

Área asuntos económicos

Ciberestafas financieras

Algunas de sus caras

defensorba.org.ar

Defensoría
Provincia de Buenos Aires

Índice

1. ¿Qué son las ciberestafas o ciberataque? ... 2
2. ¿Qué técnicas se pueden utilizar? ... 2
3. ¿Qué es el Phishing? ... 2
3.1. ¿Qué datos pueden obtener? ... 2
3.2. ¿Cómo pueden engañarte? ... 3
3.3. ¿Cómo puedo saber si los mensajes o correos son un intento de phishing? ... 4
3.4. ¿Cómo se puede prevenir el phishing? ... 5
4. Derivados del Phishing ... 5
5. ¿Qué es el Vishing? ... 5
5.1. ¿Cómo proceden a engañarte? ... 6
5.2. ¿Cómo prevenirlo? ... 6
6. ¿Qué es el Smishing? ... 7
6.1. ¿Cómo operan los estafadores? ... 7
6.2. ¿Algunos ejemplos de estafas a través del Smashing? ... 7
6.3. ¿Cómo prevenir el smishing? ... 8
7. ¿Qué es el QRshing? ... 9
7.1. Algunos ejemplos de estafas comunes con el código QR ... 9
7.2. ¿Qué puedo hacer para evitarlo? ... 9
8. ¿Qué es el Pharming? ... 10
8.1. ¿Cómo podría operar el Pharming? ... 10
8.2. Consecuencias del pharming ... 11
8.3. ¿Cómo combatimos el Pharming? ... 11
9. ¿Qué es el Sim swapping? ... 11
9.1. ¿Cómo se lleva a cabo? ... 12
9.2. ¿Qué sucede cuando la técnica de sim swapping es efectiva? ... 12
9.3. ¿Cómo lo evitamos? ... 13
9.4. Recomendaciones ante este tipo de fraude ... 13
10. Cómo proceder ante una ciberestafa financiera ... 14

1. ¿Qué son las ciberestafas o ciberataque?

Una ciberestafa es un tipo de delito informático en el que los delincuentes utilizan **medios tecnológicos y plataformas digitales para engañar o manipular** a sus víctimas con el fin de obtener un beneficio económico ilícito o información confidencial.

2. ¿Qué técnicas se pueden utilizar?[1]

- **Phishing:** suplantación de identidad por correo electrónico.
- **Vishing:** suplantación de identidad por llamada.
- **Smishing:** suplantación de identidad por mensaje SMS.
- **QRshing:** suplantación de identidad por QR.
- **Pharming:** suplantación por un sitio web ilegítimo.
- **Sim swappin:** suplantación de tarjeta SIM.

3. ¿Qué es el Phishing?[2]

La palabra *phishing* quiere decir **suplantación de identidad**. Es una técnica de ciberataque a través de correos electrónicos falsos que busca engañar a las personas para que revelen información personal confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios, haciéndose pasar por una entidad legítima.
Es como un **"pescador"** que lanza un **"anzuelo"** (un mensaje fraudulento) para **"pescar"** datos valiosos.



ROBO DE INFORMACIÓN PERSONAL
A TRAVÉS DE **CORREO ELECTRÓNICO**

3.1. ¿Qué datos pueden obtener?[3]

- Datos de contraseñas
- Números de tarjetas de crédito
- DNI
- CUIT o CUIL
- Nombres de usuario
- Códigos PIN[4]

