	<b>MANUAL DE INSTRUCCIONES</b>		<b>I523-IT-3</b>
	<b>Guía de Identificación de Phishing para Usuarios</b>		REVISIÓN: 0 FECHA: 25/08/25
Emisión: G. MONTALBETTI Fecha: Firma:	Aprobación: D. PEDROSA Fecha: Firma:		<b>PAG.: 1 / 6</b>

**Cumplimiento con TISAX e ISO/IEC 27001:2022 - Anexo A.7.2.2 (Concienciación, educación y formación en materia de seguridad)**

## 1. ¿Qué es el Phishing?

El **phishing** es un tipo de **ciberataque que utiliza ingeniería social**. Los atacantes se hacen pasar por una entidad legítima (como su banco, jefe, un servicio popular como Microsoft o Amazon, o incluso un colega) a través de correos electrónicos, mensajes de texto (smishing) o llamadas telefónicas (vishing). El objetivo es manipularlo para que:


- **Revele información confidencial (credenciales de acceso, datos personales, financieros).**
- **Descargue e instale software malicioso (ransomware, keyloggers).**
- **Realice una acción fraudulenta (transferir dinero, aprobar un pago).**

## 2. Señales de Alerta: Cómo Identificar un Phishing

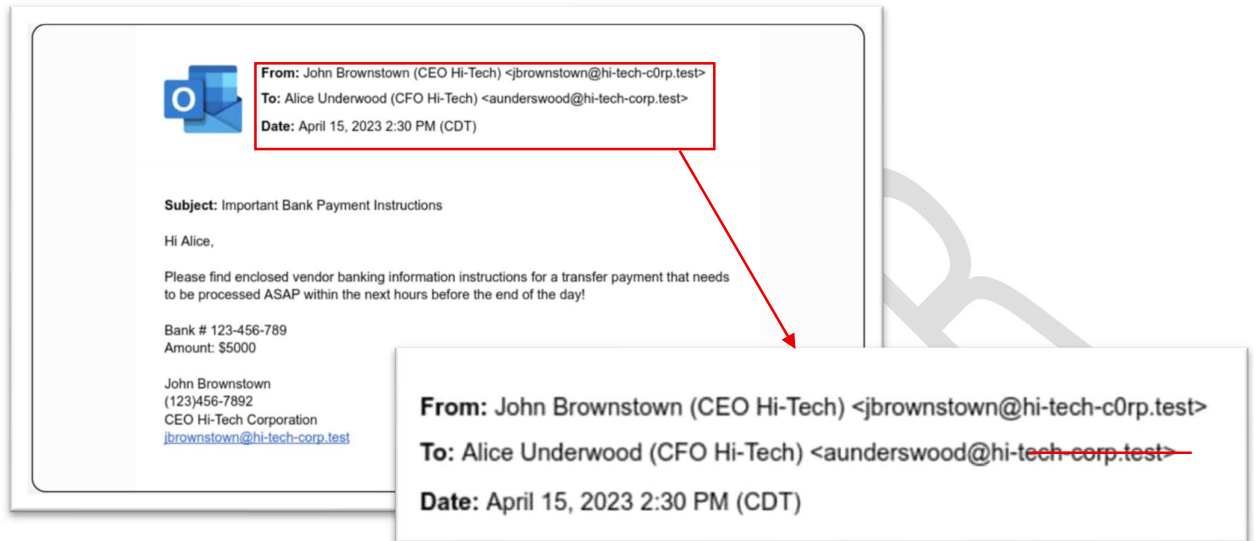
Antes de hacer clic en cualquier enlace o descargar un adjunto, pause y revise estas **7 señales de alerta** críticas:

### A. Remitente Sospechoso: La Dirección de Email no Coincide

- **Señal:** El nombre del remitente parece legítimo (ej. "Soporte IT Microsoft"), pero la dirección de correo es fraudulenta.
- **Qué buscar:** Pase el mouse sobre el nombre del remitente para ver la dirección real.  
¿Coincide exactamente con el dominio oficial de la empresa? Desconfíe de dominios con errores tipográficos (ej. micr0soft.com, amaz0n.net, support-go0gle.com) o dominios genéricos como @gmail.com pretendiendo ser una gran corporación.

	<b>MANUAL DE INSTRUCCIONES</b>	<b>MC523-IT-3</b>
	<b>Guía de Identificación de Phishing para Usuarios</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 2 / 5</b>

### Ejemplo visual:



*Imagen: El nombre parece ser de Hi-Tech, pero la dirección de correo es claramente fraudulenta.*

### B. Urgencia o Miedo: Presión para Actuar Rápidamente


- **Señal:** El mensaje crea un sentido de urgencia o miedo inmediato.
- **Frases comunes:** "Su cuenta será suspendida en 24 horas", "Acceso bloqueado", "Factura impaga - Actúe ahora", "Llamada urgente del Director", "Problema de seguridad crítico".
- **Objetivo:** Hacer que actúe por impulso, sin pensar.

### C. Saludos Genéricos o Erróneos

- **Señal:** El email no está dirigido a usted personalmente.
- **Qué buscar:** Saludos como "Estimado cliente", "Hola usuario", "Querido miembro" o, peor aún, un nombre que no es el suyo. Las empresas legítimas suelen usar su nombre y apellido.

