Smishing

Ministerio de Educación,
Deporte y Cultura

REPÚBLICA
DEL ECUADOR

EQUIPO TÉCNICO
Soledad Albán Montalvo
Hamilton Cabrera Brunes
Víctor Pazmiño Puma

DISEÑO, DIAGRAMACIÓN E ILUSTRACIÓN
Adolfo Vasco Cruz

EQUIPO TÉCNICO EXTERNO

Marcelo Javier Sotaminga Cinilin

Primera Edición, 2026

© Ministerio de Educación
Av. Amazonas N34-451 y Av. Atahualpa
Quito-Ecuador
www.educacion.gob.ec

Ministerio de Educación, Deporte y Cultura

REPÚBLICA DEL ECUADOR

DISTRIBUCIÓN GRATUITA
PROHIBIDA SU VENTA

La reproducción parcial o total de esta publicación, en cualquier forma y por cualquier medio mecánico o electrónico, está permitida siempre y cuando sea autorizada por los editores y se cite correctamente la fuente.

Contenido

1. Introducción

En la era actual, la tecnología se ha entrelazado profundamente con todos los aspectos de nuestra vida, incluyendo el ámbito educativo. La ciudadanía digital emerge como un concepto fundamental, abarcando las habilidades, conocimientos y actitudes esenciales para una participación segura, responsable y ética en el entorno digital. Sin embargo, esta inmersión en el ciberespacio conlleva riesgos inherentes, siendo uno de los más prevalentes el smishing. Este término, una contracción de "SMS" (Short Message Service) y "phishing", describe una técnica de fraude que emplea mensajes de texto fraudulentos para engañar a las víctimas y obtener información personal o financiera sensible, suplantando la identidad de entidades legítimas como bancos, empresas de servicios o instituciones gubernamentales (Fortinet, 2025; Proofpoint, 2025).

A diferencia del phishing, que se realiza principalmente a través de correos electrónicos, el smishing explota la percepción de inmediatez y confianza que los usuarios suelen depositar en los mensajes de texto, convirtiéndolo en una herramienta particularmente eficaz para el fraude (Kaspersky, 2025). Además, en dispositivos móviles, la verificación de la autenticidad de un enlace es más compleja, y la familiaridad con comunicaciones legítimas vía SMS (bancos, códigos de verificación) puede reducir la guardia del usuario ante un mensaje malicioso (Zscaler, 2025).

Este documento conceptual, desarrollado en el marco del proyecto "Exploradores Digitales con Eugenia" del Ministerio de Educación del Ecuador, tiene como objetivo principal proporcionar una comprensión profunda del smishing, abordando sus causas, consecuencias y, crucialmente, las estrategias de prevención, dirigido específicamente a estudiantes de educación básica superior y bachillerato. A través de una estructura pedagógica basada en "Conocer > Identificar > Prevenir", para empoderar a los jóvenes para que naveguen por el ciberespacio de manera segura y se conviertan en ciudadanos digitales conscientes y críticos. La información aquí presentada se basa en una investigación exhaustiva de fuentes académicas, informes institucionales y normativas recientes, con un enfoque particular en el contexto ecuatoriano y regional, así como en referencias internacionales de relevancia.

2. Ruta de aprendizaje

a. Conocer el riesgo

Definición del riesgo: Smishing

El término smishing es una amalgama de las palabras “SMS” (Short Message Service) y “phishing”, y se refiere a un tipo de ciberataque que utiliza mensajes de texto fraudulentos para engañar a las víctimas (Fortinet, 2025; Proofpoint, 2025; Wikipedia, 2016). En esencia, es una forma de ingeniería social donde los ciberdelincuentes se hacen pasar por una entidad confiable (como un banco, una tarjeta de crédito, una red social o un organismo público) con el objetivo de obtener datos confidenciales de la persona (INCIBE, 2025; Wallarm, 2024).

Los SMS maliciosos suelen incluir enlaces a sitios web falsos o solicitudes para llamar a números de teléfono; al interactuar con ellos, la víctima podría entregar contraseñas, números de tarjetas de crédito, credenciales bancarias u otra información sensible sin darse cuenta (Wikipedia, 2016). En algunos casos, los mensajes de smishing incitan a las víctimas a descargar aplicaciones maliciosas que contienen troyanos, spyware o ransomware. Estos programas pueden robar credenciales bancarias y contraseñas, registrar pulsaciones del teclado, espiar la actividad del usuario, activar la cámara o el micrófono sin autorización. Así, el simple hecho de seguir un enlace recibido por SMS puede comprometer por completo la seguridad del dispositivo y la información personal del usuario (Kaspersky, 2025). En resumen, el smishing corresponde al phishing ejecutado mediante SMS. Consiste en la suplantación de identidad digital y resulta efectivo porque explota la credibilidad que los usuarios otorgan a los mensajes móviles y la inmediatez asociada a este canal de comunicación (Zscaler, 2025).

Smishing y su relación con el phishing

El *smishing* constituye una variante del *phishing*, en la que el canal de ataque se desplaza del correo electrónico tradicional hacia los mensajes de texto (SMS) y, cada vez con mayor frecuencia, a las aplicaciones de mensajería instantánea. Ambos comparten el mismo propósito: manipular al usuario para que entregue información confidencial, haga clic en enlaces fraudulentos o descargue software malicioso.

No obstante, existen diferencias significativas en cuanto a los medios, técnicas y niveles de sofisticación empleados. Mientras que el *phishing* se ha consolidado históricamente como una amenaza a través del correo electrónico, el *smishing* aprovecha la confianza que los usuarios depositan en sus dispositivos móviles y en los mensajes que reciben en tiempo real.

La siguiente tabla presenta de manera comparativa las semejanzas y diferencias entre ambas modalidades de ataque, lo que permite comprender mejor el alcance de esta amenaza y su evolución dentro del espectro más amplio de la ciberdelincuencia.

