**VISHING**

El **vishing** es un tipo de estafa informática, en el que el ciberdelincuente, valiéndose de la telefonía o el correo electrónico, se hace pasar por una fuente fiable y alegando supuestas razones de seguridad, intenta engañar a sus víctimas para hacerse con sus datos personales. La finalidad que persigue es robarles la identidad, o bien hacerse con su información bancaria.

Este tipo de estafa opera de la siguiente forma: el usuario recibe un mensaje de texto enviado supuestamente por una institución financiera, en donde le informa que tiene cargos en una de sus cuentas, promociones del banco, aviso de que su tarjeta está siendo utilizada fraudulentamente o simplemente resolver algún problema con la cuenta.

Posteriormente, se recibe una llamada en la que una supuesta operadora con una grabación idéntica a la de cualquier servicio telefónico de atención al cliente, pide al usuario el número móvil, email, número de tarjeta bancaria y código de seguridad. Esto se hace con la promesa de que los datos que proporciones están protegidos y que la información enviada sólo la conocerá el banco, pero en realidad, se transfiere a una base de datos de los delincuentes que usarán la información para realizar compras y/o disposición de efectivo en su nombre.

**Consejos para no ser víctima de este tipo de fraude**

    – Nunca entregas información o respondas a requerimientos sobre tu tarjeta de crédito. Si tienes dudas, debes llamar al banco y notificar que te han solicitado información financiera a nombre de la entidad.

    – Jamás debes hacer click en enlaces sospechosos que hayas recibido en tu correo. Cuando vayas a iniciar la sesión en tu banco fíjate que la barra de direcciones web tenga la dirección formal del banco y busca la aparición de un “candado” que indica que la conexión con el sitio es privada.

    – No utilices ordenadores de acceso público para realizar tus transacciones financieras.

    – Cambiar con frecuencia las contraseñas, procurando utilizar números y símbolos en su combinación. Nunca escribas tus claves en papel, el ordenador u otro lugar.

    – Recuerda actualizar constantemente tu sistema de antivirus y las herramientas antispyware. Los estafadores aprovechan las brechas de seguridad que tienen las versiones más antiguas.

Es muy importante recordar que todos podemos ser víctimas de fraude. Para evitar este delito, lo más importante es no proporcionar información personal y en caso de tener alguna duda con la tarjeta de crédito, siempre llamar a los teléfonos oficiales del banco y no a otros números que sean comunicados por una llamada o mensaje de texto.

Según indica su término, que proviene de la unión de dos palabras en inglés voice y phising, **se trata de un ciberdelito que ofrece a la víctima un número de teléfono al que comunicarse**.

Para llevar a cabo el vishing, **los ciberdelincuentes hacen uso de una Voz IP o voz automatizada** que se hace creíble porque es muy similar a las utilizadas por las entidades financieras.

Se marca de forma aleatoria a algunos números hasta que alguien contesta al otro lado de la línea. **Al interlocutor se le informa**, por ejemplo, **de que su tarjeta de crédito está siendo utilizada fraudulentamente, de que es preciso actualizar la información personal, resolver un problema con una cuenta**, o cualquier otro engaño similar.

Para resolver todas estas cuestiones, **se facilita un número de teléfono específico al que llamar.** Es muy habitual que el usuario se ponga en contacto con su supuesta entidad financiera a través de este falso número de teléfono ya que, según se ha demostrado, lo que se recuerda con más facilidad es el sitio web.

Cuando se realiza esta llamada al teléfono que indican, lo que se escucha al otro lado es una grabación idéntica a la de cualquier servicio telefónico de atención al cliente.

**Lo que solicita esta voz grabada es el número de cuenta, de tarjetas de crédito, su fecha de expiración, claves o nombre de usuarios.** Esta  información es más que suficiente para completar el engaño. A partir de ese momento, el ciberdelincuente puede llevar a cabo compras y operaciones fraudulentas por vía telefónica o internet.

Como medida **para evitar ser víctima de este ciberdelito, lo más sencillo es no ofrecer información personal** **sin comprobar las verdaderas identidades.** Y, por supuesto, llamar a los teléfonos oficiales de las entidades financieras y no a otros que sean comunicados en una llamada o como mensaje de texto.

