UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

El phishing como problema social: definición e identificación

TESINA

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Cecilia Fernanda San Miguel Iturria

DIRECTORA DE TESINA

Dra. Rocío Alejandra Aldeco Pérez

Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado EL PHISHING COMO PROBLEMA SOCIAL: DEFINICION E IDENTIFICACION que presenté para obtener el titulo de INGENIERA EN COMPUTACIÓN es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

CECILIA FERNANDA SAN MIGUEL ITURRIA
Número de cuenta: 317269868

Dedicatoria ...

A mi padre y a mi madre, quienes a lo largo de mi vida me han dado todo, incluso aquello con lo que no contaron. Por impulsarme a ser mejor, por motivarme a dar siempre lo mejor de mí, y por ser los motores de mi vida. Quienes me han dado la fuerza, el valor y la calidez para seguir adelante en la búsqueda de mis sueños. Por nunca dejarme sola y por siempre estar presentes en los momentos de incertidumbre.

A mi familia, por mantenerse firme y cercana en cada paso que doy.

A mis amistades cercanas, quienes fueron un apoyo constante dentro y fuera de la universidad, quienes hicieron que los días difíciles lo fueran un poco menos.

A mi pareja, por acompañarme hasta la culminación de mis estudios, motivándome siempre a dar más y a luchar por lo que deseo.

Agradecimientos

DGAPA por su apoyo a través del proyecto PAPIME PE101125.

Agradezco profundamente a mis padres, no sólo por su amor y apoyo incondicional en todo momento a lo largo de mi vida, sino también por siempre apoyarme, por pensar en mi mejor futuro, en mis mejores intereses y en mi mejor versión del mañana.

A mis amistades cercanas, quienes me brindaron apoyo emocional y ánimo en los momentos difíciles. Cada conversación, risa y palabra de aliento fueron esenciales en este camino.

A mi pareja, por estar presente en cada paso de este proceso, por creer en mí incluso cuando yo dudé y por inspirarme a seguir creciendo.

A mis profesores y profesoras, quienes compartieron no solo sus conocimientos sino también su pasión por la enseñanza. Por motivarme a pensar críticamente, por nunca dejar de creer en mí y por motivarme a lo largo de mi trayectoria académica.

Finalmente, agradezco a todas las personas que contribuyeron a que esta meta fuera alcanzada, con ejemplos, textos, palabras y enseñanzas que hoy forman parte de este documento y de este gran logro.

Resumen

En la era tecnológica actual, donde la comunicación a través de teléfonos celulares se ha convertido en una actividad cotidiana importante, enfrentamos un creciente riesgo ante ciberataques como el *phishing*. [1, 2, 3] Este tipo de amenaza se aprovecha del uso intensivo de dispositivos conectados a Internet, así como del desconocimiento o falta de precaución al utilizarlos, más que de vulnerabilidades técnicas específicas. [4]

En América Latina los intentos de ataques de *phishing* bancario han aumentado un 50 % en los últimos años, afectando principalmente a los sectores gubernamentales, financieros y los usuarios individuales de Internet. México se encuentra entre los países más afectados de América Latina, entre agosto de 2023 y julio de 2024 se registró un crecimiento del 220 % en ataques de *phishing*, con un total de 118 millones de amenazas detectadas, lo que equivale a 325 mil ataques diarios. [5] A pesar de que el gobierno de México ha implementado estrategias nacionales contra el fraude cibernético, como por ejemplo, campañas informativas en las que se presentan los métodos utilizados por los ciberdelincuentes [6] o páginas web que brindan información sobre los tipos de fraude y cómo prevenirlos, [4] la sociedad sigue enfrentando dificultades para identificar estos ataques, exponiendo sus datos más sensibles o siendo víctimas de fraudes.

Índice general

Índice de figuras

Capítulo 1

Introducción

En la actualidad, los teléfonos celulares no son solo herramientas de comunicación, sino que se han convertido en el medio predominante y más accesible de interacción en la vida cotidiana de la sociedad en general. [9] Este aumento significativo en el uso de celulares como canal principal de comunicación ha traído consigo diversas implicaciones, especialmente en áreas como seguridad digital y educación tecnológica. No basta con disponer de un dispositivo, resulta fundamental comprender los riesgos a los que estamos expuestos a través de ellos. Entre estos, destacan los ciberataques, como el *phishing*, un ataque basado en una técnica de ingeniería social utilizado por ciberdelincuentes para obtener información confidencial como contraseñas, datos personales o bancarios, mediante correos electrónicos, mensajes o sitios web falsos que aparentan ser legítimos. [1, 2, 3]

En los últimos años, América Latina ha experimentado un crecimiento constante en las amenazas cibernéticas, siendo el *phishing* bancario una de las más frecuentes y preocupantes. Esta modalidad de ataque ha impactado de forma particular a instituciones gubernamentales y financieras, comprometiendo la seguridad de millones de usuarios. En este contexto, México destaca como uno de los países más afectados de la región: tan solo entre agosto de 2023 y julio de 2024 se detectaron más de 118 millones de intentos de *phishing*, lo que representa un alarmante incremento del 220 % y un promedio diario de 325 mil ataques. [5] Esta situación subraya la necesidad urgente de fortalecer las estrategias de prevención, concientización y respuesta ante este tipo de amenazas.

Los esfuerzos que actualmente se realizan para mitigar amenazas como el *phishing* están

mayormente orientados a apoyar a las empresas y a la detección de manera automatizada haciendo uso de algún tipo de software especializado dejando de lado a los individuos. Sin embargo, el 95 % de las violaciones de ciberseguridad se debe a errores humanos, por lo que, es necesario formar a los individuos en este tema al estar en riesgo diariamente. La exposición de datos sensibles y fraudes derivados de los ataques de *phishing* se debe principalmente al desconocimiento y la falta de habilidades por parte de estos usuarios para identificarlos.

A pesar de las estrategias Nacionales Antifraude Cibernético implementadas por el gobierno de México, la sociedad sigue siendo vulnerable a ciberataques. Ejemplo de esto son las estafas que suplantan al mismo gobierno de la CDMX vía mensajes de texto (también conocidos como SMS), que terminan siendo efectivas pues los ciudadanos no saben cómo identificar un ataque de una petición real. Por esto, es urgente presentar recursos que permitan a los individuos conocer e identificar el *phishing* a través de los recursos que utilizan comúnmente en su celular, de tal manera que estos tengan la capacidad de protegerse contra estas amenazas.

Así este trabajo tiene como objetivo crear una guía paso a paso que permita a la sociedad identificar y comprender los distintos tipos de *phishing* de manera clara y sencilla. Para lograr este objetivo, se realizó una revisión sistemática de la literatura pertinente al tema, lo que permitió definir el concepto de *phishing* así como los tipos existentes. Posteriormente, se realizó la identificación de casos reales mediante el análisis de notas periodísticas y artículos, lo cual facilitó la recopilación y análisis, así como la elaboración de un estudio comparativo sobre los trabajos y soluciones propuestas al momento. Esta información es la base de una guía que presenta ejemplos reales de estafas por medio del *phishing* e incluye algunas recomendaciones breves para su identificación. Finalmente, la guía fue validada por individuos y mejorada con su retroalimentación hasta llegar a su versión final.

Este documento se divide en seis capítulos, siendo el primero esta introducción. El segundo capítulo presenta el marco teórico, cuyo propósito es proporcionar una introducción progresiva al fenómeno del *phishing*, comenzando con la definición de conceptos fundamentales que faciliten su comprensión. A medida que avanza, se profundiza en los

aspectos técnicos relacionados con *phishing*, abordando definiciones específicas y metodologías asociadas al análisis de este tipo de ataque cibernético. Este capítulo concluye con una revisión comparativa de las soluciones actuales para mitigar los ataques de *phishing*, basándose en los enfoques más recientes descritos en la literatura técnica especializada.

En el tercer capítulo se realiza un análisis contextualizado del problema, centrado específicamente en el contexto de nuestro país, tomando como referencia los recursos proporcionados por organismos públicos especializados en la protección contra fraudes digitales y ciberseguridad.

El cuarto capítulo se dedica a la presentación de la propuesta de solución, estructurada como una guía práctica paso a paso para la identificación de ataques de *phishing*. Esta guía está diseñada para ser accesible, utilizando ejemplos reales de *phishing* que faciliten la comprensión y la detección de estos ataques. La propuesta se desarrolla alineada a los objetivos establecidos en este trabajo, orientados a promover la educación y la prevención de *phishing* en la sociedad mexicana de forma clara y sencilla.

El quinto capítulo presenta el análisis de la evaluación por parte de individuos a la información y la guía desarrollada. Finalmente, en el sexto capítulo se presentan las conclusiones de este trabajo así como el trabajo futuro.

Capítulo 2

Marco teórico

Dado que uno de los objetivos de este trabajo es definir el *phishing*, esta sección presenta una definición de ciberseguridad haciendo énfasis en las formas en las que esta es violada a través del *phishing*. Posteriormente, se describen algunos tipos de ciberataques existentes para facilitar la introducción al término *phishing*. Adicionalmente, se presenta una clasificación de los tipos de *phishing* con base en las técnicas utilizadas, para finalizar con una revisión de las soluciones actuales analizando sus características similares y presentándolas en tablas comparativas.

2.1. Ciberseguridad

La **Ciberseguridad** se refiere a cualquier práctica, tecnología o política utilizada para proteger equipos, archivos, redes, aplicaciones, datos, activos financieros y a personas. [10, 11] Existen varios tipos de amenazas a la ciberseguridad, también conocidas como ciberamenazas, que buscan acceder sin autorización al sistema de organizaciones o de individuos de distintas formas. [12]

Un **ciberataque** o **ataque cibernético** se puede definir como cualquier esfuerzo realizado por un atacante con la intención de robar, exponer/alterar datos o aplicaciones a través de un acceso no autorizado a una red, sistema informático o dispositivo digital. [13, 14] Ejemplos de ciberataques son el *ransomware*, las estafas de *phishing*, el robo de datos o de identidad, entre otos. [15]

A continuación se describen algunas amenazas a la ciberseguridad que pueden ser utilizadas para implementar ataques de *phishing*:

Definición 1 (***Malware***)**.** ***Malware*** *es el término general para cualquier programa computacional o* ***software*** *diseñado para causar daño a dispositivos o redes (alterando o eliminando archivos), acceder de manera no autorizada para extraer información confidencial (como contraseñas y números de cuenta), enviar correos electrónicos malintencionados, o interrumpir el funcionamiento de una infraestructura o servicio. [12, 15] El* ***malware*** *se puede instalar al hacer clic en un enlace o al descargar archivos adjuntos en un correo o desde internet. Ejemplo de esto son los virus. [11, 12]*

Definición 2 (***Ingeniería Social***)**.** *La* ***Ingeniería Social*** *es el nombre de una técnica de engaño utilizada para hacer que la víctima revele información confidencial, ya sea a través de engaños, solicitando un pago o pidiendo datos confidenciales. La* ***Ingeniería Social*** *puede hacer uso de cualquier otro tipo de ciberamenazas para motivar a la víctima a hacer clic en un enlace, descargar algún tipo de malware o acceder a fuentes maliciosas. [12, 16]*

Definición 3 (***Amenaza Interna***)**.** ***Amenaza Interna*** *es el nombre que se le da a una amenaza en la que las personas que ya tienen acceso a sistemas, como los empleados o clientes, provocan una vulneración de seguridad o pérdida financiera. En ocasiones se puede dar de forma involuntaria, como cuando un empleado guarda información confidencial en una cuenta de la nube personal y no en la de la empresa. [12] En otros casos se realiza de manera malintencionada. [11, 12]*

2.2. Introducción al *phishing*

El término *phishing* proviene de la palabra en inglés "*fishing*" (pesca), en alusión a la idea de lanzar un señuelo para "atrapar" a la víctima. Este tipo de ataque busca obtener información sensible, como datos personales o bancarios, mediante el engaño y la manipulación de la confianza del usuario [17].

El ataque de *phishing* generalmente se inicia con un señuelo [18], que puede presentarse dentro de un correo electrónico, mensaje de texto o llamada telefónica que aparenta provenir de una fuente legítima o confiable. El atacante se hace pasar por una persona u organización de confianza (por ejemplo, un compañero de trabajo, familiar, jefe, empresa, institución pública o entidad bancaria) con el propósito de inspirar credibilidad y obtener información valiosa [19, 20]. Estos mensajes suelen apelar a la urgencia o al interés personal de la víctima para inducirla a hacer clic en un enlace [17] que conduce a un sitio falso. Dicho sitio redirige a formularios que solicitan información personal, como nombre, usuario, contraseñas, número de identificación [21] y, con frecuencia, datos financieros o bancarios.

Alabdan [7] menciona que existen técnicas generales para realizar un ataque de *phishing* y todas estas tienen en común tres componentes que funcionan entre sí. Estos son: el *medio*, el *vector*, y el *enfoque técnico*. Ciertos vectores son adecuados para ciertos medios, y algunos enfoques técnicos son apropiados para vectores de ataque específicos. Como puede verse en la figura 2.1, `medio` se refiere al canal por el cual se lleva a cabo el ataque de *phishing*. El `vector` hace referencia a la vía de ataque, la cual está limitada por el `medio`. Los `enfoques técnicos` son los métodos que se emplean durante el ataque, a menudo utilizados en conjunto con técnicas de ingeniería social para aumentar las probabilidades de éxito del atacante.

Las técnicas generales de *phishing* se describen en el capítulo siguiente. Conocer estas técnicas es fundamental para entender por qué resulta tan difícil identificar un ataque de *phishing*, ya que puede ejecutarse de diversas formas (véase las Secciones: *Medios de phishing* 2.3, *Vectores de phishing* 2.4, *Enfoques técnicos de phishing* 2.5).

Usualmente los ataques de *phishing* utilizan alguna técnica de ingeniería social, [19, 22] que a diferencia de otros tipos de ciberataques orientados a atacar dispositivos o recursos para obtener información, estos **utilizan errores humanos, engaños y manipulación de las víctimas** [23] para que proporcionen información confidencial de manera involuntaria. Estos ataques en ocasiones hacen uso de otros *enfoques técnicos* para motivar a la víctima a hacer clic en un enlace, descargar algún tipo de *malware* o de acceder a fuentes maliciosas, [12, 16] esto para incrementar las posibilidades de éxito en el ataque, además de que permiten su automatización y masificación.

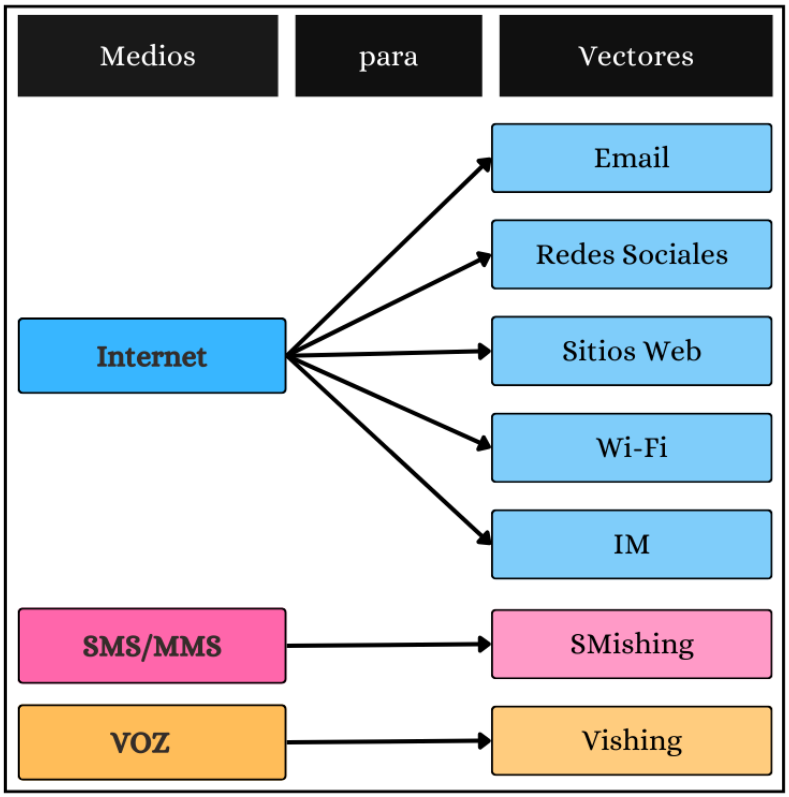


Figura 2.1: Asignación de los medios a vectores. Fuente: Alabdan [7].

En la figura 2.1 se empleó una codificación por colores para asociar y diferenciar los distintos medios de comunicación y sus vectores de ataque asociados. El color azul representa los medios relacionados con Internet, el rosa identifica al vinculado con los SMS/MMS y finalmente el naranja al que está relacionado con la voz. A continuación, se describen las técnicas generales de *phishing* resaltados siguiendo la codificación cromática para facilitar su identificación visual.

2.3. `Medios` de *phishing*

Como se ha señalado previamente, el `medio` determina los *`vectores`* y *`enfoques técnicos`* empleados en un ataque. Por tal motivo, se considera el componente más relevante dentro de los ataques de *phishing*, pues constituye el canal mediante el cual el atacante (*phisher*) interactúa directamente con la víctima. En este contexto, pueden identificarse tres `medios` principales a través de los cuales estos ataques suelen ejecutarse:

- Internet
- Servicio de mensajería corta *(SMS o Short Message Service)* o Servicio de mensajería multimedia *(MMS o Multimedia Messaging Service)*
- Voz

Para el caso del Internet, este se encuentra en constante evolución, lo que significa que continuamente se crean nuevas formas de comunicación, lo cual a su vez genera nuevos enfoques de ataque que van desde el correo electrónico hasta redes sociales como Facebook, Instagram, Snapchat, Whatsapp, etc. [24] Cada uno de estos canales de comunicación presenta vulnerabilidades que permiten al *phisher* engañar a las víctimas.

En relación a los *SMS*, comúnmente llamados "mensajes de texto", permiten la comunicación mediante mensajes cortos de texto. Con el paso del tiempo, evolucionaron a *MMS*, que además de texto permiten enviar fotos, videos o imágenes animadas. Estas opciones permiten que el *phisher* haciendo uso de estas opciones interactúe de manera más efectiva con la víctima haciéndose sentir más cercano o confiable.

Para el caso de la voz como principal medio de comunicación en nuestra vida diaria, esta también es utilizada para ejecutar este tipo de ataque, con el propósito de inducir a las personas a revelar información personal, generalmente mediante llamadas telefónicas o mensajes de audio. [24]

2.4. `Vectores` de *phishing*

Los `vectores` de ataque disponibles dependen del `medio` que utiliza el *phisher* y constituyen el canal a través del cual se lleva a cabo el ataque de *phishing* (véase la figura 2.1). A continuación, se describen los `vectores` (canales) utilizados en cada uno de los `medios` descritos previamente.

2.4.1. *Phishing* por *correo electrónico (Email)*

Este vector es la forma más común de *phishing*, ya que consiste en la distribución de correos electrónicos masivos diseñados para atraer a la víctima mediante enlaces a sitios

falsos que posteriormente son utilizados para extraer información personal. [7] Además existen diversos `enfoques técnicos` que los *phishers* pueden adoptar al utilizar este `vector` para incrementar las posibilidades de éxito, algunos de estos se definen en la **próxima sección** (véase la Sección 2.5).

2.4.2. *Phishing* por *redes sociales*

El *phishing* en redes sociales hace uso de las herramientas de mensajería incorporadas a estas aplicaciones para poder engañar a las personas. Los *phishers* emplean plataformas, como Facebook, LinkedIn, X (anteriormente Twitter) e Instagram, de manera similar al correo electrónico y los mensajes de texto, compartiendo enlaces o redactando mensajes que parecen ser de contactos de confianza. [22, 25] Los *phishers* crean perfiles falsos para establecer una relación con la víctima y ganar su confianza antes de lanzar el ataque. De esta manera se hacen pasar por usuarios que necesitan ayuda para, por ejemplo, iniciar sesión en su cuenta o fingir que la víctima ha ganado un concurso y es acreedor a un premio. Esto con el fin de robar las credenciales de inicio de sesión de la víctima y de esta manera acceder a su cuenta. [22, 25]

2.4.3. *Phishing* por *sitios web*

Existen sitios web fraudulentos que imitan la apariencia de los portales oficiales, empleando el mismo diseño, colores y denominación, con el fin de recopilar información personal de las víctimas. El atacante (*phisher*) puede además emplear diversos `enfoques técnicos` para incrementar la eficacia del fraude. Los `enfoques técnicos` relevantes se describen en la **siguiente sección** (véase la Sección 2.5).[7]

2.4.4. *Phishing* por *Wi-Fi*

Este vector suele utilizar puntos de acceso Wi-Fi públicos, por tanto, el ataque no se dirige necesariamente a un objetivo en particular. No obstante, el atacante puede aplicar un `enfoque técnico` (véase la Sección 2.5) para seleccionar un punto de acceso que es frecuentemente usado por la víctima. El *phishing* mediante Wi-Fi puede implementarse

de diversas formas, por ejemplo mediante la instalación de *malware* en el dispositivo de la víctima para extraer credenciales o mediante la redirección a sitios web falsos, de manera análoga a otras modalidades de *phishing*.

