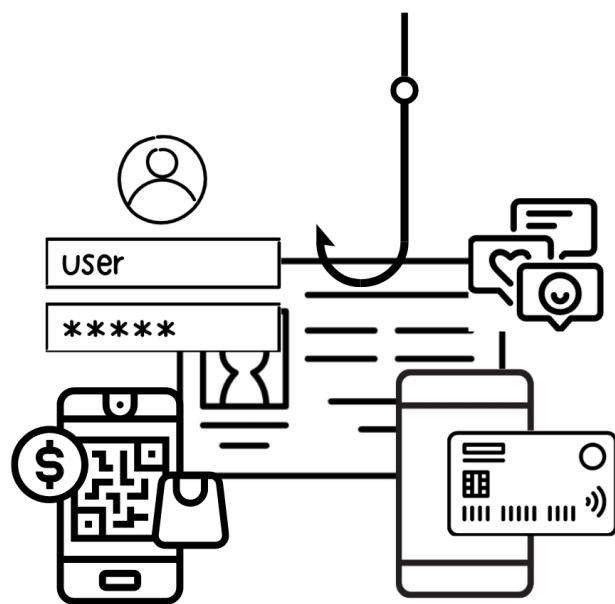


# GUÍA DE IDENTIFICACIÓN DE PHISHING



NOVIEMBRE 2024

CECILIA FERNANDA SAN MIGUEL ITURRIA

# Índice

<b>1. <i>Phishing por correo electrónico (Email)</i></b>	<b>4</b>
1.1. Analiza la <b>motivación</b> del mensaje . . . . .	4
1.2. Examina al <b>emisor</b> . . . . .	4
1.3. Verifica los <b>enlaces</b> incluidos . . . . .	4
<b>2. <i>Phishing por redes sociales</i></b>	<b>6</b>
2.1. Analiza la <b>motivación</b> del mensaje . . . . .	6
2.2. Examina al <b>emisor</b> . . . . .	6
2.3. Verifica los <b>enlaces</b> incluidos . . . . .	7
<b>3. <i>Phishing por sitios web</i></b>	<b>8</b>
3.1. Verifica la autenticidad del sitio . . . . .	8
3.2. Consulta fuentes confiables . . . . .	8
<b>4. <i>Phishing de Wi-Fi</i></b>	<b>9</b>
4.1. Conéctate a redes seguras . . . . .	9
4.2. Verificación del nombre de la red . . . . .	10
<b>5. <i>Phishing por Mensajería instantánea (IM)</i></b>	<b>11</b>
5.1. Analiza la <b>motivación</b> del mensaje . . . . .	11
5.2. Examina al <b>emisor</b> . . . . .	12
5.3. Verifica los <b>enlaces</b> incluidos . . . . .	12
<b>6. <i>SMishing</i></b>	<b>13</b>
6.1. Observa las características comunes . . . . .	13
6.2. Identifica los métodos de engaño . . . . .	14
<b>7. <i>Vishing</i></b>	<b>16</b>
7.1. Características comunes . . . . .	16
7.2. Recomendaciones de seguridad . . . . .	17

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

De manera general, el atacante envía un mensaje a la víctima que incluye un link a un sitio apócrifo, posteriormente, la víctima hace clic en este sitio y proporciona sus datos confidenciales o de acceso a cuentas, luego, el atacante guarda los datos proporcionados por la víctima y finalmente, el atacante utiliza los datos de acceso o información confidencial de la víctima para acceder a los sitios legítimos o para realizar algún tipo de estafa. Esto se puede observar en la Figura 1, que proporciona una descripción gráfica de un ataque de *phishing*.

