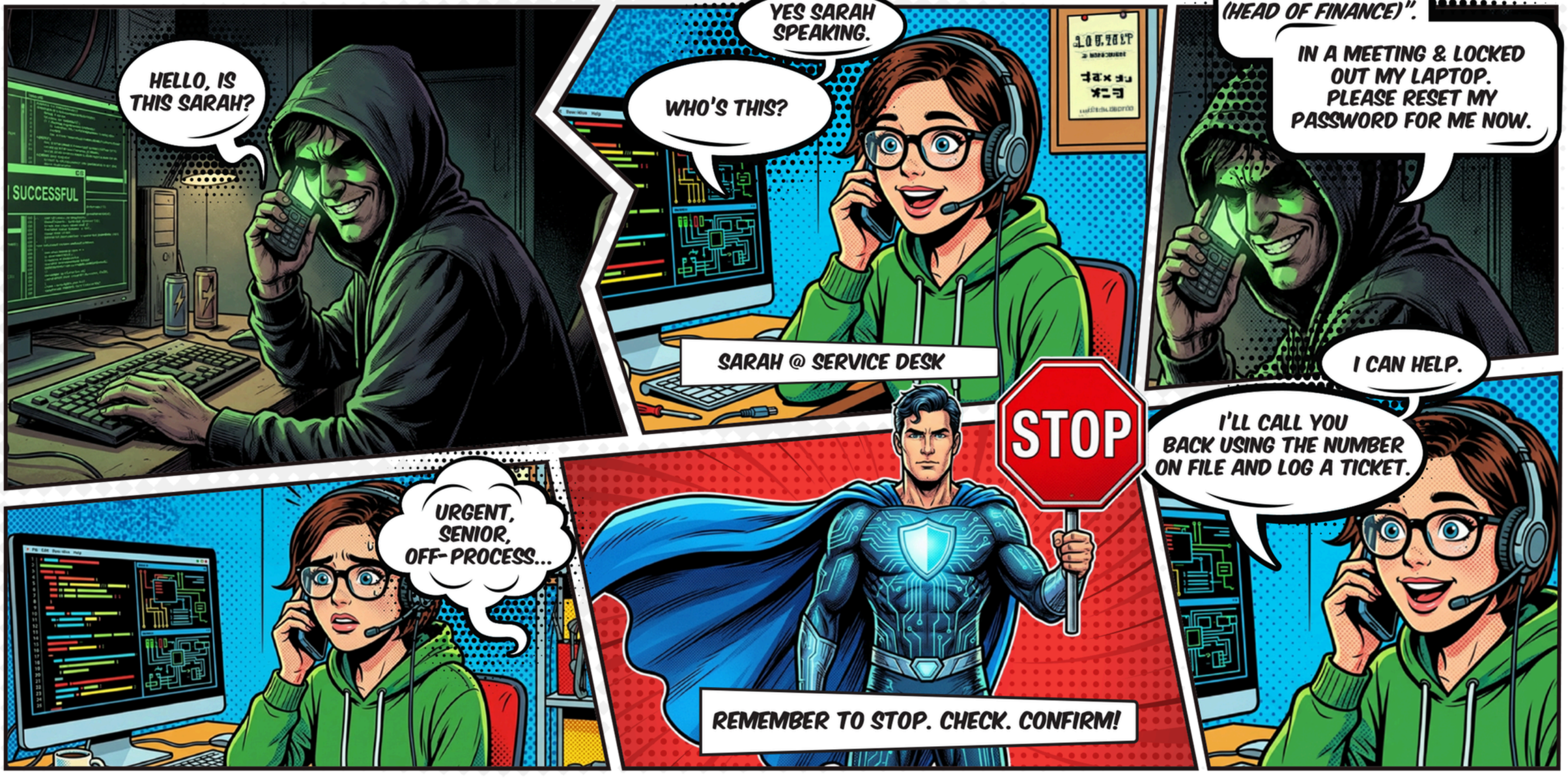
theta

VISHING SIMULATION

Test and strengthen your service desk's response to real-world vishing attacks.