2.4.5. *Phishing* por *Mensajería instantánea (IM)*

Los medios de *mensajería instantánea (IM)* más populares, y que no están directamente integrados en las redes sociales, son WhatsApp y Telegram. Estas plataformas permiten el envío de emojis, fotografías, vídeos, archivos y enlaces, así como la realización de llamadas de audio, videollamadas y el intercambio de notas de voz. Al ser un canal de comunicación masivo, accesible y de respuesta inmediata, constituyen un vector idóneo para los *phishers*, pues facilitan la interacción en tiempo real con la víctima y aumentan las oportunidades de inducirla a revelar información personal. [7]

2.4.6. *Phishing* por SMS o SMishing

El medio de SMS/MMS posibilita la existencia del vector denominado *SMishing*, término que combina las palabras *"SMS"* y *"phishing"*. En este el atacante realiza *phishing* mediante *SMS* y presenta dos enfoques principales.[26]

El primero consiste en el envío de mensajes de texto que simulan provenir de fuentes confiables (por ejemplo, bancos o empresas reconocidas) e incluyen información personalizada, como el nombre de la víctima o detalles sobre supuestos robos bancarios. Estos mensajes suelen redirigir a la persona afectada hacia un sitio web o número telefónico fraudulento para obtener sus datos personales. Una vez obtenidos, los *phishers* los emplean en su beneficio. [7, 27]

El segundo enfoque se basa en el envío de mensajes que contienen algún tipo de *malware*, ya sea mediante enlaces a sitios web maliciosos o a través de la descarga de archivos o aplicaciones comprometidas. Este tipo de ataque permite al *phisher* sustraer contactos y mensajes, crear redes de bots o robar credenciales de autenticación utilizadas en inicios de sesión o transacciones en línea. [28, 29]

2.4.7. *Phishing* por llamadas de voz o Vishing

El *phishing* de voz o por llamada telefónica, también conocido como *vishing*, consiste en la realización de llamadas telefónicas con el objetivo de hacerse pasar por otra persona y así engañar a una víctima.

El *vishing* utiliza la capacidad de falsificar un número para que una llamada parezca originarse en una fuente legítima haciendo uso de la tecnología conocida como *VoIP* que permite ocultar la ubicación física real y realizar millones de llamadas automatizadas al día, permitiendo manipular a la víctima para que revele información sensible. [7, 26] Las llamadas de *vishing* suelen alarmar a las víctimas con "advertencias" sobre problemas de pagos con tarjetas de crédito, pagos atrasados o asuntos legales, llevándolas a proporcionar información confidencial o dinero a los *phisher* para que les ayuden a "resolver" estos problemas. [25]

2.5. `Enfoques técnicos` empleados en *phishing*

A través de los `vectores` descritos anteriormente, el atacante (*phisher*) puede poner en práctica diversos `enfoques técnicos` dirigidos a la obtención y exfiltración de información personal. En esta sección se presentan y analizan dichos enfoques, enfatizando sus mecanismos operativos, condiciones de aplicación y el impacto que tienen sobre la probabilidad de éxito del ataque [7].

2.5.1. Spear *phishing* o *phishing* selectivo

El *spear phishing* es un ataque por medio del correo electrónico (*email*) (véase la Sección 2.4.1). Este está dirigido a un individuo específico que se sabe tiene acceso privilegiado a datos confidenciales o es una autoridad especial que el estafador *(spear phisher)* desea explotar. Por ejemplo, este tipo de ataque es común que se dirija a un gerente de finanzas que puede realizar transacciones con las cuentas de la empresa. [7, 25, 26]

Inicia con una investigación detallada por parte del *spear phisher* sobre sus objetivos, esto para crear mensajes convincentes. Usualmente el atacante se hace pasar por alguien

en quien el usuario objetivo confía, como un amigo, compañero de trabajo, jefe, proveedor o institución financiera, esto hace que sea más difícil de detectar y detener. [26]

Las redes sociales y los sitios de redes profesionales son actualmente fuentes de información clave para la investigación del *spear phisher* pues es donde las personas felicitan públicamente a sus compañeros de trabajo, y donde tienden a compartir información en exceso. Esto ayuda a elaborar mensajes que contienen detalles personales específicos, haciéndolo altamente creíble para el objetivo. Por ejemplo, un *spear phisher* podría hacerse pasar por el jefe del objetivo y enviar un correo electrónico que diga: "Sé que te vas esta noche de vacaciones, pero ¿puedes pagar esta factura antes del cierre de operaciones de hoy?". [25]

2.5.2. Business-Email-Compromise *(BEC)*

El *BEC* traducido como "compromiso del correo electrónico empresarial" es un tipo de ataque derivado del *spear phishing* (véase la Sección 2.5.1) cuya víctima es una organización gubernamental o comercial. A través de ese ataque se intenta robar información valiosa para la víctima, tales como son secretos comerciales, datos de clientes o información financiera.

Los ataques BEC pueden darse de varias formas. A continuación, se describen dos de los más comunes. [25]

- *Fraude del Director Ejecutivo*: El *phisher* secuestra la cuenta de correo electrónico de un ejecutivo de alto nivel y se hace pasar por él en la empresa. El *phisher* envía un mensaje a un empleado de nivel inferior dando indicaciones para que transfiera fondos, realice una compra o envíe archivos a una parte no autorizada. [25]

- *Compromiso de la cuenta de correo electrónico*: El *phisher* compromete o utiliza la cuenta de correo electrónico de un empleado de menor nivel, como la de un gerente de finanzas o ventas. Este envía facturas fraudulentas a los proveedores, instruye a otros empleados para que realicen pagos o les solicita acceso a información confidencial. [25]

Este tipo de ataque puede generar un efecto en cadena, en el que el compromiso de una cuenta inicial conduce al acceso o manipulación de otras, fenómeno conocido como

ataque de plataforma de lanzamiento [30]. Con frecuencia, los *phishers* permanecen durante semanas o incluso meses dentro de las redes de una organización, observando y analizando su funcionamiento. Este reconocimiento puede incluir el estudio del sistema de facturación, la relación con proveedores o la actividad de un empleado en particular, a menudo un ejecutivo de alto nivel. Una vez obtenida la información necesaria, el atacante envía un correo electrónico cuidadosamente diseñado para solicitar la transferencia de fondos o la ejecución de una acción financiera conforme a sus intereses [7].

2.5.3. Whaling

Cuando los *phishers* dirigen sus ataques hacia ejecutivos de alto nivel (como directores de empresas o funcionarios gubernamentales), la técnica se conoce como whaling o "caza de ballenas" [25], término que proviene del inglés *whale*, que significa ballena [22]. Debido a que se trata de un ataque altamente dirigido, los atacantes invierten tiempo y esfuerzo en diseñar mensajes sumamente convincentes, con el fin de que resulten prácticamente indistinguibles de las comunicaciones legítimas de la organización objetivo.

El `vector` más probable para este ataque es el correo electrónico (véase la Sección 2.4.1). De la misma manera en el caso del *spear phishing*, el objetivo del atacante es instruir a su víctima a instalar *malware* que proporcione acceso al sistema. Este se distribuye de la manera habitual en un archivo adjunto infectado o como un enlace para descargarlo. El propósito de este *malware* es monitorear las pulsaciones de teclas y/o otorgar al *phisher* acceso al sistema infectado, desde el cual puede continuar su ataque, utilizando así los privilegios que ha obtenido. Es posible que el *whaling* en sí mismo sea solo la etapa preliminar del ataque general, con un aumento en lo que se conoce como compromiso del *BEC* (véase la Sección 2.5.2). [7, 22, 26]

2.5.4. QRishing

Los códigos Quick Response (QR, por sus siglas en inglés), o códigos de respuesta rápida, son matrices bidimensionales compuestas por píxeles en blanco y negro que permiten almacenar y transmitir información comprimida. En comparación con los códigos de

barras unidimensionales, los códigos QR ofrecen una mayor capacidad de almacenamiento y legibilidad. Su lectura se realiza mediante un escaneo óptico, tras el cual un lector o aplicación decodifica la información contenida. Usualmente el escaneo se hace con la cámara de un teléfono celular.

El uso de códigos QR ha incrementado significativamente con la proliferación de dispositivos móviles inteligentes. Actualmente, las empresas los emplean para actividades de seguimiento, pagos, promociones, descuentos y para redirigir a los usuarios hacia sitios web o aplicaciones. Estos códigos se encuentran en empaques, medios impresos, vallas publicitarias, anuncios escolares y redes sociales, entre otros. No obstante, también pueden ser aprovechados como vectores de ataque en campañas de *phishing*. Los atacantes pueden generar códigos QR maliciosos que redirigen a un sitio o URL fraudulentos, descargan software no autorizado o facilitan el robo de credenciales. La facilidad con la que pueden crearse y distribuirse, sumada a la imposibilidad de que el usuario verifique su contenido antes de escanearlos, convierte a los códigos QR en un medio particularmente eficaz para este tipo de ataques [7].

2.5.5. Sentadillas tipográficas

Es un tipo de secuestro de URL que se aprovecha de los errores tipográficos que los usuarios cometen al ingresar la dirección de un sitio web, por ejemplo, escribir “Facebok.com” en lugar de “Facebook.com”.

Aquí los atacantes crean sitios web que imitan a los originales para engañar a los usuarios y realizar actividades maliciosas, como robar información sensible mediante formularios de inicio de sesión, venta de productos y servicios falsos. Estos sitios también pueden descargar software malicioso en el sistema de la víctima, conocido como descarga automática. [7]

En el siguiente capítulo se hace un análisis comparativo de algunas soluciones *anti-phishing* propuestas en artículos en los últimos años.

Capítulo 3

Estado del arte y análisis del problema

El presente capítulo ofrece una revisión integral de los enfoques y soluciones existentes para la detección y prevención del *phishing*, con el propósito de contextualizar el problema que aborda esta investigación y fundamentar la propuesta desarrollada en los capítulos posteriores. Se analizan los principales trabajos académicos y técnicos relacionados con las estrategias *anti-phishing*, identificando las tendencias actuales en materia de seguridad, así como sus alcances y limitaciones.

La primera parte del capítulo presenta una clasificación de las soluciones más relevantes encontradas en la literatura, distinguiendo entre las de carácter técnico (basadas en mecanismos automatizados, heurísticos y de aprendizaje automático) y aquellas orientadas a la educación y concienciación del usuario. Posteriormente, se realiza un análisis del problema desde la perspectiva social y nacional, con énfasis en el contexto mexicano, donde a pesar de los esfuerzos institucionales por informar y capacitar a la población, persisten importantes deficiencias en la accesibilidad, actualización y efectividad de los recursos disponibles.

Finalmente, se expone el diagnóstico resultante de esta revisión, el cual evidencia una brecha significativa entre los avances tecnológicos en detección de amenazas y la falta de estrategias formativas que fortalezcan las capacidades individuales para reconocerlas. Este hallazgo sustenta la necesidad de desarrollar una solución educativa accesible, actualizada y orientada al usuario común, que contribuya a la construcción de una cultura de ciberseguridad más sólida y consciente.

3.1. Estado actual de las soluciones anti-*phishing*

El *phishing* constituye una de las amenazas más persistentes y efectivas dentro del panorama de la ciberseguridad contemporánea. Su éxito radica en la manipulación de la confianza humana, lo que permite a los atacantes obtener información confidencial mediante técnicas de ingeniería social y suplantación de identidad. Ante ello, la comunidad científica y tecnológica ha desarrollado diversas estrategias de mitigación, que pueden clasificarse en dos grandes categorías: detección y prevención.

Esta revisión se basa en los trabajos más representativos y recientes en la materia [7, 22, 26, 31], los cuales permiten identificar tendencias, fortalezas y limitaciones en las estrategias actualmente utilizadas.

- *Phishing Attacks Survey: Types, Vectors, and Technical Approaches* por Rana Alabdan [7].
- *Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study* por Fauzan Prasetyo Eka Putra, Ubaidi, Achmad Zulfikri, Goffal Arifin, y Revi Mario Ilhamsyah [22].
- *Phishing Attacks: Detection and Prevention Techniques* por Daoming Li, Qiang Chen, y Lun Wang [26].
- *Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies* por Ogugua Chimezie Obi, Onyinyechi Vivian Akagha, Samuel Onimisi Dawodu, Anthony Chigozie Anyanwu, Shedrack Onwusinkwue, e Islam Ahmad Ibrahim Ahmad [31].

De acuerdo con estos estudios, entre las soluciones más comunes destacan los modelos de *Machine Learning (ML)*, una rama de la inteligencia artificial (*IA*) enfocada en desarrollar sistemas que mejoran su desempeño con base en los datos que procesan [32]. También se emplean mecanismos de control de acceso como listas negras y blancas (*blacklists*/*whitelists*), detección heurística de código malicioso y autenticación multifactor (*MFA*).

A partir del análisis de la literatura, se identificaron cinco categorías generales de soluciones. Cuatro de ellas corresponden a estrategias o herramientas de carácter técnico, mientras que la quinta se centra en la educación del usuario. Las clasificaciones técnicas se resumen en la Tabla 3.1, y las iniciativas educativas en la Tabla 3.2.

Categoría de solución	**Artículos referenciados**	**Tipo de función**
Uso de Machine Learning	*Phishing Attacks: Detection and Prevention Techniques.*, *Phishing Attacks Survey: Types, Vectors, and Technical Approaches.*, *Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies.*	Detección
Detección heurística	*Phishing Attacks: Detection and Prevention Techniques.*, *Phishing Attacks Survey: Types, Vectors, and Technical Approaches.*, *Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies.*	Detección
Autenticación multifactor (MFA)	*Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study.*, *Phishing Attacks: Detection and Prevention Techniques.*	Prevención
Listas negras y blancas *(blacklist/whitelist)*	*Phishing Attacks: Detection and Prevention Techniques.*, *Phishing Attacks Survey: Types, Vectors, and Technical Approaches.*, *Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies.*	Detección

Tabla 3.1: Soluciones técnicas contra el *phishing*

Aunque las soluciones técnicas son ampliamente adoptadas en entornos empresariales y corporativos, los individuos suelen permanecer en una posición de vulnerabilidad. Los sistemas de detección automática suelen requerir infraestructura avanzada, grandes volúmenes de datos y personal especializado, lo que restringe su aplicación a contextos empresariales. En contraste, los usuarios comunes (sin formación específica en tecnologías o ciberseguridad) permanecen en situación de vulnerabilidad. De hecho, los ataques de *phishing* representan aproximadamente el 95 % de las violaciones de ciberseguridad a nivel global [2]. Esta disparidad evidencia que, si bien las estrategias técnicas mejoran

la detección, no abordan el factor humano que posibilita la eficacia del engaño.

En consecuencia, aunque los mecanismos técnicos contribuyen a mitigar el impacto del *phishing*, no abordan la raíz del problema: la falta de alfabetización digital y de competencias para reconocer las señales de un ataque. Este hallazgo orienta la atención hacia un eje frecuentemente subestimado en la literatura: la educación como herramienta de prevención efectiva y sostenible.

Por ello, esta investigación se orienta hacia las soluciones centradas en la educación y concienciación del usuario, especialmente en contextos no empresariales. El análisis de los trabajos revisados permite concluir que la formación del usuario constituye una de las estrategias más efectivas para la prevención de ataques de *phishing*. Sin embargo, fuera del ámbito corporativo, no existe una metodología estandarizada que facilite el reconocimiento guiado de señales de ataque.

Artículo	**Enfoque de educación**
Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study	Formación continua para identificar señales de ataques de *phishing*, mediante simulaciones de correos que permiten examinar encabezados y remitentes.
Phishing Attacks: Detection and Prevention Techniques	Capacitación mediante simulaciones enfocadas en el reconocimiento de intentos de *phishing*, identificación de correos sospechosos, verificación de enlaces y protección de información sensible.
Phishing Attacks Survey: Types, Vectors, and Technical Approaches	Entrenamiento mediante correos falsos simulados que activan material educativo al hacer clic.
Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies	Formación en ingeniería social, buenas prácticas de seguridad, simulacros de *phishing* y técnicas de resistencia a la manipulación.

Tabla 3.2: Comparativa de enfoques de educación del usuario

A partir de esta brecha identificada, se propone una solución que describa y diferencie los distintos tipos de *phishing*, complementada con ejemplos reales que faciliten su detección. Esta propuesta busca ofrecer una alternativa accesible, práctica y escalable para fortalecer la conciencia de seguridad entre los usuarios individuales.

3.2. Análisis del Problema

A partir de la revisión anterior, se identifican dos vacíos principales:

1. La dependencia de soluciones técnicas orientadas a entornos empresariales.
2. La escasa atención a disminuir la brecha en alfabetización digital y de competencias que permitan a los individuos identificar amenazas de forma autónoma.

La exposición de información sensible y el incremento de fraudes digitales se deben no sólo a la sofisticación de los ataques, sino también al desconocimiento y la falta de habilidades de los usuarios para reconocer señales de riesgo. Pese a la existencia de estrategias nacionales de ciberseguridad y campañas antifraude impulsadas por el gobierno mexicano, la sociedad sigue siendo altamente vulnerable ante estafas digitales. Ejemplo de ello son los casos de suplantación del Gobierno de la Ciudad de México mediante mensajes SMS [33], en los cuales los atacantes aprovechan la falta de alfabetización digital y de criterios de verificación básica por parte de la población.

En el contexto nacional, organismos como la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) han desarrollado materiales educativos (manuales, videos e infografías) para sensibilizar a los usuarios del sector financiero sobre los fraudes cibernéticos, incluido el *phishing*. Sin embargo, durante esta investigación se identificaron deficiencias relevantes en la disponibilidad, actualización y accesibilidad de dichos recursos.

La figura 3.1 muestra un ejemplo de esta situación: el video explicativo sobre *phishing* publicado en el sitio oficial de la CONDUSEF no puede visualizarse [4]. Este hallazgo es particularmente significativo, dado que el sector financiero es uno de los principales blancos de este tipo de ataques.

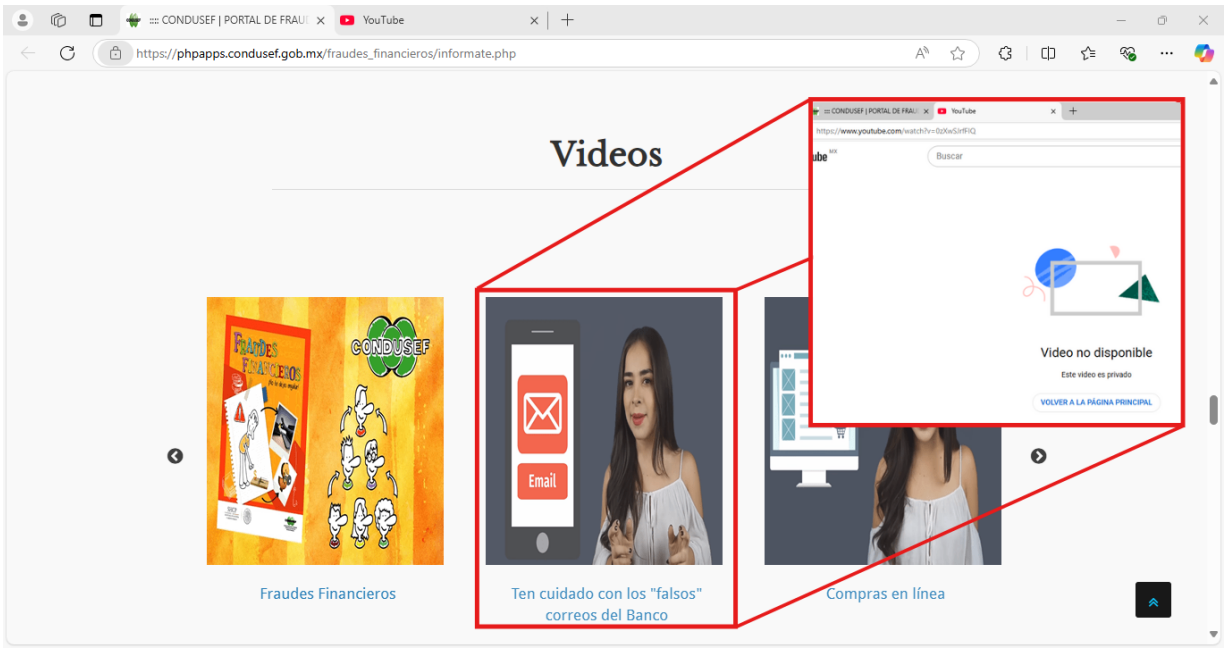


Figura 3.1: Video no disponible. Fuente: elaboración propia.

De manera similar, la figura 3.2 presenta una guía destinada a prevenir el robo de identidad, uno de los propósitos más frecuentes del *phishing*, que tampoco puede descargarse desde el sitio principal de la CONDUSEF.

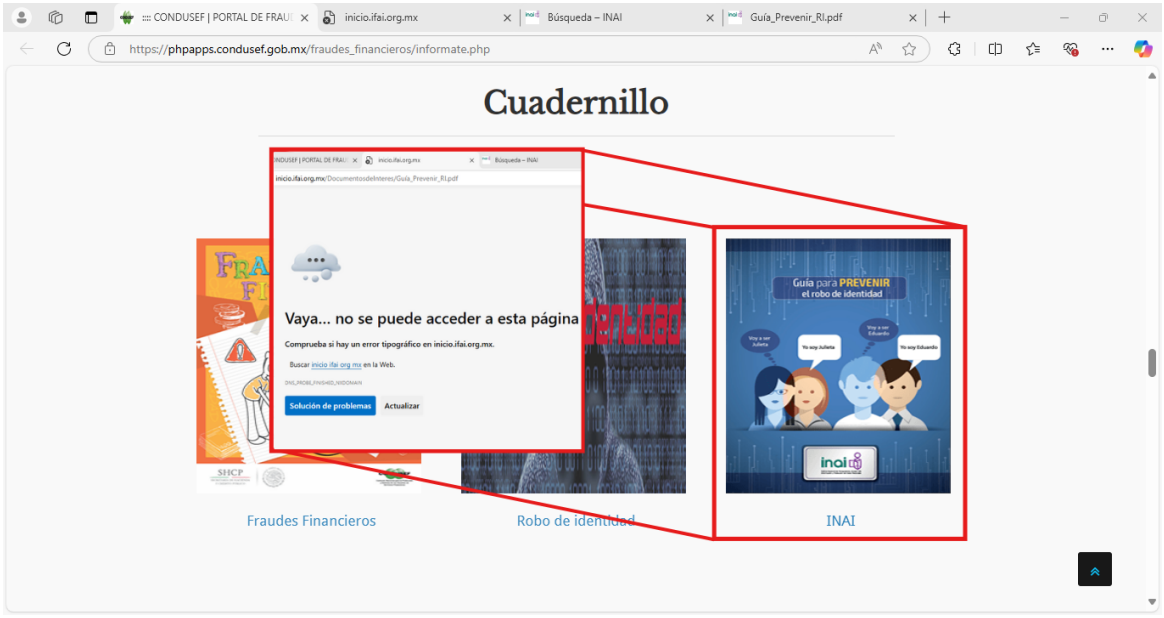


Figura 3.2: Cuadernillo no disponible. Fuente: elaboración propia.