### Descripción gráfica de un ataque de phishing

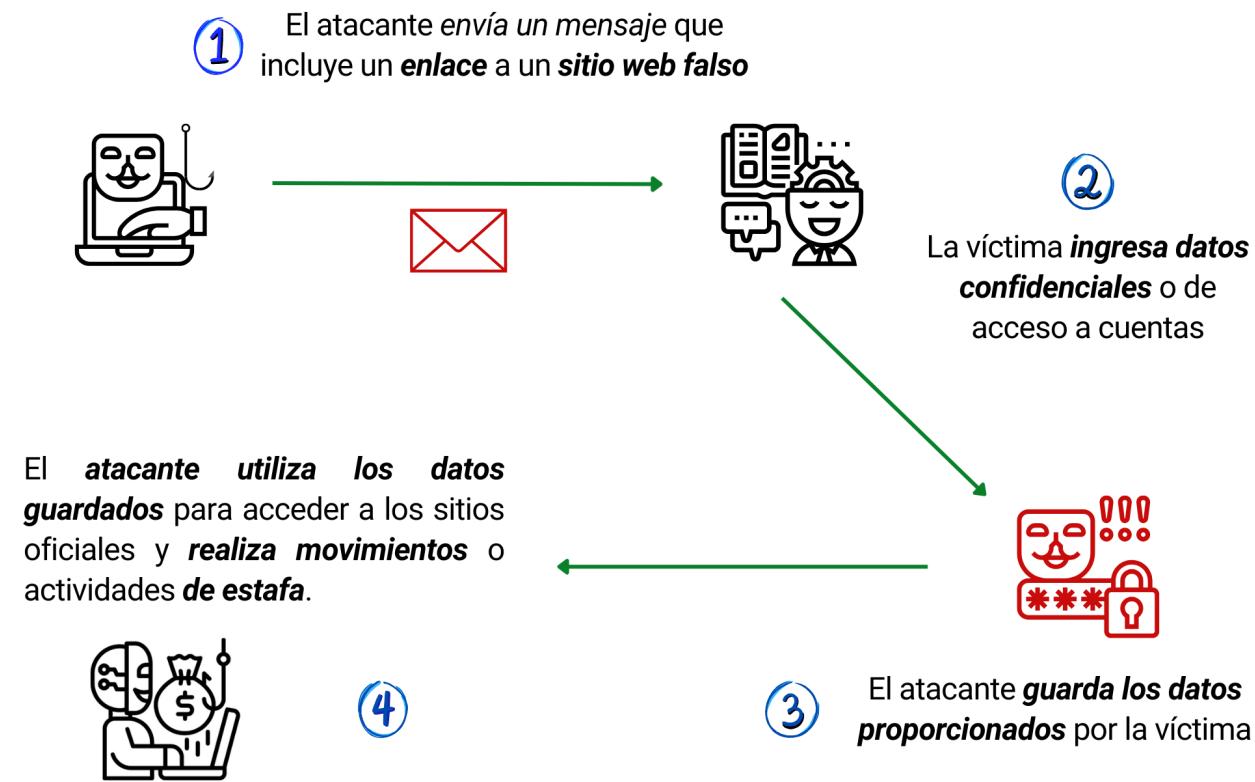


Figura 1: Ejemplo gráfico de *Phishing* [1].

Para reconocer y prevenir un ataque de *phishing* con mayor facilidad, se recomienda primero identificar la forma en que se recibe. A continuación, se ejemplifican y describen los tipos más comunes de *phishing*, además, se proporcionan algunos consejos prácticos que pueden ayudar a prevenirlas.

# 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 (en este contexto son conocidos como *phishers*) intentan engañar a las personas para obtener información personal o financiera. A continuación, se presentan algunas acciones clave que permitan 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 sido seleccionado como ‘*Ganador*’ de un premio de forma inesperada o por suerte.
- Advertirte sobre problemas o asuntos ‘*urgentes*’, como la expiración de tu cuenta, falta de espacio de almacenamiento, pérdida de licencia institucional,etc.
- Hablarte de forma profesional utilizando tu nombre de usuario o tu correo.

Si el mensaje parece ofrecer beneficios extraordinarios o te genera *presión innecesaria para realizar alguna actividad*, desconfía y verifica directamente con la persona o institución a través de sus medios de contacto oficiales.

## 1.2. Examina al emisor

Antes de interactuar con el correo:

- Revisa la dirección del remitente. Los *phishers* suelen utilizar direcciones desconocidas o que incluyen combinaciones aleatorias de letras, números y símbolos.
- Si la dirección parece legítima, es decir, tiene un nombre conocido o utiliza el nombre de una institución o empresa, pero te genera algún tipo de desconfianza, consulta directamente el sitio web oficial de la entidad o comunícate con ellos a través de sus medios de contacto oficiales.

Se recomienda siempre investigar en fuentes no pertenecientes al correo electrónico, es decir, no te comuniques por los medios de comunicación que te mencionan en este correo. *Infórmate de manera externa*, consultando directamente con la empresa, banco o institución mediante los teléfonos, correos, sitios web, chat, etc., que proporcionan de manera pública y oficial.

## 1.3. Verifica los enlaces incluidos

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

- Los enlaces pueden aparecer como botones, texto subrayado o direcciones a sitios 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.

Verifica que los enlaces siempre empiecen con **https**, pues esto indica que son sitios seguros, sin embargo, en algunos casos en empresas o servicios pequeños es seguro acceder a enlaces **http**. Si se trata de ‘comunicación’ del gobierno, los sitios oficiales suelen tener al final del enlace **.gob.mx**, en bancos e instituciones de confianza **.com** o **.mx**.

El Gobierno de México proporciona una lista de algunos sitios apócrifos que intentan suplantar a instituciones gubernamentales, disponible en *Sitios web falsos* [2]. Este sitio es una herramienta útil para confirmar la legitimidad de un sitio o enlace.

Para facilitar la identificación de este tipo de *phishing*, 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.

