

# **GUÍA DE IDENTIFICACIÓN DE PHISHING**

NOVIEMBRE 2024

CECILIA FERNANDA SAN MIGUEL ITURRIA

# Índice

<b>1</b>	<b><i>Phishing por correo electrónico (Email)</i></b>	<b>3</b>
1.1	Analiza la <b>motivación</b> del mensaje . . . . .	3
1.2	Examina al <b>emisor</b> . . . . .	3
1.3	Verifica los enlaces incluidos . . . . .	4
<b>2</b>	<b><i>Phishing por redes sociales</i></b>	<b>5</b>
2.1	Analiza la <b>motivación</b> del mensaje . . . . .	5
2.2	Examina al <b>emisor</b> . . . . .	6
2.3	Verifica los enlaces incluidos . . . . .	6
<b>3</b>	<b><i>Phishing por sitios web</i></b>	<b>7</b>
3.1	Verifica la autenticidad del sitio . . . . .	7
3.2	Consulta fuentes confiables . . . . .	8
<b>4</b>	<b><i>Phishing de Wi-Fi</i></b>	<b>8</b>
4.1	Conexión a redes seguras . . . . .	9
4.2	Verificación del nombre de la red . . . . .	9
<b>5</b>	<b><i>Phishing por Mensajería instantánea (IM)</i></b>	<b>11</b>
5.1	Identificación de mensajes sospechosos . . . . .	11
5.2	Verificación de autenticidad . . . . .	11
<b>6</b>	<b>SMishing</b>	<b>13</b>
6.1	Características comunes . . . . .	13
6.2	Métodos de engaño . . . . .	13
<b>7</b>	<b>Vishing</b>	<b>15</b>
7.1	Características comunes . . . . .	15
7.2	Recomendaciones de seguridad . . . . .	15

El término *Phishing* está basado en la palabra en inglés "fishing" que significa pescar, actúa como un señuelo que busca pescar los datos sensibles de la víctima.

Para reconocer un ataque de *phishing* con mayor facilidad, es clave identificar primero la forma en que llega. A continuación, se explican los tipos más comunes de *phishing*, junto con consejos prácticos que pueden ayudar a prevenirlos.

## 1. ***Phishing* por correo electrónico (Email)**

El *phishing* a través de correos electrónicos es una de las formas más comunes en las que los ciberdelincuentes intentan engañar a las personas para obtener información personal o financiera. A continuación, se presentan algunas recomendaciones clave para reconocer y evitar este tipo de ataques:

### 1.1. Analiza la **motivación** del mensaje

Presta atención al contenido y al propósito del correo. Los correos fraudulentos suelen:

- Notificarte que has ganado un premio inesperado.
- Advertirte sobre problemas urgentes, como la expiración de tu cuenta o la falta de espacio de almacenamiento.
- Crear una sensación de urgencia para que actúes rápidamente.

Si el mensaje parece demasiado bueno o genera presión innecesaria, desconfía y verifica directamente con la institución.

### 1.2. Examina al **emisor**

Antes de interactuar con el correo:

- Revisa la dirección del remitente. Las direcciones sospechosas suelen ser desconocidas, parecer inexistentes o incluir combinaciones extrañas de letras, números y símbolos.
- Si la dirección parece legítima, pero tienes dudas, consulta directamente el sitio web oficial de la entidad o comunícate con ellos.

### 1.3. Verifica los enlaces incluidos

Los correos de *phishing* suelen contener **hipervínculos** disfrazados que dirigen a sitios falsos. Toma en cuenta lo siguiente:

- Los enlaces pueden aparecer como botones, texto subrayado o direcciones visibles que incluyen nombres de empresas, instituciones o servicios.
- Antes de hacer clic, pasa el cursor sobre el enlace (sin pulsarlo) para visualizar la dirección real. Si no coincide con el sitio oficial, evita acceder.

A continuación se muestran algunos ejemplos reales de correos electrónicos fraudulentos. Observa cómo se destacan las características mencionadas anteriormente para ayudarte a identificar este tipo de amenazas con mayor facilidad.