Aunque el documento sigue disponible en otro dominio institucional (figura 3.3), la

falta de coherencia en la publicación y mantenimiento de los materiales limita su alcance y eficacia, reduciendo su impacto formativo. Al realizar la búsqueda desde la institución que publica el cuadernillo, se redirige a un sitio web diferente. Es decir, la guía está disponible, pero no en el sitio adecuado.

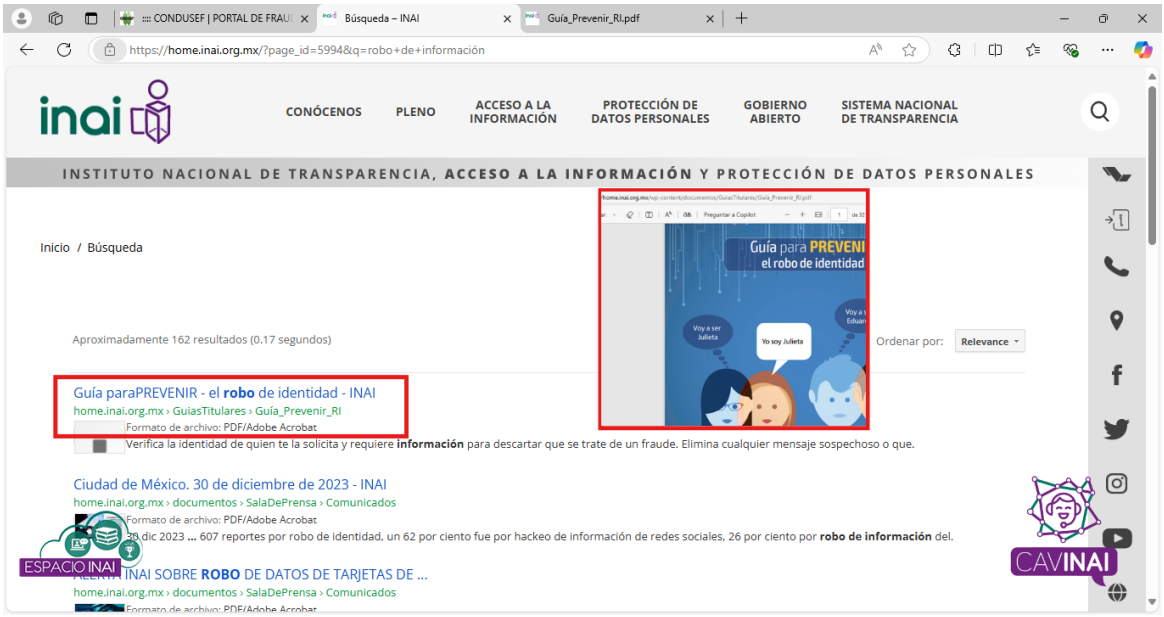


Figura 3.3: Acceso correcto a guía. Fuente: elaboración propia.

Este análisis permite evidenciar una brecha significativa entre la disponibilidad teórica de recursos educativos y su aprovechamiento real por parte de la ciudadanía. Los esfuerzos actuales se caracterizan por ser fragmentados, desactualizados o poco accesibles, lo que limita su función preventiva. En contraste, las soluciones técnicas avanzan rápidamente, pero continúan siendo inaccesibles o irrelevantes para el usuario común.

3.3. Brecha identificada y justificación de la propuesta

El diagnóstico realizado revela que la educación del usuario constituye un eje crítico y aún poco abordado en la prevención del *phishing*. Mientras que las estrategias técnicas buscan fortalecer los sistemas, la verdadera resiliencia digital requiere fortalecer a las personas.

Ante la falta de una metodología estandarizada y accesible que guíe a los usuarios

en el reconocimiento de señales de ataque, esta investigación propone el desarrollo de un recurso educativo que describa y clasifique los distintos tipos de *phishing*, complementado con ejemplos reales que faciliten y enseñen su identificación.

La solución propuesta se diseñará con tres principios rectores:

Accesibilidad. Estará disponible desde dispositivos comunes y en formatos de libre consulta.

Actualización. Reflejará la evolución de las modalidades de ataque más actuales.

Enfoque didáctico. Promoverá el aprendizaje autónomo y contextualizado mediante ejemplos concretos y visuales.

Este enfoque busca ofrecer una alternativa práctica y sostenible para fortalecer la conciencia de seguridad en los individuos, contribuyendo así a una cultura digital más informada, participativa y resiliente frente al *phishing*.

3.3.1. Metodología de desarrollo y validación

La metodología empleada en esta investigación sigue un enfoque de investigación aplicada, orientada al diseño y validación de un recurso educativo digital para la prevención de ataques de *phishing*. Este enfoque permite integrar elementos teóricos y prácticos, combinando estrategias de diseño instruccional con técnicas de evaluación empírica.

El proceso metodológico se estructura en cinco etapas principales:

1. **Análisis:** A partir de la revisión de literatura y del diagnóstico del contexto nacional presentado en este capítulo, se identificó la falta de recursos educativos *anti-phishing* accesibles, actualizados y orientados al usuario no especializado. Usando este análisis se definieron los pasos a seguir: (i) enfocarse en contenidos asociados a un ataque con alta frecuencia e impacto social; (ii) asegurar claridad terminológica y ejemplos verificables; y (iii) favorecer formatos de consulta sencilla enfocados a la población en general. Como resultado, se estableció la necesidad de desarrollar un recurso didáctico que integre señales de alerta comprensibles, casos realistas y una taxonomía de fácil entendimiento.

2. **Diseño del recurso educativo:** Elaboración de materiales visuales e interactivos que describen los distintos tipos de *phishing*, con ejemplos reales y guías de identificación.

3. **Implementación:** Desarrollo del prototipo en formato digital, publicado en un repositorio de libre acceso y acompañado de documentación técnica.

4. **Evaluación piloto:** Aplicación del recurso a un grupo reducido de usuarios para medir su comprensión y capacidad de reconocimiento de ataques simulados.

5. **Ajustes y validación:** Análisis de los resultados obtenidos, identificación de áreas de mejora y actualización del contenido antes de su difusión final.

Para la fase de evaluación se aplicarán instrumentos de medición cualitativos y cuantitativos, entre ellos cuestionarios estructurados y pruebas comparativas pre y post intervención. Los resultados permitirán determinar la eficacia del recurso como herramienta de concienciación en ciberseguridad y su potencial aplicación en contextos educativos no empresariales.

Capítulo 4

Propuesta de solución

De acuerdo con el objetivo de este trabajo y la metodología presentada en el capítulo previo, en este capítulo se presentan los pasos (1) Análisis y (2) Diseño del recurso educativo. Este recurso se diseñó como una guía práctica, sencilla y accesible que permita a los individuos identificar y comprender los ataques de *phishing* y así mitigar su impacto. Esta se creó usando las estrategias y soluciones planteadas en el capítulo anterior.

4.1. Paso 1. Análisis

Para facilitar la identificación y comprensión de los ataques de *phishing*, se presentan tanto ejemplos representativos de forma general como reales de los diferentes *vectores de phishing* descritos en el Marco Teórico de este trabajo (sin embargo, para fines prácticos y de entendimiento se describen como "tipos de *phishing*"). Los ejemplos reales fueron proporcionados por personas cercanas que estuvieron expuestas a estos tipos de ataque.

La solución propuesta se fundamenta en los vectores mostrados en la figura 2.1, ya que representan las formas de ataque más reconocidas y comúnmente asociadas por la sociedad con el *phishing* o con *estafas*, lo que facilita su identificación y entendimiento por parte de la población.

4.1.1. Criterios de análisis y selección de vectores

El análisis inicial se orientó a identificar cuáles formas de *phishing* presentan mayor prevalencia, reconocimiento social y relevancia práctica para la población general. Con base en la revisión bibliográfica, el diagnóstico nacional y los hallazgos del capítulo anterior, se establecieron los siguientes criterios:

- **Prevalencia del vector:** se priorizaron aquellas modalidades de *phishing* que aparecen de manera recurrente en reportes de instituciones financieras, organismos gubernamentales y estudios académicos.
- **Reconocimiento social:** se eligieron los vectores más comúnmente asociados por la ciudadanía con estafas digitales, dado que su familiaridad inicial facilita el aprendizaje y la identificación de señales de alerta.
- **Impacto potencial en el usuario:** se consideraron los ataques que con mayor frecuencia comprometen información personal, financiera o acceso a cuentas digitales.
- **Disponibilidad de ejemplos verificables:** únicamente se incluyeron tipos de *phishing* para los cuales se contaba con evidencia real confiable, recopilada durante el trabajo de campo o derivada de casos cercanos.
- **Valor educativo:** se seleccionaron vectores cuya estructura permite ilustrar patrones claros, señales de advertencia y recomendaciones prácticas que puedan ser fácilmente comprendidas por usuarios no especializados.

Estos criterios orientaron la selección de los vectores abordados y garantizan que el recurso educativo responda a necesidades reales y observables de la población.

A partir de los criterios establecidos, se seleccionaron los vectores descritos en el Marco Teórico y ampliamente documentados por Alabdan [7], tales como: correos electrónicos, redes sociales, sitios web fraudulentos, redes Wi-Fi abiertas, mensajería instantánea (IM), mensajes SMS (*SMishing*) y llamadas telefónicas (*vishing*).

Estos vectores representan los canales más frecuentes mediante los cuales los usuarios reciben intentos de *phishing*. Asimismo, coinciden con los medios más utilizados en la vida

cotidiana: correos institucionales, redes sociales, aplicaciones de mensajería, SMS bancarios y comunicaciones telefónicas.

Esta selección permite cubrir un espectro amplio de escenarios reales, al tiempo que facilita la comprensión del fenómeno por parte de los usuarios, quienes pueden identificar con facilidad estos medios en su interacción diaria con la tecnología.

4.1.2. Ejemplos representativos

Para complementar el análisis y asegurar que el recurso educativo representara situaciones auténticas, se recopilaron ejemplos representativos de intentos de *phishing*. Estos fueron proporcionados por personas cercanas que experimentaron directamente los ataques o estuvieron expuestas a ellos.

Los casos recopilados incluyen capturas de pantalla, fragmentos de mensajes, correos electrónicos y enlaces fraudulentos. Esta evidencia permitió identificar patrones comunes, tales como:

- la generación artificial de un sentido de urgencia o miedo.
- enlaces disfrazados que redirigen a sitios apócrifos.
- suplantación de identidades institucionales o personales.
- solicitudes de datos sensible o de códigos de acceso.
- indicadores visuales y lingüísticos propios de comunicación fraudulenta.

El uso de casos reales permitió diseñar ejemplos educativos más precisos y cercanos a las experiencias cotidianas de los usuarios, aumentando así el impacto y la utilidad del recurso propuesto.

4.1.3. Representación gráfica del ataque

Con el fin de contextualizar los módulos educativos y reforzar la comprensión del funcionamiento general de un ataque de *phishing*, se incorporó una representación gráfica del proceso típico seguido por los atacantes.

La figura 4.1 sintetiza los pasos principales: envío del mensaje inicial, interacción de la víctima con el enlace malicioso, captura de información confidencial, y posterior uso de dicha información por parte del atacante para acceder a servicios legítimos o cometer fraudes. Esta representación sirve como base conceptual para el diseño de las secciones posteriores.

De manera general, el atacante envía un mensaje a la víctima que incluye un enlace 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 4.1, que proporciona una descripción gráfica de un ataque de *phishing*.

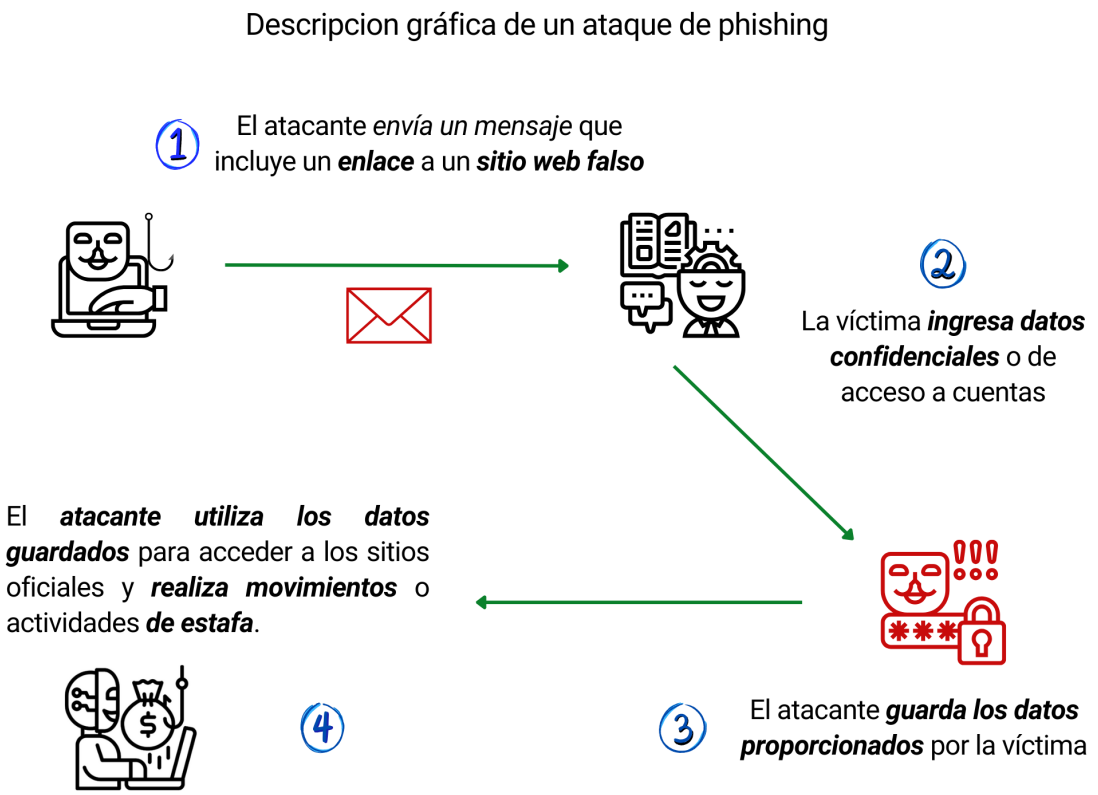


Figura 4.1: Ejemplo gráfico de *Phishing*. Fuente: CISCO [8]

4.2. Paso 2. Diseño del recurso educativo

Con base en los resultados del análisis previo, el recurso educativo se estructuró en un formato modular que organiza los contenidos por tipo de *phishing*, permitiendo que el usuario pueda identificar primero el medio por el cual recibe el mensaje y, posteriormente, reconocer las características específicas de cada modalidad de ataque.

Cada módulo sigue una estructura uniforme compuesta por cuatro elementos:

1. **Descripción del tipo de ataque:** una explicación clara sobre cómo opera la modalidad de *phishing* y por qué representa un riesgo.

2. **Señales de alerta:** un conjunto de indicadores visuales, lingüísticos o contextuales que permiten identificar la posible amenaza.

3. **Ejemplos reales:** evidencia obtenida durante la fase de análisis, que incluye capturas de pantalla y mensajes auténticos que ilustran patrones comunes.

4. **Recomendaciones de prevención:** consejos prácticos y verificables que ayudan a evitar caer en este tipo de engaños.

Esta estructura modular ofrece claridad, coherencia y un formato didáctico que facilita la consulta rápida y la comprensión autónoma de los contenidos.

El diseño del recurso educativo se fundamentó en principios de aprendizaje autónomo y construcción significativa del conocimiento. La estrategia pedagógica adoptada integra los siguientes elementos:

- **Aprendizaje basado en ejemplos reales:** Se emplean casos auténticos para que los usuarios reconozcan patrones delictivos que podrían encontrar en su vida cotidiana.

- **Uso de recursos visuales:** Capturas de pantalla, comparaciones de enlaces, y señalamientos gráficos facilitan la identificación inmediata de señales de riesgo.

- **Lenguaje claro y accesible:** Los contenidos se redactaron en un estilo comprensible para personas sin formación técnica, evitando terminología especializada innecesaria.

- **Organización modular:** Los contenidos se dividen por canales de comunicación (correo, SMS, redes sociales, etc.), lo que permite al usuario localizar rápidamente el tipo de ataque que desea analizar.

- **Enfoque preventivo:** Más allá de describir el ataque, cada módulo incluye recomendaciones directas que fomentan conductas seguras, tales como verificar el emisor, inspeccionar enlaces y usar canales oficiales.

Esta estrategia busca no solo informar, sino promover la capacidad del usuario para identificar señales de alerta de manera autónoma, contribuyendo a su alfabetización digital y a la prevención de fraudes.

4.2.1. Módulos de la guía

Con base en la estructura y la estrategia pedagógica previamente descritas, el recurso educativo se organiza en una serie de módulos temáticos, cada uno correspondiente a un tipo específico de *phishing*. Esta organización permite que el usuario identifique primero el canal por el cual se recibe el mensaje fraudulento y, posteriormente, explore las características particulares que distinguen a cada modalidad de ataque.

Cada módulo sigue un formato uniforme que facilita su consulta: se presenta una descripción del tipo de ataque, las señales de alerta más comunes, ejemplos reales recopilados durante la fase de análisis y recomendaciones prácticas orientadas a la prevención. Esta estructura coherente busca promover una comprensión gradual y autónoma, permitiendo que la guía sea utilizada tanto como material formativo como herramienta de referencia en situaciones cotidianas.

A continuación, se presentan los módulos que conforman la guía, organizados según los canales de comunicación más empleados por los atacantes, primero se describen las acciones clave para reconocer y evitar los diferentes tipos de ataque, posteriormente se encuentran los ejemplos reales que señalan de forma clara como reconocerlos.
De forma visual, las acciones clave se relacionan con los ejemplos mediante el resaltado de palabras clave. En cada módulo, dichas palabras se presentan resaltadas con un color

específico y posteriormente, los ejemplos utilizan el mismo color o uno similar para resaltar las señales asociadas y así facilitar la identificación.

4.2.1.1. *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:

4.2.1.1.1. 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 por sorteo 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.

4.2.1.1.2. 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.

4.2.1.1.3. 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, especialmente en empresas o vendedores de servicios pequeños es seguro acceder a enlaces **http**. Si se tratara de algún tipo de **comunicación gubernamental**, 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 la página *Sitios web falsos* [34]. 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.

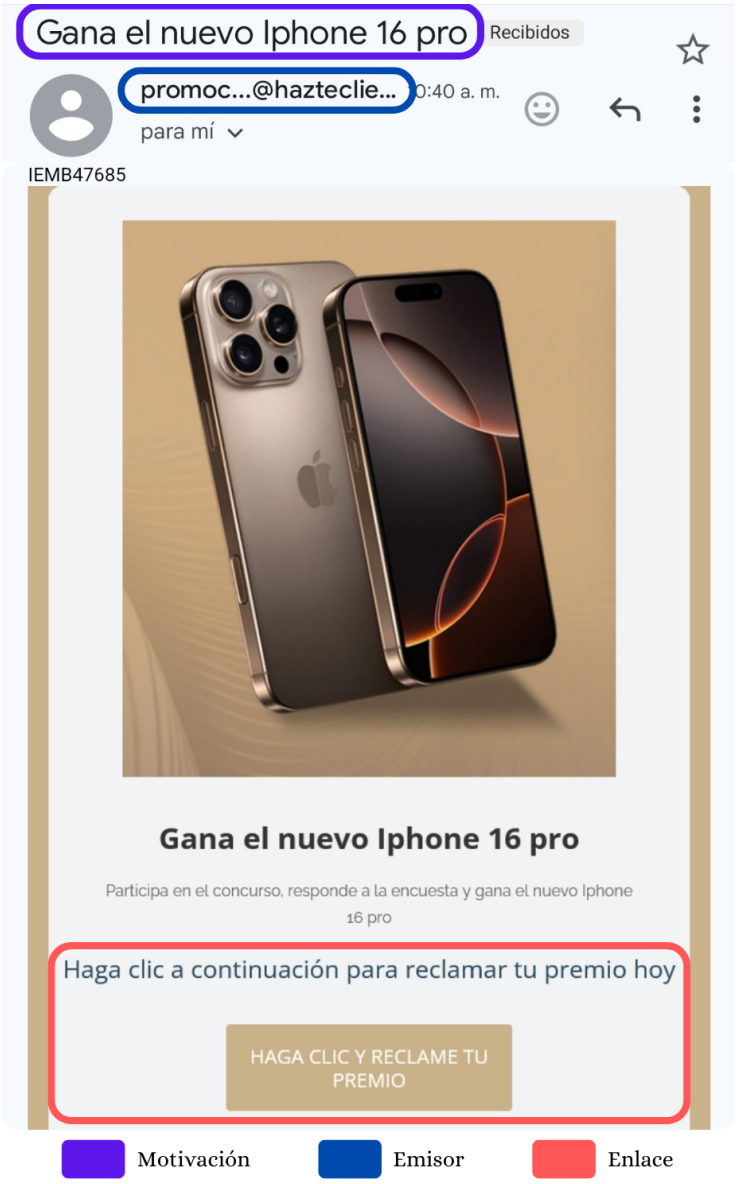


Figura 4.2: *Phishing* por "ganar un premio". Fuente: elaboración propia.