### D. Enlaces Fraudulentos: El Texto no Coincide con la URL

- **Señal:** El texto del enlace parece legítimo (ej. "Acceder a mi cuenta"), pero el destino real es malicioso.

	<b>MANUAL DE INSTRUCCIONES</b>	<b>MC523-IT-3</b>
	<b>Guía de Identificación de Phishing para Usuarios</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 3 / 5</b>

- **Qué hacer: ¡NUNCA haga clic directamente!** Pase el mouse sobre el enlace (sin hacer clic) para ver la URL real en la barra de estado de su navegador. Desconfíe de URLs acortadas ([bit.ly](#), tinyurl) y de direcciones que no coinciden con el sitio web oficial.

#### Ejemplo visual:




Imagen: El enlace muestra "[www.ebay.com](#)", pero al pasar el mouse se ve la URL real maliciosa.

#### F. Archivos Adjuntos Inesperados o Sospechosos

- **Señal:** Recibe un archivo adjunto que no solicitó, incluso de un remitente conocido.
- **Qué buscar:** Archivos con extensiones como .zip, .exe, .scr, .js, o documentos de Office que piden habilitar macros (.docm, .xlsm). Estos son vectores comunes de malware.

#### G. Errores Gramaticales y Ortográficos

- **Señal:** El mensaje contiene errores gramaticales, ortografía pobre o un lenguaje poco profesional.
- **Nota:** Los ataques de phishing más avanzados (spear phishing) ya no suelen tener estos errores, por lo que su ausencia **no garantiza** que el correo sea seguro.

	<b>MANUAL DE INSTRUCCIONES</b>	<b>MC523-IT-3</b>
	<b>Guía de Identificación de Phishing para Usuarios</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 4 / 5</b>


#### H. Solicitud de Información Confidencial

- **Señal:** Le piden que confirme, actualice o verifique credenciales de acceso, datos de tarjetas de crédito o información personal.
- **Regla de oro:** Ninguna organización legítima le pedirá nunca que envíe contraseñas, PIN's o datos sensibles por correo electrónico.

### 3. ¿Qué Hacer? Protocolo de Actuación

Si identifica una o más señales de alerta, siga estos pasos:

1. **NO HAGA CLIC** en ningún enlace.
2. **NO DESCARGUE** ni abra ningún archivo adjunto.
3. **NO PROPORCIONE** ninguna información.
4. **VERIFIQUE** la autenticidad del mensaje:
  - **Contacte directamente a la supuesta fuente** utilizando un método de confianza, **no** respondiendo al correo sospechoso. Llame por teléfono a un número oficial de la empresa o escriba un nuevo correo a una dirección conocida.
  - Por ejemplo, si el correo parece ser de su banco, acceda a su banca en línea escribiendo la URL manualmente en el navegador, no usando el enlace del correo.
5. **REPORTE** el incidente:
  - **Reporte el correo** al departamento de TI/Seguridad siguiendo los procedimientos internos establecidos (ej., usando el botón "Reportar Phishing" en su cliente de correo).
  - Marque el mensaje como **SPAM** o **CORREO NO DESEADO**.
6. **ELIMINE** el correo de su bandeja de entrada.

	<b>MANUAL DE INSTRUCCIONES</b>	<b>MC523-IT-3</b>
	<b>Guía de Identificación de Phishing para Usuarios</b>	REVISIÓN: 0 FECHA: 25/08/25
		<b>PAG.: 5 / 5</b>

#### 4. Ejemplos Visuales y Videos

##### Galería de Ejemplos de Phishing:

- **Google Phishing Quiz:** Una excelente herramienta interactiva para poner a prueba sus conocimientos.
  - <https://phishingquiz.withgoogle.com/>
- **Phishing.org - Ejemplos:**
  - <https://www.phishing.org/phishing-examples>
- **KnowBe4 - Biblioteca de Phishing:**
  - <https://www.knowbe4.com/phishing-examples> (Contiene numerosos ejemplos visuales de diferentes tácticas).

##### Videos Explicativos (Recomendados para Sesiones de Capacitación):

- **¿Qué es el Phishing? (Video explicativo - 2:18 min):**
  - <https://www.youtube.com/watch?v=YXVoqCEwQvo>
- **Cómo Identificar un Email de Phishing (Video práctico - 4:02 min):**
  - <https://www.youtube.com/watch?v=o2o4sYN76E4>
- **El Peligro de los Adjuntos (Video con ejemplo - 1:47 min):**
  - [https://www.youtube.com/watch?v=Ov\\_sOBcjDpl](https://www.youtube.com/watch?v=Ov_sOBcjDpl)

#### 5. Recordatorio Final: Su Rol es Crucial

La seguridad de la información es una responsabilidad compartida. **De acuerdo con ISO 27001 y TISAX, USTED es la primera línea de defensa.** Su capacidad para detectar y reportar intentos de phishing protege no solo sus datos, sino también los activos críticos de la empresa, nuestra reputación y la confianza de nuestros clientes.

**En caso de duda, ¡siempre pregunte a su equipo de Soporte IT/Seguridad!**