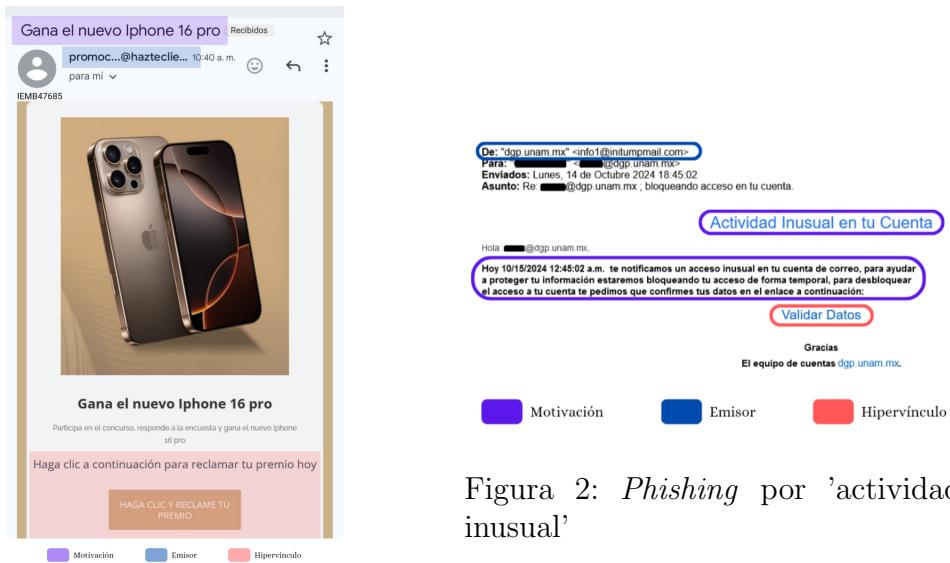


Figura 1: *Phishing* por 'ganar un premio'

Figura 2: *Phishing* por 'actividad inusual'



Figura 3: *Phishing* por 'expiro de cuenta'

## 2. *Phishing* por redes sociales

El *phishing* en redes sociales aprovecha las plataformas con herramientas de mensajería integradas, de manera similar al correo electrónico y los mensajes de texto. Este tipo de ataque busca captar la atención de las víctimas con promesas atractivas, como haber ganado un concurso o recibir algún tipo de beneficio. En la mayoría de los casos, el objetivo principal es robar las credenciales de inicio de sesión para acceder a cuentas personales, por lo que, suelen incluir enlaces sospechosos.

### 2.1. Analiza la **motivación** del mensaje

Presta atención al tipo de notificación o mensaje que recibes. Los mensajes fraudulentos suelen:

- Prometer beneficios económicos, regalos o incentivos atractivos.
- Crear un sentido de urgencia para que actúes rápidamente.
- Fingir que provienen de una fuente confiable o conocida.

Si el mensaje genera presión innecesaria o contiene un beneficio extremista, desconfía y verifica directamente con la persona o entidad.

## 2.2. Examina al emisor

Antes de interactuar con el mensaje:

- Verifica el nombre de usuario o perfil del emisor. Los indicios de un ataque incluyen nombres desconocidos, perfiles con combinaciones extrañas de caracteres o la suplantación de identidad de un conocido.
- Si el mensaje proviene de un familiar o amigo, confirma directamente con ellos para asegurarte de que no se trata de un caso de suplantación.

## 2.3. Verifica los enlaces incluidos

Los mensajes de *phishing* en redes sociales suelen contener **hipervínculos** que dirigen a sitios falsos. Considera que:

- Los enlaces pueden aparecer como texto, botones o direcciones visibles relacionadas con empresas o servicios conocidos.
- Antes de hacer clic, pasa el cursor sobre el enlace para visualizar su dirección real. Si no coincide con un sitio legítimo, evita acceder.

En la Figura 4 se muestra un ejemplo típico de *phishing* en redes sociales. El emisor es completamente desconocido; sin embargo, ofrece un beneficio lo suficientemente atractivo para incitar a hacer clic en el enlace incluido. Observa las características clave mencionadas anteriormente destacadas para ayudarte a identificar este tipo de amenazas.