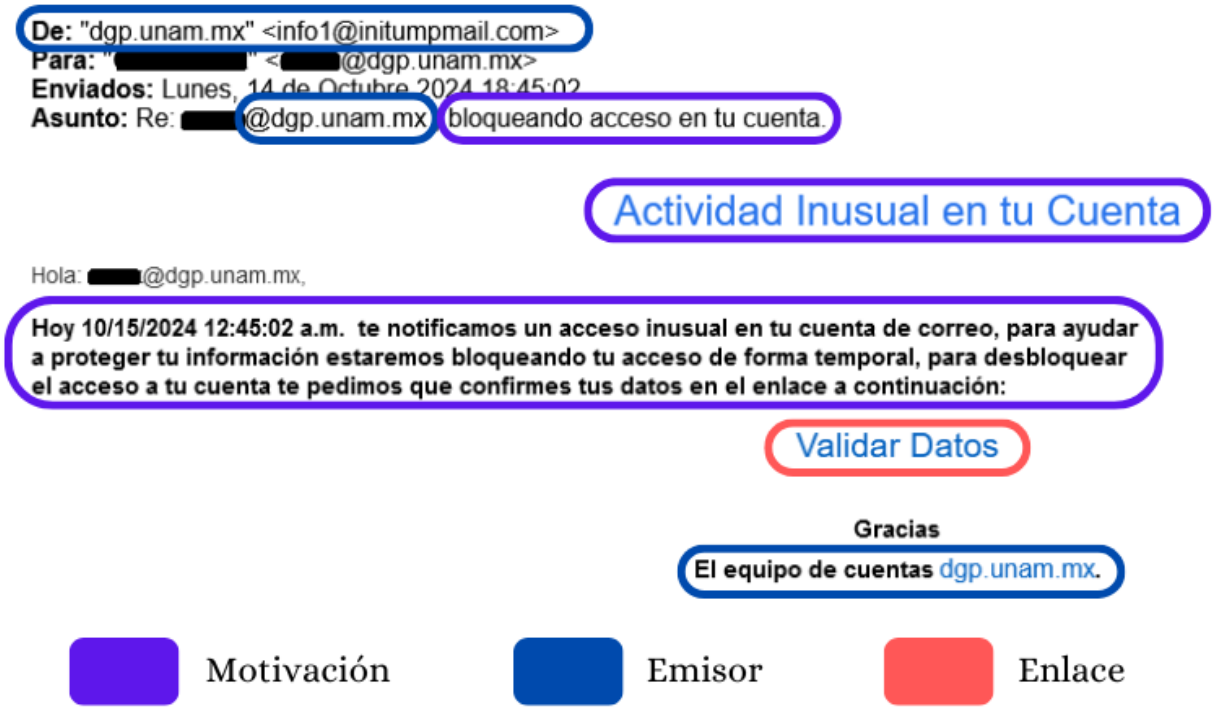


Figura 4.3: *Phishing* por "actividad inusual". Fuente: elaboración propia.

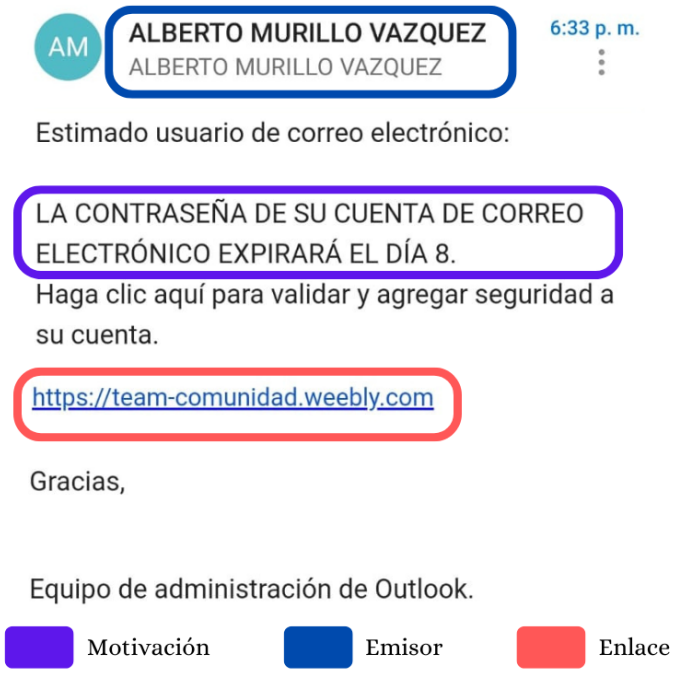


Figura 4.4: *Phishing* por "cuenta expirada". Fuente: elaboración propia.

4.2.1.2. *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 maliciosos.

4.2.1.2.1. Analiza la motivación del mensaje.

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

- Prometer incentivos económicos o regalos costosos.
- 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.

4.2.1.2.2. 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.

4.2.1.2.3. 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 tratara de algún tipo de **comunicación** gubernamental, los sitios oficiales suelen tener al final del enlace **.gob.mx**, en bancos e instituciones de confianza **.com** o **.mx**.

En la figura 4.5 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.

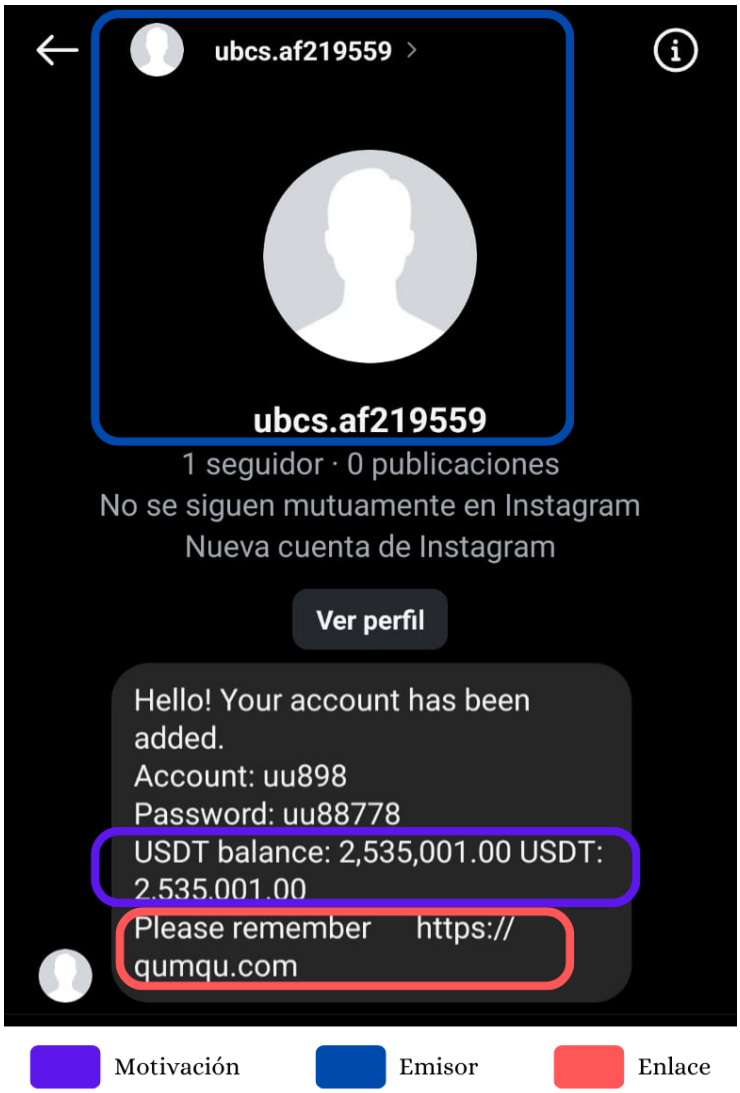


Figura 4.5: Ejemplo de *phishing* por redes sociales. Fuente: elaboración propia.

4.2.1.3. *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:

4.2.1.3.1. 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**, en el caso de bancos e instituciones de confianza en México son **.com** o **.com.mx**.

4.2.1.3.2. Consulta fuentes confiables.

El Gobierno de México proporciona una lista de sitios falsos o apócrifos que intentan suplantar a instituciones gubernamentales, disponible en la página *Sitios web falsos* [34]. 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 4.6. 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 4.6: Ejemplo de *phishing* por sitios web. Fuente: elaboración propia.

4.2.1.4. *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.

4.2.1.4.1. Conéctate a redes seguras.

Se recomienda conectarse a redes Wi-Fi conocidas privadas, familiares o personales 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.

4.2.1.4.2. 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 4.7 y 4.8 se muestran algunos formularios únicamente de ejemplo, 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*.**

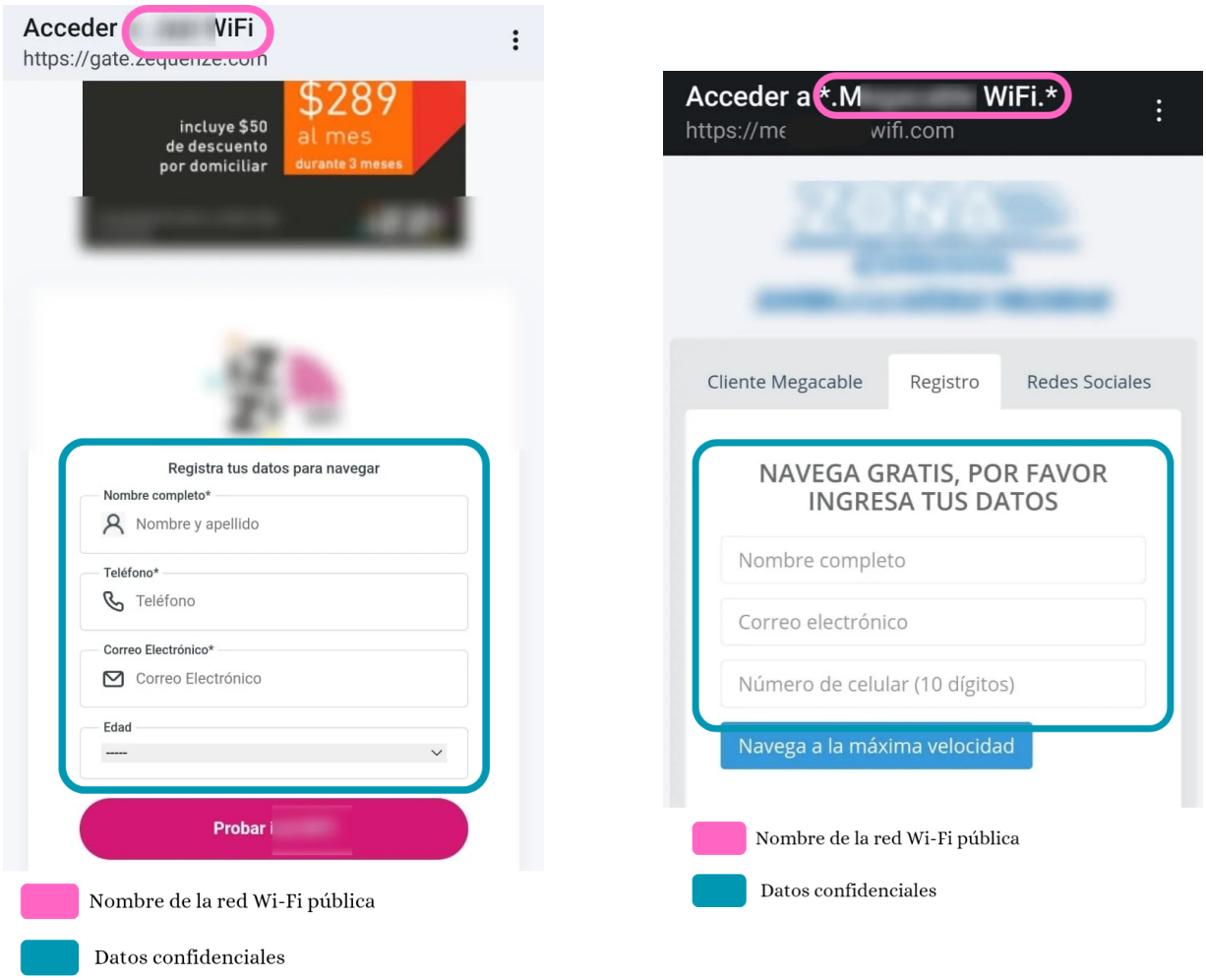


Figura 4.7: Ejemplos de formularios que solicitan nombre, teléfono y correo. Fuente: elaboración propia.

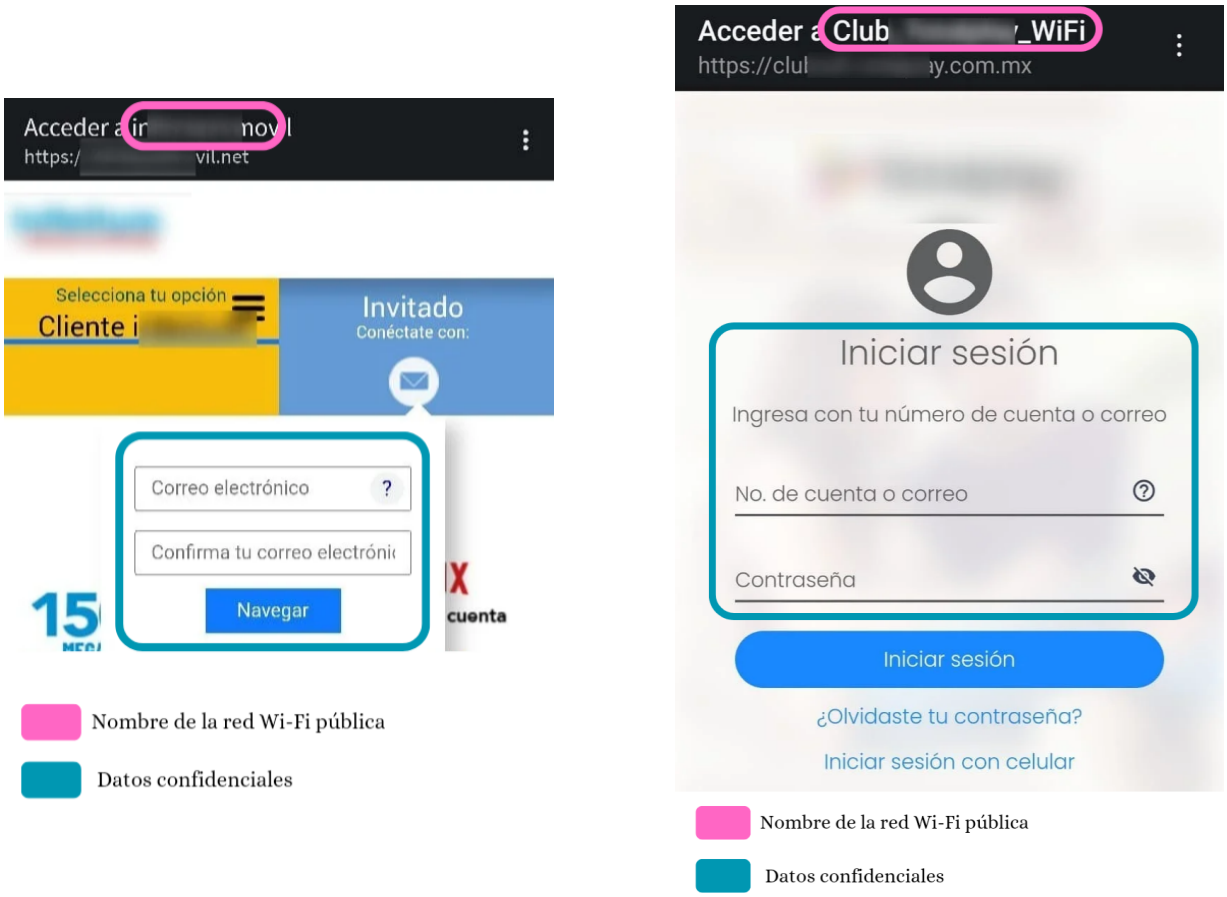


Figura 4.8: Ejemplos de formularios que solicitan correo y contraseña. Fuente: elaboración propia.

4.2.1.5. *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 comunicación inmediata de forma sencilla permitiendo tener una interacción en tiempo real.

4.2.1.5.1. 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.

4.2.1.5.2. 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*

4.2.1.5.3. 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 4.9 y 4.10 se muestran ejemplos de mensajes con ofertas laborales, mientras que la figura 4.11 presenta una "invitación", diseñada así para generar un sentido de pertenencia.

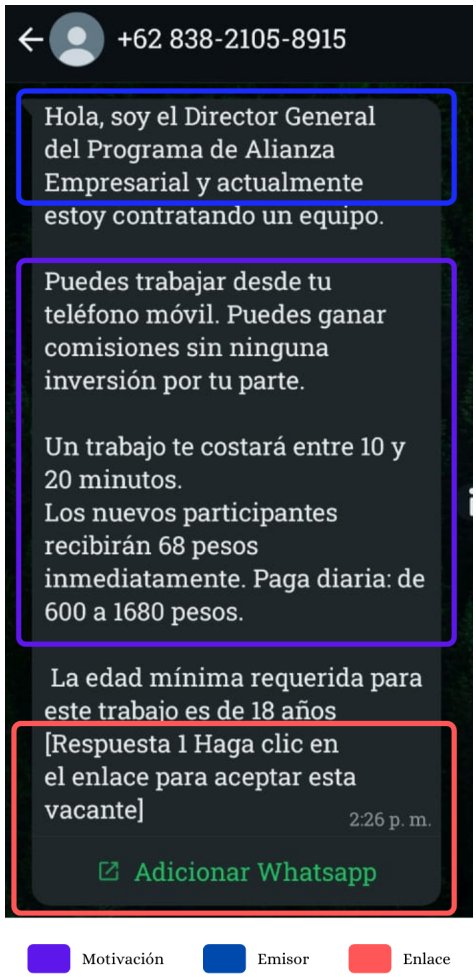


Figura 4.9: *Phishing* por IM por el "Director". Fuente: elaboración propia.

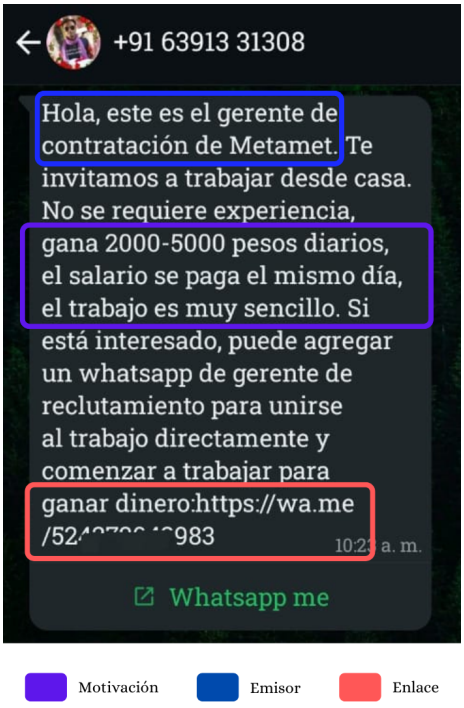


Figura 4.10: *Phishing* por IM por el "gerente". Fuente: elaboración propia.

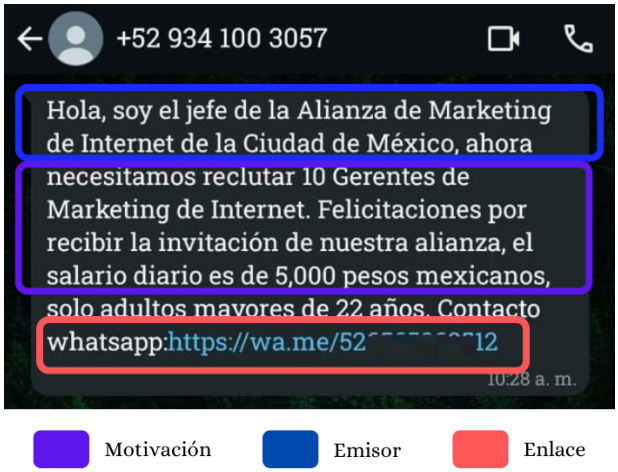


Figura 4.11: *Phishing* por IM por el "jefe". Fuente: elaboración propia.

4.2.1.6. *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.

4.2.1.6.1. 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 4.12).
- Hacen mención a empresas o servicios reconocidos (véase la figura 4.15) o a asistencia jurídica (véase la figura 4.13).

4.2.1.6.2. 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 4.12 y 4.13 se muestran ejemplos de *SMishing* que dirigen a números telefónicos externos, mientras que en la figura 4.14 y 4.15 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.

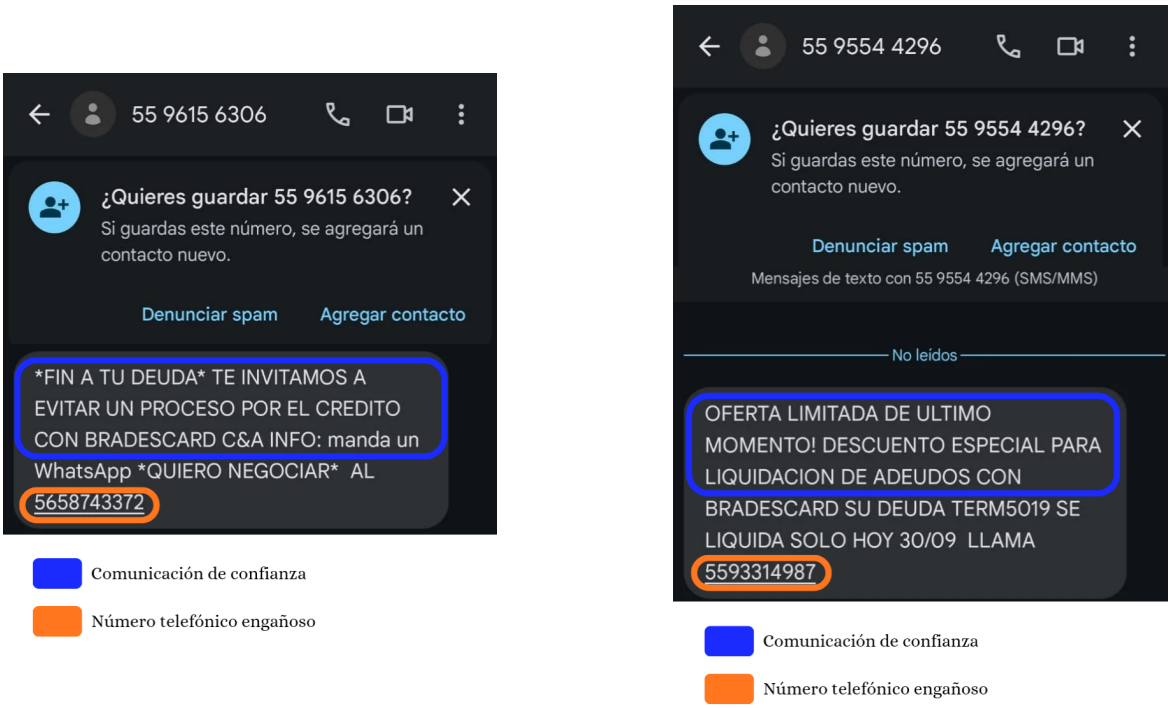


Figura 4.12: *SMishing* por adeudos. Fuente: elaboración propia.

