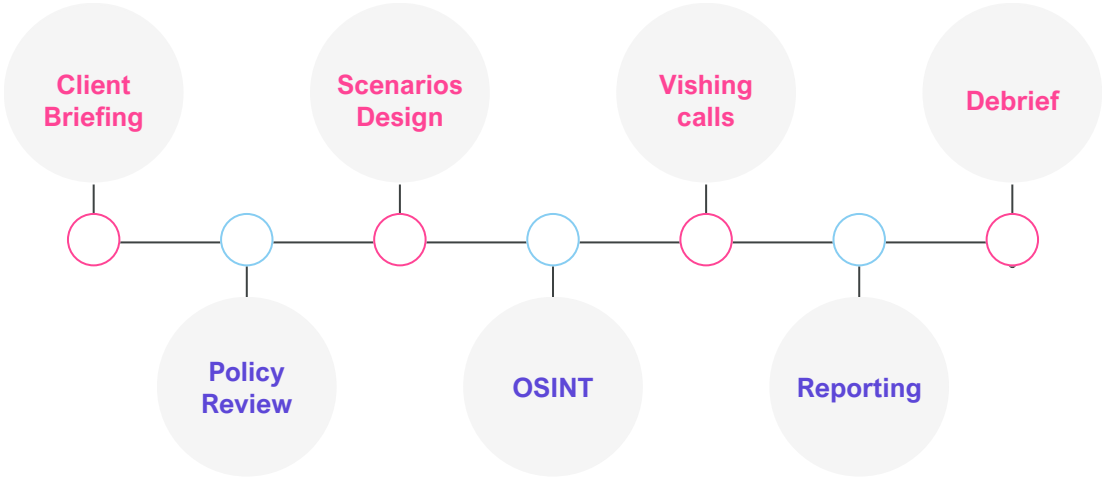
Vishing Attack Simulation

ishing attack simulations are used to determine how effective your policies, staff and online exposure are at preventing a call-based attack. It achieves this through three phases:

Overtly reviewing policies
We will review the policies and discuss with key stakeholders the policies and procedures for how staff should handle inbound calls, particularly in relation to verifying an individual's identity before carrying out actions or providing information (e.g. security questions, lockout policy, etc.).

Open-Source Intelligence (OSINT) gathering
Publicly available information will be targeted based on weaknesses identified from the policy review phase. This may include staff identity enumeration, job roles, start dates, etc.

Vishing Attack
Using the information from phases one and two, targeted vishing attacks will be carried out to evidence the vulnerabilities of the implemented policies, and the organisation's online exposure.



Tailored Solutions

NCC Group's social engineering services are scalable to suit any sized organisation. Our detailed and accurate reporting provides you with a deep insight across the different areas of your organisation to understand where you are vulnerable. We then provide the support to improve and reduce your overall exposure to social engineering attacks. For more information about AI and deepfakes, please contact us.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com