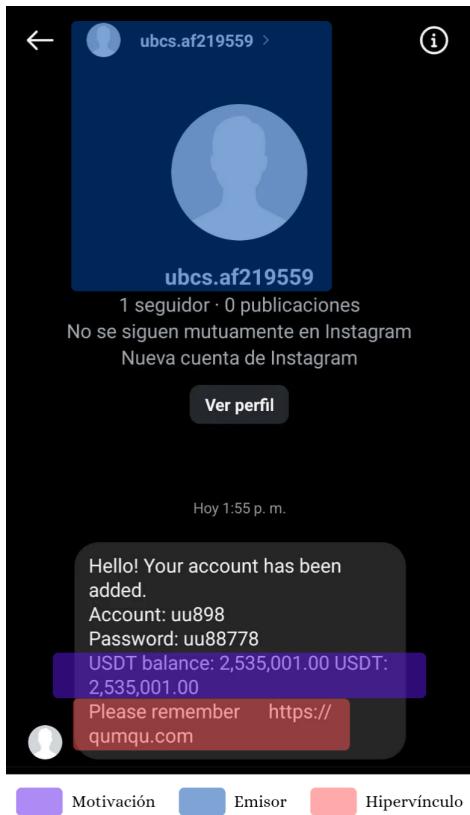


Figura 4: Ejemplo de *phishing* por redes sociales

### 3. *Phishing* por sitios web

Los sitios web fraudulentos están diseñados para parecer legítimos, pero su propósito es recopilar información personal de las víctimas. A continuación, se presentan algunas recomendaciones para identificar y evitar estos sitios:

#### 3.1. Verifica la autenticidad del sitio

Es importante comprobar si el sitio web es genuino antes de proporcionar cualquier tipo de información personal. En el caso de sitios web gubernamentales en México, asegúrate de que el enlace termine con *.gob.mx*.

### 3.2. Consulta fuentes confiables

El Gobierno de México proporciona una lista de sitios apócrifos que intentan suplantar a instituciones gubernamentales, disponible en [?]. Esta herramienta es útil para confirmar la legitimidad de un sitio antes de interactuar con él.

En la Figura 5 se ilustra una comparación entre un enlace legítimo (lado izquierdo) y uno fraudulento (lado derecho). Los sitios apócrifos suelen incluir apartados donde solicitan información personal, lo que los convierte en una amenaza significativa para los usuarios. Revisa siempre el formato del enlace y evita proporcionar datos sensibles en sitios sospechosos.

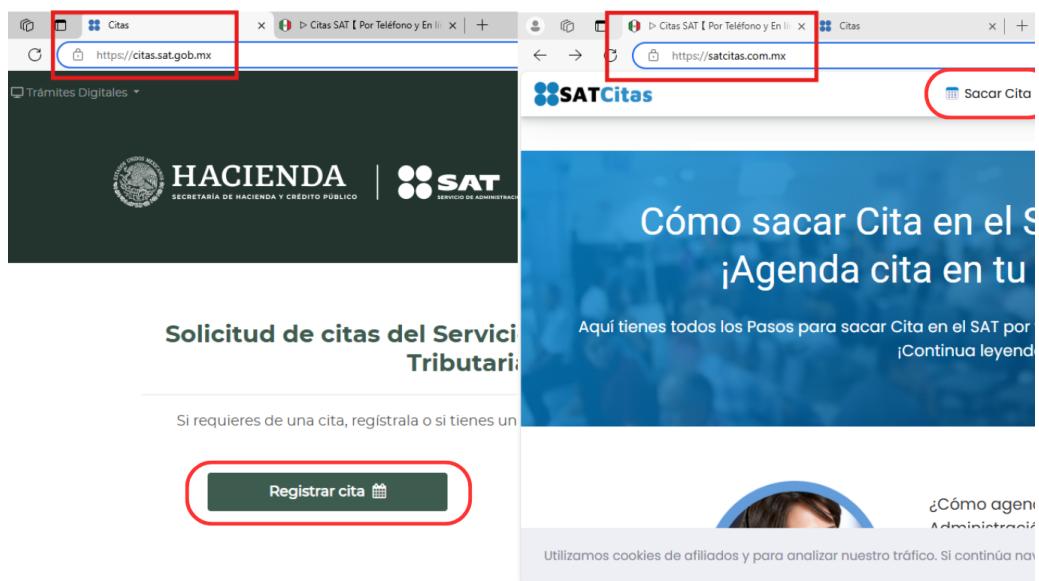


Figura 5: Ejemplo de *phishing* por sitios web

### 4. *Phishing* de Wi-Fi

Este tipo de ataque utiliza puntos de acceso Wi-Fi públicos, también conocidos como redes abiertas. Aunque no están dirigidos a un objetivo específico, los atacantes pueden usar estas redes para instalar *malware* en los dispositivos de las víctimas, recopilar credenciales o abrir el navegador con formularios que solicitan datos personales.