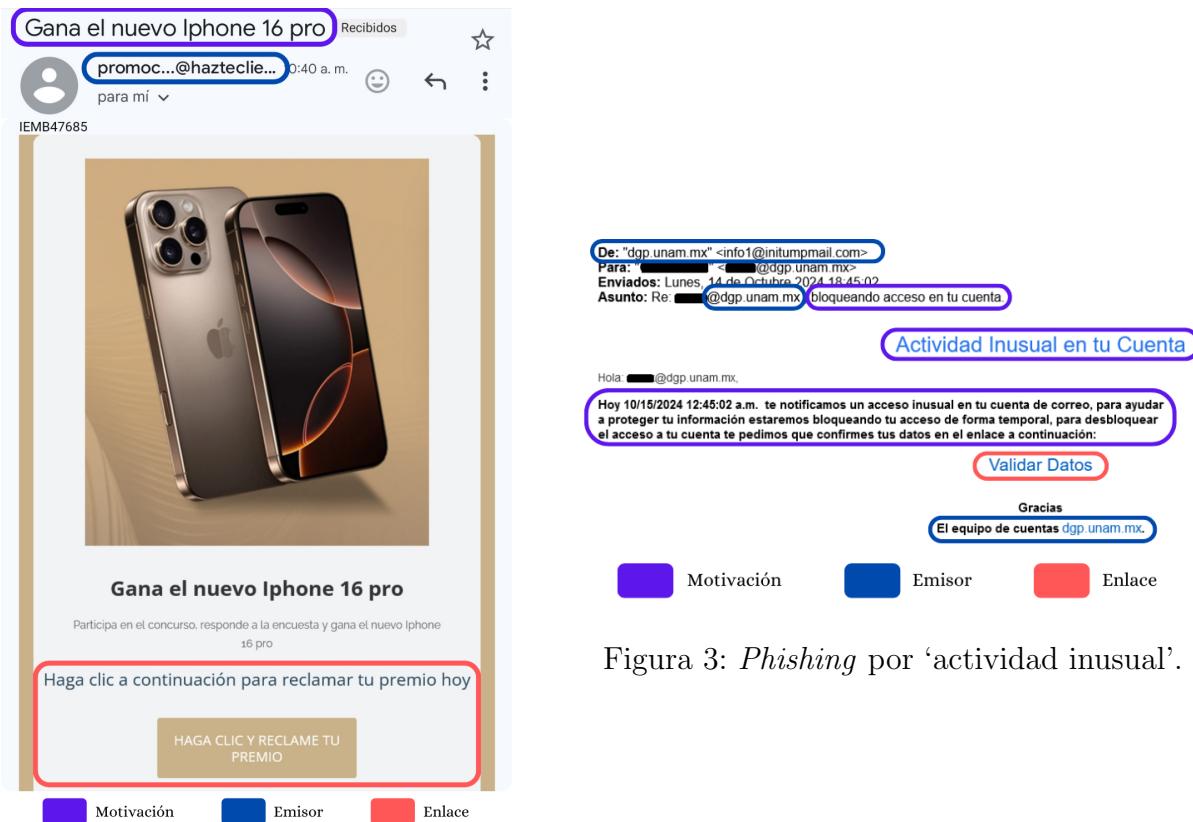


Figura 2: *Phishing* por ‘ganar un premio’.

Figura 3: *Phishing* por ‘actividad inusual’.

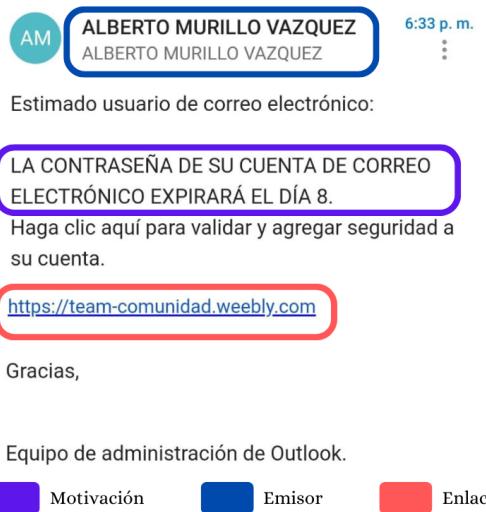


Figura 4: *Phishing* por ‘expiro de cuenta’.

## 2. *Phishing* por redes sociales

El *phishing* en redes sociales se realiza por medio de las herramientas de mensajería integradas en las aplicaciones, de manera similar al correo electrónico y a los mensajes de texto. Este tipo de ataque busca captar la atención 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 los datos de inicio de sesión para acceder a cuentas personales, por lo que, suelen incluir enlaces sospechosos.

### 2.1. Analiza la motivación del mensaje

Pon atención al tipo de mensaje que recibes. Los mensajes fraudulentos suelen:

- Prometer beneficios económicos, regalos o cualquier tipo de incentivo económico.
- Crear un sentido de urgencia para provocar que actúes rápidamente.
- Fingir que provienen de una fuente confiable o conocida utilizando tu nombre o tu correo para dirigirse a ti.

Si el mensaje te genera presión innecesaria o provee un beneficio material, desconfía y verifica directamente con la persona o entidad.

### 2.2. Examina al emisor

Antes de establecer una relación o de interactuar con el mensaje:

- Verifica el nombre de usuario o perfil del emisor. En estos ataques incluyen nombres desconocidos, combinaciones aleatorias de caracteres o bien la suplantación de identidad de un conocido.

- Si el mensaje ‘*proviene*’ de un amigo o familiar, confirma de forma directa con ellos la veracidad del mensaje para asegurarte que no se trata de un caso de suplantación de identidad.

### 2.3. Verifica los **enlaces** incluidos

Los mensajes de *phishing* en redes sociales suelen contener enlaces que pueden dirigir a sitios falsos. Considera siempre que:

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

Verifica que los enlaces siempre empiecen con **https**, pues esto indica que son sitios seguros, sin embargo, en algunos casos en empresas o servicios pequeños es seguro acceder a enlaces **http**. Si se trata de ‘comunicación’ del gobierno, los sitios oficiales suelen tener al final del enlace **.gob.mx**, en bancos e instituciones de confianza **.com** o **.mx**.

En la Figura 5 se muestra un ejemplo típico de *phishing* en redes sociales. El emisor es completamente desconocido, sin embargo, ofrece un beneficio lo suficientemente atractivo o desconocido para incitar a hacer clic en el enlace incluido. Observa las características clave mencionadas anteriormente, ahora señalizadas en la figura para ayudarte a identificar este tipo de amenazas de manera más sencilla.