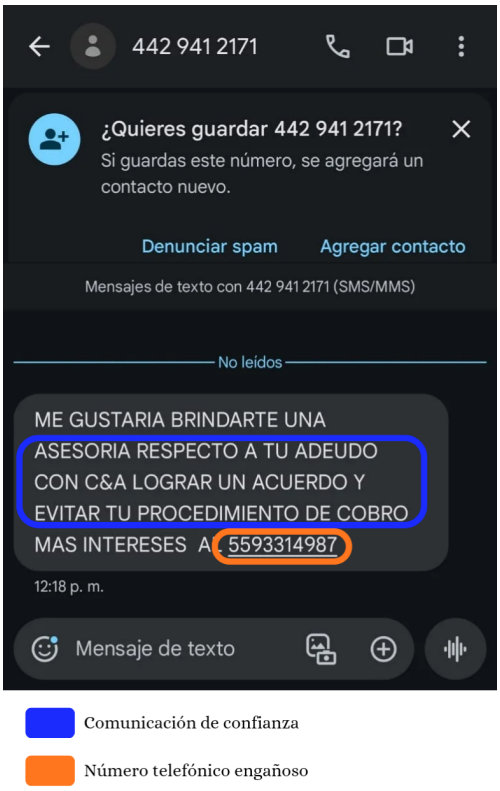


Figura 4.13: *SMishing* por servicios. Fuente: elaboración propia.

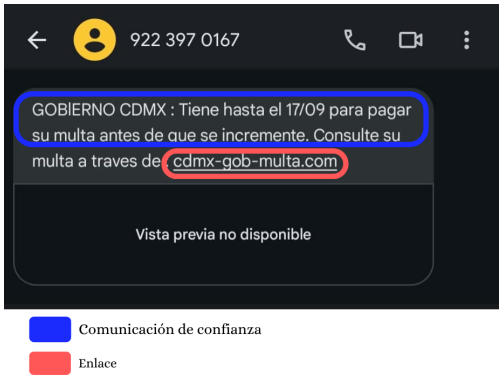


Figura 4.14: *SMishing* por "Gobierno". Fuente: elaboración propia.

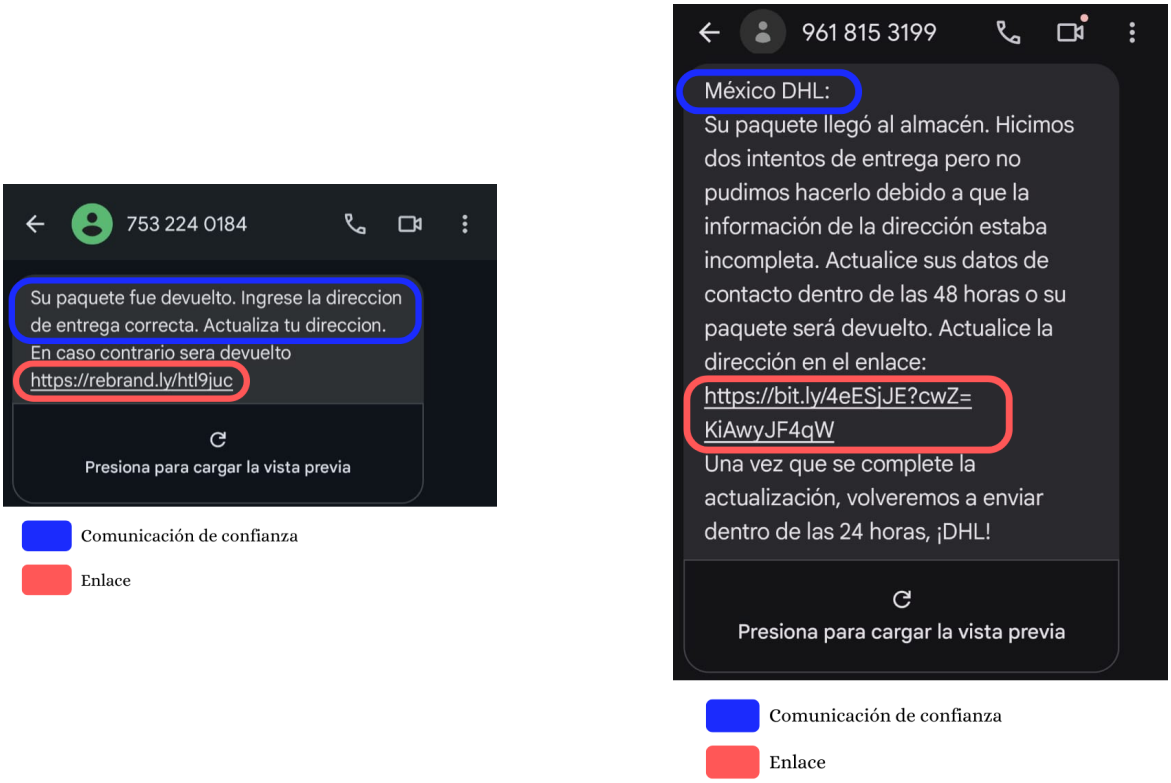


Figura 4.15: *SMishing* por "empresas". Fuente: elaboración propia.

4.2.1.7. 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 (véase la figura 4.16).

4.2.1.7.1. 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.

4.2.1.7.2. 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 4.17 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”, ilustradas en la figura 4.16.

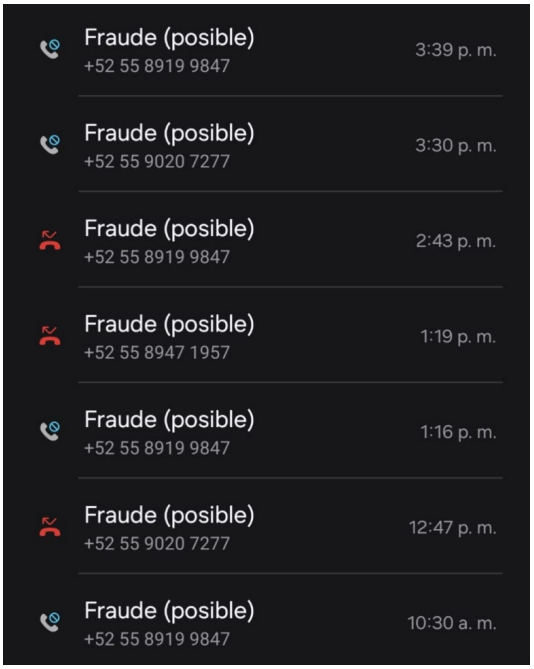


Figura 4.16: Ejemplo de llamadas detectadas como fraude. Fuente: elaboración propia.

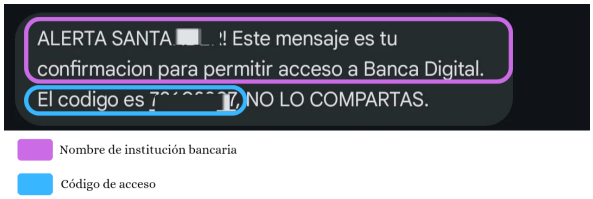


Figura 4.17: SMishing derivado de vishing. Fuente: elaboración propia.

La guía completa y las infografías derivadas del proceso descrito anteriormente se pueden consultar en el *sitio web* de Github personal [35]. Adicionalmente, las infografías se difundieron de forma abierta en el *perfil personal profesional* de LinkedIn [36] y se pueden consultar a continuación en el Apéndice B.

4.3. Discusión

Los módulos presentados en este capítulo constituyen la materialización de los pasos de análisis y diseño de la metodología propuesta. A partir de vectores de ataque comunes y ejemplos reales, se estructuró un recurso educativo orientado a facilitar la identificación autónoma de intentos de *phishing* en distintos contextos de comunicación digital.

En el siguiente capítulo se abordará la implementación y la evaluación del recurso, con el fin de analizar su efectividad como herramienta de concienciación y apoyo para la prevención de fraudes digitales en la población general.

Capítulo 5

Evaluación

Este capítulo presenta la evaluación del recurso educativo desarrollado como propuesta de solución para fortalecer las capacidades de la población en la identificación y prevención de ataques de *phishing*. En concordancia con la metodología descrita previamente, este capítulo aborda los pasos (3) Implementación, (4) Evaluación piloto y (5) Ajustes y validación.

El objetivo de esta fase es determinar la eficacia del recurso educativo para mejorar la comprensión del *phishing* entre usuarios sin formación técnica, así como identificar áreas de mejora para su posterior optimización y difusión a mayor escala.

A continuación se describe cada una de las etapas y resultados obtenidos, incorporado información cuantitativa y cualitativa que permiten determinar el grado de utilidad, claridad y pertinencia de la guía e infografías educativas.

5.1. Paso 3: Implementación del recurso educativo

En esta sección se describe la estructura del instrumento utilizado para evaluar los recursos educativos. Se describe la organización del banco de preguntas así como el proceso de publicación del prototipo que permitió la aplicación a los encuestados.

5.1.1. Diseño del instrumento de evaluación

Con base en el objetivo de este documento, orientado a fortalecer la educación en ciberseguridad entre la población en general, se diseñó un instrumento de evaluación en formato digital. La difusión de la evaluación se realizó mediante redes personales, académicas y profesionales (perfiles de redes sociales, grupos de trabajo, grupos de amigos y familiares, espacios estudiantiles y docentes), lo cual acotó de manera práctica el alcance de la muestra a personas de la Ciudad de México. Además, la evaluación incluía la leyenda: *"La presente encuesta está dirigida a personas mayores de 18 años, residentes en la Ciudad de México, que cuenten con al menos un dispositivo electrónico con acceso a Internet"*. La elección de la Ciudad de México como marco muestral responde a dos razones: (a) constituye una población accesible y manejable, (b) permite obtener una muestra local representativa con los recursos disponibles. No se requirió conocimiento previo sobre el *phishing*, ya que uno de los propósitos de la evaluación fue medir la comprensión generada exclusivamente a partir del recurso educativo.

La encuesta se estructuró en tres secciones:

1. **Diagnóstico inicial:** preguntas que permiten identificar el conocimiento previo de los participantes sobre el *phishing*.

2. **Presentación del contenido:** exposición del material educativo mediante infografías basadas en la guía desarrollada en el capítulo anterior.

3. **Evaluación posterior:** preguntas diseñadas para medir el entendimiento adquirido y la capacidad de reconocimiento de señales de alerta.

Este instrumento permitió evaluar el impacto inmediato del recurso educativo en términos de comprensión, claridad y utilidad práctica.

5.1.2. Construcción del banco de preguntas

Para estructurar adecuadamente la evaluación, se definió un banco de preguntas clasificado en cinco categorías: *diagnóstico*, *evaluación*, *retroalimentación*, *preguntas sociodemo-*

gráficas y *sugerencias*. Cada categoría cumplió un propósito específico dentro del proceso evaluativo.

- **Diagnóstico:** permitió explorar el nivel de conocimiento previo de los encuestados.
- **Evaluación:** midió la comprensión del contenido y la capacidad de identificar señales de *phishing*.
- **Retroalimentación:** recogió percepciones sobre claridad, utilidad y diseño del recurso.
- **Sociodemográficas:** ayudaron a identificar el perfil de los participantes para contextualizar los resultados.
- **Sugerencias:** brindaron información cualitativa adicional respecto a la percepción del recurso.

En la figura 5.1 se pueden observar las preguntas conforme a la clasificación mencionada.

Preguntas diagnóstico	Preguntas de evaluación	Preguntas de retroalimentación	Preguntas generales	Sugerencias
¿Con qué frecuencia utiliza internet?	Según las infografías, ¿qué es el phishing?	¿Qué tan útil encontraste la información sobre los diferentes tipos de phishing?	¿En qué rango de edad se encuentra?	¿Qué aspectos de la infografía crees que podrían mejorarse?
¿Ha escuchado antes sobre el phishing?	¿Cuál de estas señales indica un posible intento de phishing?	¿Las infografías te ayudaron a entender mejor qué es el phishing?	¿Cuál es su ocupación?	Comentarios y/o sugerencias
¿Ha sido víctima de un intento de phishing?	¿Qué acción recomiendan las infografías si recibes un mensaje sospechoso?	¿Qué tan claro te pareció el contenido de las infografías?	¿Cuál es su género?	
	¿Cómo se recomienda en las infografías verificar si un enlace es seguro?	¿Cómo te pareció el diseño de las infografías en términos de colores, imágenes y legibilidad?	¿Cuál es su nivel de estudios?	
	¿Cuáles son los tipos de phishing mencionados en las infografías de manera general?	¿Las infografías proporcionan ejemplos claros y comprensibles de intentos de phishing?		
	¿Después de leer las infografías, cómo actuarías ante un mensaje sospechoso que pide información personal?	¿Sientes que la información proporcionada te ayuda a protegerte mejor contra el phishing?		
		¿Cuáles de las recomendaciones mencionadas en las infografías aplicarías en tu vida diaria?		

Figura 5.1: Clasificación del banco de preguntas. Fuente: elaboración propia.

5.1.3. Publicación del prototipo

El recurso educativo, incluyendo la guía completa y las infografías utilizadas durante la evaluación, fue publicado en un repositorio de acceso abierto con el fin de garantizar su disponibilidad para cualquier persona interesada. El repositorio contiene:

- El documento principal en formato PDF.
- Las infografías individuales empleadas en la encuesta.
- La documentación técnica correspondiente.
- Las instrucciones de uso para facilitar su integración en procesos formativos.

La publicación en un entorno abierto responde al objetivo central del proyecto: proporcionar un recurso accesible para la sociedad en general y fomentar la alfabetización digital en materia de ciberseguridad.

5.2. Paso 4: Evaluación piloto

Esta sección resume la evaluación piloto aplicada a los recursos educativos. Se describen los participantes, el procedimiento seguido y los resultados obtenidos en cada parte del instrumento, incluyendo el diagnóstico inicial, la comprensión posterior al uso de la guía y la retroalimentación obtenida.

5.2.1. Participantes

Antes de la aplicación del instrumento de evaluación se estimó el tamaño de la muestra necesario para lograr resultados estadísticos confiables. Para este calculó se empleó la herramienta SurveyMonkey, una plataforma utilizada para la elaboración y análisis de encuestas que incorpora modelos estadísticos estándar para determinar tamaños de muestra basados en niveles de confianza y márgenes de error comúnmente aceptados.

En investigaciones sociales y educativas, el margen estándar consiste en utilizar un nivel de confianza del 95 % y un margen de error del 5 %. De acuerdo con SurveyMonkey,

estos parámetros requieren aproximadamente 384 participantes en poblaciones grandes como la de la Ciudad de México. En un periodo aproximado de 4 meses se obtuvieron 215 respuestas. Considerando la población total de la Ciudad de México hasta el año 2020 ($N = 9,209,944$) [37], y empleando la calculadora antes mencionada, con una proporción $p = 0.5$, se tuvo un nivel de confianza del 95 % y un margen de error aproximado del 6.7 %.

La encuesta fue contestada por personas con distintos rangos de edad, niveles educativos y frecuencias de uso de internet, lo cual permitió analizar la efectividad del recurso en un público diverso. Esto se muestra de forma gráfica en la figura 5.2.

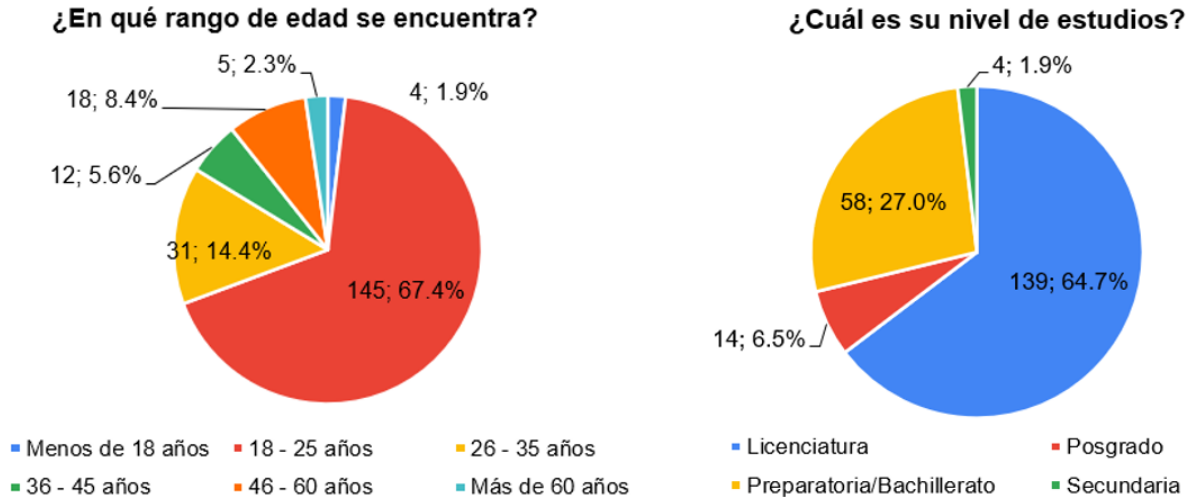


Figura 5.2: Preguntas sociodemográficas. Fuente: elaboración propia.

Los resultados indican que la mayoría de los encuestados (145 personas) se encuentra en el rango de 18 a 25 años. Sin embargo, también participaron personas menores de 18 años, mayores de 60 años y adultos en otros rangos de edad. De la misma manera, el 64.7 % cuenta con estudios de nivel licenciatura, seguidos por bachillerato, posgrado y secundaria.

Estos datos confirman que el recurso presenta un nivel de accesibilidad adecuado para una audiencia amplia y heterogénea.

5.2.2. Procedimiento de evaluación

La aplicación del instrumento se llevó a cabo completamente en línea mediante un formulario digital dividido en secciones. Cada participante avanzó de manera secuencial,

lo que permitió medir la comprensión generada inmediatamente después de revisar el contenido educativo. El procedimiento fue el siguiente:

1. Los participantes leyeron una descripción inicial del estudio, sus propósitos, los criterios de participación y el uso de la información proporcionada. Posteriormente iniciaron con preguntas diagnósticas sobre su conocimiento previo del *phishing*

2. Se les presentó el contenido educativo dentro del mismo formulario: primero dos infografías introductorias sobre qué es el *phishing* y cómo funciona, y posteriormente siete infografías adicionales sobre los distintos tipos de *phishing*. Las infografías aparecían en orden y debían revisarse antes de avanzar.

3. Inmediatamente después de cada bloque de contenido, los participantes respondieron preguntas diseñadas para evaluar su comprensión del material mostrado.

4. Posteriormente, analizaron veinte ejemplos reales de los distintos tipos de *phishing* con el fin de identificar señales de alerta.

5. Finalmente, proporcionaron retroalimentación sobre la claridad, utilidad y diseño de las infografías, así como sugerencias para mejorar el recurso.

Este procedimiento permitió medir tanto el nivel inicial de los participantes como los aprendizajes adquiridos después de interactuar con el recurso.

5.2.3. Sección general o sociodemográfica

Las respuestas a estas preguntas fueron por medio de opciones, y tienen el objetivo de proporcionar información sociodemográfica, en este contexto importante para determinar si el contenido es apto para la sociedad en general. En la figura 5.2 se muestra el gráfico de pasteles que permite ver los rangos de edad, el nivel de estudios y la frecuencia del uso del internet de los encuestados.

El gráfico izquierdo refleja que la mayor población encuestada se encuentra en el rango entre los 18 y los 25 años con un total de 145 personas, sin embargo, existe diversidad de población pues tenemos que 4 personas son menores de 18 años, 5 personas tienen más de

60 años, 18 personas están entre los 46 y los 60 años, 12 personas están entre los 36 y los 45 años, finalmente 31 personas están entre los 26 y los 35 años.

El gráfico derecho muestra que el nivel estudios dominante es la licenciatura con 139 personas, seguido del bachillerato con 58 personas, después el posgrado con 14 personas y por último la secundaria con 4 personas.

En el contexto de este documento es importante conocer estos datos, pues lo que se busca es concientizar a la población sobre este riesgo latente en internet, además la guía presentada como una propuesta de solución busca que cualquier persona pueda leerla y utilizarla como una guía paso a paso para prevenir y detectar el *phishing* por lo que, es importante destacar que no se requiere ningún conocimiento específico sobre el tema para poder entender el contenido.