## 4.1. Conexión a redes seguras

Siempre se recomienda conectarse a redes Wi-Fi conocidas que, por lo general, requieren una contraseña para acceder. Sin embargo, si es necesario utilizar una red pública o abierta, es importante:

- Evitar ingresar **datos confidenciales** o personales en formularios. Si es posible, omite este paso.
- Usar herramientas de navegación seguras, como redes privadas virtuales (VPN), para proteger tu información.

## 4.2. Verificación del nombre de la red

En muchas redes Wi-Fi públicas, al conectarse se abre una pestaña en el navegador que incluye el nombre de la empresa o **el nombre de la red**. Si estos datos no coinciden entre sí, podría tratarse de un punto de acceso no legítimo.

Algunos formularios en estas redes pertenecen a empresas oficiales y cuentan con términos y condiciones claros, como se muestra en la Figura 4.2. Sin embargo, también existen formularios que no especifican de manera transparente quién tendrá acceso a los datos personales proporcionados.

**Acceder WiFi**  
https://gate.zequenze.com

include \$50 de descuento por domiciliar

\$289 al mes durante 3 meses

Registra tus datos para navegar

- Nombre completo\*
- Teléfono\*
- Correo Electrónico\*
- Edad

Probar

Nombre de la red Wi-Fi pública

Datos confidenciales

**Acceder a novil**  
https://.../vii.net

Selección tu opción

Cliente i Invitado

Conéctate con:

Correo electrónico

Confirma tu correo electrónico

Navegar

Nombre de la red Wi-Fi pública

Datos confidenciales

**Acceder a WiFi.\***  
https://mcwifi.com

Cliente Megacable Registro Redes Sociales

NAVEGA GRATIS, POR FAVOR INGRESA TUS DATOS

- Nombre completo
- Correo electrónico
- Número de celular (10 dígitos)

Navega a la máxima velocidad

Nombre de la red Wi-Fi pública

Datos confidenciales

**Acceder a Club WiFi**  
https://club...com.mx

Iniciar sesión

Ingresa con tu número de cuenta o correo

No. de cuenta o correo

Contraseña

Iniciar sesión

¿Olvidaste tu contraseña?

Iniciar sesión con celular

Nombre de la red Wi-Fi pública

Datos confidenciales

Figura 6: Ejemplos de formularios en puntos de acceso públicos

## **5. *Phishing por Mensajería instantánea (IM)***

Las aplicaciones de mensajería, como WhatsApp y Telegram, son plataformas comunes utilizadas para llevar a cabo este tipo de ataque debido a su popularidad y accesibilidad. Estas permiten una **interacción en tiempo real**, lo que facilita la comunicación inmediata entre el atacante y la víctima.

### **5.1. Identificación de mensajes sospechosos**

En este tipo de ataques, es frecuente recibir mensajes relacionados con:

- Ofertas laborales que prometen ingresos elevados por realizar poco o ningún esfuerzo.
- Propuestas de empleo enviadas supuestamente por personas en ".<sup>a</sup>ltos cargos".
- Enlaces externos o números desconocidos para contactar directamente con el remitente.

### **5.2. Verificación de autenticidad**

Es crucial confirmar la legitimidad de estas propuestas laborales antes de interactuar. Presta especial atención a:

- La credibilidad del remitente y el lenguaje utilizado en el mensaje.
- Los salarios ofertados que parecen excesivamente altos en comparación con el promedio o el mínimo.

En las Figuras 7 y 9 se muestran ejemplos de mensajes con ofertas laborales engañosas, mientras que la Figura 8 presenta una oferta en forma de "invitación", diseñada para generar un sentido de pertenencia en la víctima.