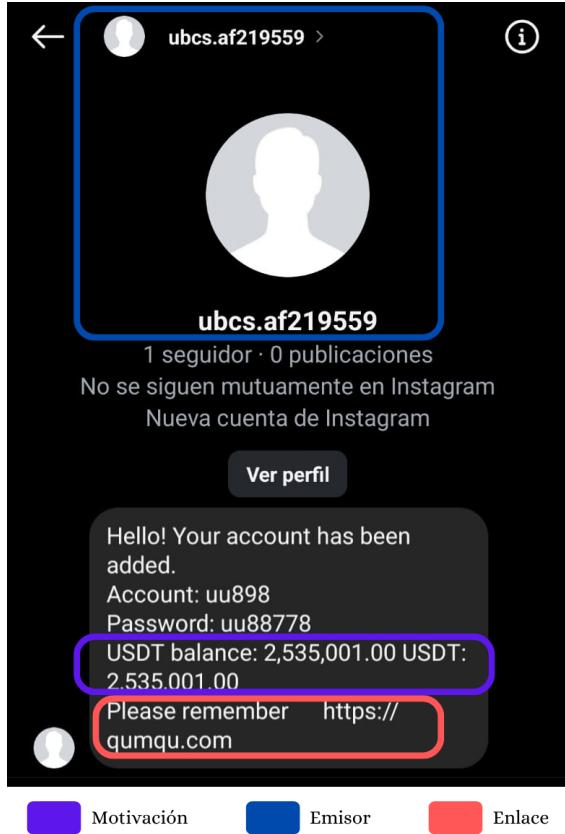


Figura 5: Ejemplo de *phishing* por redes sociales.

### 3. *Phishing* por sitios web

Los sitios web fraudulentos están diseñados con la finalidad de parecer legítimos, es decir, tratan de ser una copia del sitio original, sin embargo, su propósito es recopilar información personal de las víctimas. Se presentan algunas recomendaciones para poder identificar y evitar acceder a 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 y confidencial. Observa que los enlaces siempre empiecen con **https**, dado que indica que son sitios seguros, además, en caso de ser sitios gubernamentales oficiales suelen tener la terminación del enlace en **.gob.mx**, para bancos e instituciones de confianza en México **.com** o **.com.mx**.

#### 3.2. Consulta fuentes confiables

El Gobierno de México proporciona una lista de sitios falsos o apócrifos que intentan suplantar a instituciones gubernamentales, disponible en *Sitios web falsos* [2]. Esta lista es

una herramienta útil para confirmar la legitimidad de un sitio o enlace antes de interactuar.

Se ilustra una comparación entre un enlace legítimo (lado izquierdo) y uno fraudulento (lado derecho) en la Figura 6. Los sitios apócrifos suelen incluir apartados donde solicitan información personal, convirtiéndolos en una amenaza significativa. Evita proporcionar datos sensibles en sitios que no conozcas o que no sean proporcionados de forma oficial.

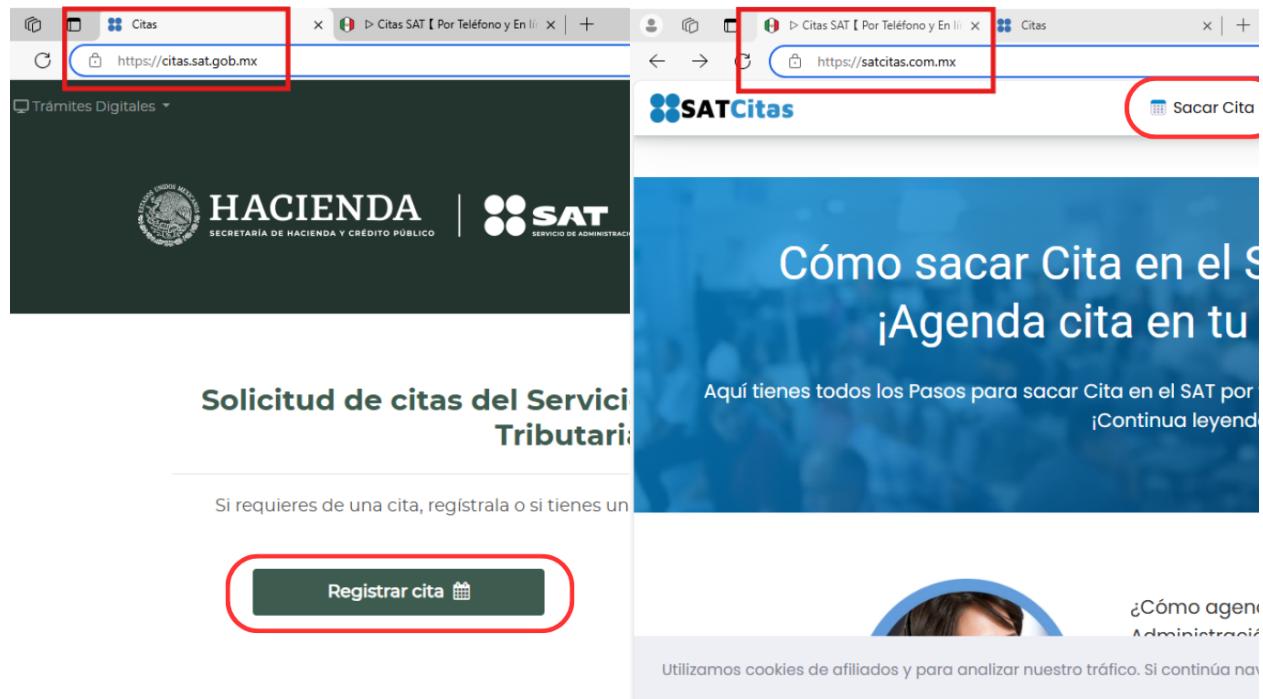


Figura 6: Ejemplo de *phishing* por sitios web.

## 4. *Phishing* de Wi-Fi

Este tipo de ataque utiliza puntos de acceso Wi-Fi o también conocidas como redes abiertas. Aunque el ataque no está dirigido a una persona u objetivo específico, estas redes pueden ser utilizadas para instalar *malware* en los dispositivos de las personas, recopilar información de inicios de sesión o abrir el navegador con formularios que solicitan datos personales o confidenciales.

### 4.1. Conéctate a redes seguras

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. De ser posible, se recomienda buscar la forma de omitir este paso.