Criterio	Phishing	Smishing
Medio de ataque	Correos electrónicos (principalmente).	Mensajes de texto (SMS) y aplicaciones de mensajería móvil (WhatsApp, Telegram, etc.).
Alcance	Global, especialmente vía correo masivo.	Más localizado y personal, directo al número de teléfono.
Forma de engaño	Enlaces fraudulentos en correos que simulan ser de instituciones legítimas.	Enlaces o mensajes en SMS que buscan redirigir a páginas falsas o solicitar datos directamente.
Tácticas comunes	Uso de logotipos falsos, remitentes aparentemente legítimos, urgencia en el mensaje.	Mensajes cortos, apelan a la urgencia (paquetes, bancos, premios).
Datos objetivo	Credenciales de acceso (emails, banca online, redes sociales).	Información personal, bancaria o instalación de malware en dispositivos móviles.
Nivel de sofisticación	Puede incluir adjuntos maliciosos, enlaces, o incluso spear phishing dirigido.	Generalmente mensajes breves con enlaces; algunos incluyen malware disfrazado en apps o links.
Detección	Más conocido por usuarios y filtrado por sistemas de correo.	Más difícil de detectar porque se recibe en el canal de confianza del usuario (mensajes SMS).
Evolución	Ha incorporado spear phishing, business email compromise (BEC).	Evoluciona hacia smishing por apps de mensajería y “quishing” (QR codes).
Ejemplos comunes	Correos de “su banco”, “PayPal”, “servicios en la nube”.	SMS de “su paquete no pudo ser entregado”, “su banco requiere validación”, “ha ganado un premio”.

¿Cómo obtienen los estafadores los números telefónicos?

El éxito del *smishing* depende de que los delincuentes logren acceder a bases de números telefónicos. Existen diversas vías mediante las cuales los atacantes consiguen estos datos:

1. Filtraciones de datos (data breaches):

Grandes filtraciones en plataformas digitales, bancos o empresas de telecomunicaciones pueden exponer millones de números. Según el informe de Kaspersky (2023), la venta de bases de datos filtradas es una práctica común en foros clandestinos de la dark web.

2. Compra y venta de bases de datos ilegales:

A pesar de estar prohibido por la normativa de protección de datos, en mercados ilegales circulan listas de números telefónicos extraídos de registros comerciales o bases de clientes. Un reporte de ESET (2022) destaca que estas bases suelen estar segmentadas por país, aumentando el riesgo para regiones específicas como Latinoamérica.

3. Ingeniería social:

En muchos casos, los atacantes obtienen los números mediante engaños simples, como encuestas falsas en línea, formularios de sorteos inexistentes o llamadas disfrazadas de servicios al cliente. Zscaler (2021) advierte que esta técnica es especialmente peligrosa porque combina manipulación psicológica con recopilación directa de información.

4. Exposición en redes sociales:

La publicación de números personales en perfiles abiertos, grupos de compraventa o formularios compartidos en línea también facilita el acceso. En Ecuador, la Dirección Nacional de Registro de Datos Públicos (DINARDAP) ha alertado sobre el riesgo de la sobreexposición de datos personales en redes sociales y plataformas digitales (DINARDAP, 2022).

En resumen, el *smishing* no ocurre en el vacío: depende de un ecosistema donde los datos personales circulan sin control. Por ello, la prevención también pasa por fortalecer la protección de la información personal y reducir su exposición en espacios digitales.

Contexto actual en Ecuador y a nivel global

El smishing no es un fenómeno aislado, sino parte de una creciente ola de ciberdelincuencia que afecta a usuarios en todo el mundo. A nivel global, el smishing se ha extendido considerablemente en los últimos años. Según un informe de Proofpoint, el 75% de las organizaciones reportó haber sufrido ataques de smishing durante 2023 (Proofpoint, 2023). Varias tendencias explican este aumento: las personas tienden a hacer clic más en enlaces recibidos por SMS que por correo electrónico, y los filtros anti-spam han dificultado otras vías como el phishing por email, lo cual empuja a los estafadores a enfocarse en los mensajes de texto (Kaspersky, 2025; Staysafeonline.org, 2025).

Además, en dispositivos móviles es más difícil verificar la autenticidad de un enlace (por ejemplo, no se puede previsualizar la URL pasando el cursor como en una computadora), y muchos usuarios están acostumbrados a recibir comunicaciones legítimas vía SMS (bancos, códigos de verificación, promociones), lo que puede bajar la guardia ante un mensaje malicioso (Trend Micro, 2025). Todo esto ha creado un terreno fértil para los ataques de smishing a nivel mundial.

En Ecuador, este riesgo es también una realidad presente. En los últimos tiempos se ha observado un incremento de ataques de smishing en el país (El Comercio, 2024). Este no es un hecho aislado, en otros países como en México muchos usuarios han recibido SMS aparentemente legítimos de bancos o servicios conocidos, que en realidad son fraudes (Santander México, 2025).

Un caso reciente en 2025 que ocurrió en Ecuador, involucró la suplantación de Club Miles (programa de millas de tarjeta de crédito): los estafadores enviaron mensajes informando falsamente que las millas acumuladas estaban por caducar e instaban a la víctima a seguir un enlace para canjearlas (Bermeo, 2025). En realidad, el enlace dirigía a un sitio web fraudulento (usando un dominio muy similar al real, como clubmiless.com en lugar de clubmiles.com.ec) diseñado para robar datos personales y bancarios (Scotiabank México, 2024).

De igual forma, se han detectado mensajes falsos a nombre de bancos ecuatorianos; por ejemplo, un SMS desde un número corto “2626” afirmando que puntos de recompensa de un banco estaban por expirar e invitando a clicar en un enlace sospechoso (El Comercio, 2024). Autoridades locales como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y Servicios Postales del Ecuador han emitido alertas sobre estos intentos de estafa (ARCOTEL, 2025; Servicios Postales del Ecuador, 2024).

A nivel global, organizaciones como la OCDE y la UNESCO han destacado la importancia de la ciberseguridad y la alfabetización digital en un mundo cada vez más conectado (Herrera et al., 2025; OECD, 2023). El smishing, al ser una técnica de ingeniería social, se beneficia de la falta de conciencia y educación digital de los usuarios. La proliferación de dispositivos móviles y la dependencia de las comunicaciones por SMS han creado un terreno fértil para que estos ataques prosperen.

Los informes de seguridad cibernética a nivel regional, como los de BioCatch, señalan un aumento en el fraude digital en América Latina, con un incremento en los casos de malware que a menudo se distribuye a través de mensajes de smishing (BioCatch, 2024). Todo ello evidencia que el smishing no es un problema lejano, sino un riesgo digital concreto en el contexto ecuatoriano actual.