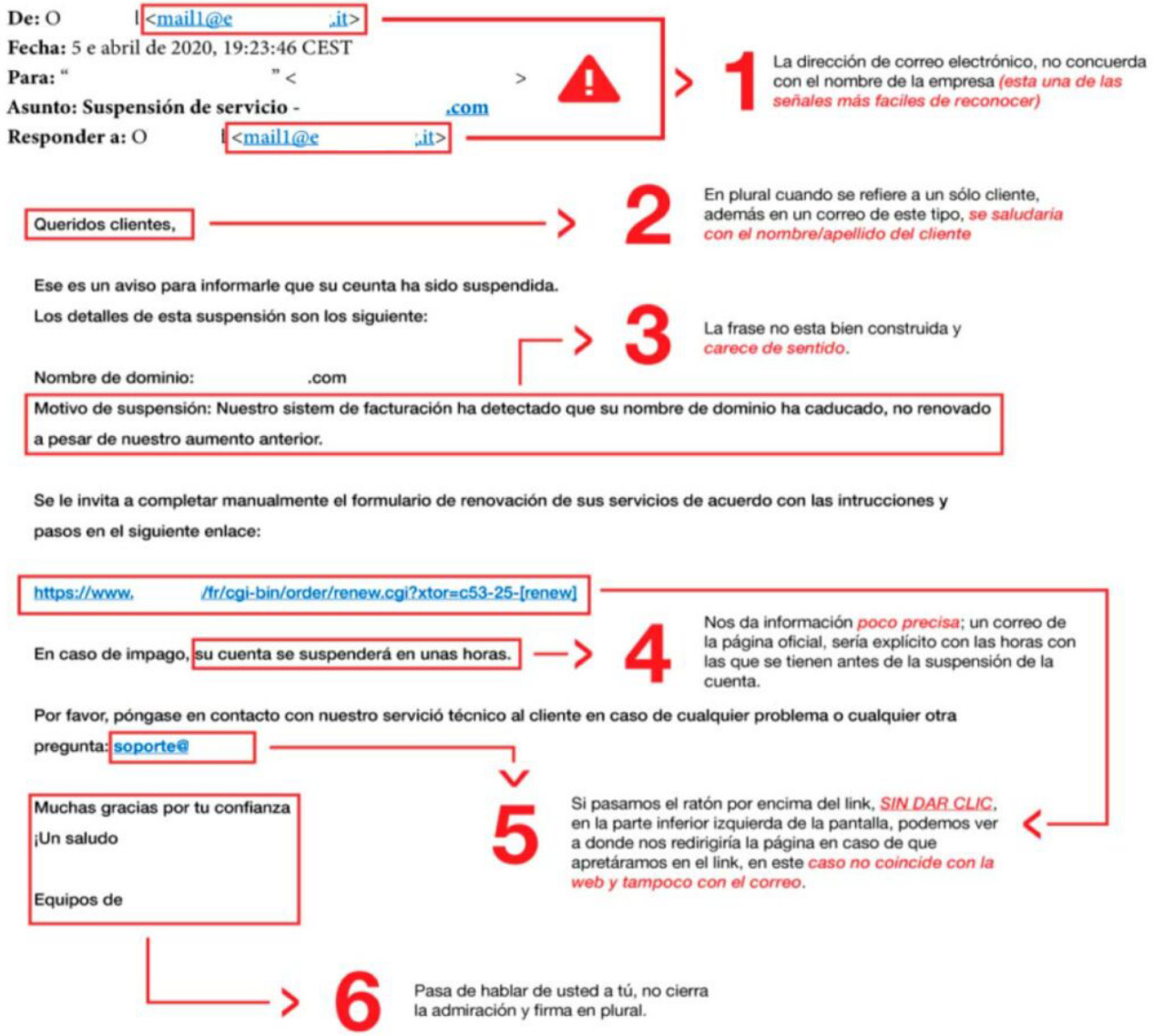
Cuando obtienen estos datos realizan compras, reservas o extracciones de dinero en tu nombre.

[1]Recuperado de: https://www.argentina.gob.ar/sites/default/files/descargable_ciberestafas.pdf
[2,3]Recuperado de: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing
[4]Código numérico o alfanumérico que se utiliza para autenticar a una persona y otorgarle acceso a un sistema o dispositivo.

3.2. ¿Cómo pueden engañarte?[5]

