¿POR QUÉ NO DEBEMOS FIARNOS DE CORREOS, SMS Y LLAMADAS AUNQUE PAREZCAN PROCEDER DE UNA ENTIDAD DE CONFIANZA?

Las comunicaciones digitales, como **correos electrónicos, SMS y llamadas,** se han convertido en herramientas cotidianas de nuestro día a día, pero también son utilizadas por **ciberdelincuentes** para engañar a personas desprevenidas. Los fraudes más comunes incluyen ***phishing, smishing y vishing***, donde los estafadores se hacen pasar por entidades de confianza para **robar información personal o financiera.**

Identificar estas tácticas te ayudará a mantenerte alerta y a proteger tu información personal.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Introducción

Vivimos en una época en la que la tecnología nos facilita la vida, pero también abre la puerta a **nuevos riesgos.** Cada día utilizamos correos electrónicos, mensajes de texto y llamadas telefónicas para comunicarnos con empresas, instituciones y personas. Sin embargo, los estafadores han aprendido a aprovecharse de nuestra confianza, creando **mensajes falsos que parecen legítimos** y utilizando tácticas que pueden engañar incluso a los más precavidos.

Esta técnica, conocida como ***spoofing,*** busca engañarnos para que proporcionemos información sensible, como **contraseñas, números de tarjetas o datos personales,** que luego los delincuentes pueden usar para robarnos dinero o cometer otros fraudes. Lo preocupante es que estos engaños suelen parecer tan auténticos que es fácil caer en la trampa si no sabemos qué señales debemos buscar.

¿Qué es el *spoofing* y cómo se relaciona con otras amenazas?

El ***spoofing*** es una técnica utilizada por ciberdelincuentes para **suplantar la identidad de una persona,** empresa o entidad de confianza con el objetivo de engañar a la víctima. Esto se logra falsificando información como direcciones de correo electrónico, números de teléfono o nombres de remitentes, haciendo que el mensaje o la llamada parezca legítima.

Se manifiesta de diferentes formas, dependiendo del medio que los ciberdelincuentes utilicen para engañar a sus víctimas. A continuación, se describen los tipos más comunes y las técnicas que emplean los estafadores para suplantar identidades:

Phishing

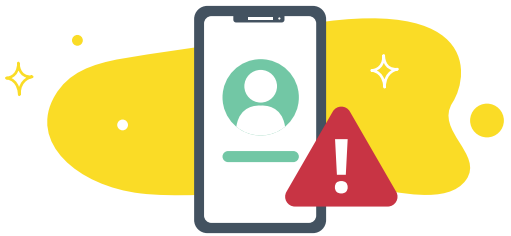
En estos correos se puede utilizar la técnica de *spoofing* para **falsificar el remitente,** haciéndolo parecer legítimo (como si proviniera un banco o una empresa de mensajería y/o paquetería), con el objetivo de engañar a la víctima para **que haga clic en enlaces maliciosos,** descargue archivos infectados o proporcione información confidencial, como contraseñas o datos bancarios. Algunos métodos comunes incluyen el uso de **dominios similares,** donde se imitan las direcciones de correo de entidades reales cambiando letras o añadiendo caracteres, como "soporte@banc0-oficial.com" en lugar de "soporte@banco-oficial.com". Otra técnica es la manipulación del nombre del remitente, donde el campo "De" muestra un nombre confiable, como "Banco XYZ", pero la dirección real es completamente diferente.

Smishing

En este tipo de mensajes de texto los ciberdelincuentes **falsifican el número de teléfono** o el nombre del remitente en **un mensaje de texto.** Algunas técnicas incluyen el uso de números cortos o personalizados que parecen oficiales o incluyen el nombre de una empresa o entidad en el identificador, como "Amazon" o "Correos". También suelen enviar **mensajes urgentes** que generan alarma, como "Su paquete no ha podido ser entregado" o "Su cuenta ha sido bloqueada", incluyendo en el mensaje un enlace fraudulento o una solicitud de información personal.