Características del riesgo

El smishing combina tácticas tecnológicas y psicológicas para lograr su éxito (Metacompliance, 2024). En cuanto a lo técnico, los estafadores pueden enmascarar el número remitente utilizando servicios de mensajes masivos, spoofing de números o dispositivos especializados conocidos como SMS blasters, haciendo que el SMS parezca provenir de una fuente confiable (Cybeready, 2025; Cynet, 2025). Se han reportado casos donde se emplean equipos IMSI Catchers (dispositivo de escucha telefónica que se utiliza para interceptar el tráfico de telefonía móvil y rastrear la ubicación de los usuarios) o estaciones base falsas que envían miles de SMS fraudulentos de manera indiscriminada, imitando incluso numeraciones cortas oficiales (Red Seguridad, 2022; Wallarm, 2024). Esto permite que un mismo mensaje malicioso llegue a cientos o miles de usuarios.

No obstante, la esencia del smishing reside en la manipulación psicológica. Los mensajes suelen estar diseñados para provocar urgencia o miedo (ejemplos: “¡Tu cuenta será bloqueada si no verificas ahora mismo!”, “Tus puntos/millas expirarán hoy”, “Oferta limitada, último día para reclamar el premio”) o para aprovechar la confianza de la víctima (ej. fingir ser un banco solicitando confirmación de una transacción). Casi siempre implican un pretexto o historia falsa: un problema con una cuenta bancaria, una multa pendiente, un paquete que no pudo entregarse, o un familiar/amigo en apuros. El objetivo es que el destinatario actúe rápido y sin pensar, haciendo clic en el enlace o compartiendo datos confidenciales (IBM, 2023; Nationwide, 2021).

Smishing

Otras características clave que hacen al smishing particularmente peligroso y efectivo incluyen:

- **Suplantación de identidad (Spoofing)**: Los atacantes falsifican el remitente del mensaje para que parezca provenir de una fuente legítima y conocida por la víctima, como un banco, una empresa de paquetería, una entidad gubernamental o incluso un contacto personal (Proofpoint, 2025).

- **Enlaces maliciosos o números de teléfono falsos:** El mensaje a menudo contiene un enlace (URL) que dirige a la víctima a un sitio web falso diseñado para robar credenciales, o un número de teléfono al que se le pide llamar para "verificar" información, donde un operador fraudulento intentará obtener datos sensibles (INCIBE, 2025).

- **Descarga de malware:** En algunos casos, el enlace malicioso puede iniciar la descarga de software dañino (malware) en el dispositivo de la víctima, lo que permite a los atacantes acceder a información, monitorear actividades o incluso tomar control del dispositivo (Kaspersky, 2025).

- **Ingeniería social:** La base del smishing es la manipulación psicológica. Los ciberdelincuentes explotan la confianza, el miedo, la curiosidad o la avaricia de las víctimas para que revelen información o realicen acciones que normalmente no harían (Staysafeonline.org, 2025).

- **Personalización:** Aunque no siempre, algunos ataques de smishing pueden ser altamente personalizados, utilizando información obtenida previamente sobre la víctima para hacer el mensaje más creíble.

- **Universalidad del ataque:** El smishing apunta a cualquier persona con un teléfono móvil, sin requerir que la víctima tenga computadora o conexión fija; basta un celular con servicio SMS. Como resultado, la población en riesgo se amplía, abarcando a estudiantes adolescentes que, desde edades cada vez más tempranas, acceden a teléfonos móviles y se ven expuestos a este tipo de amenazas digitales.

- **Dificultad de rastreo:** La dificultad para rastrear a los remitentes (que a menudo usan números desechables o plataformas anónimas) hace complejo frenar rápidamente estas campañas. En suma, el smishing se caracteriza por su bajo costo y alta efectividad para los atacantes, aprovechando vulnerabilidades tanto técnicas (seguridad móvil, redes 2G menos seguras, etc.) como humanas (confianza, desconocimiento o descuido).

Tabla 1. Modalidades frecuentes de smishing y ejemplos con señales de alerta (fuentes: IBM, 2024; Lupa, 2025; El Comercio, 2024)

Modalidad	Descripción	Señales de alerta	Referencia
Bancaria	SMS que simula un banco e indica bloqueo/actividad sospechosa para "verificar datos".	Urgencia, enlace no oficial, petición de credenciales.	(El Comercio, 2024; IBM, 2023)
Fidelización (Club Miles)	Aviso falso de millas/ puntos por caducar con enlace a canje.	Dominio similar (p. ej. variación mínima), número corto no habitual.	(Bermeo, 2025)
Paquetería	Problema de entrega y solicitud de pago o actualización de datos mediante enlace.	Pago mínimo "de trámite", URL acortada.	(IBM, 2023)
Gobierno/ Educación	Supuestas multas, becas o matrículas urgentes con enlace a formulario.	Tono intimidante, datos sensibles por SMS.	(El Comercio, 2024)
"Número equivocado"/ perfil falso	Conversación casual que deriva en fraude (inversión, sextorsión, etc.).	Desconocido insistente, cambio rápido al tema económico.	(IBM, 2023)
Recuperación 2FA	Piden reenviar un código que llega por SMS para "ayudar a un amigo".	Solicitud de códigos OTP (One-Time Password, o contraseña de un solo uso); urgencia emocional.	(IBM, 2023)

b. Identificar el riesgo

Señales de alerta

Reconocer un mensaje de smishing es el primer paso crucial para protegerse. Aunque los ciberdelincuentes perfeccionan constantemente sus técnicas, existen señales de alerta comunes que pueden indicar que un SMS es fraudulento (Acrelia, 2024; Banco Santander, 2025):

- **Mensajes de números desconocidos o inusuales:** Si el mensaje proviene de un número desconocido o que aparenta ser un número de teléfono móvil personal, pero afirma representar a una entidad oficial, es una señal de alarma, es necesario verificar su autenticidad por medios oficiales. Las empresas y bancos suelen usar números cortos o remitentes alfanuméricos. Si el remitente no coincide con registros oficiales, desconfiar de inmediato (IBM, 2023).

- **Urgencia y presión para actuar:** Los mensajes de smishing a menudo intentan crear una sensación de pánico o urgencia, solicitando una acción inmediata (por ejemplo, “Su cuenta será bloqueada si no verifica ahora”, “Su paquete está retenido, haga clic aquí para reprogramar la entrega”) (Nationwide, 2021). Esta urgencia busca que la víctima actúe sin pensar críticamente.

- **Errores gramaticales y ortográficos:** Muchos mensajes fraudulentos aún contienen errores de ortografía, gramática inusual, o traducciones literales que delatan su origen no legítimo. Las instituciones legítimas suelen tener comunicaciones impecables (Kaspersky, 2025).