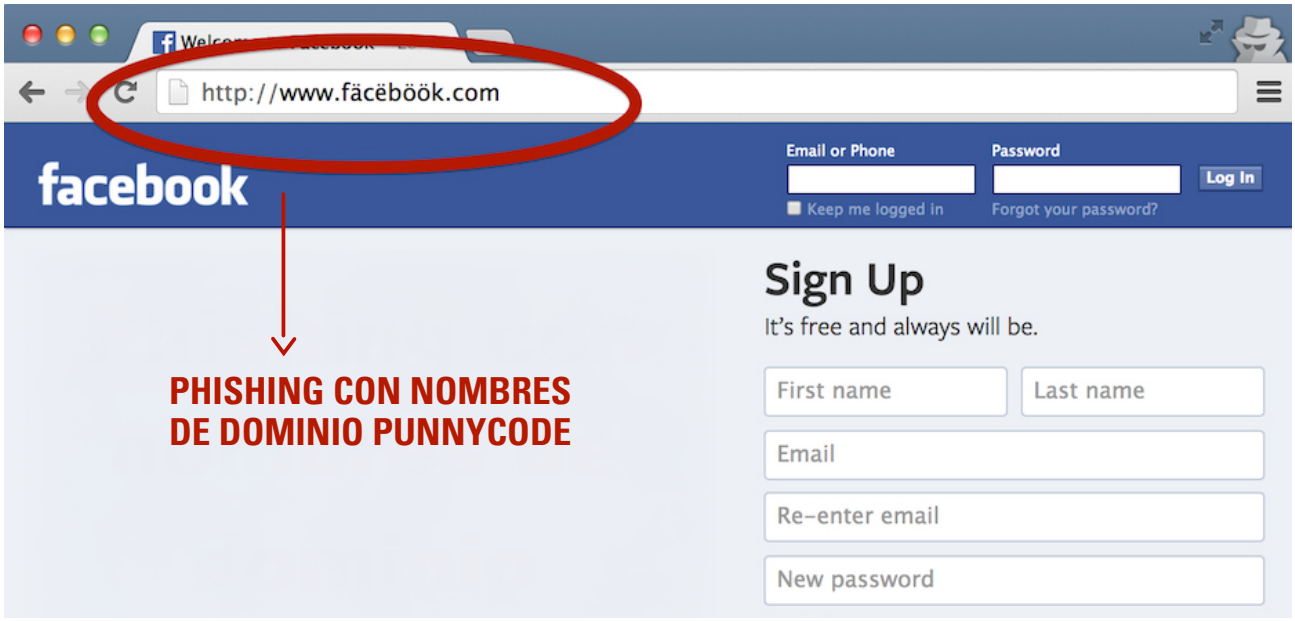
Dichos correos electrónicos falsos **contienen información falsa** y enlaces que redirigen tus respuestas hacia páginas de internet falsas con formularios y preguntas para obtener tus datos personales.
Estos correos electrónicos pueden aparecer como comunicaciones de bancos, servicios de pago, mercados de compra en línea o proveedores de servicios públicos.
Estos correos electrónicos fraudulentos suelen incluir el logotipo o la imagen de marca de la entidad.

Por ejemplo:



[5]Recuperado de: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing
https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html

Otro ejemplo:



3.3. ¿Cómo puedo saber si los mensajes o correos son un intento de phishing?[6]

Es necesario prestar atención a los **detalles** como, por ejemplo:

- Correos o mensajes de WhatsApp enviados por remitentes desconocidos;
- El uso de remitentes parecidos a los de las páginas oficiales y legales;
- Faltas de ortografía: errores gramaticales y ortográficos, la falta de acentos o diéresis o la presencia de caracteres en otros idiomas;
- La presencia de enlaces y links dudosos;
- El tono del correo electrónico: las empresas se dirigen a sus clientes en tono cálido y personal, en general te llaman por tu nombre porque tus datos ya figuran en sus bases de datos;
- El objetivo del correo: ningún proveedor de servicios en línea les pide a sus clientes la introducción de datos por medio del correo electrónico;
- Faltan o sobran letras en las direcciones URL: no es lo mismo "argentina.gob.ar"
- que "argentina.io", esta última dirección URL es falsa;
- La página no tiene el candadito verde o gris con su certificado de seguridad.



En caso de dudas, es recomendable NO hacer clic sobre el enlace ni tampoco escribir manualmente la dirección en el navegador.

[6] Recuperado de: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

3.4. ¿Cómo se puede prevenir el phishing?[7]

- Chequeá el remitente: antes de abrir cualquier correo electrónico es importante analizar que no sea falso. Observa cuál es la dirección completa del remitente.
- Comprobá la dirección de internet (URL[8]): pasa el mouse sobre el enlace (sin hacer clic), antes de hacer clic en cualquier enlace de un correo electrónico o mensaje, pasá el cursor del mouse por encima. La URL real a la que te dirigirá ese enlace aparecerá en la parte inferior izquierda de la ventana de tu navegador. Comprobá que coincida con la URL oficial de la empresa.
- Podés hacer una búsqueda en internet de la empresa y comparar las URLs.
- Utilizar contraseñas únicas para cada cuenta o aplicación. De ser posible, cambiarlas con regularidad.
- No utilizar contraseñas débiles o predecibles como '123456' o 'password'o datos que podrían ser públicos como mi dirección legal o mi fecha de cumpleaños.
- Habilitar la verificación en dos pasos siempre que sea posible.
- Verificá el certificado de seguridad de la página de internet: es importante verificar que tenga el candado gris o verde y que sea una dirección HTTPS (con 's').
- Desconfía de los archivos adjuntos.
- No contestes formularios en línea enviados por destinatarios desconocidos.



4. Derivados del Phishing

- Vishing
- Smishing
- Qrshing
- Pharming
- Sim swapping

5. ¿Qué es el Vishing?[9]

El término deriva de la unión de dos palabras: 'voice' y 'phishing' y se refiere al tipo de amenaza que combina **una llamada telefónica fraudulenta** con información previamente obtenida desde internet. El objeto es engañar a la víctima mediante la suplantación de la identidad de un tercero de confianza.