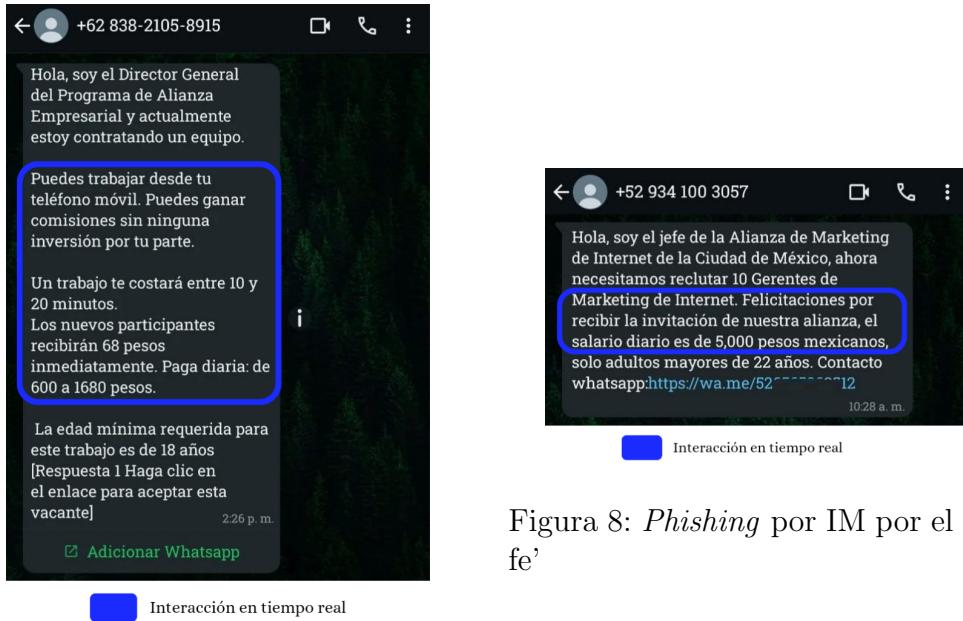


Figura 7: *Phishing* por IM por el 'Director'

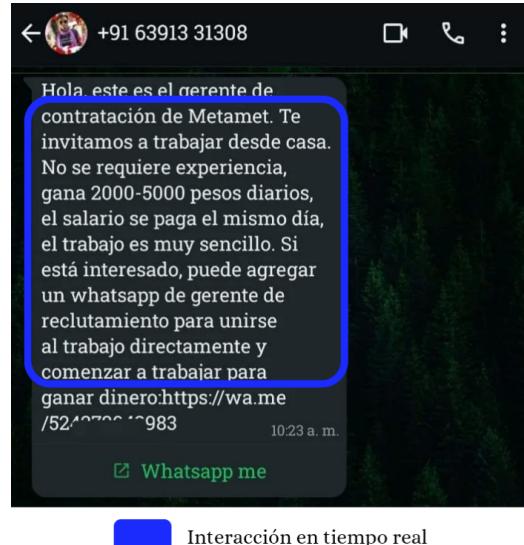


Figura 9: *Phishing* por IM por el 'gerente'

## 6. SMishing

El *phishing* por SMS, conocido como *smishing*, busca engañar a las víctimas haciéndose pasar por **comunicaciones de confianza**, como bancos, empresas o servicios reconocidos.

### 6.1. Características comunes

Este tipo de mensajes suelen incluir:

- Información relevante, como el nombre del destinatario.
- Detalles sobre problemas financieros, como robo de información bancaria, adeudos o pagos pendientes (véase las Figuras 10 y 11).
- Referencias a empresas o servicios reconocidos (véase la Figura 13) o asistencia jurídica (véase la Figura 12).

### 6.2. Métodos de engaño

Los atacantes dirigen a las víctimas a:

- **Sitios web fraudulentos** diseñados para recopilar información personal.
- **Números telefónicos engañosos** que pretenden ser líneas legítimas para obtener datos confidenciales.

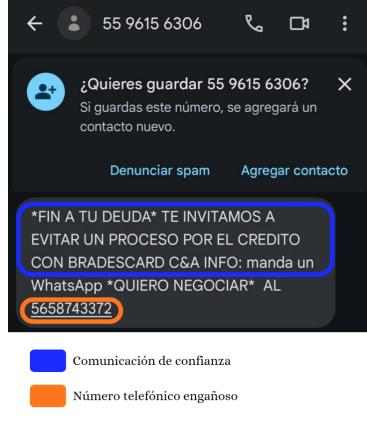


Figura 10: SMishing por adeudos

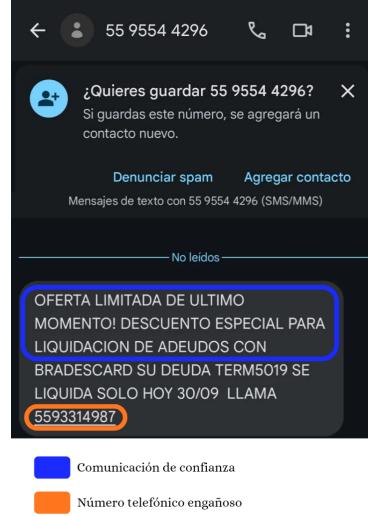


Figura 11: SMishing por adeudos

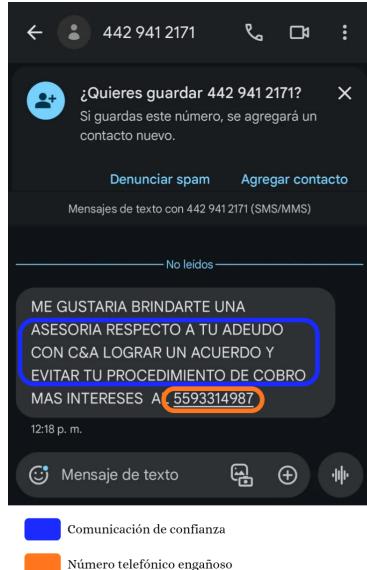


Figura 12: SMishing por servicios

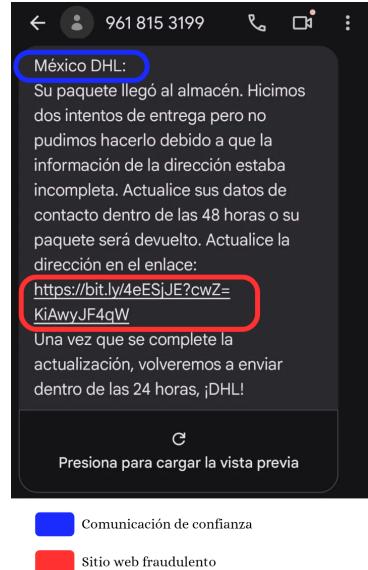


Figura 13: SMishing por empresas

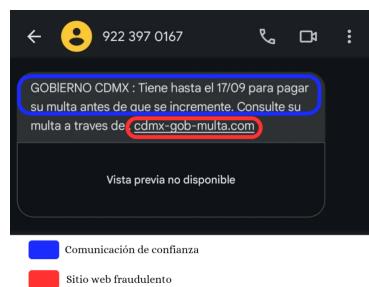


Figura 14: SMishing por 'Gobierno'



Figura 15: SMishing por empresas

## 7. Vishing

El *phishing* por llamada telefónica, conocido como *vishing*, consiste en llamadas diseñadas para engañar a las víctimas y obtener información confidencial. Este tipo de ataque se basa en la capacidad de falsificar números telefónicos, haciendo que las llamadas aparenten ser legítimas.

### 7.1. Características comunes

Este ataque se identifica principalmente por los siguientes aspectos:

- Las llamadas suelen estar enfocadas en el robo de información bancaria.
- Generalmente, los atacantes se presentan utilizando el **nombre de una institución bancaria** reconocida.
- Durante la interacción, solicitan un código que es enviado por SMS. Al compartir este código, los atacantes pueden acceder a aplicaciones bancarias desde otros dispositivos.

### 7.2. Recomendaciones de seguridad

Para protegerse de este tipo de ataques:

- Nunca comparta claves, códigos de acceso o contraseñas (independientemente de si son de 4, 6 u 8 dígitos).

- Verifique cualquier solicitud comunicándose directamente con la institución bancaria a través de un canal oficial.

En la Figura 17 se muestra un ejemplo de SMS que proporciona un **código de acceso**, utilizado comúnmente en este tipo de ataques. Además, algunas herramientas de telefonía pueden detectar estas llamadas como “Spam” o “Possible Fraude”, como se ilustra en la Figura 16.

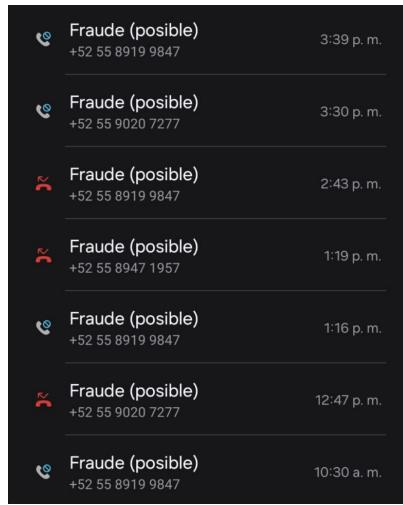


Figura 16: Ejemplo de llamadas detectadas como fraude



Figura 17: SMishing derivado de vishing