Vishing

En el caso de las **llamadas fraudulentas** los estafadores manipulan el identificador de llamadas para mostrar **un número o nombre falso.** Algunas técnicas comunes son la suplantación de números oficiales, donde hacen que la llamada parezca provenir de una entidad confiable, como un banco o un proveedor de telefonía móvil e Internet. También utilizan grabaciones automatizadas que simulan ser alertas legítimas, como "Hemos detectado actividad sospechosa en su cuenta", con el fin de obtener información confidencial o convencer a la víctima de realizar acciones perjudiciales, como transferir dinero o instalar *software* malicioso.



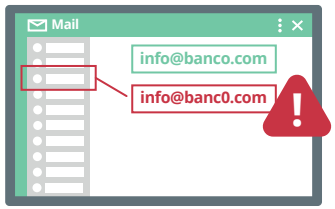
Cómo suplantan identidades

Utilizan diversas estrategias para ganarse la confianza de sus víctimas. Una de ellas es la **imitación de algunas empresas o entidades,** donde copian logotipos, colores y estilos de comunicación de empresas reales para que los mensajes parezcan auténticos. También emplean un lenguaje persuasivo, utilizando un **tono urgente** o alarmante para incitar a la acción inmediata, como **"Actúe ahora o su cuenta será suspendida".** Además, se aprovechan de contextos creíbles, como facturas pendientes, paquetes no entregados o problemas técnicos, para que el mensaje resulte creíble.

¿Cómo podemos detectar estas amenazas?

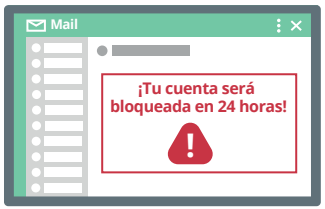
Detectar intentos de ***spoofing*** puede parecer complicado al principio, pero si aprendemos a identificar ciertas **señales de alerta,** es posible protegernos de estas amenazas. A continuación, se muestran una serie de aspectos que te ayudarán a **reconocer las tácticas** más comunes de los estafadores en **correos electrónicos, SMS y llamadas:**

Correos electrónicos



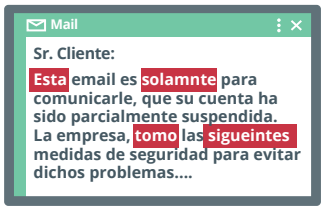
1. Revisa el remitente.

Aunque el nombre del remitente parezca legítimo, **revisa la dirección completa del correo.** Los estafadores suelen usar **direcciones muy parecidas a las reales,** con pequeñas diferencias como **letras cambiadas** o añadidas (por ejemplo, "info@banc0.com" en lugar de "info@banco.com").



2. Urgencia innecesaria.

Frases como **"¡Actúa ahora!"** o **"Tu cuenta será bloqueada en 24 horas"** buscan presionarte para que tomes decisiones apresuradas.

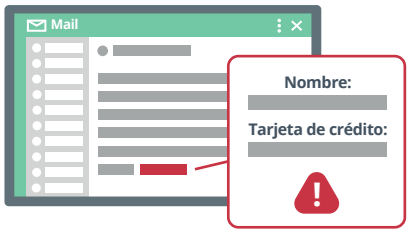


3. Errores gramaticales o de ortografía.

Los mensajes falsos pueden tener **fallos en el lenguaje,** como frases mal redactadas o **faltas de ortografía.**

4. Enlaces sospechosos.

Al pasar el cursor sobre un enlace (sin hacer clic), **verifica si la dirección que aparece es diferente a la oficial.** Los estafadores suelen usar páginas falsas que parecen reales.



5. Solicitudes de datos personales.

Ninguna entidad de confianza te pedirá contraseñas, números de tarjeta o códigos por correo electrónico.

