Recognising Social Engineering & Phishing Attacks

Best For

This program is ideal for:
Early to mid-career professionals
Non-technical staff across all departments
Professionals handling emails, messages, calls, or external requests
Organizations aiming to reduce human-factor cybersecurity risks

Delivery Style

The learning experience is highly practical, awareness-driven, and focused on helping professionals recognize, question, and respond safely to manipulation-based cyber threats encountered in everyday work.

Outcome Level

Participants develop stronger threat-recognition skills, improved confidence in identifying suspicious interactions, and the ability to prevent security incidents caused by deception rather than technology failure.

Program Positioning

Social engineering attacks exploit **human trust, urgency, fear, and authority** rather than technical vulnerabilities. Phishing emails, fake messages, impersonation calls, and manipulation tactics remain the leading cause of data breaches and financial loss worldwide.

This program is designed to help professionals understand **how attackers think and operate**, recognize warning signs early, and respond safely without panic or embarrassment. It focuses on real-world scenarios, behavioral cues, and decision discipline — not fear-based training.

The content reflects current threat patterns across the USA, Australia, Canada, and global organizations, where employee awareness is the strongest line of cyber defense.

✅ Ideal for professionals with 0–15 years of experience
✅ Ideal for organizations strengthening human-layer cybersecurity

LEARNING STRUCTURE (8 HOURS)

Block 1 — Understanding Social Engineering Attacks

This session builds a strong foundation by explaining what social engineering is and why attackers target people instead of systems. Participants learn how manipulation techniques bypass technical security controls.

It covers:

- What social engineering means in simple terms
- Why humans are targeted
- Common manipulation techniques
- The psychology behind successful attacks

✅ **Outcome:** Clear understanding of how social engineering works.

Block 2 — Phishing, Spear Phishing & Smishing Explained

This session focuses on the most common attack formats used today. Participants learn how different phishing methods appear across email, messaging apps, and mobile platforms.

It covers:

- Email-based phishing
- Targeted spear-phishing attempts
- SMS and messaging-based attacks
- Fake links, attachments, and requests

✅ **Outcome:** Improved recognition of phishing techniques.

Block 3 — Identifying Red Flags & Suspicious Signals

This session strengthens the ability to spot warning signs before damage occurs. Participants learn to pause, question, and verify instead of reacting emotionally.

It covers:

- Urgency, fear, and authority cues
- Inconsistent sender details
- Unusual requests or payment instructions
- Language, formatting, and timing clues

✅ **Outcome:** Stronger instinct to detect suspicious interactions.

Block 4 — Impersonation, Pretexting & Trust Exploitation

This session addresses advanced social-engineering tactics that rely on impersonation and fabricated scenarios.

It covers:

- Impersonation of executives, vendors, or IT staff

- Fake support or internal requests
- Manipulation using trust and familiarity
- Avoiding compliance under pressure

✅ **Outcome:** Better resistance to impersonation attacks.

Block 5 — Safe Verification & Response Practices

This session focuses on what professionals should do when they suspect an attack — without escalating risk.

It covers:

- Verifying requests safely
- Using trusted communication channels
- Avoiding direct replies to suspicious messages
- Protecting oneself and the organization

✅ **Outcome:** Confident and safe response behavior.

Block 6 — Protecting Credentials & Sensitive Information

This session reinforces why attackers aim to steal credentials and how professionals can prevent accidental disclosure.

It covers:

- Recognizing credential-harvesting attempts
- Avoiding unsafe login pages
- Protecting passwords and authentication details
- Understanding why “just one click” matters

✅ **Outcome:** Stronger credential-protection awareness.

Block 7 — Reporting & Incident Prevention Culture

This session emphasizes early reporting as a protective measure — not a failure.

It covers:

- Why reporting matters
- Overcoming fear or embarrassment
- Supporting rapid response and containment
- Contributing to a security-aware culture

✅ **Outcome:** Increased confidence in reporting suspicious activity.

Block 8 — Social Engineering Defense Action Plan

This final session helps participants convert awareness into daily protective behavior.

It covers:

- Identifying personal risk areas
- Strengthening verification habits
- Applying caution consistently
- Creating a personal anti-phishing action plan

✅ **Outcome:** Clear, practical plan to defend against social-engineering threats.

✅ What You Will Walk Away With

Participants complete the program with:
Stronger ability to recognize phishing and manipulation attempts
Improved confidence questioning suspicious requests
Reduced risk of human-driven cyber incidents
Better response discipline under pressure
A structured approach to social-engineering defense
A Knowledge Que Course Completion Certificate (8 PDUs)

✅ Certification (Delivery-Neutral & Legally Safe)

On successful completion of the program, learners receive:
Knowledge Que – Course Completion Certificate
Recognition of 8 Professional Development Units (PDUs)
A digital certificate suitable for:
LinkedIn
Resume & Portfolio
Professional Profiles
Issued by Knowledge Que – Powered by Experts

✅ Why Knowledge Que

Expert-led, practical professional skills training
Real-world workplace threat scenarios
Skill-focused learning with immediate application
Programs designed specifically for modern professionals

Copyright