- **Enlaces sospechosos (URLs) o con ligeras alteraciones:** El mensaje incluye un enlace que no corresponde con el sitio web oficial de la entidad que supuestamente lo envía. Es fundamental no hacer clic en estos enlaces. Por ejemplo, en el caso de Club Miles el enlace fraudulento era clubmiless.com (con una “s” extra) en lugar del dominio oficial clubmiles.com.ec (Bermeo, 2025; Scotiabank México, 2024). En su lugar, se debe verificar la URL pasando el cursor sobre ella (si es posible en un dispositivo móvil, manteniendo presionado el enlace) o tecleando la dirección web directamente en el navegador (INCIBE, 2025).

- **Enlaces acortados o desconocidos:** A veces los estafadores usan servicios de URL corta (tipo bit.ly, tinyurl) para ocultar el destino real. Aunque las empresas legítimas también los usan en ocasiones, si un SMS no esperado trae un enlace acortado, es preferible no clickear y verificar primero por otros medios.

- **Solicitud de información personal o financiera:** Ninguna entidad legítima solicitará información sensible como contraseñas, números de tarjeta de crédito completos, códigos PIN o números de seguridad social a través de un SMS o un enlace enviado por SMS (Experian, 2024). “Tu banco nunca te pedirá tu clave por SMS” debe ser una regla fundamental.

- **Ofertas demasiado buenas para ser verdad:** Mensajes que prometen premios, herencias, descuentos increíbles o grandes sumas de dinero a cambio de una pequeña acción o información personal son casi siempre fraudulentos. Esta manipulación emocional es deliberada para anular el pensamiento crítico de la víctima (Trend Micro, 2025).

- **Mensajes inesperados:** Si recibes un mensaje de un banco, una empresa de paquetería o una entidad gubernamental con la que no esperabas tener contacto o sobre un tema que no te concierne, desconfía.

Tabla 2. Lista rápida de señales de alerta

Señal	Qué observar
Remitente	¿Número corto habitual? ¿Nombre alfanumérico verificable?
Enlace	¿Dominio oficial de la entidad? Evitar acortadores y variantes sospechosas.
Tono	¿Urgencia, amenaza o premio exagerado?
Solicitud de datos	Piden contraseñas, PIN, OTP o tarjeta: indicio claro de fraude.
Ortografía/estilo	Errores, traducciones literales, formatos extraños.
Coherencia	¿Tengo relación vigente con esa entidad? Si no, desconfíe.

En resumen, ante cualquier SMS no solicitado que pida acciones inmediatas, datos personales o clics en enlaces dudosos, debemos encender las alarmas. Cuando "suena raro, es raro" —lo mejor es detenerse, dudar y verificar por canales oficiales antes de responder.

Casos comunes y ejemplos reales

El smishing se manifiesta en diversas formas, adaptándose a las circunstancias y explotando la credulidad de las víctimas. Algunos de los casos más comunes incluyen:

- **Suplantación de entidades financieras:** Es la modalidad de smishing más común a nivel mundial, representando alrededor del 10% de todos los mensajes de estafa por SMS. Un ejemplo típico es el SMS que aparenta venir de un banco indicando un problema con la cuenta o tarjeta. En Ecuador, se vio el caso del Banco del Pacífico, donde un SMS desde un código corto falso informaba sobre puntos por caducar e incluía un enlace fraudulento (El Comercio, 2024). De igual manera, se han reportado mensajes fingiendo ser de cooperativas de ahorro u otros bancos, notificando transacciones sospechosas o bloqueo de cuenta, e invitando a "verificar" datos en un enlace. Al ingresar, la página copia la apariencia del banco y roba las credenciales del usuario.

- **Programas de puntos o millas y promociones:** Los estafadores explotan servicios de fidelización. El caso de Club Miles mencionado es ilustrativo: un SMS notificaba la expiración inminente de 68.054 millas y urgía a canjearlas vía un enlace falso (Bermeo, 2025). Muchos usuarios desprevenidos pudieron haber ingresado pensando que perderían sus beneficios. También se han visto mensajes suplantando a operadoras móviles ofreciendo "bonos de recarga gratis" o a tiendas comerciales anunciando falsos sorteos ganados, todo con el fin de dirigir a la víctima a un formulario malicioso.

- **Organismos gubernamentales o educativos:** Otra táctica es hacerse pasar por una institución pública. Por ejemplo, durante la pandemia en varios países circularon SMS apócrifos del Ministerio de Salud sobre supuestas campañas de vacunación, con enlaces que instalaban malware. En el contexto educativo, podría presentarse un mensaje fingiendo ser del Ministerio de Educación anunciando un trámite urgente (matrícula, beca, cupo escolar) y solicitando datos. Siempre que recibamos comunicaciones inesperadas supuestamente de entes oficiales, debemos validar la información por los canales formales (sitio web institucional, líneas telefónicas oficiales).

- **Servicios de entrega de paquetes (smishing de mensajería):** Muy común internacionalmente es el SMS que alega un problema con la entrega de un paquete (correo, DHL, servicio postal). El mensaje pide al destinatario que siga un enlace para reprogramar la entrega o pagar una tarifa pendiente (Keepnet Labs, 2024). Dado que muchas personas hacen compras en línea, es fácil engancharlas con esta treta. Al ingresar en el link, la víctima puede terminar en un sitio falso donde le solicitan el pago de una supuesta tasa de aduana o le instalan un malware móvil. Esta variante suele intensificarse en épocas de altas compras (por ejemplo, Navidad).

- **Estafas de "número equivocado" o perfiles falsos:** Una modalidad más reciente es cuando un desconocido te escribe por error fingiendo haber contactado a la persona equivocada"(Hola, ¿nos vemos mañana? oh disculpa me equivoqué de número..."). Si la víctima responde, el estafador entabla conversación amigable durante días o semanas, ganando confianza, para eventualmente introducir una estafa (generalmente de inversión fraudulenta o extorsión emocional). Aunque esto suele ocurrir más en apps de mensajería que por SMS tradicional, es un ejemplo de ingeniería social prolongada a través de texto (Phonexia, 2022). Los estudiantes deben mantenerse alerta a extraños que inician chats con pretextos dudosos.

- **Suplantación de identidad personal (amigos o familiares):** Otra variante peligrosa es cuando el atacante tiene ya parte de tus credenciales y busca completar un acceso. Puede enviar un SMS haciéndose pasar por un amigo o familiar en apuros pidiendo un código de verificación"(Hola, te llegará un código a tu celular, ¿me lo pasas? Es que estoy bloqueando mi cuenta"). En realidad, es el estafador intentando entrar a la cuenta del propio estudiante (por ejemplo, Instagram) y el código que llega corresponde al segundo paso de la autenticación en dos pasos. Este mecanismo funciona solicitando, además de la contraseña (primer paso), un código temporal enviado por SMS o aplicación (segundo paso), con el que el estudiante protege sus datos y accesos. Si la persona se lo entrega creyendo ayudar a su amigo, el delincuente toma control de su cuenta. Este tipo de engaño explota la confianza entre contactos cercanos.

