

Vigilance and Trust:

Our Shared Responsibility

Protecting What Matters:
Awareness Series by Turicum

2 minute read

Introduction

Throughout this series, we have explored how modern fraud increasingly targets people rather than systems.

From understanding how social engineering exploits trust, to recognising the warning signs of impersonation and adopting stronger digital habits, one theme remains constant, awareness is only effective when it is applied.

The final feature of our Protecting What Matters awareness series focuses on vigilance and trust, and why security in modern banking is strongest when shared.

Technology is essential, but informed judgement, both within the bank and among our clients, remains irreplaceable.

Today's fraud rarely begins with a "system breach." More often it begins with a convincing message, a trusted name, or an urgent instruction designed to bypass normal checks. That is why vigilance matters, pausing to verify the unexpected is one of the simplest and most effective ways to prevent loss.

The shared model

Financial institutions invest heavily in cybersecurity, yet attackers continue to exploit human trust.

In 2025, several UK banks reported incidents where fraudsters used deep-fake voice technology to impersonate senior executives and authorise internal payments. These cases show that even institutions with

strong infrastructure must rely on people who feel confident challenging the unexpected.

A secure system can be undermined in seconds by a fraudulent instruction that sounds convincing.

Turicum's controls

Turicum operates under GFSC supervision and maintains a secure, resilient infrastructure supported by:

Specialist led training so employees recognise manipulation and respond confidently.

Strict verification protocols with independent verification for sensitive instructions.

Regular audits and penetration testing to continuously validate resilience.

Comprehensive vendor-risk oversight to manage third-party exposure.

Encrypted client communication channels for secure, trusted interaction.

These defences are designed to protect client interests, even when attackers attempt increasingly sophisticated deception.



Client partnership

Clients and intermediaries contribute directly to this protection by:

Verifying payment instructions or changes to bank details through official channels.

Treating urgent or unexpected requests with caution and confirming before acting.

Reporting suspicious messages or calls immediately.

Keeping contact details current to support rapid verification.

A recent Gibraltar case involved attackers posing as a law firm team to redirect property-purchase funds. The fraud was stopped only because the client called the firm before approving the transfer.

One call prevented a significant financial loss.

Our commitment

Turicum continues to invest in technology, training, and communication.

Every verification step is taken seriously because every step protects something of value.

Security is not simply a promise.

It is a partnership between the bank, our clients, and the community we serve.



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 strengthen their confidence in an increasingly digital world.

For independent guidance, 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.