

Understanding Social Engineering

Protecting What Matters:
Awareness Series by Turicum

2 minute read



Introduction

Cybercrime in banking has shifted dramatically. Criminals rarely “hack” systems first, they hack people. Social engineering is the art of manipulating trust, routine, and emotion to make someone take an action they normally wouldn’t. Banks worldwide continue to report cases where attackers used personal details found online like holiday photos, job titles, even charity-event announcements, to craft convincing messages. The technology behind these scams has evolved, but the core vulnerability continues to be human nature.

At Turicum Private Bank, awareness is our strongest defence. Understanding how deception works empowers clients and colleagues to recognise and resist it, before harm is done.

How it works

Social engineering succeeds because it **feels personal**. Criminals rely on emotional triggers that override critical thinking, such as:

Urgency “Your account will be frozen in 15 minutes.”

Authority “Calling from the Bank’s Fraud Department.”

Fear “A suspicious transfer was just attempted.”

By the time doubt arises, the attacker may already have gained a foothold.



Common techniques in real banking scenarios

With artificial intelligence being used to create realistic emails, voice calls, and video content, fraudulent approaches can closely resemble genuine communication, which reinforces the need for careful verification.

Phishing

Emails tailored using publicly available information including company roles, recent events, press activity. Attackers increasingly mimic banking communications, using logos, tone, and formatting copied from genuine client letters.

Smishing

Text messages warning of a failed login, asking recipients to call a fake “security line.” Several banks in Gibraltar have seen clients receive SMS alerts that appeared to come from the same thread as legitimate notifications.

Vishing

Phone calls from individuals claiming to be auditors, risk teams, or law enforcement officers. In many cases, criminals will call clients **while simultaneously sending emails** to reinforce legitimacy.

Spoofing

Email addresses or websites almost indistinguishable from official ones, often differing by a single letter or character. Attackers use these to schedule calls, send instructions, or request confirmations that appear routine.

Why banks are targeted

Financial institutions provide a unique combination of **high value assets, sensitive data, and deeply trusted relationships.**

For attackers, impersonating a bank or its staff allows them to exploit the credibility that clients rely on.

Several Gibraltar-based institutions have experienced coordinated social engineering attempts in recent years. While Turicum has not been affected, these incidents reaffirm a truth that even the most advanced systems rely on human vigilance.

The cost of misplaced trust



When an attacker succeeds, the consequences extend far beyond financial loss.

Emotional pressure during the event.

Disruption of long-standing professional relationships.

Reputational concerns for both clients and institutions.

Administrative and legal burdens associated with recovery.

Rebuilding trust takes far longer than compromising it, which is why prevention is essential.

Turicum's approach

At Turicum, protection is a shared responsibility. We invest in:

Specialist-led cyber awareness training for all staff.

Regular testing using real-world deception scenarios.

Zero trust, embedded verification steps for payment approvals.

Advanced phishing and impersonation detection.

Layered controls designed to catch unusual activity early.



If something feels unusual, unfamiliar, or urgent, verify it directly with your Relationship Manager.

A 30-second call can prevent significant loss.

This feature forms part of *Turicum's Protecting What Matters: Awareness Series*, a collection designed to help clients and intermediaries stay alert to fraud risks and protect their information online.

For guidance on protecting yourself from fraud in Gibraltar, visit the Gibraltar Bankers' Association:

GBA fraud prevention →

For more information:

Contact us →