5.2.4. Resultados del diagnóstico inicial

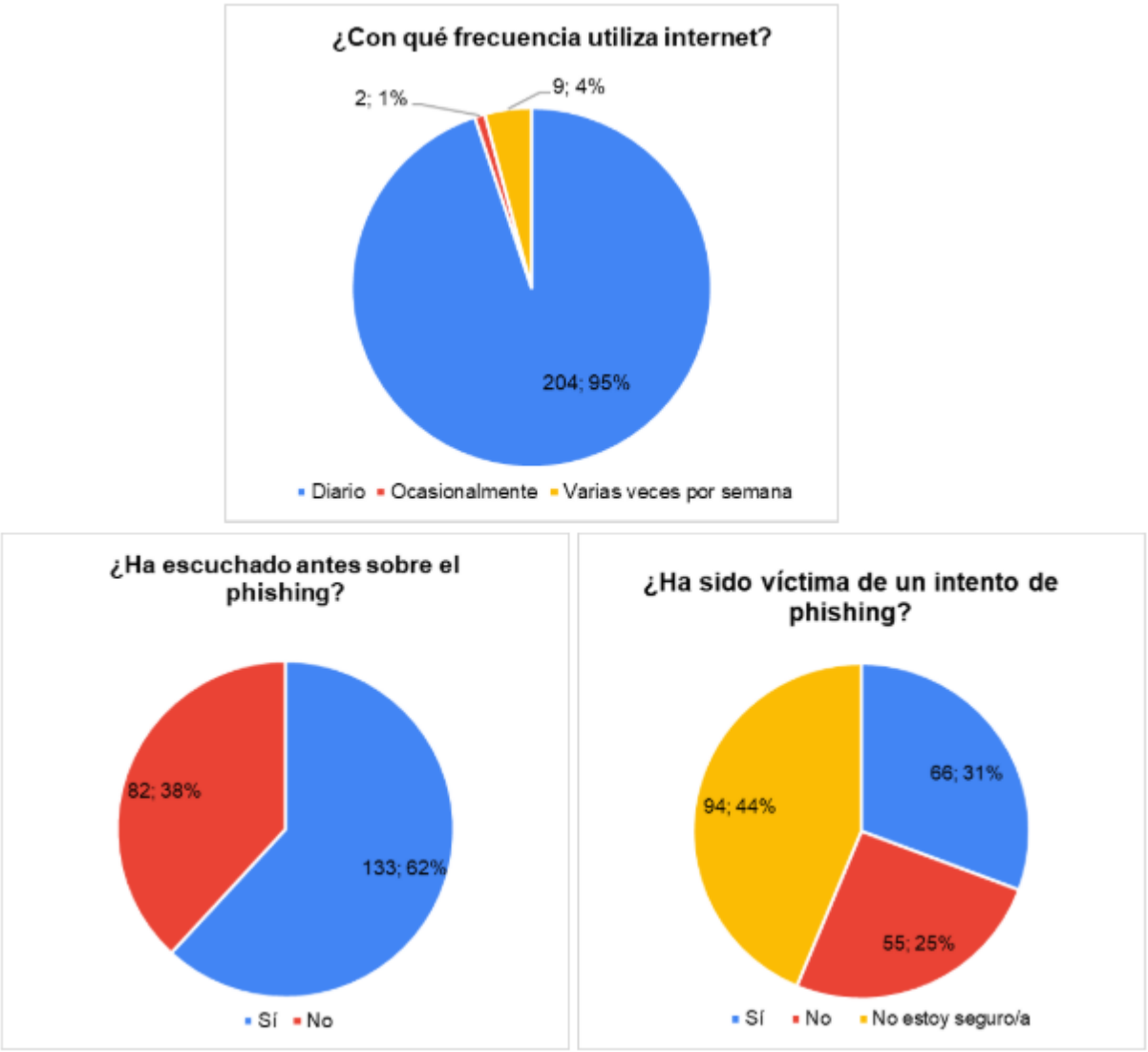


Figura 5.3: Preguntas diagnósticas. Fuente: elaboración propia.

Las preguntas relacionadas al diagnóstico se observan en la figura 5.3 y tienen opciones múltiples, la primera gráfica de la parte superior refleja la frecuencia del uso del internet y las gráficas inferiores que reflejan el conocimiento general del tema.

El gráfico superior muestra que al menos el 95 % de la población encuestada utiliza el internet diariamente, lo cual significa que al menos 204 personas tienen el riesgo de sufrir un ataque de *phishing*. El gráfico de la izquierda refiere que al menos 82 personas no tiene acercamiento al *phishing*. Finalmente el gráfico de la derecha indica que 66 personas han

sido víctimas y que solo 55 están seguras de no haber sido víctimas, mientras que las 94 personas restantes no están seguras de haber sido víctimas o no de *phishing*.

5.2.5. Resultados de comprensión posterior al uso del recurso

En esta sección se realizaron preguntas de opción múltiple que impulsaban a reflexionar sobre el contenido presentado y que buscan poder reflejar el entendimiento del tema de lo general a lo particular. En la figura 5.4 se muestran las preguntas que pueden hacer un contraste entre el antes y después de la información mientras que en la figura 5.5 se muestran las preguntas que pueden quedar a consideración del encuestado en cuanto a entendimiento de las recomendaciones propuestas con opciones múltiples en las que se puede seleccionar más de una opción.

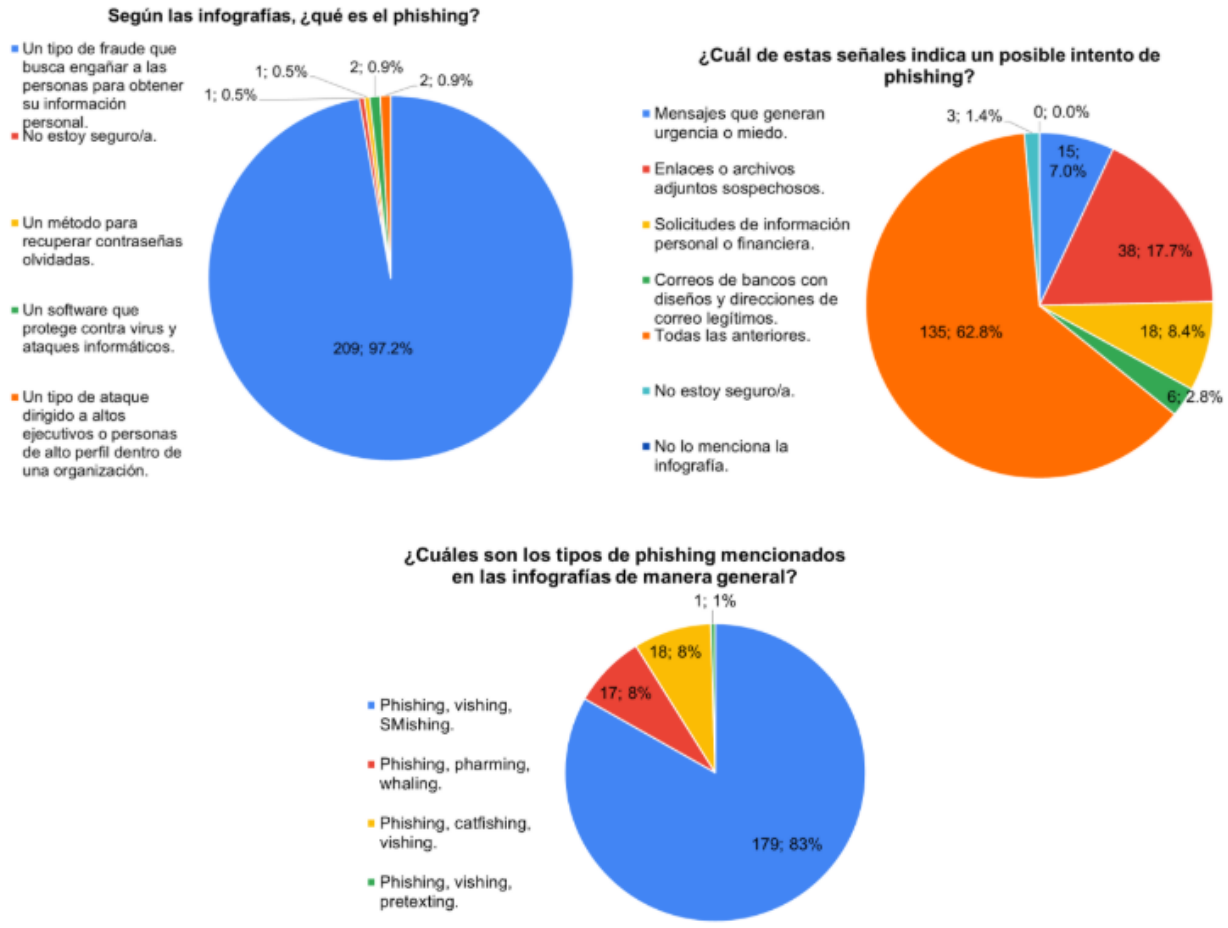


Figura 5.4: Preguntas de comprensión del tema. Fuente: elaboración propia.

Del gráfico superior izquierdo se puede notar que el 97.2 % de los encuestados pueden definir el *phishing* de manera adecuada. Del gráfico superior derecho que el 62.8 % identifica todas las señales de un intento de *phishing*, solo un 1.4 % no está seguro de las señales de un intento de *phishing*, mientras que el resto identifica al menos una señal. Finalmente el gráfico inferior muestra que el 83 % identifica correctamente los tipos de *phishing* de manera general.

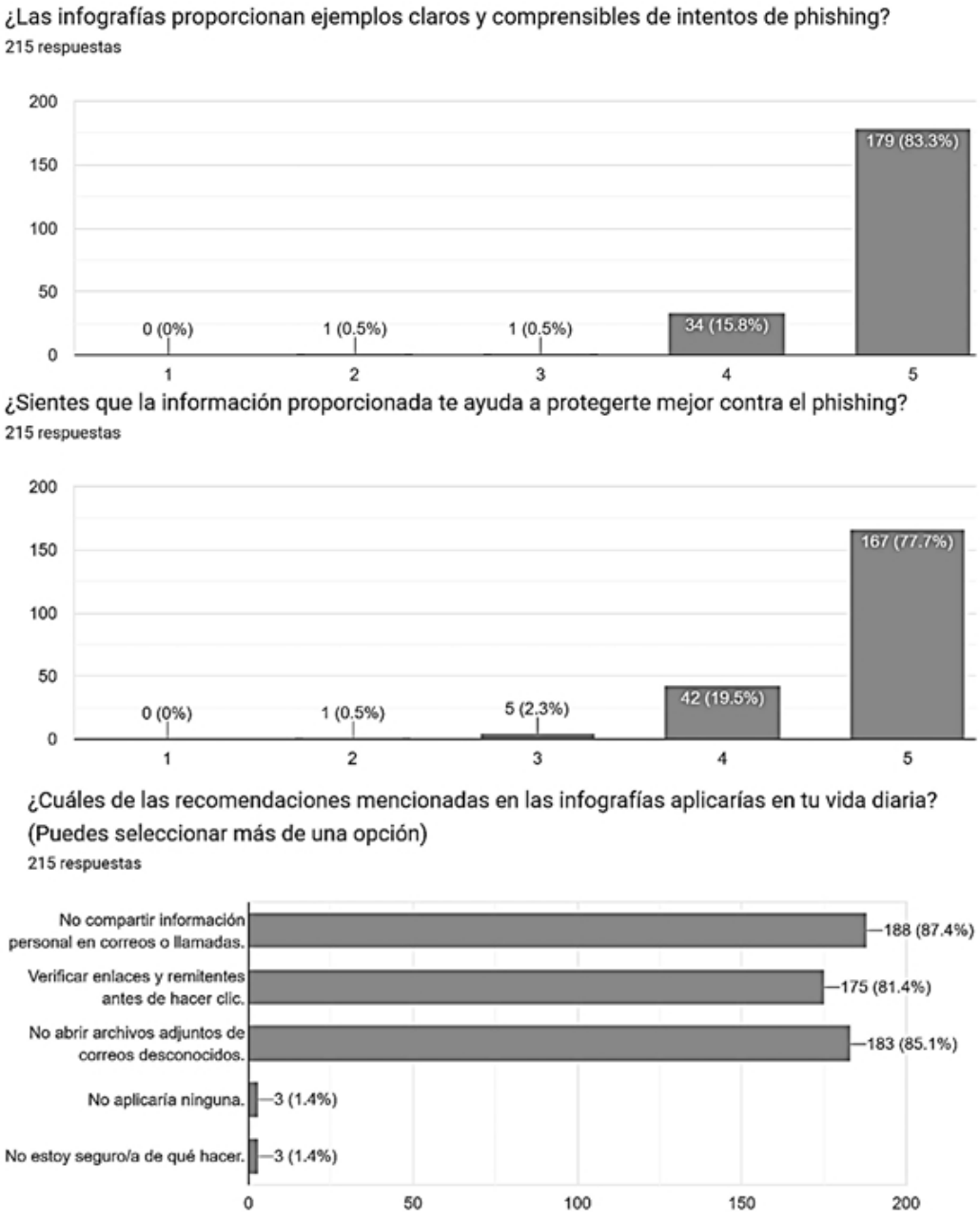
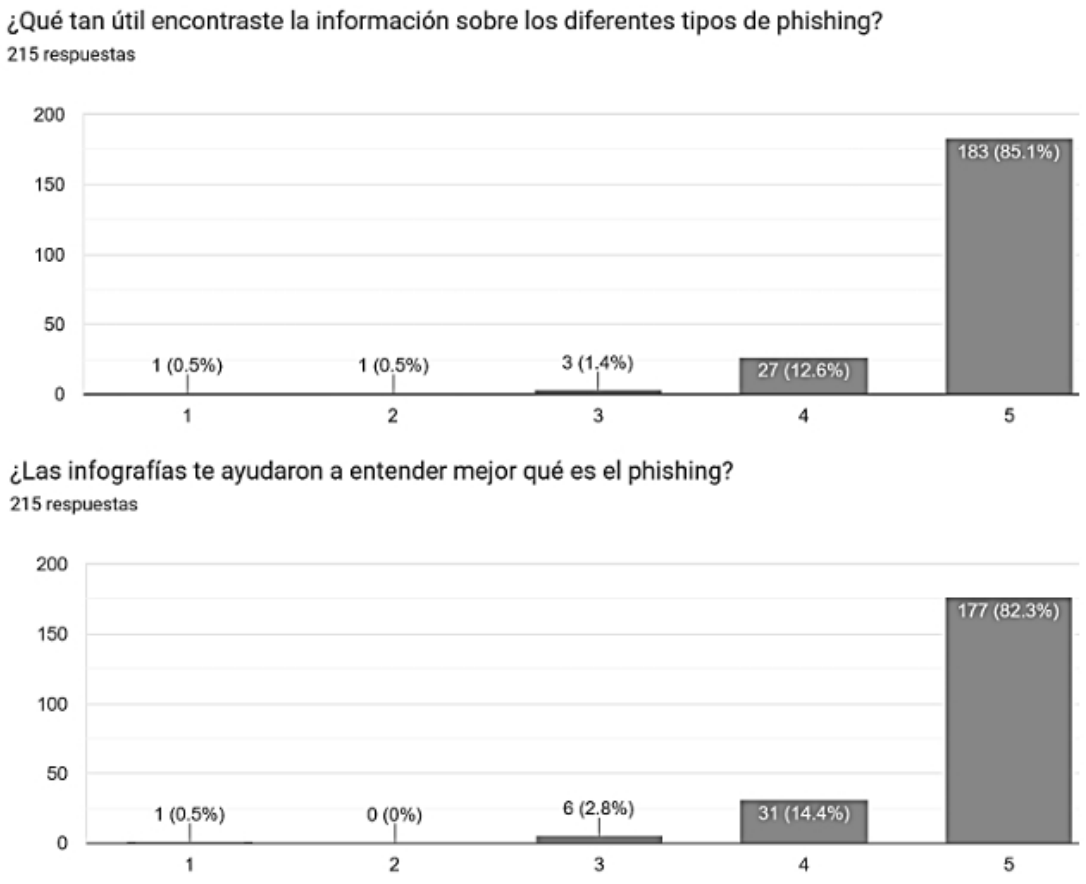


Figura 5.5: Preguntas sobre recomendaciones. Fuente: elaboración propia.

Las preguntas de la figura 5.5 muestran las opciones que los encuestados identificaron de las recomendaciones proporcionadas. De manera general mayormente seleccionan las recomendaciones que fueron proporcionadas sobre aquellas que no fueron proporcionadas o mencionadas.

5.2.6. Retroalimentación del recurso

En esta sección se presentan preguntas en las que las opciones de respuestas se miden del número 1 al 5 donde el 1 puede representar "Nada", "Poco" o "No" y el 5 puede ser "Mucho", "Muy" o "Sí". La figura 5.6 muestra la primera parte de la retroalimentación que se enfoca en evaluar la utilidad de las definiciones del *phishing*, además de la claridad del tema y el diseño de las infografías. La figura 5.7 permitió evaluar los ejemplos proporcionados, el sentido de protección resultante y la identificación de recomendaciones de seguridad generales en la vida diaria.



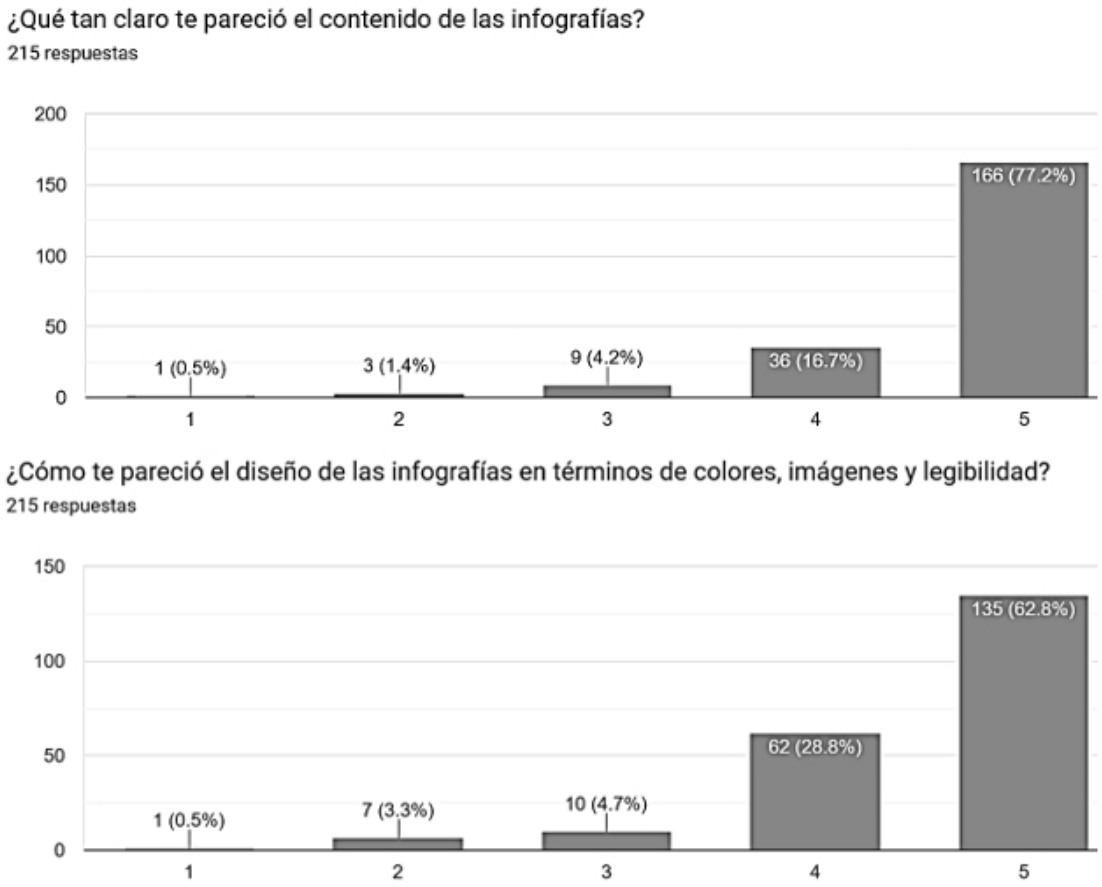


Figura 5.6: Retroalimentación sobre utilidad, contenido y diseño. Fuente: elaboración propia.

De la figura 5.6 se puede notar que de manera general hubo una mayoría de respuestas con valores entre 4 y 5 de más del 94 % de personas para todas las preguntas con lo que se puede determinar que la mayoría de las personas están satisfechos con los aspectos evaluados.

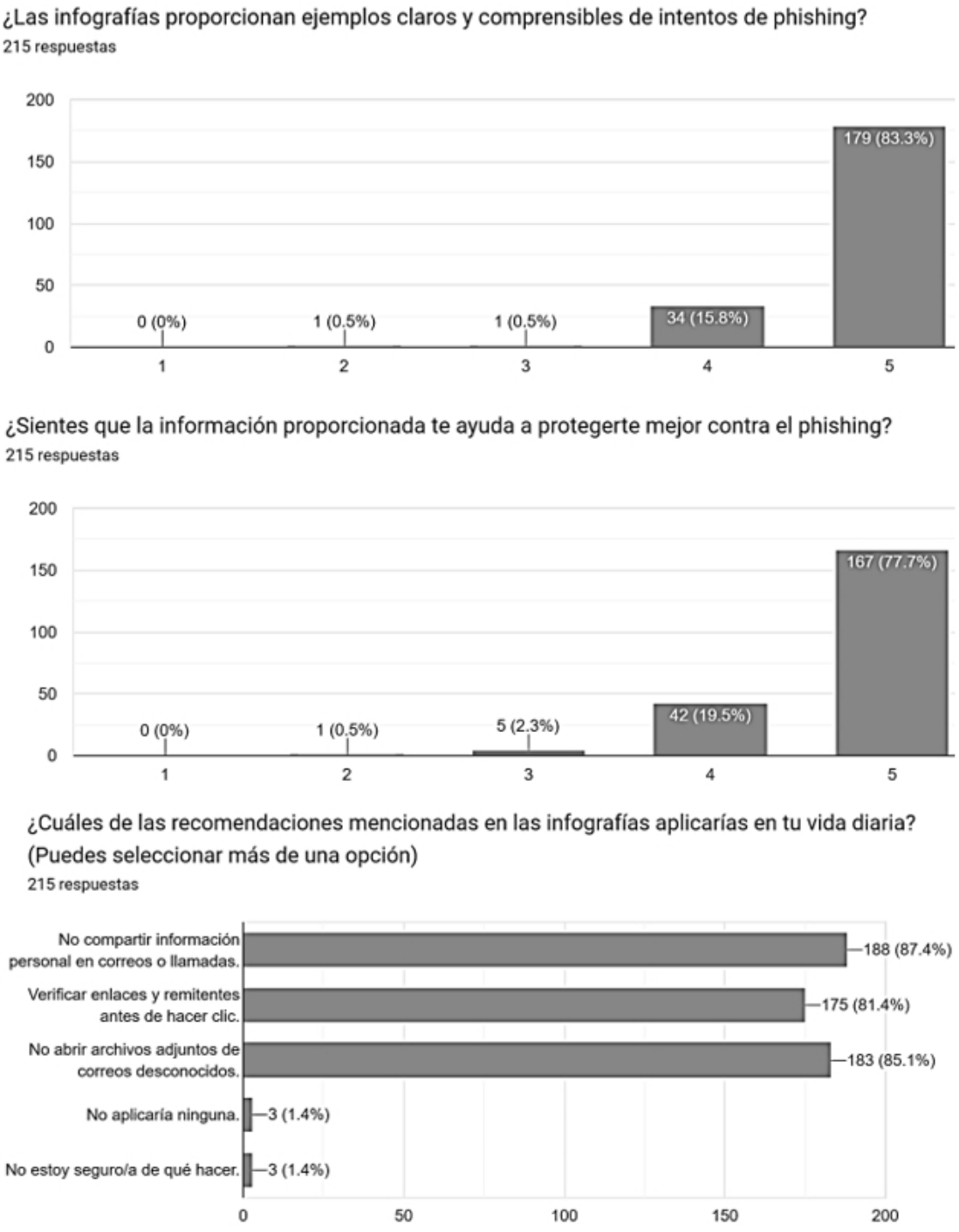


Figura 5.7: Retroalimentación sobre ejemplos. Fuente: elaboración propia.