SMS

1. Nombre de remitente aparentemente legítimo.

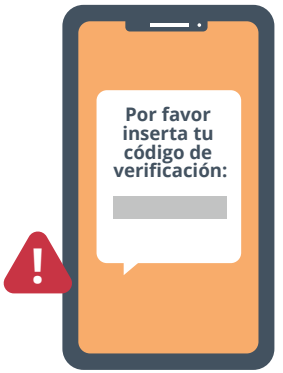
Gracias a la técnica de ***spoofing*** estos SMS **parecen enviados por entidades bancarias,** compañías de paquetería e incluso servicios públicos. Revisa si el número o nombre del **remitente coincide con el oficial.**

2. Mensajes alarmantes o demasiado atractivos.

"Se ha detectado actividad sospechosa en tu cuenta", "¡Felicidades, has ganado un premio!" o **"Confirma tus datos para evitar el bloqueo"** son mensajes comunes en estas estafas.

3. Enlaces abreviados o sospechosos.

URLs como "bit.ly/123abc" o enlaces con **nombres desconocidos** pueden redirigirte a **sitios fraudulentos.**



4. Solicitudes de información personal o códigos.

Ninguna entidad te pedirá datos confidenciales de carácter personal o códigos mediante un mensaje de texto.

Llamadas

1. Números falsificados.

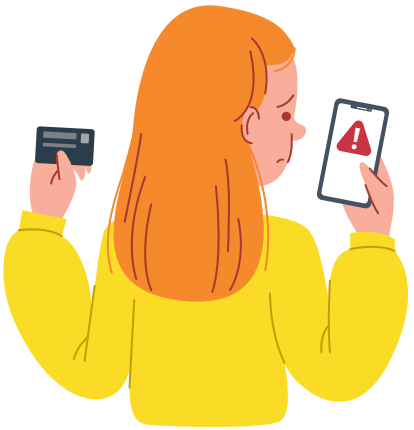
Aunque la llamada parezca venir de un número oficial, los estafadores pueden **usar tecnología para falsificarlo.**

2. Tono alarmante o metiendo presión para decidir.

Frases como **"Si no hacemos esto ahora, perderás tu dinero"** son tácticas comunes para asustarte y hacer que **tomes decisiones rápidas** y sin meditar.

3. Solicitud de datos confidenciales.

Ninguna entidad legítima te pedirá tu contraseña, códigos de doble verificación o los datos de tu tarjeta bancaria por teléfono.