[7] Fuente: https://www.argentina.gob.ar/sites/default/files/descargable_ciberestafas.pdf

[8] URL: La Uniform Resource Locator, o en español Localizador Uniforme de Recursos, es la dirección única y específica de cada recurso en internet. Piensa en ella como la "dirección de casa" de una página web, una imagen, un video o cualquier otro archivo que se encuentre en la web.

[9] Recuperado de: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

5.1. ¿Cómo proceden a engañarte?[10]

Este método consta de dos pasos. Primero, el ciberdelincuente tiene que haber robado información confidencial a través de un correo electrónico o web fraudulenta ('phishing'), pero necesita la clave SMS o token digital para realizar y validar una operación.
Es en este momento en que se produce otro paso, **la llamada directa**: el ciberdelincuente llama por teléfono al cliente identificándose, como por ejemplo, personal del banco y, con mensajes particularmente alarmistas, intenta de que el cliente revele el número de su clave SMS o token digital, que son los necesarios para autorizar transacciones.
Por otro lado, tenemos la **doble llamada** que requiere una mayor elaboración por parte del estafador, pero que genera también más confianza en los usuarios. Utilizando un mensaje grabado -generado por un robot, principalmente-, "se informa a la víctima sobre un supuesto problema, por ejemplo, un acceso no autorizado a su aplicación de banca digital, y se indica un número de teléfono para que contacte, con el fin de solucionarlo". Cuando el usuario llama a dicho número fraudulento y entrega la información solicitada -credenciales de acceso, entre otros-, se consuma la estafa.

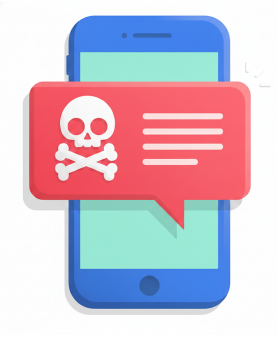
No podemos descartar la **combinación de técnicas**, es decir, los ciber-delincuentes también suelen utilizar métodos adicionales para complementar el vishing. Por ejemplo, en lugar de hacer una primera llamada a la víctima, deciden enviar un mensaje de texto (smishing) para que sea ella la que llame a un número de teléfono que aparenta ser de la entidad bancaria, pero que en realidad es controlado por el timador[11].

5.2. ¿Cómo prevenirlo?[12]

- Si recibís un llamado "inesperado" de tu banco, no brindes ningún dato sensible como contraseñas, códigos de confirmación que llegan por SMS o información similar. Ninguna entidad bancaria te solicitará esta información.
- Jamás brindar ante cualquier llamado sospechoso ningún dato personal, ya que los ciberdelincuentes utilizarán cualquier información aportada por el usuario para poder cometer más adelante estafas más sofisticadas.
- Cuidado con las ofertas excesivamente buenas, promociones o devoluciones de dinero que no hayas solicitado. Si tienes dudas con lo que te ofrecen, ponte en contacto con la entidad legítima o infórmate en sus canales oficiales.
- Mantén tu información a salvo y duda de los llamados desconocidos.
- ¿Cómo debes actuar? Mantén la calma y no sigas las indicaciones del ciberdelincuente. Es preferible interrumpir la comunicación y ponerse en contacto con el banco o la entidad para denunciar lo sucedido. Por otro lado, es importante bloquear y reportar el llamado.

[10] Recuperado de: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/
[11] Recuperado de: https://www.santander.com/es/stories/vishing-una-llamada-con-mucha-trampa
[12] Recuperado de: https://www.bancosantander.es/glosario/vishing

6. ¿Qué es el Smishing?[13]



Así como las llamadas telefónicas son una vía para tratar de engañar a los clientes, también lo son los **mensajes de texto o mensajes por WhatsApp** y de ahí deriva la modalidad conocida como 'smishing'. El objetivo es mediante textos falsos engañar a los usuarios con el fin de que descarguen malware, accedan a páginas fraudulentas o compartan información confidencial para enviar dinero a los ciberdelincuentes. El término **"smishing"** es una combinación de "SMS" (o "servicio de mensajes cortos", la tecnología detrás de los mensajes de texto) y **"phishing"**.

6.1. ¿Cómo operan los estafadores?

Los estafadores utilizan **mensajes falsos y enlaces maliciosos para engañar** a la gente y comprometer sus teléfonos móviles, cuentas bancarias o datos personales. La principal diferencia es el medio. **En los ataques de smishing, los estafadores utilizan SMS o aplicaciones de mensajería para llevar a cabo sus ciberdelitos** en lugar de correos electrónicos o llamadas telefónicas.

6.2. ¿Algunos ejemplos de estafas a través del Smashing?[14]

- Pretender ser una institución financiera: Los estafadores pueden hacerse pasar por el banco de la víctima para alertarle de un problema con su cuenta, a menudo a través de una notificación falsa. Si la víctima hace clic en el enlace, accede a un sitio web o una aplicación falsos que roban información financiera confidencial, como PIN, credenciales de acceso, contraseñas e información sobre cuentas bancarias o tarjetas de crédito.
- Fingir ser el gobierno: Los estafadores pueden hacerse pasar por agentes de policía, funcionarios del gobierno, u otros. Estos mensajes de smishing suelen afirmar que la víctima debe una multa o tiene que actuar para reclamar un beneficio gubernamental, etc. Los mensajes contienen un enlace a un sitio falso que roba el dinero y la información de las víctimas.
- Hacerse pasar por el servicio de atención al cliente: Los atacantes se hacen pasar por agentes de atención al cliente de marcas y minoristas fiables, o incluso el proveedor de servicios inalámbricos de la víctima. Suelen decir que hay un problema con la cuenta de la víctima o una recompensa o reembolso no reclamados. Por lo general, estos textos envían a la víctima a un sitio web falso que roba sus números de tarjeta de crédito o información bancaria.
- Fingir ser un transportista: Estos mensajes de suplantación de identidad afirman proceder de una empresa de transporte. Le dicen a la víctima que hay un problema con la entrega de un paquete y le piden que pague una "tarifa de entrega" o que acceda a su cuenta para corregir el problema. Entonces, los estafadores roban el dinero o la información de la cuenta y huyen. Estas estafas pueden ser más comunes durante las fiestas cuando mucha gente espera paquetes.

[13] Recuperado de: https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

[14] Recuperado de: https://www.ibm.com/es-es/think/topics/smishing

- Fingir enviar un mensaje de texto al número equivocado: Los estafadores envían un mensaje de texto que parece dirigido a alguien que no es la víctima. Cuando la víctima corrige el "error" del estafador, éste entabla una conversación con la víctima. Estas estafas con números erróneos suelen ser a largo plazo, ya que el estafador intenta ganarse la amistad y la confianza de la víctima mediante contactos repetidos durante meses o incluso años. El objetivo es robar el dinero de la víctima a través de una oportunidad de inversión falsa, una solicitud de préstamo o una historia similar.
- Fingir estar bloqueado en una cuenta: En esta estafa ya se tiene el nombre de usuario y la contraseña de la víctima y se intenta robar el código de verificación o la contraseña de un solo uso necesarios para acceder a la cuenta de la víctima. El estafador podría hacerse pasar por uno de los amigos de la víctima, afirmar que ha sido bloqueado de su cuenta de Instagram o Facebook y pedir a la víctima que reciba un código para ellos. La víctima obtiene dicho código, que en realidad es para su propia cuenta, y se lo da al estafador.
- Fingir ofrecer aplicaciones gratuitas: Algunas estafas de smishing engañan a las víctimas para que descarguen aplicaciones aparentemente legítimas (por ejemplo, gestores de archivos, aplicaciones de pago digital, incluso aplicaciones antivirus) que en realidad son malware.

6.3. ¿Cómo prevenir el smishing?[15]

- No pulse vínculos en mensajes de números desconocidos.
- Compruebe y verifique la URL de los vínculos que le envíen.
- Tenga cuidado con los mensajes que le presionen para que responda con urgencia y que no le resulten familiares.
- Verifique todos los números desconocidos antes de responder.
- Llame directamente a una empresa o persona para verificar si un mensaje de texto es real.
- Instale un software antivirus fiable para ayudarle a mantener el programa maligno alejado de su dispositivo.



[15] Recuperado de: https://www.avg.com/es/signal/what-is-smishing

7. ¿Qué es el QRshing?[16]



Es un tipo de **phishing a través de códigos QR**, que mediante el escaneo lleva al usuario a un sitio web fraudulento que puede descargar malware (programa maligno) o solicitar información confidencial. Una posibilidad es que los ciberdelincuentes envíen correos electrónicos de phishing, donde está el código QR, que se hace pasar por una empresa real o una entidad financiera. Le piden al usuario que escanee el código con el que llevan a cabo ataques como extraer información o descargar documentos que contienen virus.

7.1. Algunos ejemplos de estafas comunes con el código QR

- Una estafa común se produce cuando un ciberdelincuente coloca un código QR fraudulento sobre el original sin que se aprecie que es una calcomanía. Esto sucede con frecuencia en los menús de los restaurantes y en publicidad exterior.
- La estafa del código QR inverso: en esta el estafador crea un código malicioso que después utiliza como supuesta forma de pago, pero en realidad no tiene ese fin. En cambio, cuando el usuario lo escanea le está haciendo una solicitud de dinero. Así, en lugar de efectuar el abono del bien o servicio, lo que se consigue es llevar a cabo la operación inversa. Por ejemplo, a la hora de abonar un producto en un establecimiento, si el estafador presenta uno de estos códigos manipulados, no se paga por el artículo que se va a llevar, sino que el propio establecimiento será quien lo abone. A través de esta estafa también se pueden robar datos personales y bancarios.



7.2. ¿Qué puedo hacer para evitarlo?

- Antes de escanear cualquier código público, como en un restaurante o en la calle, obsérvalo y comprueba que no haya sido manipulado o se trate de una pegatina colocada encima del original por los estafadores.
- Para evitar que descarguen en tu dispositivo un virus, u otro malware, puedes instalar un software antivirus para comprobar que los códigos QR son originales y no contienen enlaces fraudulentos.
- Presta atención a la vista previa del enlace del código QR. Cuando escanees un código, debería aparecer una vista previa de la URL en tu teléfono. Comprueba que la dirección web o URL a la que te redirecciona parezca legítima. Recuerda buscar un símbolo de candado junto a la URL y que empiece por "https://". Estas URL son seguras.



- Si la aplicación o página web de destino te pide datos personales, desconfía. En ese caso verifica su autenticidad.

[16] Recuperado de: https://www.santander.com/es/stories/estafa-codigo-qr

8. ¿Qué es el Pharming?[17]

Es un tipo de ataque informático cuyo objetivo no es otro que el **robo de información sensible**. Para ello, **los ciberdelincuentes realizan un ataque al dominio de un sitio web** con el que consiguen redirigir a los usuarios a una página web falsa, que cuenta con el nombre de dominio oficial, para robarles su información privada.

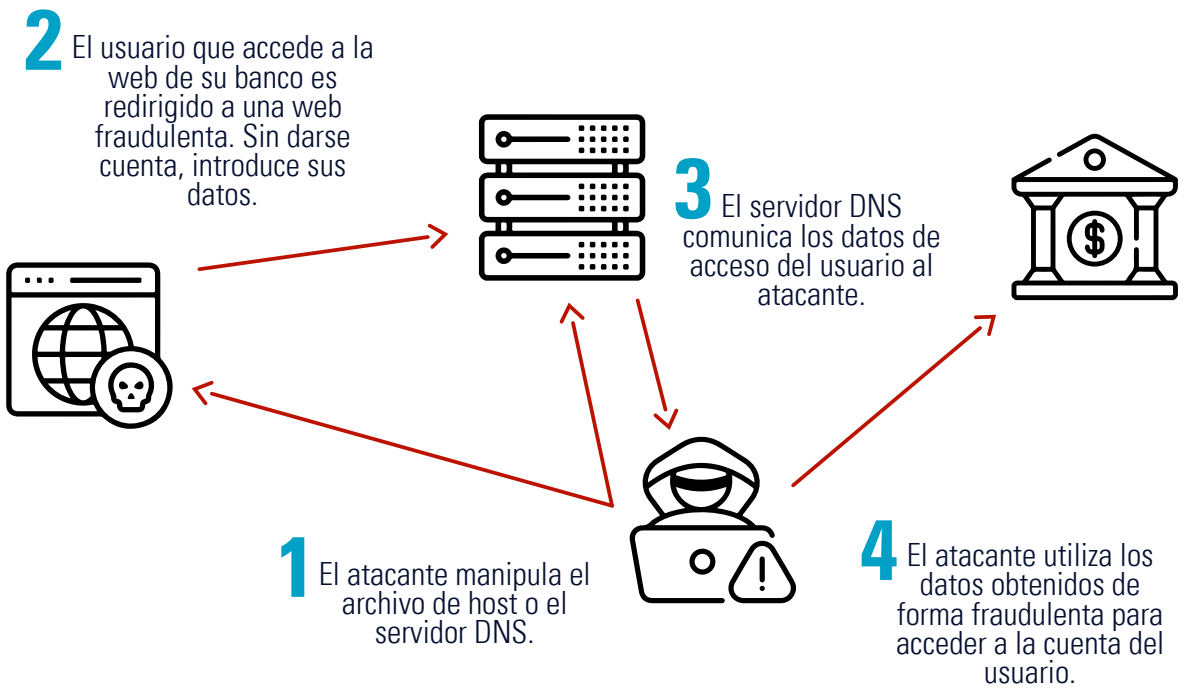


ROBO DE INFORMACIÓN PERSONAL A TRAVÉS DE UNA **PÁGINA WEB FALSA CON APARIENCIA REAL**

8.1. ¿Cómo podría operar el Pharming?

- Ataque al archivo host de la PC (o pharming local): requiere la instalación del virus o troyano en la PC. El objetivo es modificar dicho archivo y reconducir, con ello, el rumbo del tráfico a un sitio web malicioso de su elección (en el que se lleva a cabo el robo de datos sensibles).
- Modificación de los archivos host, es decir, nombres de dominio (como "www.google.com"): Los ciberdelincuentes pueden introducir malware en tu computadora que modifica este archivo. De esta manera, cuando intentas acceder a un sitio web específico (por ejemplo, tu banco), tu computadora es redirigida al sitio falso que está alojado en una dirección IP diferente, sin que el navegador muestre ningún cambio en la URL.

Desarrollo de un ataque de Pharming:



[17] Recuperado de: https://www.bbvapivot.com/es/ciberseguridad/que-es-el-pharming-y-como-puedes-evitarlo/

8.2. Consecuencias del Pharming

Las consecuencias del pharming pueden ser graves:

- Robo de identidad: Al obtener tus credenciales, los atacantes pueden acceder a tus cuentas en línea y suplantar tu identidad.
- Pérdidas financieras: Pueden realizar transacciones fraudulentas desde tus cuentas bancarias o tarjetas de crédito.
- Acceso a información sensible: Si acceden a tu correo electrónico u otras cuentas, pueden obtener información personal valiosa.

8.3. ¿Cómo combatimos el Pharming?

- Comprobar que la URL es correcta (se corresponde con la que accedes habitualmente). Si detectas que no es la misma, puedes estar ante una copia.
- Revisar que incluye la 's' tras el 'http' (visualizando 'https').
- Evaluar bien la página antes de empezar a navegar por ella (su aspecto es el de siempre). Hay que vigilar tanto sus componentes como los distintos enlaces que incluya.
- No pulsar en enlaces ni descargar archivos que no parezcan seguros.
- Visualizar las notificaciones del antivirus o el navegador. Si indican que la página no es segura, lo mejor es no entrar y buscar una opción diferente.
- Contar con un buen software de seguridad y hacerlo, si es posible, en su versión de pago (y no la gratuita, más limitada). También se pueden encontrar opciones específicas para este tipo de vulneraciones, más adecuadas a la hora de evitar el robo de información delicada.

9. ¿Qué es el SIM Swapping?[18]

Básicamente es una estafa que consiste en **duplicar de forma fraudulenta la tarjeta SIM del teléfono móvil de una persona**. Requiere del conocimiento de pocos datos personales de la víctima para llevarse a cabo.



[18] Recuperado de: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-sim-swapping.html

9.1. ¿Cómo se lleva a cabo?[19]

En esta técnica de ingeniería social se suelen aplicar los ataques más convencionales: *Phishing*, *Vishing* y *Smishing*. En la misma, visualizamos tres problemáticas muy claras.
Los ciberatacantes se suelen contactar con las empresas proveedores de servicios de telefonía móvil, luego mediante técnicas de ingeniería social, logran convencer a tu proveedor de servicios de telefonía de que transfiera tu número a una nueva tarjeta SIM que ellos controlan.

Ahondemos un poco más:

Primero, **los delincuentes se hacen pasar por la víctima**, es decir, por el titular legítimo de la línea telefónica. Pueden usar información personal que han obtenido previamente de otras fuentes (**como filtraciones de datos, phishing, o búsquedas en redes sociales**) para parecer más convincentes. Esta información puede incluir tu nombre completo, dirección, fecha de nacimiento, o incluso detalles de tu última factura.
Segundo, es importante entender que los empleados/as de las empresas prestadoras de telefonía móvil, también son víctimas de este engaño ya que es a quienes se les solicita una nueva SIM o bien, la transferencia de un número telefónico determinado a otra SIM -en el poder del/la ciberatacante-, obviamente, suplantando la identidad del/de la titular del servicio. Es aquí en donde entra en juego las técnicas de **ingeniería social**, como por ejemplo el **vishing** (Phishing de voz): Si la interacción es por teléfono, pueden usar técnicas de manipulación de voz para sonar creíbles y urgentes.
Tercero, **la obtención de la tarjeta SIM**: si la ingeniería social tiene éxito, la empresa de telefonía desactiva la tarjeta SIM original de la víctima y activa una nueva tarjeta SIM en poder de los estafadores, asociándola al número de teléfono de la víctima.

9.2. ¿Qué sucede cuando la técnica de sim swapping es efectiva?

En caso de tener la información almacenada en la SIM, se podría tener acceso –sin autorización- a:

- Agenda de contactos
- SMS
- Registro de llamadas

Y de esta forma, **¿qué más puede llegar a suceder?**

Acceso al perfil de todos tus contactos: Muchos servicios de mensajería y redes sociales vinculan tu cuenta a tu número de teléfono. Al tener tu SIM, pueden recuperar acceso a estas cuentas y, potencialmente, a tu lista de contactos.

[19]Recuperado de: https://buenosaires.gob.ar/noticias/sim-swapping
https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-sim-swapping.html
https://www.santander.com.ar/personas/canales-de-atencion/sim-swapping

Obtener datos de la cuenta bancaria o información financiera: Esta es una de las consecuencias más graves. Muchos bancos y servicios financieros utilizan el número de teléfono como un factor de autenticación para enviar códigos de verificación (SMS). Con el control de tu SIM, los estafadores pueden interceptar estos códigos, lo que les permitiría:

- Restablecer contraseñas de cuentas bancarias en línea.
- Realizar transferencias de dinero.
- Acceder a aplicaciones de pago o billeteras digitales vinculadas al número.

9.3. ¿Cómo lo evitamos?

- Si la técnica es utilizada a través del Phishing, **revisa detenidamente la dirección del remitente** de un correo para comprobar si es el oficial o si, por el contrario, contiene palabras o caracteres extraños que no se corresponden con la compañía o persona que dice ser. **No descargues archivos adjuntos** en emails que te resulten sospechosos o que no estabas esperando **ni proporciones datos personales o bancarios** en una página web a la que has accedido a través de un **enlace incluido en un correo**. Siempre es preferible teclear la dirección web en el navegador para acceder a un sitio web.
- **No descargues documentos, programas o vídeos** de páginas web a las que has accedido a través de un **enlace incluido en un correo electrónico o en un SMS si no estás seguro/a de su origen**. Se recomienda descargar siempre las aplicaciones desde los **mercados oficiales**.
- Mantén actualizados el **sistema operativo, las aplicaciones** y el navegador de tus dispositivos.
- Ten **actualizados y en funcionamiento** los programas **antivirus y antimalware** que tu compañía tenga instalados en tu equipo.
- **Haz copias de seguridad regularmente**: guarda tus archivos en dispositivos externos o en la nube con doble factor de autenticación.
- **Habilita la autenticación en dos pasos**: añade una capa extra de seguridad.
- **Descarga aplicaciones solo de fuentes oficiales** como Google Play o App Store.
- **Protege tu red doméstica**: cambia periódicamente la contraseña del wifi y revisa los dispositivos conectados.
- Utiliza con discreción las **redes sociales**.

9.4. Recomendaciones ante este tipo de fraude[20]

- **Si eres víctima de SIM Swapping o cambio de chip o tarjeta SIM**, o simplemente percibes que tu chip dejó de funcionar, debes comunicarte inmediatamente con tu proveedor de servicios de telefonía para recuperar el control de tu número telefónico. Después de esto se recomienda **cambiar las contraseñas de todas las cuentas**.
- Si hubo alguna afectación patrimonial, **presenta una queja sobre cargos no reconocidos**.
- Para mantener el control de tus transacciones, da de alta el servicio de notificaciones a través de correo electrónico, de manera que revises todos los movimientos de tu cuenta y puedas notar algún cargo que no reconozcas. La mayoría de los bancos lo ofrecen sin costo alguno.
- Revisa si te llegó un correo electrónico de tu banco mencionando que la contraseña de tu banca móvil ha sido modificada y, en caso de que lo hayan hecho, comunícate con ellos para **bloquear el acceso**.

[20] Recuperado de: https://www.condusef.gob.mx/?p=contenido&idc=1594&idcat=3

- **No respondas a llamadas, correos electrónicos o mensajes de texto que soliciten información personal**, limita la información personal que compartas en línea, configurar un PIN o contraseña en la cuenta de tu celular.
- Ten a la mano tu número **IMEI (Identidad Internacional de Equipo Móvil)**, es decir, el código numérico que identifica a cada celular. Esto te servirá para bloquearlo en caso de robo o extravío. Para obtener el **número IMEI** de tu teléfono celular marca el código ***#06#** en el teclado de tu celular. El IMEI se mostrará automáticamente en la pantalla. También se puede encontrar en una etiqueta blanca debajo de la batería de tu dispositivo.

10. Cómo proceder ante una ciberestafa financiera

En caso de haber sido víctima de una ciberestafa financiera puede acceder al **"PROTOCOLO DE ACTUACIÓN ANTE UNA CIBERESTAFA FINANCIERA"** a través del siguiente enlace https://www.defensorba.org.ar/pdfs/protocolo-ciberestafa-2025.pdf donde encontrará todos los pasos a seguir.