

Spotting the Signs:

Phishing, Impersonation & Social Engineering

Protecting What Matters:
Awareness Series by Turicum

2 minute read



Introduction

Most fraud attempts start quietly with a message that looks legitimate. A familiar signature, a recognisable logo, or an email arriving shortly after a genuine conversation can make even cautious individuals react without hesitation. Phishing, impersonation, and social engineering remain the most common entry points for attackers.

Their success depends not on technical complexity, but on catching us in a moment of routine.

A typical scenario

Imagine receiving an email that appears to be from your bank, informing you of a blocked transaction. The message arrives just minutes after you used your card overseas - information that can be easily harvested from social media posts or compromised travel booking databases.

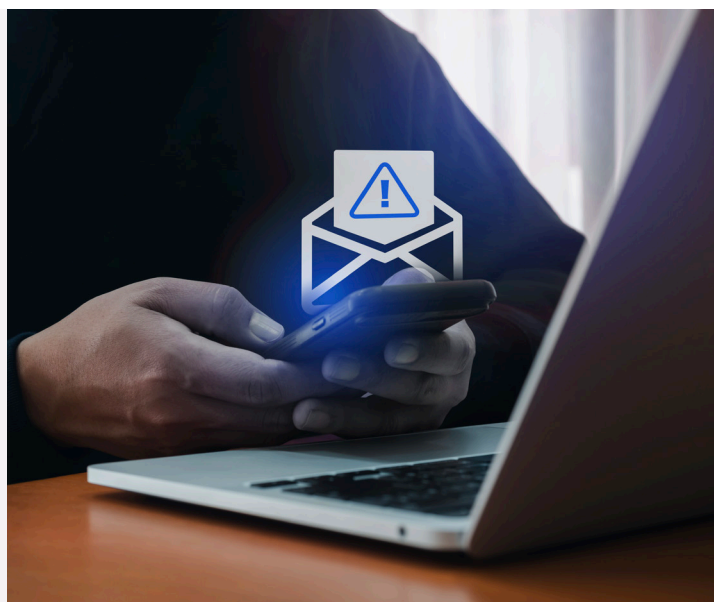
The link takes you to a near perfect imitation of the bank's website.

The login works.

Everything looks normal.

But the credentials entered are captured instantly.

This type of attack has been reported by institutions across Europe, often triggered by a single click during an otherwise ordinary day.



Why these attacks work



Attackers do not need to breach systems directly. Instead, they exploit **trust, familiarity, and routine**.

They study how organisations communicate.

They replicate email signatures, formatting, and language.

They reference previous interactions or plausible scenarios.

The goal is simple: reduce doubt just enough to prompt action.

Red flags to watch for

Attackers rely on subtle details to create credibility. Look for:

Unusual urgency - messages that demand immediate action, threaten consequences, or impose artificial deadlines.

Sender inconsistencies - mail addresses that appear correct at first glance but include extra characters, substitutions, or misspellings.

Unexpected attachments or shortened links - especially when unrelated to prior discussions or sent without explanation.

Requests for authentication codes, logins, or device access - banks do not request these under any circumstances.

Tone mismatch - messages that feel too casual, overly formal, or inconsistent with previous communication.

Requests that bypass normal process - messages or phone calls encouraging you to skip verification “just this once” due to urgency or convenience.

How attackers exploit trust

In recent cases, attackers have begun by reviewing publicly available professional profiles. They replicate job titles, internal roles, and even meeting references. Clients are then contacted under the guise of a follow-up conversation or administrative request.

Similar “business email compromise” attempts have targeted intermediaries, legal firms, and asset managers, often using details scraped from social platforms to appear authentic.

The message may be polished.

The request may seem reasonable.

The sender may look familiar.

That is precisely the intent.

Turicum’s guidance

To safeguard communications, official messages are sent only from @turicum.com addresses.

We will never ask for passwords, authentication codes, or to install remote access tools. Fraud prevention is not about suspicion of every message, but about **verification when something is unexpected**.

If a message or call feels unexpected, unusual, or urgent, you should verify directly by calling **+350 200 44144**.

A moment of caution before you click may be the most valuable pause you take today.

This feature forms part of *Turicum’s Protecting What Matters: Awareness Series*, highlighting how to recognise and prevent social-engineering and digital-fraud attempts.

For guidance on protecting yourself against financial fraud, visit the Gibraltar Bankers' Association:

[GBA fraud prevention](#) →

For more information:

[Contact us](#) →

Turicum Private Bank Limited is registered with Companies House Gibraltar under Incorporation Number 47119. It is regulated by the Gibraltar Financial Services Commission under Permission Number 543.