4. Petición de pagos inmediatos

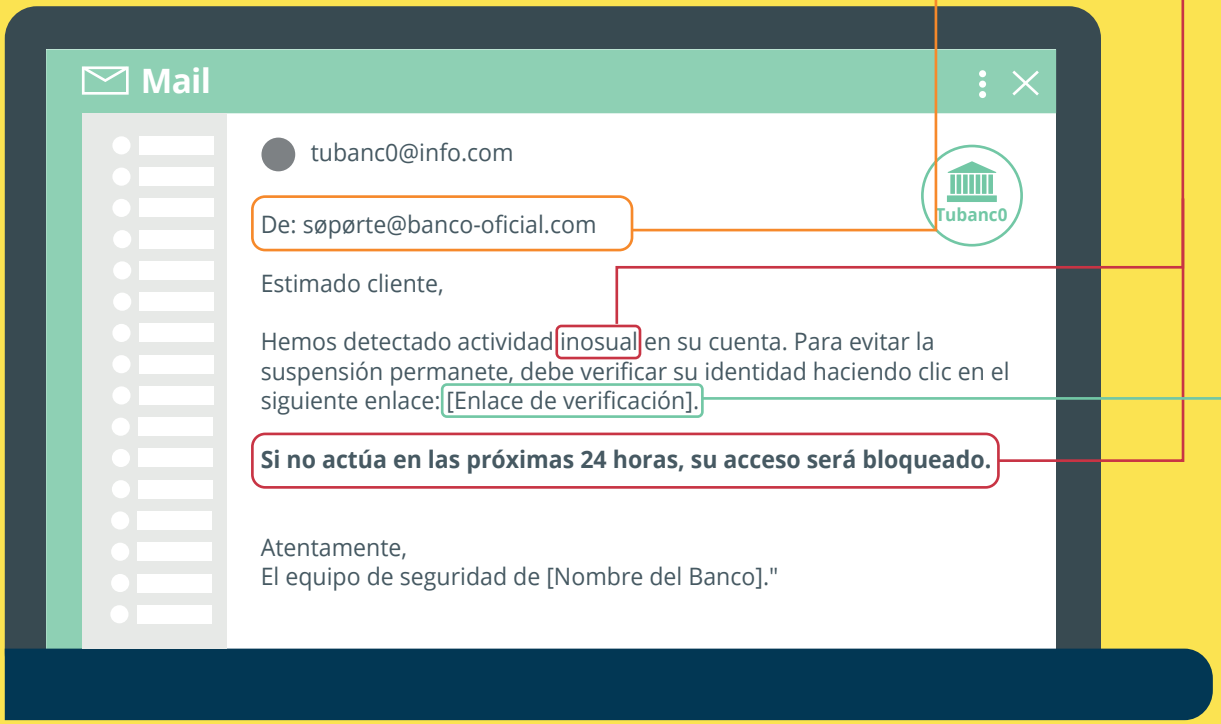
Si alguien **te pide que transfieras dinero,** realices un pago o descargues una aplicación, **cuelga inmediatamente.**

Recuerda que, **si algo no parece estar del todo bien,** es mejor detenerte, **comprobar la información** directamente en las páginas o números oficiales y **nunca actuar bajo presión.** Si tienes cualquier duda al respecto, no te lo pienses y contacta con **la Línea de Ayuda en Ciberseguridad de INCIBE.** Puedes llamarnos gratuitamente al **017** o contactarnos a través de mensajería instantánea en **WhatsApp (900 116 117) y Telegram (@INCIBE017).** ¡La calma y la precaución son tus mejores herramientas para detectar estas amenazas!

Ejemplo práctico

Caso simulado de *phishing*

Imagina que recibes un correo electrónico con el asunto: **"Actualización urgente requerida: Su cuenta será suspendida".** El mensaje parece provenir de tu banco y contiene el logotipo oficial, colores corporativos y un tono profesional. El correo dice:



Verificar el remitente

Aunque el nombre del remitente parece legítimo (ej. "Banco XYZ"), la dirección de correo **no coincide con el dominio oficial del banco.** Por ejemplo, el correo proviene de "søpørte@banco-oficial.com" en lugar de "soporte@banco-oficial.com".

Revisar el contenido del mensaje

Adopta un **tono alarmista y urgente,** una táctica frecuente para presionar a la víctima a actuar rápidamente sin reflexionar, e **incluye errores gramaticales,** además de redacción inusual para estas entidades.

Inspeccionar los enlaces

Examina los enlaces con atención. Algunas URL pueden contener algunos **caracteres modificados** que intentan pasar desapercibidos para engañarte y que creas que ese enlace es legítimo, como, por ejemplo, **g00gle.com en lugar de google.com.**

Buscar solicitudes de información confidencial

El mensaje pide que se verifique la identidad, lo que suele ser una excusa para obtener datos personales, como contraseñas, números de tarjetas o códigos de seguridad.

Confirmar con la entidad

Si hay dudas, lo más seguro es **contactar directamente al banco** o entidad de confianza través de sus canales oficiales (sitio web, aplicación móvil o número de atención al cliente) para **verificar la autenticidad del mensaje.**

Caso simulado de *smishing*

Imagina que recibes un **SMS en tu teléfono móvil** con el siguiente mensaje:

Verificar el remitente

Aunque el mensaje parece provenir de una compañía de mensajería conocida, **el número de teléfono no coincide con los canales oficiales de la empresa,** por ejemplo, si estás esperando recibir un paquete a través de Correos, DHL, Seur o cualquier otra empresa de paquetería, **comprueba que es el oficial** antes de realizar alguna acción.