**Técnicas de Vishing comúnmente utilizadas:**

Los estafadores organizan técnicas de vishing logran los ilícitos:

* **Información correcta:** tienen su nombre, dirección, número telefónico e información bancaria. De hecho, toda la información que usted esperaría escuchar de un funcionario de verdad.
* **Urgencia:** se le hace creer que su dinero está en peligro, y que debe actuar con rapidez. El miedo suele llevar a las personas a actuar sin pensar.
* **Suplantación de identidad de llamada:** el número de teléfono parece provenir de otro sitio (spoofing). Existen servicios, como Spoofcard, Burner (aplicación móvil gratuita), que permiten hacer «spoofing» (suplantar) a su número, de modo que llame usted a quien llame, éste no tiene forma de saber que es usted
* **Atmósfera empresarial:** se escucha mucho ruido de fondo, de modo que da la impresión de ser un «call center». Los estafadores tienen un «call center», o logran montar efectos de sonido en la llamada.
* **Wardialing:** Es cuando el visher utiliza un sistema automatizado para llamar a códigos de área específicos con un m ensaje que involucra bancos o cooperativas de crédito locales o regionales. Una vez que alguien contesta el teléfono, comienza una grabación genérica o específica, solicitando que el oyente ingrese los números de cuenta bancaria, tarjeta de crédito o débito, junto con los códigos PIN.
* **VoIP :** Voz sobre Protocolo de Internet, o VoIP, es un sistema telefónico basado en Internet que puede facilitar la visualización permitiendo que múltiples tecnologías funcionen en conjunto.
* **Ingeniería social:** La ingeniería social es una forma más elegante y más técnica de mentir. Las técnicas de ingeniería social se utilizan para evitar sofisticados softwares de seguridad. Las grabaciones automáticas utilizadas por vishers tienden a ser relativamente profesionales y convincentes.
* **Buceo en el contenedor:** Una forma de “pirateo” es simplemente buscar en el contenedor de un banco y recuperar cualquier lista de números de teléfono de clientes. Una vez que el visher tiene la lista, puede programar los números en su sistema para un ataque más específico.

**Caso real de Vishing**

* Usted llega a casa del trabajo y revisa su correo de voz para ver si alguien ha llamado. Su correo de voz tiene el siguiente mensaje:

*“Hola, le habla Eva, de la Compañía de Telecomunicaciones ABC. Le estoy llamando para confirmar la baja de su cuenta. Tanto la conexión telefónica como la internet de su dirección serán canceladas definitivamente mañana 6 de mayo a las 8:00 AM. Nuestros registros indican que tiene usted un saldo pendiente. Por favor, comuníquese con nuestro departamento de atención al cliente al 00-… para abonar el saldo pendiente”.*

Esto se hace para crearle un sentido de urgencia y obligarle a tomar el teléfono y llamar al número indicado. La Compañía de Telecomunicaciones ABC le responde, ofreciéndole de inmediato una forma automática de evitar la baja de su cuenta. Se le pide que introduzca su DNI y la tarjeta de crédito afiliada a su cuenta, para verificar que usted en verdad es el dueño de su cuenta. Después de que usted introduce ambos números, la llamada se corta.

## Cómo evitar las llamadas fraudulentas

La forma más efectiva de evitar el vishing es **no facilitar ninguna información personal ni bancaria a través del teléfono** cuando recibas una llamada. Tanto el banco como la compañía telefónica disponen de esa información, por lo que no es necesario que se la proporciones de nuevo a quien está llamando.

Ante cualquier sospecha cuando recibas una llamada alertándote sobre un fraude, lo primero que debes hacer es **ponerte en contacto con el banco** a través de otro medio para verificar que es cierta esa información. Por otro lado, si la llamada es para que te pongas en contacto con otro número de teléfono, no llames a ese número.

También es importante **comprobar el número de teléfono desde el que se hace la llamada** antes de responder. Muchos móviles ya incluyen la posibilidad de bloquear llamadas no deseadas y de filtrar el spam, marcando cuando un número es sospechoso.

**Frente a caso de Vishing puedes hacer la denuncia** ante la dependencia policial más cercana a su domicilio (comisaría de tu barrio en cualquier lugar del país) o al fiscal en cibercrimen de la Procuración General de la Nación, Dr. Horacio Azzolin, cibercrimen@mpf.gov.ar, teléfono de contacto, 6089-9000, interno N° 9266.

División Delitos Tecnológicos de la Policía Federal Argentina.
Cavia 3350 1° Ciudad Autónoma de Buenos Aires.
Tel. 4800-1120/4370-5899.
Correo electrónico: delitostecnologicos@policiafederal.gov.ar

Unidad de ciberdelitos en Córdoba:

 **Fiscalía General de la Provincia**
(0351) 4481000 – 4481600
Caseros 551 – 1° piso - CP 5000 - Córdoba. <https://www.mpfcordoba.gob.ar/>

Pro f. Alejandra Farneti y María José Barciocco

Información extraída de:

<https://protecciondatos-lopd.com/empresas/vishing/>

<https://blog.mailfence.com/es/vishing-2/>