## 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, podrías estar accediendo a una red no legítima.

En la Figura 7 y 8 se muestran algunos formularios, sin embargo, estas redes pertenecen a empresas oficiales y cuentan con términos y condiciones para el uso de datos ingresados, pero, existen formularios que no especifican de manera transparente quién tendrá acceso a los datos personales proporcionados en los formularios. Estas imágenes son solo ejemplos de formularios, no significan un ataque de *phishing*.

The figure displays two examples of web forms for connecting to public Wi-Fi networks. Both forms include fields for name, phone number, and email, which are highlighted with colored boxes to indicate they are sensitive data.

**Left Form (Acceder WiFi):**

- Header:** Acceder WiFi  
https://gate.zequenze.com
- Content:** Includes a promotional banner for \$289 per month with a \$50 discount for three months.
- Form Fields:** Registra tus datos para navegar
  - Nombre completo\*
  - Teléfono\*
  - Correo Electrónico\*
  - Edad
- Buttons:** Probar i

**Right Form (Acceder a \*.\* WiFi.\*):**

- Header:** Acceder a \*.\* WiFi.\*  
https://m... wifi.com
- Content:** Includes a logo for Zona WiFi.
- Form Fields:** NAVEGA GRATIS, POR FAVOR INGRESA TUS DATOS
  - Nombre completo
  - Correo electrónico
  - Número de celular (10 dígitos)
- Buttons:** Navega a la máxima velocidad

**Legend:**

- Nombre de la red Wi-Fi pública (Pink box)
- Datos confidenciales (Blue box)

Figura 7: Ejemplos de formularios que solicitan nombre, teléfono y correo.

The figure consists of two side-by-side screenshots of mobile web pages. Both pages are for 'Club WiFi' and feature a large pink button at the top labeled 'Acceder a WiFi'. Below this, there's a header with 'Invitado' and 'Conéctate con:' followed by a QR code. The main area contains a yellow box on the left with 'Selección tu opción' and 'Cliente i' (with a dropdown arrow), and a blue box on the right with 'Invitado' and 'Conéctate con:'. Below these are two input fields: 'Correo electrónico' (with a question mark icon) and 'Confirmá tu correo electrónico' (with a checkmark icon). A teal button labeled 'Navegar' is positioned between them. In the bottom left corner, there's a logo for '15 MESES'. At the bottom of the screen, there are two colored boxes: a pink one on the left and a teal one on the right. The pink box contains the text 'Nombre de la red Wi-Fi pública' and the teal box contains 'Datos confidenciales'. The right screenshot is identical to the left one, except it has a larger teal box covering the bottom half of the screen, which also contains the pink box.

Figura 8: Ejemplos de formularios que solicitan correo y contraseña.

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

Las aplicaciones de mensajería, como WhatsApp y Telegram, son las plataformas más comunes utilizadas para llevar a cabo este tipo de ataque debido a su popularidad y accesibilidad. Estas permiten una la comunicación inmediata de forma sencilla permitiendo tener una interacción en tiempo real.

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

Se pueden identificar este tipo de ataques, pues es frecuente recibir mensajes donde:

- Los salarios ofertados son excesivamente altos en comparación con el salario mínimo o con el promedio.
- Las ofertas laborales prometen ingresos de manera casi inmediata por realizar poco o ningún esfuerzo.

Si el mensaje ofrece beneficios materiales de alto valor, desconfía y rectifica la existencia de la institución a través de medios de contacto oficiales.

## 5.2. Examina al emisor

Es crucial confirmar la legitimidad del emisor o de las propuestas laborales antes de aceptar o interactuar de mayor manera con el emisor. Presta especial atención a:

- Propuestas de empleo realizadas por “altos cargos”.
- Revisar los datos del contacto, en ocasiones los contactos de empresas tienen la leyenda *Cuenta de empresa*

## 5.3. Verifica los enlaces incluidos

Incluyen enlaces externos o números desconocidos para ‘contactar’ directamente con la persona encargada de la contratación, contradiciendo el motivo principal del mensaje.

En las Figuras 10 y 11 se muestran ejemplos de mensajes con ofertas laborales, mientras que la Figura 9 presenta una ‘invitación’, diseñada así para generar un sentido de pertenencia.

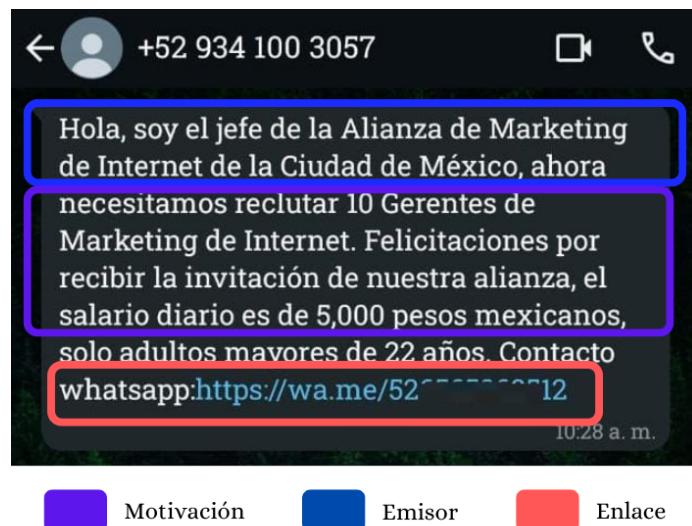
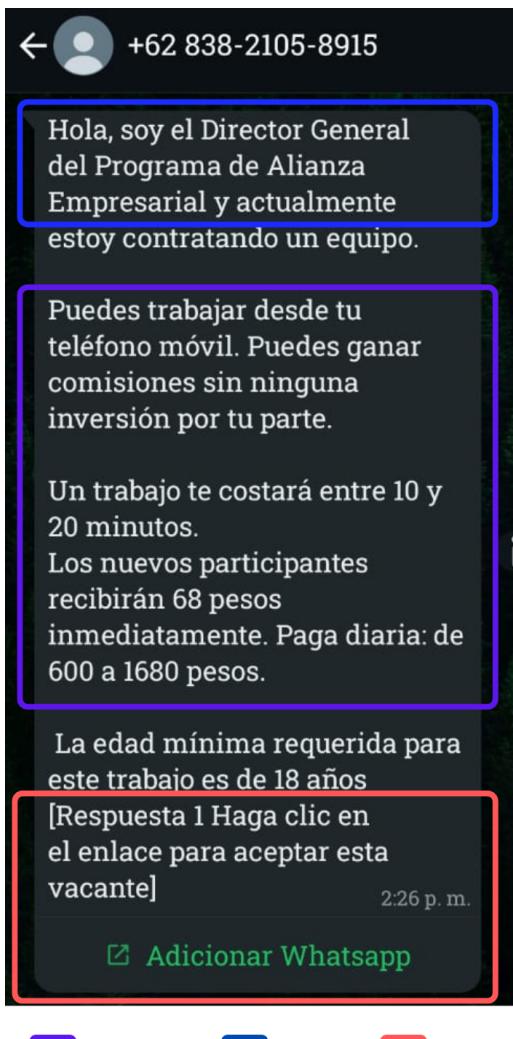


Figura 9: *Phishing* por IM por el ‘jefe’.



Motivación      Emisor      Enlace

Figura 10: *Phishing* por IM por el ‘Director’.

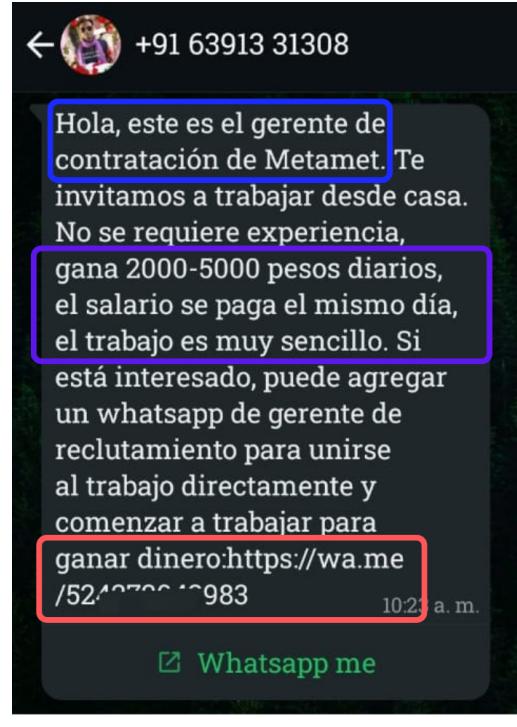
## 6. *SMishing*

El *phishing* por SMS (Servicio de mensajería corta), conocido como *SMishing*, busca engañar a las víctimas haciéndose pasar por **comunicaciones de confianza**, como bancos, empresas o servicios reconocidos.

### 6.1. Observa las características comunes

Este tipo de mensajes suelen incluir lo siguiente:

- Información personal como tu nombre.
- Detalles sobre problemas financieros, como robo de información bancaria, adeudos o pagos pendientes (véase la Figura 12).



Motivación      Emisor      Enlace

Figura 11: *Phishing* por IM por el ‘gerente’.

- Hacen mención a empresas o servicios reconocidos (véase la Figura 15) o a asistencia jurídica (véase la Figura 13).

## 6.2. Identifica los métodos de engaño

Los atacantes pueden incluir:

- **Enlaces** a sitios web falsos diseñados para recopilar tu información personal.
- **Números telefónicos** que pretenden ser líneas de contacto legítimas para establecer una comunicación externa y poder obtener tus datos confidenciales.

En la Figura 12 y 13 se muestran ejemplos de *SMishing* que dirigen a números telefónicos externos, mientras que en la Figura 14 y 15 dirigen a sitios falsos o apócrifos por medio de un enlace. Observa como utilizan a los servicios, empresas y a las instituciones financieras y de gobierno, para poder fingir establecer una **comunicación de confianza** y así no desconfíes de ellos.

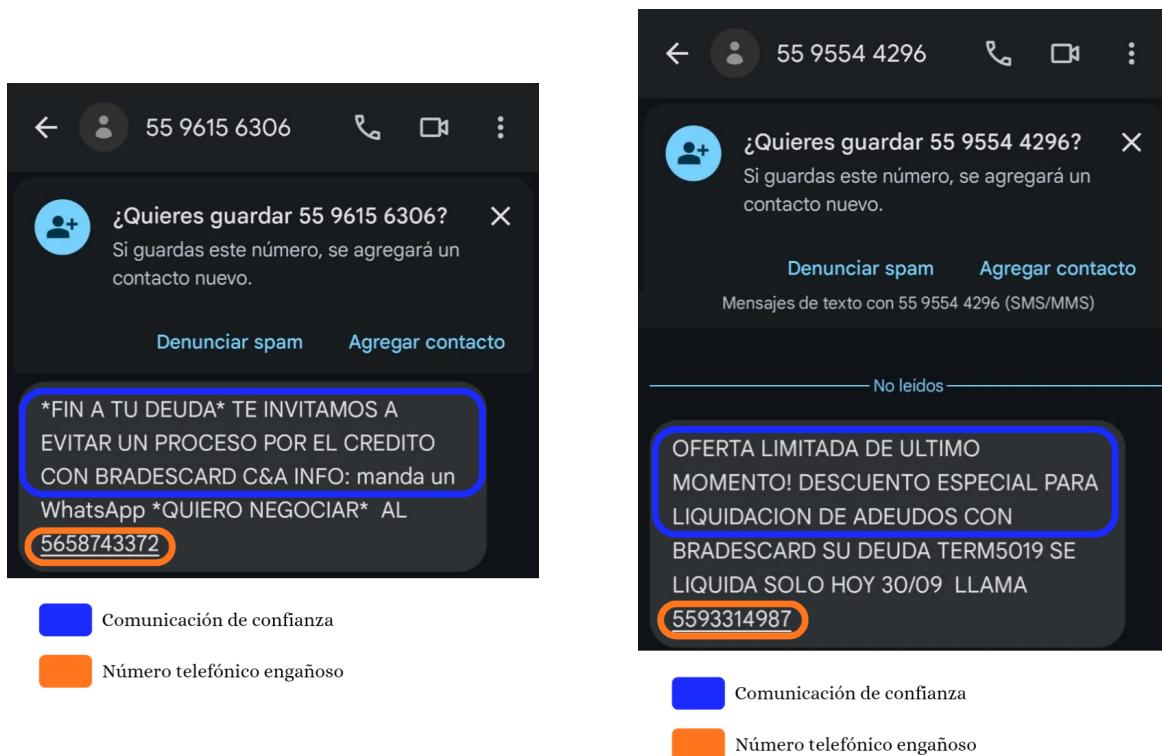
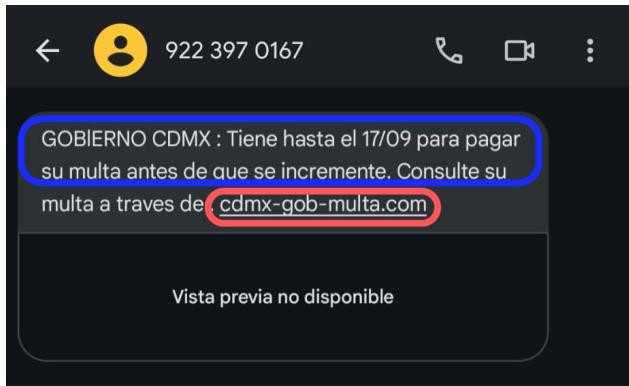
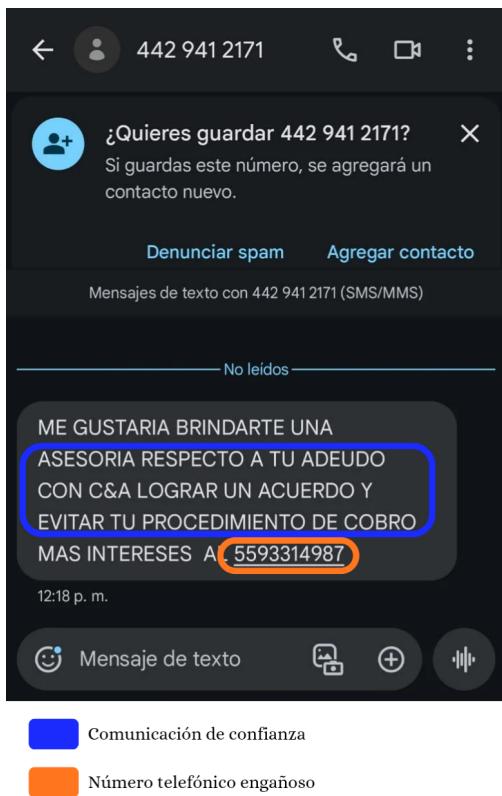


Figura 12: *SMishing* por adeudos.



Comunicación de confianza

Enlace

Figura 13: *SMishing* por servicios.

Figura 14: *SMishing* por ‘Gobierno’.