Revisar el contenido del mensaje

El mensaje es breve y genera una sensación de urgencia, lo que es común en los intentos de *smishing*. Además, este caso particular contiene **errores ortográficos,** si bien la ausencia de los mismos no es indicativa de legitimidad y hay que realizar todas las comprobaciones.

Inspeccionar los enlaces

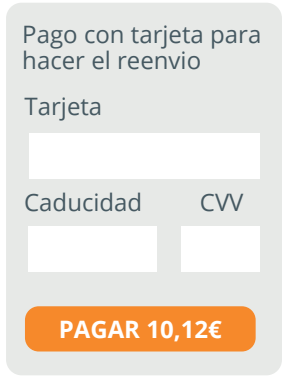
Puedes comprobar si el enlace proporcionado coincide con el sitio web oficial de la compañía, de todas formas, **no es aconsejable acceder a ninguna URL desde un SMS que hayas recibido.**

https://x9l.io/ßG7v_ ✗

https://www.correos.es ✓

Buscar solicitudes de información confidencial:

Ten cuidado si en el mensaje **se te pide información personal.** A veces dicen que necesitan tus datos o un pago para "reprogramar una entrega" o cualquier otro pretexto, pero puede ser un **intento de fraude.**



Confirmar con la entidad

Si tienes dudas, **contacta directamente a la compañía de mensajería** o donde hayas realizado la compra online a través de sus canales oficiales para **verificar la autenticidad del mensaje.**

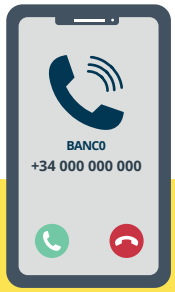
Caso simulado de *vishing*

Imagina que recibes una **llamada telefónica** en la que el identificador de llamadas muestra el nombre de una empresa conocida, cómo podría ser el de cualquier operador de telecomunicaciones. Al responder, escuchas un **mensaje pregrabado o un tono de voz que te resulta extraño:**

"Hemos detectado actividad sospechosa en tu cuenta. Para evitar la suspensión,diga "Sí" para conectarse con un representante de soporte técnico."

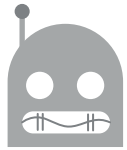
Verifica el número de teléfono

Aunque el identificador de llamadas muestra el nombre de una empresa confiable, **el número de teléfono no coincide con los canales oficiales de la empresa.**



Revisa el contenido del mensaje

El mensaje que se transmite en la llamada es **alarmista y urgente,** además de ser una grabación de **un robot** con un tono extraño o una mala pronunciación.



Busca solicitudes de información confidencial

El mensaje puede pedir que **proporciones datos personales** o de pago para "verificar tu identidad" o "solucionar el problema". También podrías ser redirigido a un **soporte técnico fraudulento** que intente convencerte de realizar un pago por servicios falsos, instalar software malicioso en tu dispositivo o **acceder a tus cuentas bancarias para robar tu dinero.**

Confirma con la entidad

Si tienes dudas, cuelga y contacta directamente con la empresa a través de sus canales oficiales para verificar la autenticidad de la llamada.