En el caso de la figura 5.7 el gráfico superior y medio se evalúan de la misma manera, en un rango del 1 al 5, mientras que el gráfico inferior muestra una pregunta donde se podía seleccionar más de una opción. Observamos que nuevamente la mayoría de respuestas es

con valores entre 4 y 5 de al menos 98 % de personas. En el gráfico superior observamos que las personas están satisfechas con la claridad de los ejemplos presentados, el gráfico intermedio hace notar que las personas se sienten mejor protegidas contra el *phishing*, siguiendo el sentido de protección el gráfico inferior muestra las recomendaciones que las personas están dispuestas a aplicar en su vida diaria.

5.2.7. Comentarios y sugerencias

En esta sección se integraron dos apartados que podían ser contestados de forma voluntaria por las personas. La figura 5.8 se refiere a una pregunta específica sobre las infografías proporcionadas y la figura 5.9 es una pregunta más general abierta a cualquier comentarios o sugerencia que las personas desearan realizar.

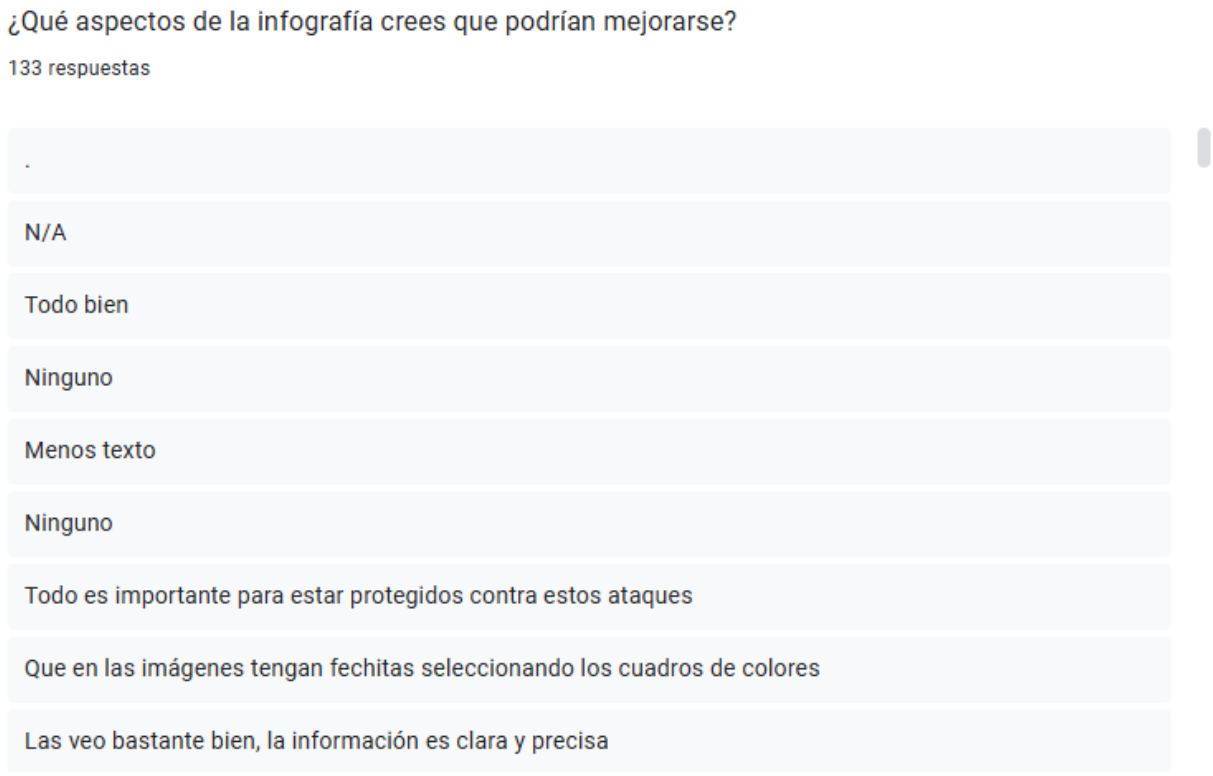


Figura 5.8: Aspectos a mejorar en infografías. Fuente: elaboración propia.

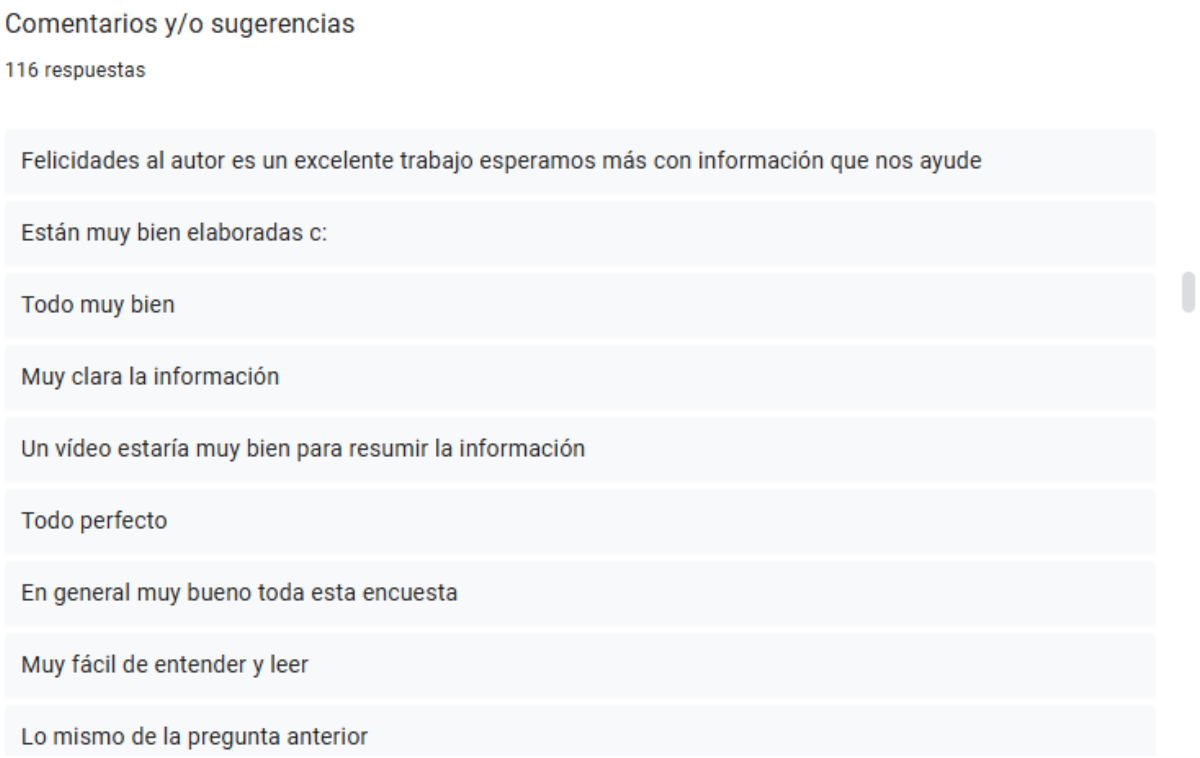


Figura 5.9: Comentarios y/o sugerencias. Fuente: elaboración propia.

Estas preguntas permitieron conocer las opiniones sobre el tema y también sobre el diseño de las infografías. La mayoría de las opiniones indican que el diseño y el contenido de las infografías es adecuado, pero existieron opiniones divididas sobre la cantidad de información presentada pues en algunos casos sugerían agregar más infografías y texto, mientras que en otros casos sugerían resumir más la información.

5.3. Paso 5: Ajustes y validación final

A partir de los resultados de la evaluación piloto, esta sección detalla los aspectos positivos identificados en el recurso, las áreas de mejora señaladas por los usuarios y los ajustes realizados para la versión final.

5.3.1. Elementos positivos identificados

El análisis de los resultados refleja una alta efectividad del recurso educativo. La mayoría de los participantes evaluó positivamente:

- La claridad de los conceptos explicados.
- La utilidad de los ejemplos reales.
- La comprensión del tema posterior a la lectura del recurso.
- El diseño visual y la estructura de las infografías.

Estos resultados confirman que el enfoque pedagógico adoptado es adecuado para una audiencia diversa.

5.3.2. Áreas de mejora

Del análisis cualitativo surgieron oportunidades de mejora relacionadas con:

- Equilibrar la cantidad de información presentada.
- Ampliar ciertos ejemplos.
- Sintetizar contenido en algunos módulos.
- Mejorar la legibilidad de algunos elementos visuales.

Estas observaciones fueron esenciales para fortalecer el recurso educativo.

5.3.3. Ajustes realizados

Con base en las áreas de mejora identificadas, se realizaron ajustes específicos al recurso:

- Revisión y depuración del contenido textual.
- Reorganización de la información en infografías para mejorar la claridad.
- Incorporación de ejemplos adicionales en módulos con alta demanda de detalle.

- Estandarización del estilo visual para mejorar la consistencia del material.

Estos ajustes mejoraron la coherencia, claridad y utilidad práctica del recurso.

5.3.4. Validación final

Tras la incorporación de los ajustes, se verificó que el recurso educativo cumple con su finalidad: facilitar la identificación de ataques de *phishing* mediante explicaciones claras, ejemplos reales y recomendaciones prácticas. La evaluación piloto, junto con los ajustes realizados, permiten validar el recurso como una herramienta efectiva para la alfabetización digital en materia de ciberseguridad dentro de la población general.

Además, como parte de la validación final del recurso, se compartieron de forma pública las infografías en la plataforma profesional de LinkedIn. Esta publicación permitió observar el alcance orgánico del material y su recepción fuera de la evaluación piloto. En total, las infografías alcanzaron 1,055 impresiones, es decir, el número de veces que la publicación fue mostrada en la plataforma, y fueron visualizadas por 419 miembros, lo que sugiere un nivel de interés significativo y confirma que el formato utilizado resulta accesible y atractivo para audiencias generales.

5.4. Discusión

La evaluación del recurso educativo permitió comprobar su impacto positivo en la comprensión del *phishing* entre los participantes, así como identificar áreas de mejora que fortalecieron su diseño final. Con ello, se cumple el propósito de los pasos 3, 4 y 5 de la metodología propuesta, dejando el recurso listo para su difusión y uso en iniciativas de educación digital orientadas a la prevención del fraude en línea.

Capítulo 6

Conclusiones

Las estafas basadas en *phishing* representan un riesgo en aumento para la sociedad mexicana, frente al cual la educación digital constituye una herramienta esencial de prevención. El objetivo central de esta tesina fue crear una guía clara, accesible y basada en ejemplos reales que permitiera a la población identificar y comprender los distintos tipos de *phishing*. Para lograrlo, se realizó una revisión sistemática de literatura especializada, donde se recopilaron casos reales provenientes de notas periodísticas, artículos y testimonios cercanos, y se desarrolló un análisis comparativo de soluciones existentes. Con ello se construyó un recurso educativo fundamentado en evidencia y orientado a las necesidades reales de la ciudadanía.

La evaluación piloto realizada con 215 participantes permitió constatar la eficacia de la guía para mejorar la comprensión del fenómeno. En el diagnóstico inicial, 82 personas (38 %) reportaron sólo haber escuchado de este tipo de ataque. Sin embargo, tras la lectura de la guía, el 97.2 % logró definir correctamente el concepto de *phishing*, lo que representa un incremento aproximado de 59.2 puntos porcentuales. Asimismo, la capacidad para identificar señales de alerta aumentó en cerca de 19.1 puntos porcentuales y alcanzó un 62.8 % de respuestas correctas. En cuanto a la clasificación de los tipos de *phishing*, el 83 % de los encuestados logró reconocerlos adecuadamente. Además, más del 94 % evaluó positivamente la claridad, utilidad y aplicabilidad de las definiciones, ejemplos e infografías incluidas. Estos indicadores respaldan que una guía breve, visual y basada en casos reales constituye un recurso pedagógico eficaz para fortalecer la alfabetización digital

de la población en torno al *phishing*.

Entre las aportaciones principales de este trabajo destacan: (1) la elaboración de un marco conceptual actualizado que define y diferencia los tipos de *phishing* en un lenguaje accesible, (2) la incorporación de ejemplos reales que reflejan prácticas delictivas vigentes en México, (3) el desarrollo de un recurso educativo práctico, estructurado por vectores de ataque y orientado a situaciones cotidianas (Apéndice B), y (4) la validación participativa del material mediante un proceso de retroalimentación que permitió mejorar su claridad, pertinencia y usabilidad.

Sin embargo, el estudio presenta limitaciones que deben ser consideradas. La muestra estuvo conformada exclusivamente por personas residentes de la Ciudad de México, lo que limita la generalización de los resultados a otros contextos socioculturales. Además, aunque la evaluación piloto permitió medir comprensión inmediata, no se evaluó la retención del conocimiento a mediano o largo plazo ni la transferencia del aprendizaje a situaciones reales de riesgo.

A partir de estos hallazgos, se identifican varias líneas de trabajo futuro. Entre ellas se propone realizar análisis de consistencia interna del instrumento de evaluación, así como estudios de validez de contenido y de impacto prolongado. Asimismo, dado que el *phishing* bancario es particularmente frecuente, sería valioso explorar escenarios de alta vulnerabilidad social, como por ejemplo, los periodos de pago de "aguinaldo" y "buen fin", para diseñar estrategias preventivas contextualizadas y culturalmente pertinentes. Finalmente, la guía podría ampliarse mediante módulos interactivos, simuladores de *phishing* o recursos audiovisuales que incrementen su alcance y efectividad.

En conjunto, este trabajo demuestra que es posible contribuir de manera significativa a la prevención del *phishing* mediante recursos educativos accesibles, basados en evidencia y adaptados al contexto social mexicano. La guía desarrollada y validada en esta tesina constituye un paso hacia una ciudadanía mejor informada y más preparada para enfrentar los riesgos del entorno digital actual.

Apéndice A

Glosario

Amenaza. Actividad, evento, fenómeno o circunstancia que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Amenaza interna. Nombre que se le da a una amenaza donde las personas que ya tienen acceso a sistemas, como los empleados o clientes, provocan una vulneración de seguridad o pérdida financiera. Se puede dar de forma involuntaria o malintencionada.

Análisis heurístico. Proceso para detectar la presencia de nuevos virus que aún no han sido documentados por los fabricantes de soluciones de seguridad. Se basan en la experiencia, realizando comparación de archivos sospechosos con fragmentos de código de virus de comportamiento similar o detectando actividades sospechosas de un programa por similitud con actividades conocidas de programas maliciosos.

Ataque. Acción intencional que busca acceder, alterar o comprometer la seguridad de un sistema, datos o recursos.

Autenticación. Proceso mediante el cual se verifica la identidad de una persona para permitir el acceso.

Autenticación multifactor. Proceso de verificación de identidad de una persona de dos o más formas para permitir el acceso a un sistema.

Ciberataque. Intento deliberado de acceder sin autorización a sistemas para alterar, robar o exponer información.

Ciberseguridad. Práctica de proteger equipos, sistemas, redes, programas y datos de ataques digitales.

Exfiltración de información. Extracción secreta y no autorizada de datos desde un sistema comprometido.

Inteligencia Artificial. Sistemas o programas que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o razonamiento lógico.

Ingeniería Social. Técnica de engaño utilizada para hacer que la víctima revele información confidencial, ya sea a través de engaños, solicitando un pago o pidiendo datos confidenciales. Puede hacer uso de ciberamenazas para motivar a la víctima a hacer clic en un enlace, descargar algún tipo de malware o acceder a fuentes maliciosas.

Machine Learning. Rama de la inteligencia artificial que permite a los sistemas aprender patrones a partir del uso de datos. Es traducida al español como Aprendizaje Máquina.

Malware. Término general para cualquier programa computacional o software diseñado para causar daño a los dispositivos o redes, acceder de manera no autorizada para extraer información confidencial, enviar correos electrónicos malintencionados o interrumpir el funcionamiento de una infraestructura o servicio.

Phishing. Técnica de fraude basada en ingeniería social que busca obtener datos personales o bancarios.

QRishing. Ataque basado en el uso de códigos QR modificados que redirigen a sitios fraudulentos.

Señuelo. Elemento inicial de un ataque de phishing, como un mensaje, enlace o llamada, diseñado para captar la atención de la víctima.

SMishing. Mensajes SMS enviados con la finalidad de robar información por medio de enlaces a sitios falsos.

Software. Conjunto de instrucciones o reglas programadas incluidas en un programa que permite interactuar con el sistema de forma fácil e intuitiva.

Riesgo. Posibilidad de que una amenaza se convierta en un daño real para la empresa o en la pérdida de información.

URL. Las siglas URL (Uniform Resource Locator) hacen referencia a la dirección que identifica contenido en internet.

Vishing. Llamadas telefónicas que tienen como objetivo la manipulación de las personas para obtener acceso a información confidencial.

VoIP. Tecnología que transforma la voz en señales digitales, para transmitirlas a través de Internet y, en el extremo receptor, las vuelve a transformar en audio. De esta manera se pueden realizar llamadas con calidad similar a las de la telefonía tradicional, pero usando redes de datos. Este acrónimo viene del inglés **Voice over IP** o Voz sobre IP.

Vulnerabilidad. Debilidad de un sistema que puede ser utilizado con fines malintencionados.

Apéndice B

Infografías

A continuación se presentan las infografías creadas como parte del recurso educativo durante la evaluación (Capítulo 5). Todas estas fueron elaboradas especialmente para este estudio, sin embargo, pueden ser posteriormente difundidas en un contexto fuera del estudio. Estas se muestran en el mismo orden en que fueron presentadas a las personas participantes.

B.1. Infografías introductorias

Figura B.1: Introducción al *phishing*. Fuente: elaboración propia.

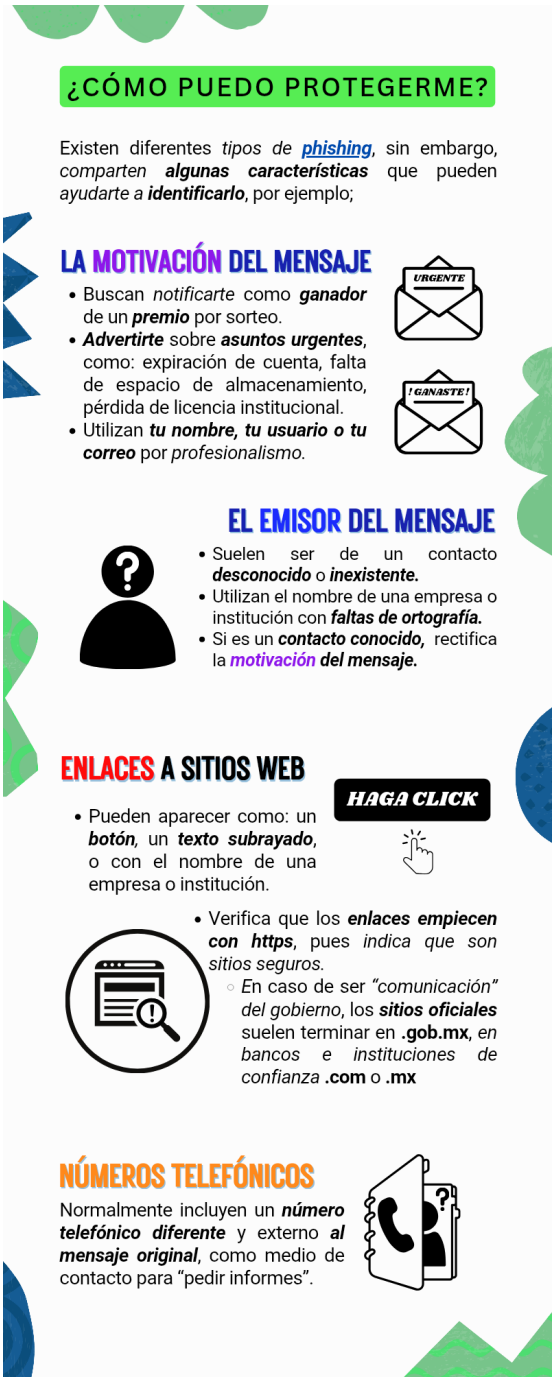


Figura B.2: Características del *phishing*. Fuente: elaboración propia.

B.2. Infografías sobre tipos de phishing

EJEMPLOS

Existen diferentes *tipos de* ***phishing*** que buscan *obtener* ***tus datos sensibles y confidenciales*** de diferentes formas, a continuación, se presentan los *tipos de* ***phishing*** y algunas de sus ***características.***

PHISHING POR REDES SOCIALES

Buscan captar la atención con promesas atractivas y en la mayoría de los casos, el objetivo principal es robar los datos de inicio de sesión de cuentas personales.

1. Analiza la **motivación** del mensaje
Pon atención al tipo de mensaje, suelen:
- ***Prometer*** *beneficios económicos* o regalos.
- ***Fingir*** que provienen de una *fuente conocida* o confiable utilizando tu nombre.

2. Examina al **emisor**
Antes de interactuar con el mensaje:
- ***Verifica*** *el nombre de usuario* o perfil del emisor. Incluyen *nombres con combinaciones aleatorias de caracteres* o bien, suplantan la identidad de un conocido.

Si el mensaje 'proviene' de un amigo o familiar, confirma de forma directa con ellos el mensaje.

3. Verifica los **enlaces** incluidos
Considera que:
- Los **enlaces** pueden aparecer como ***botones***, *texto subrayado o direcciones a sitios* que incluyen nombres de empresas, instituciones o servicios.

En la Figura 1 se muestra un ejemplo típico donde el emisor es completamente desconocido, sin embargo, ofrece un beneficio atractivo o desconocido para incitar a hacer clic en el enlace incluido.

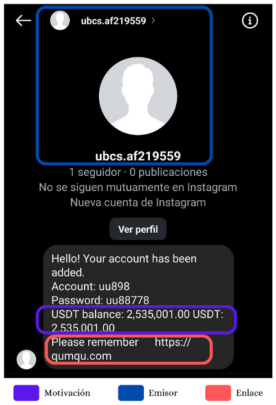


Figura 1: Ejemplo de *phishing* por redes sociales.

Figura B.3: Ejemplo de *phishing* por redes sociales. Fuente: elaboración propia.

EJEMPLOS

PHISHING POR CORREO ELECTRÓNICO

Es una de las *formas más comunes* en las que los *ciberdelincuentes* actúan. Puedes identificarlo a través de los siguientes puntos:

1. Analiza la **motivación** del mensaje
Presta atención al propósito del correo, suelen:
- ***Notificarte*** que has sido seleccionado *como* ***'Ganador'*** *de un premio* por suerte.
- ***Advertirte*** sobre problemas o asuntos ***'urgentes'***, como la expiración de tu cuenta, falta de espacio de almacenamiento, pérdida de licencia institucional, etc.

2. Examina al **emisor**
Antes de interactuar con el correo:
- *Revisa la dirección de correo del remitente.*
- Suelen utilizar ***direcciones*** *desconocidas* o que incluyen ***combinaciones aleatorias de letras****, números y símbolos.*

3. Verifica los **enlaces** incluidos
Considera que:
- Los **enlaces** pueden aparecer como ***botones***, *texto subrayado o direcciones a sitios* que incluyen nombres de empresas, instituciones o servicios.

En la Figura 2 se presenta un ejemplo de este tipo.

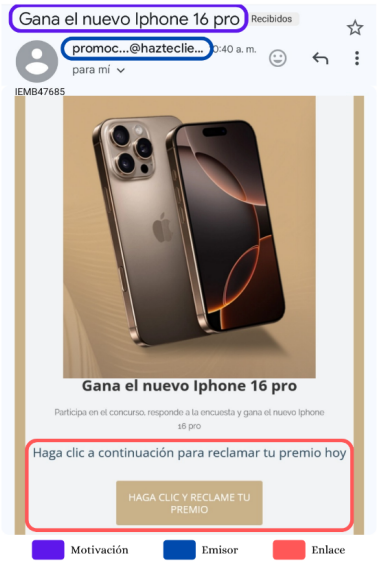


Figura 2: Ejemplo de *phishing* por *'ganar un premio'*.

Figura B.4: Ejemplo de *phishing* por correo electrónico. Fuente: elaboración propia.

EJEMPLOS

PHISHING POR MENSAJERÍA INSTANTÁNEA

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 accesibilidad.

1. Analiza la **motivación** del mensaje

Es frecuente recibir mensajes donde:

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

2. Examina al **emisor**

Es crucial confirmar la legitimidad del emisor o de las propuestas laborales antes de interactuar 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***

3. Verifica los **enlaces** incluidos

Incluyen enlaces externos para 'contactar' directamente con la persona encargada de la contratación, contradiciendo el motivo principal del mensaje

En la Figura 3 se muestra una *oferta laboral* mientras que la Figura 4 presenta una *'invitación'*, diseñada así para generar un sentido de pertenencia

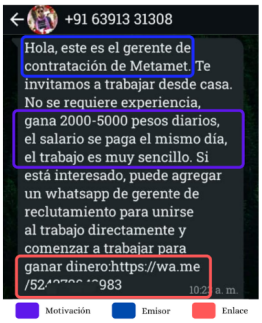


Figura 3: *Phishing* por IM por el 'gerente'.

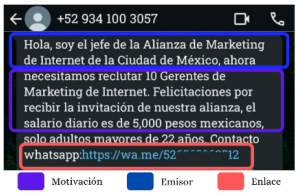


Figura 4: *Phishing* por IM por el 'jefe'.

Figura B.5: Ejemplo de *phishing* por mensajería instantánea. Fuente: elaboración propia.

EJEMPLOS

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.

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.
- En caso de ser ***sitios gubernamentales*** en México suelen tener la terminación del enlace en **.gob.mx**, para bancos e instituciones de confianza **.com** o **.com.mx**.

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 con el.

Se ilustra una ***comparación entre un sitio legítimo*** (lado izquierdo) ***y uno fraudulento*** (lado derecho) en la Figura 5.

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 5: Ejemplo de *phishing* por sitios web.

[2] Servicio de Administración Tributaria. Sitios web falsos, 10 2024. Disponible en: https://www.gob.mx/sat/acciones-y-programas/sitios-web-falsos.

Figura B.6: Ejemplo de *phishing* por sitios web. Fuente: elaboración propia.

EJEMPLOS

PHISHING POR 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.*

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.

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 6 y 7 se muestran algunos formularios, sin embargo, *estas redes pertenecen a empresas oficiales y cuentan con términos y condiciones* claros con respecto al uso de los datos, 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*.

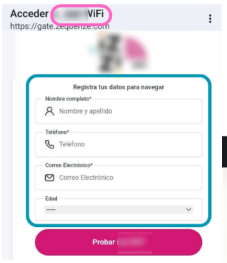


Figura 6: Ejemplo de formulario que solicita nombre, teléfono y correo.

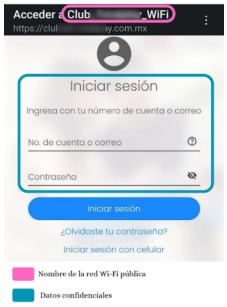


Figura 7: Ejemplo de formulario que solicita correo y contraseña.

Figura B.7: Ejemplo de *phishing* por Wi-Fi. Fuente: elaboración propia.

EJEMPLOS

PHISHING por SMS (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.*

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 8)
- ***Hacen mención*** a *empresas o servicios reconocidos* (véase la Figura 9) o a asistencia jurídica.

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 8 se muestra un ejemplo de *SMishing* que dirige a un ***número telefónico*** *externo*, mientras que en la Figura 9 dirige a *un sitio falso* o apócrifo por medio de un **enlace**.
Observa como *utilizan el nombre de servicios, empresas y a las instituciones financieras y de gobierno*, para poder fingir establecer una **comunicación de confianza** y así no desconfíes de ellos.

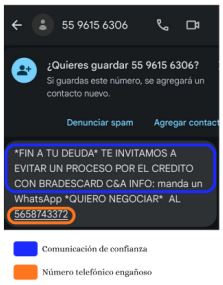


Figura 8: *SMishing* por adeudos.

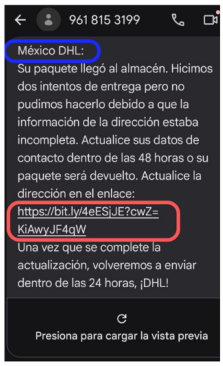


Figura 9: *SMishing* por 'empresa'.

Figura B.8: Ejemplo de *phishing* por SMS (SMishing). Fuente: elaboración propia.

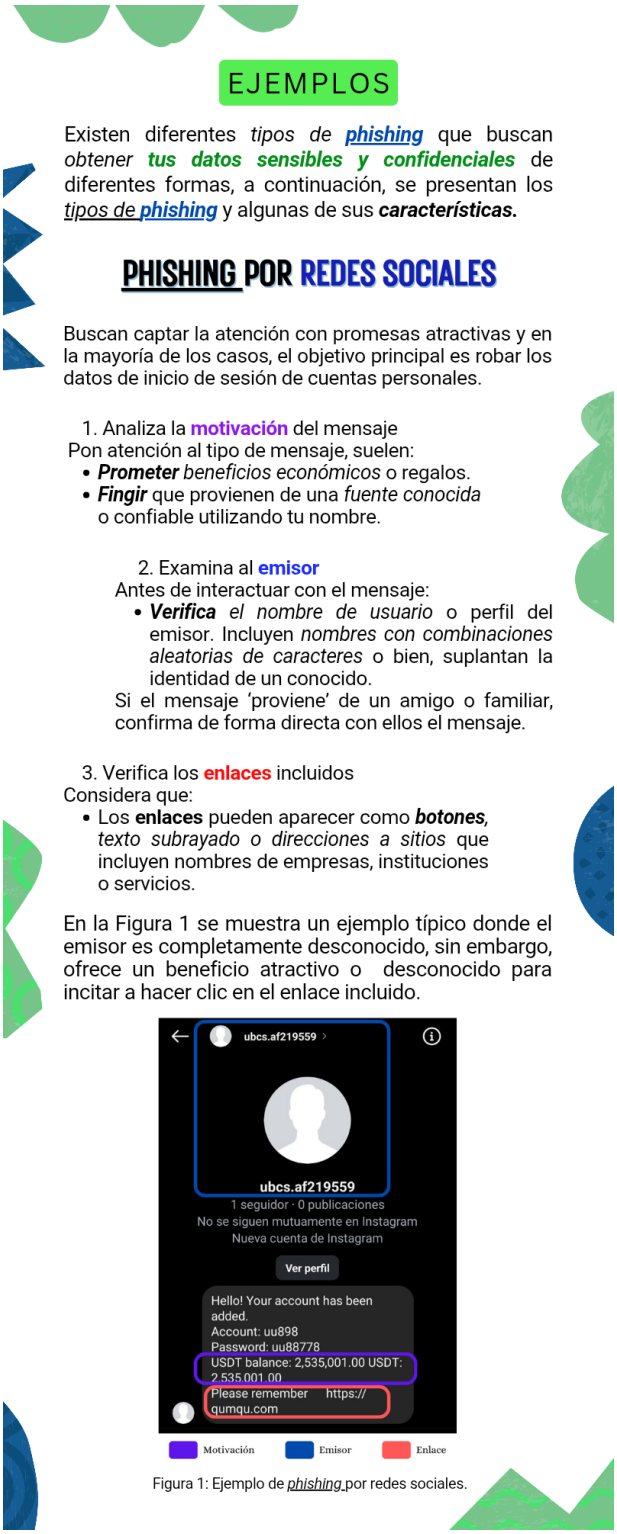


Figura B.9: Ejemplo de *phishing* por llamadas (vishing). Fuente: elaboración propia.

Bibliografía

[1] INEGI and IFT, "Encuesta Nacional sobre Disponibilidad y uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023," pp. 1–28, 6 2024, disponible en: https://www.inegi.org.mx/programas/endutih/2023/. Accedido: 26-ago-2024. [Online]. Available: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/ENDUTIH/ENDUTIH_23.pdfhttps://www.inegi.org.mx/programas/endutih/2023/

[2] A. Rojas, "México, uno de los países más expuestos a la inseguridad digital en 2024," *Expansión*, 3 2024, disponible en: https://expansion.mx/opinion/2024/03/14/mexico-uno-de-los-paises-mas-expuestos-a-la-inseguridad-digital-en-2024. Accedido: 19-sept-2024. [Online]. Available: https://expansion.mx/opinion/2024/03/14/mexico-uno-de-los-paises-mas-expuestos-a-la-inseguridad-digital-en-2024

[3] K. Team, "Los ataques contra celulares crecen un 70 %, lo que marca un récord en américa latina," 8 2024, disponible en: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2024/27591/. Accedido: 19-sept-2024. [Online]. Available: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2024/27591/

[4] CONDUSEF, "PORTAL DE FRAUDES FINANCIEROS | Infórmate y Protégete," disponible en: https://phpapps.condusef.gob.mx/fraudes_financieros/informate.php. Accedido: 25-sept-2024. [Online]. Available: https://phpapps.condusef.gob.mx/fraudes_financieros/informate.php

[5] K. Team, "Panorama en América Latina 2023," 8 2023, disponible en: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/

26586/. Accedido: 18-sept-2024. [Online]. Available: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

[6] P. F. del Consumidor, "Campaña nacional antifraude cibernético," 12 2020, disponible en: https://www.gob.mx/profeco/articulos/campana-nacional-antifraude-cibernetico-260577?idiom=es. Accedido: 19-ago-2024. [Online]. Available: https://www.gob.mx/profeco/articulos/campana-nacional-antifraude-cibernetico-260577?idiom=es

[7] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet 2020, Vol. 12, Page 168*, vol. 12, p. 168, 9 2020, disponible en: https://www.mdpi.com/1999-5903/12/10/168/htmhttps://www.mdpi.com/1999-5903/12/10/168. Accedido: 25-sept-2024. [Online]. Available: https://www.mdpi.com/1999-5903/12/10/168/htmhttps://www.mdpi.com/1999-5903/12/10/168

[8] Cisco Networking Academy, "Fundamentos de Ciberseguridad," Curso en línea, disponible en: https://www.netacad.com/courses/cybersecurity-essentials?courseLang=es-XL (Se requiere registro). [Online]. Available: https://www.netacad.com/courses/cybersecurity-essentials?courseLang=es-XL

[9] INEGI, "Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2024," 2025. [Online]. Available: https://www.inegi.org.mx/contenidos/programas/endutih/2024/doc/presentacion_endutih2024.pdf

[10] CISCO, "What is cybersecurity?" disponible en: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html. Accedido: 01-oct-2024. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

[11] AWS, "¿Qué es la ciberseguridad? - Explicación de la ciberseguridad," disponible en: https://aws.amazon.com/what-is/cybersecurity/. Accedido: 01-oct-2024. [Online]. Available: https://aws.amazon.com/what-is/cybersecurity/

[12] Microsoft, "¿Qué es la ciberseguridad?" disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-cybersecurity. Accedido: 21-oct-2024. [Online]. Available: https://www.microsoft.com/es-mx/security/business/security-101/what-is-cybersecurity

[13] IBM, "¿Qué es un ciberataque?" disponible en: https://www.ibm.com/es-es/topics/cyber-attack. Accedido: 15-nov-2024. [Online]. Available: https://www.ibm.com/es-es/topics/cyber-attack

[14] S. de Microsoft, "¿qué es un ciberataque?" disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-a-cyberattack?msockid=3544ed23478e67d30b46fe98464266a7. Accedido: 15-nov-2024. [Online]. Available: https://www.microsoft.com/es-es/security/business/security-101/what-is-a-cyberattack?msockid=3544ed23478e67d30b46fe98464266a7

[15] CISCO, "What is cybersecurity?" disponible en: https://www.ibm.com/think/topics/cybersecurity. Accedido: 01-oct-2024. [Online]. Available: https://www.ibm.com/think/topics/cybersecurity

[16] ——, "What Is Cybersecurity?" 11 2023, disponible en: https://www.cisco.com/c/en_uk/products/security/what-is-cybersecurity.html. Accedido: 01-oct-2024. [Online]. Available: https://www.cisco.com/c/en_uk/products/security/what-is-cybersecurity.html

[17] OCU, "¿qué es el phishing?" 1 2023, disponible en: https://www.ocu.org/tecnologia/antivirus/consejos/evitar-ataque-phishing. Accedido: 25-sept-2024. [Online]. Available: https://www.ocu.org/tecnologia/antivirus/consejos/evitar-ataque-phishing

[18] C. Martínez, "¿qué es el phishing?" *UNAM-CERT*, 1 2019, disponible en: https://www.seguridad.unam.mx/que-es-el-phishing-2. Accedido: 25-sept-2024. [Online]. Available: https://www.seguridad.unam.mx/que-es-el-phishing-2

[19] M. Kosinski, "¿qué es el phishing?" *IBM*, 5 2024, disponible en: https://www.ibm.com/es-es/topics/phishing. Accedido: 25-sept-2024. [Online]. Available: https://www.ibm.com/es-es/topics/phishing

[20] Kaspersky, "Estafas y ataques de phishing: cómo protegerte," disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/phishing-prevention-tips. Accedido: 25-sept-2024. [Online]. Available: https://www.kaspersky.es/resource-center/preemptive-safety/phishing-prevention-tips

[21] BBVA, "¿qué es el phishing y cuáles son sus consecuencias?" 3 2023, disponible en: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html. Accedido: 25-sept-2024. [Online]. Available: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html

[22] F. P. E. Putra, A. Zulfikri, G. Arifin, R. M. Ilhamsyah, F. Teknik, I. U. M. J. R. P. NoKm, K. Tlanakan, K. Pamekasan, and J. Timur, "Analysis of phishing attack trends, impacts and prevention methods: Literature study," *Brilliance: Research of Artificial Intelligence*, vol. 4, pp. 413–421, 8 2024, disponible en: https://jurnal.itscience.org/index.php/brilliance/article/view/4357. Accedido: 31-ago-2024. [Online]. Available: https://journal.itscience.org/index.php/brilliance/article/view/4357

[23] IBM, "¿qué es la ingeniería social?" disponible en: https://www.ibm.com/es-es/topics/social-engineering. Accedido: 25-sept-2024. [Online]. Available: https://www.ibm.com/es-es/topics/social-engineering

[24] L. Kleinrock, "An early history of the internet [history of communications]," *IEEE Communications Magazine*, vol. 48, pp. 26–36, 8 2010, disponible en: https://ieeexplore.ieee.org/document/5534584. Accedido: 21-oct-2024. [Online]. Available: https://ieeexplore.ieee.org/document/5534584

[25] M. Kosinski, "What is phishing?" 5 2024, disponible en: https://www.ibm.com/

topics/phishing. Accedido: 21-oct-2024. [Online]. Available: https://www.ibm.com/topics/phishing

[26] D. Li, Q. Chen, and L. Wang, "Phishing attacks: Detection and prevention techniques," *Journal of Industrial Engineering and Applied Science*, vol. 2, pp. 48–53, 8 2024, disponible en: https://www.suaspress.org/ojs/index.php/JIEAS/article/view/131. Accedido: 29-oct-2024. [Online]. Available: https://www.suaspress.org/ojs/index.php/JIEAS/article/view/131

[27] Microsoft, "¿qué es el phishing?" disponible en: https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing. Accedido: 21-oct-2024. [Online]. Available: https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing

[28] M. Jakobsson, "The human factor in phishing," *ResearchGate*, 1 2017, disponible en: https://www.researchgate.net/publication/228837083_The_human_factor_in_phishing. Accedido: 21-oct-2024. [Online]. Available: https://www.researchgate.net/publication/228837083_The_human_factor_in_phishing

[29] E. D. Frauenstein and S. V. Flowerday, "Social network phishing: Becoming habituated to clicks and ignorant to threats?" *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, pp. 98–105, 2016, disponible en: https://ieeexplore.ieee.org/document/7802935. Accedido: 21-oct-2024. [Online]. Available: https://ieeexplore.ieee.org/document/7802935

[30] M. Jakobsson, "The rising threat of launchpad attacks," *IEEE Security and Privacy*, vol. 17, pp. 68–72, 9 2019, disponible en: https://ieeexplore.ieee.org/abstract/document/8821474. Accedido: 21-oct-2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8821474

[31] O. C. Obi, O. V. Akagha, S. O. Dawodu, A. C. Anyanwu, S. Onwusinkwue, I. A. I. Ahmad, and C. Author, "COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES," *Computer*

Science & IT Research Journal, vol. 5, pp. 293–310, 2 2024, disponible en: https://fepbl.com/index.php/csitrj/article/view/758. Accedido: 29-oct-2024. [Online]. Available: https://fepbl.com/index.php/csitrj/article/view/758

[32] O. México, "¿Qué es el aprendizaje automático?" disponible en: https://www.oracle.com/mx/artificial-intelligence/machine-learning/what-is-machine-learning/. Accedido: 01-dic-2024. [Online]. Available: https://www.oracle.com/mx/artificial-intelligence/machine-learning/what-is-machine-learning/

[33] I. Gómez, "Ciberdelincuentes suplantan al gobierno de cdmx en nueva estafa vía sms," *Publimetro*, 8 2024, disponible en: https://www.publimetro.com.mx/noticias/2024/08/07/ciberdelincuentes-suplantan-al-gobierno-de-cdmx-en-nueva-estafa-via-sms/. Accedido: 18-sept-2024. [Online]. Available: https://www.publimetro.com.mx/noticias/2024/08/07/ciberdelincuentes-suplantan-al-gobierno-de-cdmx-en-nueva-estafa-via-sms/

[34] Servicio de Administración Tributaria, "Sitios web falsos," 10 2024, disponible en: https://www.gob.mx/sat/acciones-y-programas/sitios-web-falsos. Accedido: 17-nov-2024. [Online]. Available: https://www.gob.mx/sat/acciones-y-programas/sitios-web-falsos

[35] Cecilia San Miguel, "Guía de Identificación de Phishing." 2024, disponible en: https://github.com/CecySamitu/GuiaDeIdentificacionDePhishing.git. Accedido: 01-dic-2024. [Online]. Available: https://github.com/CecySamitu/GuiaDeIdentificacionDePhishing.git

[36] ——, "Identificación y prevención del phishing," 2024, disponible en: https://www.linkedin.com/posts/cecysamitu_ciberseguridad-phishing-educaciaejndigital-activity-7320999536850595840-yQwo?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEAjtKEBftl83duqY8hp053lURseumsdQBM. Accedido: 21-oct-2024. [Online]. Available: https://www.linkedin.com/posts/cecysamitu_ciberseguridad-phishing-educaciaejndigital-activity-7320999536850595840-yQwo?

utm_source=share&utm_medium=member_desktop&rcm=
ACoAAEAjtKEBftl83duqY8hp053lURseumsdQBM

[37] INEGI, "México en cifras," disponible en: https://www.inegi.org.mx/app/areasgeograficas/?ag=09#tabMCcollapse-Indicadores. Accedido: 05-dic-2025. [Online]. Available: https://www.inegi.org.mx/app/areasgeograficas/?ag=09#tabMCcollapse-Indicadores