STOP. CHECK. CONFIRM: THE VISHING CALL.



RESET DENIED UNTIL VERIFIED

What is vishing (in a business context)?

Vishing, or “voice phishing”, is a scam in which an attacker uses a phone call or voice message to trick employees into disclosing sensitive information, such as passwords, MFA codes, banking details, or company system access.

*442% increase in vishing activity over the past year**

Attackers are relying more heavily on voice-based social engineering to bypass technical controls.

*Crowdstrike 2025 Global Threat Report

Service desks and contact centres are prime targets

Attackers are increasingly targeting service desks and contact centres to gain access to systems, reset credentials, and bypass normal controls.

In these campaigns, attackers may impersonate employees or customers to pressure staff into resetting passwords, changing MFA settings, updating account details, or disclosing confidential information. These attacks are often multi-channel, with phone calls used as a key social engineering vector.

‘Attacks on the helpdesk’ is a focus area for security.*

This means it has been identified as a particular area of concern.

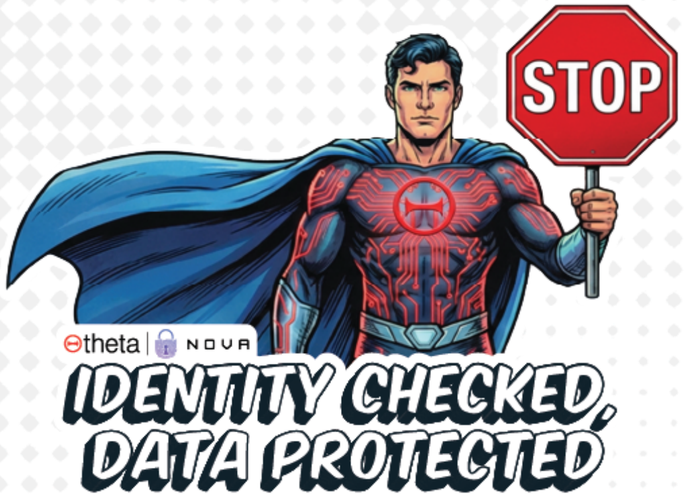
*NZ National Cyber Security Centre (NCSC), Quarter Two Cyber Security Insights 2025

What can businesses do to reduce risks?

Regular vishing simulations help to audit and evaluate your existing risk, as well as train your service desk and contact centre teams to recognise and respond to these types of vishing attacks.

As a result of a vishing simulation, you will improve your organisational vishing resilience.

The most effective approach is to make sure people know exactly how to respond when they suspect a vishing call.



How the vishing simulation works

In scope

- Kick-off workshop to confirm your existing processes and rules of engagement.
- Reconnaissance and intelligence gathering.
- Scenario development across helpdesk, HR and executive themes.
- Telephone-based social engineering simulation.
- Vishing attempts for up to 4 targets.
- Summary report and recommendations.

Approach

- Develop realistic pretexts aligned to your processes, including password resets, MFA changes and data requests.
- Place controlled calls to service desk or contact centre staff using the agreed dates, scope and rules.
- Assess the effectiveness of identity verification and escalation procedures during each interaction.
- Evaluate how staff respond to urgent, senior or off-process requests.

Stop. Check. Confirm.

is the core behaviour vishing simulation reinforces.

Many organisations already have procedures and training in place; this simulation shows whether those controls hold up under pressure in realistic telephone scenarios.

Investment

- Estimated effort: 40 hours
- End-to-end vishing simulation: $12,500 ex GST
- Joint engagement with Nova Security

Optional add-ons

- Head of / CXX deepfake impersonation
- Customised spear/whale phishing
- Follow-up security awareness training

Additional information

- The simulation covers vishing only.
- The customer grants permission for calls to be recorded for evidence and reporting.
- Recordings are securely handled and permanently deleted after the final report is delivered.
- List of users to be impersonated, if relevant.
- Latest service desk playbook, script or SOP for handling incoming calls.
- Relevant points of contact available during planning and execution.

Ready to get started?

Book a 30 minute scoping call

enquiries@theta.co.nz | 0800 4 THETA