Medidas para protegerte y recomendaciones

Protegerte contra intentos de *spoofing* es más fácil si sigues algunos consejos prácticos y **adoptas hábitos seguros** al usar el correo, el teléfono o los mensajes de texto. Aquí te mostramos estrategias claras y **herramientas útiles para mantenerte a salvo.**

Consejos prácticos para evitar caer en este tipo de estafas:

1. Desconfía de mensajes alarmantes o demasiado buenos

Si recibes un correo, SMS o llamada con mensajes como **"Tu cuenta será bloqueada"** o **"Has ganado un premio",** mantén la calma. Tómate un momento para **verificar antes de actuar.**

2. No compartas información sensible.

Nunca des contraseñas, códigos de verificación, números de tarjeta o datos personales a través de correos, mensajes o llamadas. **Ninguna entidad legítima lo pedirá de esta manera.**

3. Evita hacer clic en enlaces sospechosos

Siempre verifica las direcciones web antes de hacer clic. Si tienes dudas, escribe la dirección oficial directamente en tu navegador en lugar de confiar en el enlace del mensaje.

4. No te dejes presionar.

Los estafadores suelen **insistir en que tomes decisiones rápidas** para que no tengas tiempo de reflexionar. Si te sientes presionado, cuelga, ignora el mensaje y verifica directamente con la entidad oficial.

5. Comprueba la autenticidad de las comunicaciones

Si dudas sobre un correo, SMS o llamada, **contacta directamente a la empresa** o institución utilizando los canales oficiales que aparezcan en su página web.

Herramientas y hábitos de seguridad:

1. Configura la autenticación en dos pasos.

Activa esta opción en tus cuentas bancarias, correos y aplicaciones importantes. De esta forma, aunque un estafador obtenga tu contraseña, necesitará un código adicional que solo tú puedes proporcionar.

2. Mantén tus dispositivos actualizados.

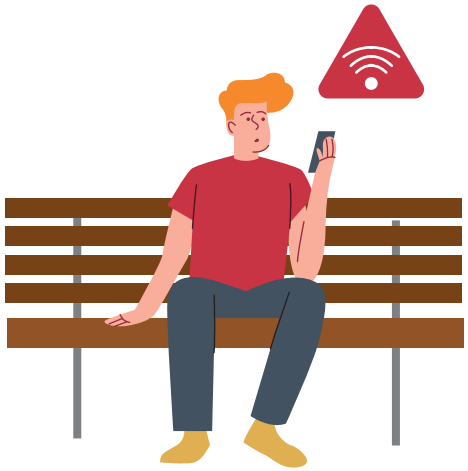
Las actualizaciones de *software* incluyen mejoras de seguridad que te protegen contra amenazas recientes. **Asegúrate de mantener actualizado tu teléfono, ordenador y aplicaciones.**

3. Instala un antivirus de confianza.

Un buen **antivirus** puede detectar correos maliciosos, mensajes sospechosos y páginas web falsas.

4. Usa contraseñas seguras y únicas.

Crea **contraseñas difíciles** de adivinar combinando letras, números y carácteres especiales**. Usa una contraseña diferente para cada cuenta.**



5. Revisa regularmente tus cuentas bancarias.

Consulta tus movimientos para asegurarte de que no haya transacciones sospechosas. Esto te permitirá actuar rápido si detectas algo inusual.

6. Guarda los números oficiales de contacto.

Ten a mano **los números de tu banco, operadora telefónica** y otros servicios importantes para que puedas contactarlos directamente en caso de dudas.

7. Evita conectarte a redes Wi-Fi públicas.

Cuando uses tu correo o realices operaciones bancarias, **hazlo desde redes seguras. Las redes públicas pueden ser peligrosas** si no están protegidas.

8. Utiliza herramientas de verificación

Algunas páginas web te permiten comprobar enlaces o remitentes sospechosos antes de interactuar con ellos. **Investiga y utiliza herramientas como verificadores de URL** o servicios de denuncia de fraudes.

¿Qué puedes hacer si crees que has sido víctima?

Si sospechas que has caído en una trampa de *phishing, smishing o vishing* relacionada con técnicas de *spoofing,* **debes actuar rápidamente** para minimizar el daño y proteger tu información. Para ello, sigue los siguientes pasos:

Cambia tus contraseñas y asegúrate de que sean robustas

Si proporcionaste contraseñas o datos de acceso,**cambia inmediatamente las credenciales** de las cuentas afectadas. **Utiliza contraseñas robustas y únicas.**

Escanea tu dispositivo

Usa un antivirus para escanear tu dispositivo y eliminar cualquier amenaza que pueda haber sido instalada.