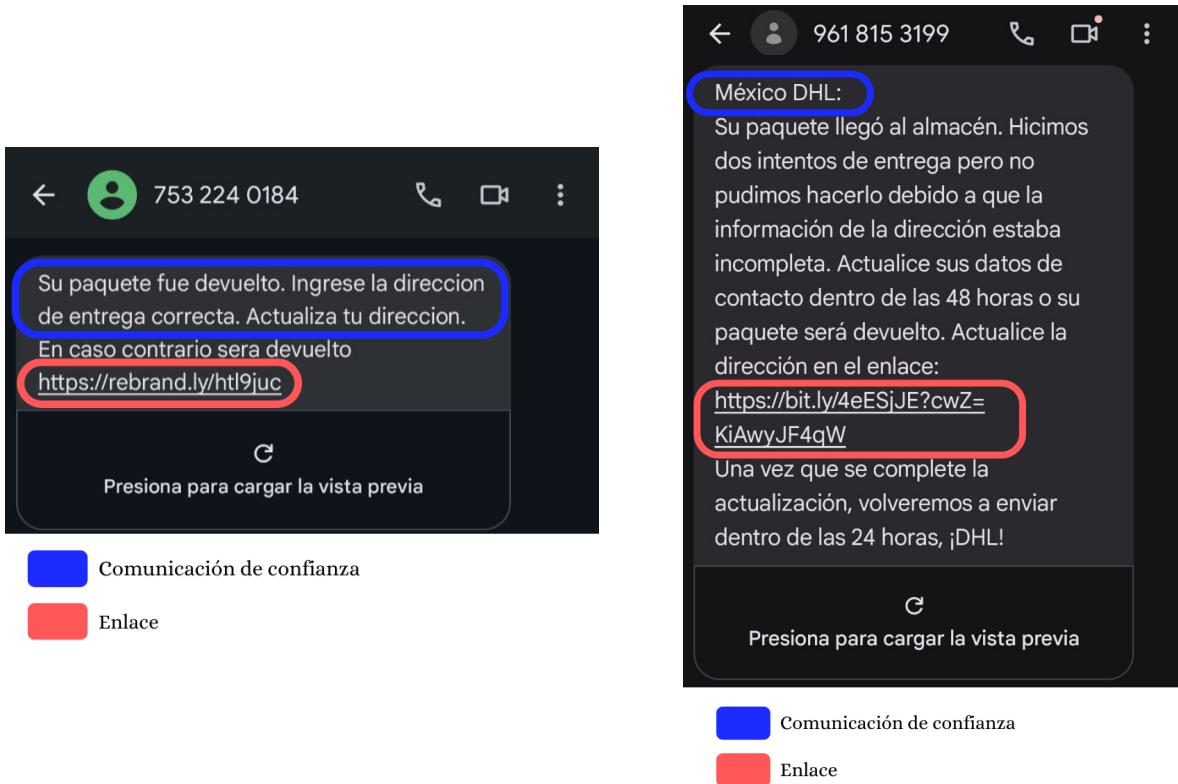


Figura 15: *SMishing* por ‘empresas’.

## 7. Vishing

El *phishing* por llamada telefónica, conocido como *vishing*, consiste en llamadas diseñadas para engañar y así obtener información confidencial, mayormente enfocadas a obtener acceso a aplicaciones de mensajería instantánea como WhatsApp y al robo de información bancaria. Este tipo de ataque utiliza la capacidad de falsificar números telefónicos, haciendo que las llamadas aparenten ser legítimas y no puedan ser detectadas fácilmente como sospechosas o como spam (veáse la Figura 16).

### 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 o por aplicaciones de mensajería instantánea. 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 compartas claves, códigos de acceso o contraseñas (sin importar que sean de 4, 6 u 8 dígitos).
- Verifique cualquier solicitud o movimiento comunicándose directamente con la institución bancaria a través de sus medios de contacto oficial.
- Si no desea ingresar desde otro dispositivo a sus cuentas, no proporcione claves de ningún tipo.

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 llamadas que herramientas de telefonía pueden detectar como “Spam” o “Posible Fraude”, como se ilustra en la Figura 16.

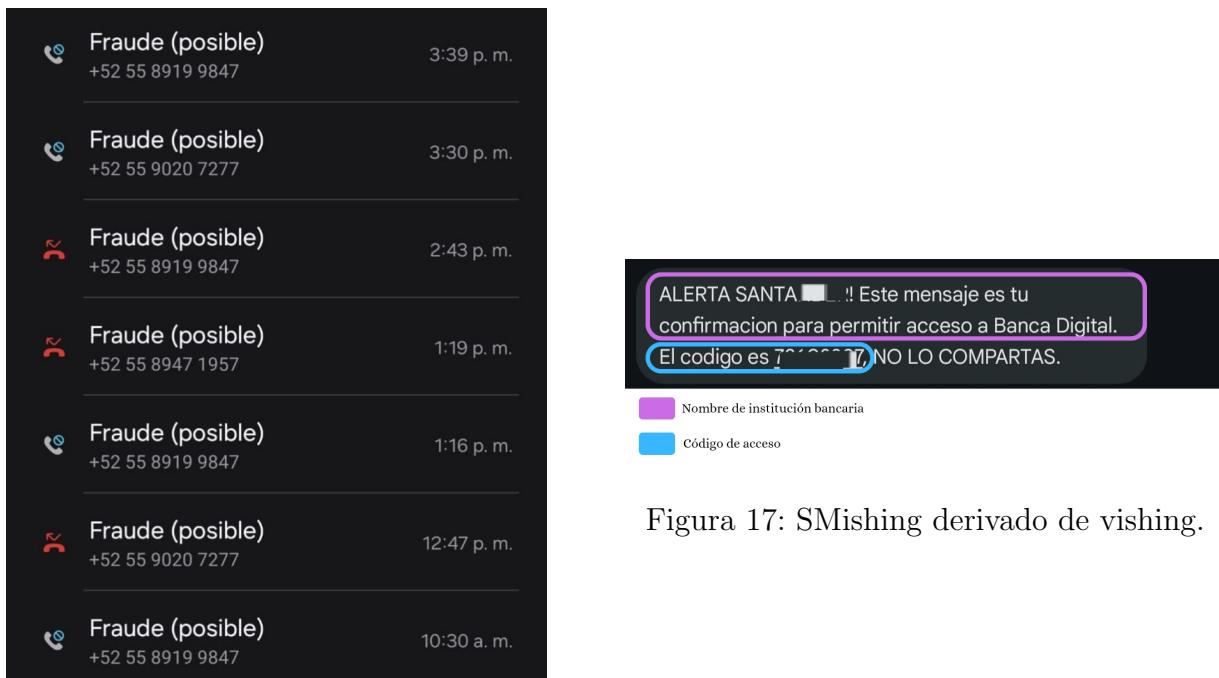


Figura 16: Ejemplo de llamadas detectadas como fraude.

Figura 17: SMishing derivado de vishing.

## Referencias

- [1] Cisco Networking Academy. Fundamentos de ciberseguridad. Curso en línea. Disponible en: <https://www.netacad.com/courses/cybersecurity-essentials?courseLang=es-XL> (Se requiere registro).
- [2] Servicio de Administración Tributaria. Sitios web falsos, 10 2024. Disponible en: <https://www.gob.mx/sat/acciones-y-programas/sitios-web-falsos>.