Estos ejemplos muestran que los contextos pueden variar, pero el mecanismo central es el mismo: un mensaje que aparenta legitimidad, un enlace o instrucción engañosa, y una víctima que, bajo presión o confianza, entrega información o realiza una acción perjudicial. Conocer casos reales ayuda a los estudiantes a comprender mejor cómo luce la trampa en la práctica.

Factores de vulnerabilidad

La vulnerabilidad al smishing no solo depende de la sofisticación del ataque, sino también de ciertos factores relacionados con el usuario y el entorno. Cualquier usuario de móvil puede ser blanco de smishing, pero existen factores que pueden aumentar la vulnerabilidad, especialmente en el caso de niños, niñas y adolescentes:

- **Falta de conocimiento y concienciación:** La principal vulnerabilidad es la ignorancia sobre cómo operan estos fraudes. Si el estudiante desconoce la existencia de este tipo de fraudes, será más propenso a creer que el mensaje es legítimo. La brecha de generación también puede influir: jóvenes muy familiarizados con la tecnología pueden tener confianza excesiva en que "a mí no me pasará", mientras que otros pueden no distinguir un SMS falso de uno real. La educación en ciberseguridad es clave; quienes no la han recibido están en desventaja (Metacompliance, 2024).

- **Confianza y hábito en el uso de SMS/chat:** Muchas personas confían inherentemente en los SMS, considerándolos más seguros que los correos electrónicos, lo que reduce su nivel de alerta (Cynet, 2025). Los jóvenes se comunican informalmente todo el tiempo vía mensajes y están acostumbrados a recibir notificaciones, enlaces de amigos, códigos de verificación de juegos, etc., sin mucho análisis. Ese hábito de clic fácil puede jugar en contra si no se cultiva el pensamiento crítico. Como indican los estudios, las personas tienen mayor probabilidad de hacer clic en un enlace enviado por texto que en uno por correo electrónico (Kaspersky, 2025), en parte porque el SMS se percibe como más personal o inmediato. Esta tendencia natural es explotada por los delincuentes.

- **Impulsividad y manejo de la urgencia:** La tendencia a reaccionar impulsivamente ante mensajes que generan miedo o una sensación de urgencia es un factor clave que los ciberdelincuentes explotan (Wallarm, 2024). Los adolescentes, por desarrollo, pueden ser más impulsivos y propensos a responder rápidamente a estímulos, sobre todo si un mensaje les genera miedo (ej. "¡Mi cuenta bancaria, el dinero de mis padres!") o emoción (ej. "¡Gané algo!"). Si no han desarrollado la pausa reflexiva, pueden caer antes de consultar con alguien. Los estafadores lo saben y por eso sus textos buscan provocar reacciones viscerales.

- **Falta de verificación:** No verificar la autenticidad del mensaje a través de canales oficiales (llamando directamente a la entidad, visitando su sitio web oficial) antes de tomar cualquier acción .

- **Software desactualizado o falta de seguridad:** No tener el sistema operativo del móvil y las aplicaciones actualizadas, o no contar con software de seguridad (antivirus, antimalware) puede dejar el dispositivo expuesto a la instalación de malware si se hace clic en un enlace malicioso (Red Seguridad, 2022).

- **Exposición de información personal:** Si el número de teléfono del estudiante circula ampliamente (por ejemplo, publicado en redes sociales, grupos públicos, formularios en línea), aumenta la probabilidad de recibir smishing. En general, los delincuentes obtienen bases de números de distintas fuentes (filtraciones, directorios, redes). La información personal disponible públicamente (redes sociales, bases de datos filtradas) puede ser utilizada por los atacantes para personalizar los mensajes y hacerlos más creíbles, aumentando la probabilidad de éxito del fraude (McAfee, 2023).

Comprender estos factores es esencial para desarrollar estrategias de prevención más efectivas y fortalecer la resiliencia de los usuarios frente a los ataques de smishing.

c. Prevenir el riesgo

Buenas prácticas y recomendaciones

La prevención es la herramienta más poderosa contra el smishing. Adoptar una serie de buenas prácticas y recomendaciones puede reducir significativamente el riesgo de ser víctima de estos fraudes:

- **Desconfiar de mensajes inesperados y no responder:** Si recibes un SMS de un número desconocido o de una entidad que no esperabas, mantén la cautela. No respondas al mensaje, ya que esto podría confirmar a los estafadores que tu número está activo (SoSafe, 2025).

- **Verificar la fuente a través de canales oficiales:** Si el mensaje parece ser de una entidad legítima (banco, empresa de servicios, etc.), no utilices los datos de contacto proporcionados en el SMS. En su lugar, contacta directamente a la entidad a través de sus canales oficiales (número de teléfono de atención al cliente, sitio web oficial) que ya conozcas o que busques de forma independiente. Llama a la entidad usando un número oficial, no el que aparece en el SMS (Banco Santander, 2025).

- **No hacer clic en enlaces sospechosos:** Los enlaces en mensajes de smishing suelen dirigir a sitios web falsos. Si necesitas acceder a una cuenta, escribe la dirección URL directamente en tu navegador o utiliza la aplicación oficial de la entidad. Evita hacer clic en enlaces acortados o desconocidos (INCIBE, 2025).

- **No proporcionar información personal o financiera:** Las entidades legítimas nunca solicitarán información sensible (contraseñas, números de tarjeta de crédito, PIN, códigos de verificación) a través de SMS o enlaces enviados por SMS (Experian, 2024). "Tu banco nunca te pedirá tu clave por SMS" debe ser una regla fundamental.

- **Mantener el software actualizado:** Asegúrate de que el sistema operativo de tu dispositivo móvil y todas tus aplicaciones estén siempre actualizadas. Las actualizaciones suelen incluir parches de seguridad que protegen contra vulnerabilidades conocidas (Red Seguridad, 2022).

- **Utilizar soluciones de seguridad:** Considera instalar un software antivirus o de seguridad móvil en tu smartphone. Estas herramientas pueden ayudar a detectar y bloquear mensajes maliciosos o sitios web fraudulentos.

- **Habilitar la autenticación de dos factores (2FA):** Siempre que sea posible, activa la autenticación de dos factores en tus cuentas online. Esto añade una capa extra de seguridad, ya que incluso si un atacante obtiene tu contraseña, necesitará un segundo factor (como un código enviado a tu teléfono) para acceder a tu cuenta (Imperva, 2025).

- **Reportar mensajes sospechosos:** Si recibes un mensaje de smishing, repórtalo a tu proveedor de servicios móviles y a las autoridades competentes. Esto ayuda a las autoridades a rastrear y combatir estas actividades fraudulentas.

- **Educación continua:** Mantente informado sobre las últimas tácticas de smishing y otros ciberataques. La concienciación es clave para la prevención.

- **No guardar contraseñas en el móvil:** Utiliza un gestor de contraseñas seguro para almacenar tus credenciales y evitar guardarlas directamente en el dispositivo.

- **Revisar los permisos de las aplicaciones:** Asegúrate de que las aplicaciones instaladas en tu móvil solo tengan los permisos necesarios para su funcionamiento. Desactiva aquellos que no sean esenciales (Google, 2025).

- **Desactivar la previsualización de mensajes en la pantalla de bloqueo:** Esto evita que información sensible o enlaces sospechosos sean visibles para cualquiera que tenga acceso físico a tu teléfono (Apple, s/f).

- **Eliminar mensajes sospechosos:** Una vez identificado un SMS como smishing, elimínalo para evitar confusiones futuras o clics accidentales (FCC, 2024).

Rol del estudiante, la familia y el docente

La lucha contra el smishing y otros riesgos digitales es una responsabilidad compartida que involucra a toda la comunidad educativa y familiar. Un aspecto clave es la concientización sobre la información personal que se comparte en redes y plataformas digitales: números de teléfono, direcciones, contraseñas o datos bancarios pueden ser utilizados por los atacantes para personalizar sus fraudes y hacerlos más convincentes. Proteger estos datos y reflexionar antes de publicarlos es el primer paso para reducir la exposición a amenazas.

- **Rol del estudiante:** Los estudiantes son los principales receptores de estos mensajes y, por lo tanto, deben ser los primeros en desarrollar una actitud crítica y vigilante. Deben aprender a identificar las señales de alerta, a no reaccionar impulsivamente y a buscar ayuda o verificar la información cuando tengan dudas. Fomentar la curiosidad sana sobre la tecnología, pero también la cautela ante lo desconocido, es fundamental. Los estudiantes deben sentirse cómodos reportando incidentes sin temor a ser juzgados. Es crucial que desarrollen la pausa reflexiva y la importancia de consultar con un adulto de confianza antes de tomar cualquier acción ante un mensaje sospechoso .

- **Rol de la familia:** Los padres y tutores juegan un papel crucial en la educación digital de sus hijos. Deben establecer un diálogo abierto sobre los riesgos online, supervisar el uso de dispositivos y aplicaciones, y modelar un comportamiento seguro en línea. Es importante que las familias creen un entorno de confianza donde los jóvenes puedan compartir sus experiencias y preocupaciones sin miedo a represalias. La familia debe ser un espacio de aprendizaje y apoyo en temas de ciberseguridad.

- **Rol del docente:** Los docentes tienen la oportunidad de integrar la ciudadanía digital y la ciberseguridad en el currículo escolar. Esto incluye enseñar a los estudiantes sobre los diferentes tipos de fraudes digitales, cómo identificarlos y cómo protegerse. Los educadores pueden utilizar ejemplos prácticos, simulaciones y debates para hacer el aprendizaje relevante y atractivo. Además, los docentes deben estar actualizados sobre las amenazas emergentes y servir como guías y recursos para los estudiantes y sus familias. La escuela, como espacio de formación integral, debe promover activamente la alfabetización digital crítica y responsable.

Tabla 3. Rol del estudiante, la familia y el docente en la prevención (UNESCO, 2024; Formtic, 2025).

Estudiante	Familia	Docente
Aplicar checklist de señales; pedir ayuda ante dudas; no reenviar SMS sospechosos.	Modelar verificación; conversar sobre riesgos; acordar reglas de respuesta ante SMS.	Integrar ciudadanía digital en clase; usar casos reales y simulaciones; actualizarse periódicamente.

Enfoque educativo

Más allá de las medidas técnicas y las buenas prácticas, la prevención del smishing y otros riesgos digitales requiere una profunda reflexión crítica y el desarrollo de una sólida ciudadanía digital. Esto implica:

- **Pensamiento crítico:** Cuestionar la información que se recibe, especialmente si genera urgencia o promesas extraordinarias. Desarrollar la capacidad de analizar la credibilidad de la fuente y el contenido del mensaje.
- **Conciencia de la ingeniería social:** Entender cómo los ciberdelincuentes manipulan las emociones y la psicología humana para lograr sus objetivos. Reconocer que el fraude no siempre se basa en fallos técnicos, sino en la explotación de la confianza y la falta de información.
- **Responsabilidad digital:** Comprender que nuestras acciones en línea tienen consecuencias, no solo para nosotros mismos, sino también para otros. Esto incluye no compartir información personal indiscriminadamente y ser conscientes de la huella digital que dejamos.
- **Resiliencia digital:** Desarrollar la capacidad de recuperarse de incidentes de seguridad, aprender de ellos y fortalecer las defensas. Esto implica saber a quién acudir en caso de ser víctima de un fraude y cómo mitigar los daños.
- **Participación:** Involucrarse en la promoción de la ciberseguridad y la educación digital en la comunidad. Compartir conocimientos y experiencias para ayudar a otros a protegerse.

La ciudadanía digital no es solo un conjunto de habilidades técnicas, sino una forma de ser y actuar en el mundo digital, basada en el respeto, la responsabilidad y la ética. Al fomentar esta mentalidad, empoderamos a los estudiantes para que se conviertan en agentes de cambio en la construcción de un ciberespacio más seguro y confiable.

3. Conclusiones y recomendaciones

a. Conclusiones

- El smishing representa una amenaza significativa en el panorama digital actual, especialmente para poblaciones vulnerables como los estudiantes de educación básica superior y bachillerato. Su naturaleza engañosa, basada en la suplantación de identidad y la ingeniería social a través de mensajes de texto, lo convierte en un vector de ataque eficaz para el robo de información personal y financiera, así como para la distribución de malware. La creciente digitalización en Ecuador y a nivel global, sumada a la confianza inherente en los SMS, crea un entorno propicio para la proliferación de estos fraudes.

- Para mitigar este riesgo, es imperativo adoptar un enfoque multifacético que involucre la educación, la concienciación y la implementación de buenas prácticas de ciberseguridad. La estructura pedagógica "Conocer > Identificar > Prevenir" propuesta en este documento busca precisamente empoderar a los estudiantes con el conocimiento y las habilidades necesarias para navegar de forma segura en el ciberespacio. Reconocer las señales de alerta, comprender los factores de vulnerabilidad y aplicar medidas preventivas son pasos fundamentales para evitar ser víctima de smishing.

b. Recomendaciones

- **Fortalecer la educación digital:** Integrar de manera transversal la ciudadanía digital y la ciberseguridad en el currículo educativo, utilizando metodologías interactivas y ejemplos prácticos que resuenen con la realidad de los estudiantes.

- **Promover la verificación constante:** Inculcar la práctica de verificar la autenticidad de cualquier mensaje sospechoso a través de canales oficiales, en lugar de hacer clic en enlaces o responder directamente.

- **Fomentar el diálogo abierto:** Crear espacios de confianza en el hogar y la escuela donde los estudiantes puedan compartir sus experiencias y dudas sobre riesgos digitales sin temor a ser juzgados.

- **Actualización y uso de herramientas de seguridad:** Enfatizar la importancia de mantener actualizados los sistemas operativos y aplicaciones, así como el uso de soluciones de seguridad y la autenticación de dos factores.

- **Colaboración interinstitucional:** Impulsar la colaboración entre el Ministerio de Educación, entidades de ciberseguridad, instituciones financieras y proveedores de servicios de telecomunicaciones para generar campañas de concienciación y recursos educativos conjuntos.

Al empoderar a los estudiantes con una sólida ciudadanía digital y un pensamiento crítico, no solo los protegemos del smishing, sino que también los preparamos para ser ciudadanos responsables y activos en un mundo cada vez más digitalizado. El proyecto “Exploradores Digitales con Eugenia” es un paso fundamental en esta dirección, sentando las bases para una generación de usuarios digitales conscientes y seguros.

4. Anexos

Glosario de términos

1. Smishing:

   Fraude digital que utiliza mensajes de texto (SMS) para engañar a las víctimas y obtener información personal o financiera, haciéndose pasar por entidades legítimas.

2. Phishing:

   Técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial (como contraseñas o datos bancarios) a través de comunicaciones electrónicas fraudulentas, comúnmente correos electrónicos.

3. Ingeniería Social:

   Manipulación psicológica de personas para que realicen acciones o divulguen información confidencial. Es la base de muchos ciberataques, incluyendo el smishing y el phishing.

4. Spoofing:

   Suplantación de identidad donde un atacante falsifica el remitente de una comunicación (SMS, correo electrónico, llamada) para que parezca provenir de una fuente legítima y de confianza.

5. Malware:

   Software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario. Puede ser descargado a través de enlaces maliciosos en mensajes de smishing.

6. URL (Uniform Resource Locator):

   Dirección única que identifica un recurso en internet, como una página web. En el smishing, los enlaces a URLs maliciosas dirigen a sitios web falsos.

7. Autenticación de Dos Factores (2FA):

   Medida de seguridad que requiere dos formas diferentes de identificación para verificar la identidad de un usuario, añadiendo una capa extra de protección a las cuentas en línea.

8. Ciudadanía Digital:

   Conjunto de habilidades, conocimientos y actitudes necesarias para participar de forma segura, responsable, ética y crítica en el entorno digital.

9. Ciberseguridad:

   Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de gestión de riesgos, acciones, formación, mejores prácticas y tecnologías que se utilizan para proteger los activos de la organización y los usuarios en el ciberentorno.

10. Datos Personales:

    Cualquier información concerniente a una persona física identificada o identificable, como nombre, dirección, número de teléfono, correo electrónico, etc.

11. Credenciales:

    Conjunto de información (como nombre de usuario y contraseña) utilizada para verificar la identidad de un usuario y permitirle el acceso a un sistema o servicio.

12. Vulnerabilidad:

    Debilidad o fallo en un sistema, aplicación o procedimiento que puede ser explotado por un atacante para comprometer la seguridad.

13. Concienciación:

    Estado de estar informado y alerta sobre los riesgos y amenazas digitales, así como sobre las mejores prácticas para protegerse de ellos.

14. Fraude Digital:

    Acto intencional de engaño o falsedad realizado a través de medios digitales con el fin de obtener un beneficio ilícito, generalmente económico, a expensas de la víctima.

15. SMS Blaster:

Dispositivo o servicio utilizado por ciberdelincuentes para enviar grandes volúmenes de mensajes de texto (SMS) fraudulentos de forma masiva, a menudo enmascarando el número de origen.

16. OTP (One-Time Password / Contraseña de un solo uso):

    Código temporal de verificación que se utiliza como medida de seguridad adicional en la autenticación de dos pasos. Generalmente se envía por SMS, correo electrónico o aplicaciones de autenticación, y solo es válido por un corto periodo de tiempo o para una única transacción. Su función es reforzar la protección de cuentas y accesos digitales, reduciendo el riesgo de suplantación de identidad.

17. Dark Web (Internet oscura):

Parte de internet que no está indexada por los motores de búsqueda convencionales y sólo puede accederse mediante navegadores especiales, como Tor. En este espacio se protegen el anonimato y la privacidad de los usuarios, lo que facilita tanto usos legítimos (defensa de la privacidad, comunicación en contextos represivos) como actividades ilícitas, entre ellas la venta de datos personales, números telefónicos o credenciales robadas.

5. Referencias bibliográficas

Acrelia. (2024). *Cómo detectar un sms fraudulento*. https://www.acrelia.com/es/blog/post/como-detectar-un-sms-fraudulento

Apple. (s/f). *Cambiar las notificaciones en el iPhone*. https://support.apple.com/es-es/guide/iphone/iph64a02636d/ios

ARCOTEL. (2025, abril 30). *IMPORTANTE | El smishing es un ciberataque dirigido...* https://m.facebook.com/arcotel/photos/%EF%B8%8F-importante-el-smishing-es-un-ciberataque-dirigido-a-las-personas-a-trav%C3%A9s-de-s/1074942034662203/

Banco Santander. (2025). *What is Smishing: Avoid the SMS scam*. https://www.bancosantander.es/en/glosario/smishing

Bermeo, C. (2025, mayo 25). ¿Club Miles solicita a sus usuarios canjear millas vía SMS? *LupaMedia*. https://lupa.com.ec/verificaciones/estafa-club-miles-millas-sms/

BioCatch. (2024, septiembre 23). *2024 Digital Banking Fraud Trends in Latin America*. https://www.biocatch.com/white-paper-digital-banking-fraud-trends-latam-2024-en

Cybeready. (2025). *The Complete Guide to Smishing (SMS Phishing)*. https://cybereready.com/category/the-complete-guide-to-smishing/

Cynet. (2025, abril 26). *5 Types of Smishing Attacks and 5 Ways to Prevent Them*. https://www.cynet.com/cybersecurity/5-types-of-smishing-attacks-and-5-ways-to-prevent-them

DINARDAP. (2022). *Informe Rendición de Cuentas 2022 – Ley Orgánica de Protección de Datos Personales*. Dirección Nacional de Registro de Datos Públicos. https://www.registrospublicos.gob.ec/wp-content/uploads/downloads/2022/10/Informe-Rendicion-de-Cuentas-2021-DINARP-1.pdf

El Comercio. (2024, septiembre 16). *Smishing, Vishing y Spooging, los delincuentes informáticos y sus...* https://www.elcomercio.com/opinion/smishing-vishing-spooging-delincuentes-informaticos-formas-ataque-lorena-naranjo-columnista/

ESET. (2022). *ESET Threat Report T3 2022*. ESET. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset_threat_report_t32022.pdf

Experian. (2024, diciembre 13). *What Is Smishing?* https://www.experian.com/blogs/ask-experian/what-is-smishing/

FCC. (2024, febrero 1). *Avoid the Temptation of Smishing Scams*. https://www.fcc.gov/avoid-temptation-smishing-scams

Fortinet. (2025). ¿Qué es el Smishing? Definición y protección Suplantación de identidad. https://www.fortinet.com/lat/resources/cyberglossary/smishing

Google. (2025). *Revisar y cambiar los permisos de las apps*. https://support.google.com/googleplay/answer/6014972?hl=es

Herrera, P., Huepe, M., & Trucco, D. (2025). *Education and the development of digital competences in Latin America and the Caribbean*.

IBM. (2023). ¿Qué es el smishing (phishing por SMS)? https://www.ibm.com/es-es/think/topics/smishing

Imperva. (2025). *What is Smishing (SMS Phishing) | Types & Prevention*. https://www.imperva.com/learn/application-security/smishing/

INCIBE. (2025). *Cómo evitar ser víctima de smishing*. https://www.incibe.es/node/485669

Kaspersky. (2023). *Enterprise threats in 2023: media blackmail, fake data leaks and more attacks via clouds* [Nota de prensa]. Kaspersky Lab. https://www.kaspersky.com/about/press-releases/enterprise-threats-in-2023-media-blackmail-fake-data-leaks-and-more-attacks-via-clouds

Kaspersky. (2025). *Qué es el smishing y cómo puedes protegerte de esta amenaza*. https://latam.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Keepnet Labs. (2024, noviembre 14). *10 Real-Life Smishing Examples to Strengthen Cybersecurity Awareness*. https://keepnetlabs.com/blog/10-real-life-smishing-examples-to-strengthen-cybersecurity-awareness

McAfee. (2023). *What Is Smishing? Here's How to Spot Fake Texts and Keep Your Info Safe*. https://www.mcafee.com/blogs/mobile-security/what-is-smishing-heres-how-to-spot-fake-texts-and-keep-your-info-safe/

Metacompliance. (2024). *Smishing: Significado y estrategias efectivas de prevención*. https://www.metacompliance.com/es/blog/phishing-and-ransomware/smishing-attacks-how-to-stay-safe

Nationwide. (2021). ¿Qué son las estafas de phishing, vishing y smishing? https://espanol.nationwide.com/business/solutions-center/cybersecurity/phishing-vishing-smishing

OECD. (2023, septiembre 22). *Building a Skilled Cyber Security Workforce in Latin America*. https://www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-latin-america_9400ab5c-en.html

Phonexia. (2022, agosto 8). *3 Examples of Typical Smishing and Vishing Attacks in 2022*. https://www.phonexia.com/blog/3-examples-of-typical-smishing-and-vishing-attacks-in-2022/

Proofpoint. (2023). *2023 Human Factor Report*. https://www.proofpoint.com/us/resources/threat-reports/human-factor

Proofpoint. (2025). *Definición de smishing—Ejemplos y cómo evitarlo*. https://www.proofpoint.com/es/threat-reference/smishing

Red Seguridad. (2022, abril 8). *"Smishing": Cómo evitar este ciberataque a través de SMS*. https://www.redseguridad.com/actualidad/cibercrimen/smishing-como-evitar-este-ciberataque-a-traves-de-sms_20220408.html

Santander México. (2025). *Smishing: Qué es y Cómo Evitarlo*. https://www.santander.com.mx/educacion-financiera/blog/smishing-que-es-y-como-evitarlo.html

Scotiabank México. (2024, enero 11). *Ejemplos de smishing y cómo protegerte*. https://www.scotiabank.com.mx/blog/para-ti-ejemplos-smishing-y-como-protegerte

Servicios Postales del Ecuador. (2024, agosto 21). *Información a la ciudadanía—Casos de suplantación de información (phishing)*. https://www.serviciopostal.gob.ec/sin-categoria/informacion-a-la-ciudania-casos-de-suplantacion-de-informacion-phishing/

SoSafe. (2025). *What is Smishing? Examples & Prevention Tips*. https://sosafe-awareness.com/en-us/glossary/smishing/

Staysafeonline.org. (2025, julio 14). ¿Qué es el smishing? Cómo funcionan las estafas por mensajes de... https://www.staysafeonline.org/es/articles/what-is-smishing-how-text-message-scams-work-(and-how-to-avoid-them)

Trend Micro. (2025). ¿Qué es el smishing? | Ejemplos y como evitarlo. https://www.trendmicro.com/es_es/what-is/phishing/smishing.html

Wallarm. (2024, noviembre 22). ¿Qué es un ataque de smishing? Significado, definición y ejemplos. https://lab.wallarm.com/what/ataque-de-smishing-en-la-ciberseguridad/?lang=es

Wikipedia. (2016). *Smishing*. https://es.wikipedia.org/wiki/Smishing

Zscaler. (2025). ¿Qué es el smishing (phishing por SMS)? https://www.zscaler.com/es/zpedia/what-is-smishing-sms-phishing

Ministerio de Educación,
Deporte y Cultura

@MinisterioEducacionEcuador

@Educacion_Ec

www.educacion.gob.ec