Bloquea tarjetas y cuentas bancarias

Si compartiste información financiera, como números de tarjetas o cuentas bancarias, **contacta con tu banco** o entidad emisora **para bloquear las tarjetas** y monitorear movimientos sospechosos.

Habilita la autenticación de dos factores (2FA)

Activa la autenticación de dos factores en todas tus cuentas importantes para añadir una capa adicional de seguridad.

Desconecta dispositivos comprometidos

Si has accedido a un enlace malicioso o descargaste un archivo sospechoso, **desconecta el dispositivo de Internet** para evitar la propagación de *malware* o el robo de más datos.

Cómo reportar el incidente a las Fuerzas y Cuerpos de Seguridad del Estado o entidades afectadas

1. Reúne y almacena todas las evidencias

Guarda capturas de pantalla, correos electrónicos, mensajes de texto o cualquier otra prueba relacionada con el fraude. Puedes hacer uso de herramientas como testigos *online* para verificar y documentar las pruebas que recopiles.

2. Contacta con la entidad suplantada

Si el fraude involucra a una empresa o entidad (como un banco, servicio de mensajería u otra entidad de confianza), informa del incidente a través de sus canales oficiales.

3. Contacta con la Línea de Ayuda en Ciberseguridad

Comunícate con servicios especializados, como **la Línea de Ayuda en Ciberseguridad de INCIBE** para ayudarte con cualquier duda relacionada con la ciberseguridad, de esta manera puedes recibir asesoramiento personalizado e informar sobre el fraude. Esto no solo te ayudará a tomar medidas adecuadas, sino que también contribuirá a prevenir que otras personas sean víctimas del mismo fraude.

4. Dirígete a las Fuerzas y Cuerpos de Seguridad del Estado

Presenta una denuncia formal ante las autoridades competentes, como la Policía Nacional, adjuntando todas las pruebas recopiladas. Esto permitirá iniciar una investigación y aumentar las posibilidades de identificar a los responsables.

Conclusión

En un mundo cada vez más digitalizado, **el *spoofing*** representa una amenaza real y en constante evolución, utilizada por **ciberdelincuentes para engañar a sus víctimas** y obtener información sensible. **A través de correos electrónicos, mensajes de texto o llamadas telefónicas falsas, los estafadores buscan manipular a las personas aprovechándose de la urgencia y la confianza en entidades legítimas.** Por ello, es fundamental reconocer las señales de alerta y adoptar medidas preventivas para minimizar el riesgo de caer en estos engaños.

La clave para protegerse radica en **la formación y la precaución.** Verificar siempre la autenticidad de las comunicaciones, evitar compartir información personal en canales no verificados y **mantenerse informado sobre las técnicas más utilizadas por los delincuentes** son prácticas esenciales. Además, el uso de herramientas de seguridad, como la **autenticación en dos pasos** y los **antivirus actualizados,** refuerza la protección contra posibles ataques.

En caso de ser víctima de *spoofing,* **actuar rápidamente** puede marcar la diferencia. **Cambiar contraseñas, bloquear cuentas afectadas y reportar el incidente** a las autoridades son pasos fundamentales para mitigar el daño y evitar que otros caigan en la misma trampa. En definitiva, la seguridad digital es responsabilidad de todos. Con un enfoque preventivo y una actitud crítica frente a posibles fraudes, es posible reducir significativamente la exposición a estos ataques y utilizar con mayor confianza las tecnologías de las que disponemos.

El conocimiento es tu mejor defensa. Aprende a identificar las señales de fraude y protege tus datos.

¡No te dejes engañar!

Utiliza el código QR para más información: