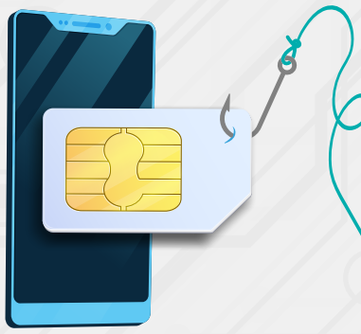
ift
INSTITUTO FEDERAL DE TELECOMUNICACIONES

inai

SIM SWAPPING

UNA MANERA DE ROBAR TU IDENTIDAD



De acuerdo con la “Guía para Prevenir el Robo de identidad” elaborada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) "es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre.

El robo o usurpación de identidad implica la obtención y uso NO autorizado e ilegal de datos personales"[1].

1. ¿Qué es el SIM Swapping?

La Secretaría de Seguridad Ciudadana de la Ciudad de México (SSC) reconoce al **“SIM Swapping” como la duplicación de la tarjeta SIM[2]** con la intención de **suplantar la identidad de clientes de instituciones bancarias por medio del número telefónico** y, de esta forma, acceder a las cuentas bancarias ligadas al dispositivo móvil[3].

2. ¿Cómo funciona?

En primera instancia, es importante señalar que **los atacantes o ciberdelincuentes** que recurren al método “SIM Swapping” siguen un patrón en su actuar:

1. Identificar a la víctima: En la mayoría de los casos los ciberdelincuentes o atacantes cuentan con información que les permite identificar a sus potenciales víctimas y, a su vez, contestar preguntas para hacerse pasar por ellos e identificar el número de teléfono móvil de la víctima y su operador.

2. Cambiar la tarjeta SIM: Por medio de ingeniería social el ciberdelincuente o atacante persuade a un representante del servicio de atención al cliente de la compañía de telefonía móvil para transferir el número de teléfono de la víctima a una nueva tarjeta SIM que está bajo el control de los atacantes.

1. Disponible en: https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guía_Prevenir_RI.pdf
2. La tarjeta SIM o Subscriber Identity Module es una pequeña tarjeta de plástico que tiene un chip pegado a ella, y que tienes que insertar en tu teléfono móvil o smartphone. En este chip, almacena de manera segura tu número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de telefonía. Disponible en: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya.
3. Disponible en: https://www.ssc.cdmx.gob.mx/blog/post/policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-nueva-modalidad-de-fraude-denominada-sim-swapping-o-duplicacion-de-sim

3. Restablecimiento de contraseñas: Realizado lo anterior, el atacante inicia el restablecimiento de las contraseñas de las cuentas de correo electrónico, de almacenamiento en la nube y de las redes sociales de la víctima que se encuentran ligadas al teléfono móvil (el restablecimiento de las contraseñas suele realizarse mediante mensajes de texto al número de teléfono de la víctima).

4. Acceder a las cuentas: El atacante accede a las cuentas de la víctima e identifica las claves, las carteras y las cuentas que puedan estar almacenadas en ellas. Elimina cualquier autentificación de dos factores basada en SMS o en aplicaciones móviles en cualquier cuenta con el control del número de teléfono de la víctima.

5. Robo: El atacante, en el caso de las cuentas bancarias, transfiere los fondos de la cuenta de la víctima a cuentas controladas por los atacantes[4].

De manera más específica, la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)** describe el modus operandi del "SIM Swapping" de la siguiente manera:

1. Algún tercero solicita a la compañía telefónica el cambio de tarjeta SIM por un presunto daño, extravío o pérdida.

2. Una vez que se concretó este proceso, la supuesta persona titular de la línea acude con una identificación falsa para recoger el chip y con ello tener acceso a números telefónicos, cuentas bancarias, información en la nube, entre otros datos.

3. La supuesta persona titular, teniendo en su poder la tarjeta SIM, pueden iniciar sesión en cuentas que usan mensajes de texto como una forma de autenticación, simplemente porque reciben los mensajes con los códigos de verificación.

4. Es posible que este tipo de acto ilícito no sea exclusivo para la obtención de información bancaria, puesto que también se puede tener acceso a los contactos e información personal contenidos en el dispositivo móvil[5].

3. El SIM Swapping y la ingeniería social.

El Instituto Nacional de Ciberseguridad de España (INCIBE) concibe a la ingeniería social como el **conjunto de técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial** o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente[6].

Dentro de la ingeniería social, existen diversas técnicas que utilizan mecanismos de manipulación para cometer ilícitos, como son el pishing, vishing y el smishing[7].

4. Disponible en: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping.
5. Disponible en: https://www.gob.mx/condusef/articulos/modalidad-de-fraude-tambien-conocido-como-sim-swapping?idiom=es.
6. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse
7. El phishing consiste en usurpar la identidad de una empresa u organización gubernamental. Se hacen llegar correos electrónicos a la víctima con un enlace a una página aparentemente legal, pero en realidad es duplicada, en donde piden datos personales para después cometer el fraude. Dos variantes del phishing son el vishing y el smishing; en el primer caso se utilizan mensajes de texto SMS fraudulentos para obtener datos personales de la víctima y, en el segundo, llamadas telefónicas o mensajes de voz. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-248-21.pdf.

El “SIM Swapping”, como parte de la ingeniería social, requiere de diversas acciones de ataque no digitales como el engaño, la manipulación psicológica y técnicas de persuasión, con el fin de invalidar los protocolos de seguridad de las empresas y así facilitarles a los ciberdelincuentes la obtención de información directamente de los usuarios u obtener el acceso a los datos personales engañando a los proveedores de estos servicios.

Edgar Sandoval, en su artículo **“Ingeniería social: corrompiendo la mente humana”**, señala que este es el método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente. Las personas más susceptibles suelen ser las más “inocentes”, por lo que no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima[8].

Precisamente, a través de este tipo de manipulación o persuasión, los ciberdelincuentes obtienen la duplicación de la tarjeta SIM de un equipo móvil, provocando que las personas que trabajan para un proveedor de servicios de telecomunicaciones en el área de atención a clientes, por confusión o cualquier otro motivo (incluso, algunas veces a través del phishing), otorguen una SIM asociada al número telefónico de la víctima.

4. Riesgos principales.

El “SIM Swapping” **permite a la persona delincuente utilizar la información de la persona usuaria para extorsionarla**, utilizar indebidamente sus datos personales o apropiarse de sus cuentas personales o laborales. Sin embargo, el principal riesgo es la usurpación de identidad.

Por lo que se refiere a las consecuencias de la usurpación de identidad, el INAI señala que estas pueden ser graves pues requieren “[...] de tiempo y recursos económicos para resolverse. Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada, y una vez que sucede es muy difícil recuperarla y es común tener problemas en el futuro”[9]. Es importante señalar que la usurpación de identidad no sólo permite a la persona que comente el acto ilícito obtener recursos monetarios, sino que también pueden afectar la reputación de la persona titular de los datos e incluso afectar otras esferas de su vida privada.

5. Consecuencias.

Como se mencionó anteriormente, existen diversas consecuencias al ser víctima de la ingeniería social, y en específico del “SIM Swapping”, como las siguientes:

- Tratamiento indebido de datos personales.
- Pérdidas financieras.
- Robo de cuentas asociadas al dispositivo móvil.

8. Disponible en: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana
9. Disponible en: https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Gu%C3%ADa_Prevenir_RI.pdf

ift
INSTITUTO FEDERAL DE TELECOMUNICACIONES

inai

6. Recomendaciones.

Para evitar ser víctima del “SIM Swapping”, se recomienda lo siguiente:

- **Añadir una clave o PIN de seguridad** u otros mecanismos de autenticación para desbloquear la tarjeta SIM del teléfono y evitar compartirlo con terceras personas.
- **Evitar guardar información de carácter confidencial en la tarjeta SIM** para que la persona ciberdelincuente que llegue a tener acceso a ella no pueda obtener los datos almacenados.
- **Utilizar aplicaciones de banca móvil** para consultar sus estados de cuenta, realizar transferencias y revisar sus movimientos bancarios con frecuencia.
- **Usar una red virtual privada para navegar** desde el móvil u otros dispositivos y practicar la navegación segura.
- **Tener cuidado con los correos, llamadas o mensajes de remitentes desconocidos**, los archivos adjuntos sospechosos o las páginas web de dudosa fiabilidad y evitar realizar descargas desde estos.
- **Minimizar los datos personales que compartimos** en internet.
- **Evitar utilizar contraseñas únicas**: Protege las cuentas en línea con contraseñas robustas y no reutilices la misma contraseña en todas las cuentas.
- **Cambiar claves y contraseñas** de forma periódica
- **Si eres víctima de “SIM Swapping”** o simplemente percibes que el chip del teléfono celular dejó de funcionar, debes **comunicarte con el proveedor de servicios** de telefonía móvil para recuperar el control del dispositivo.
- **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 IMEI, marca ***#06#** desde el teclado telefónico de tu celular.
- De ser posible, **utiliza el doble factor de autenticación**. Esto te permitirá acceder a un servicio utilizando tu contraseña y un código aleatorio que te proporcione una aplicación o a través de un mensaje SMS.

ift
INSTITUTO FEDERAL DE TELECOMUNICACIONES

inai

7. Consultar más información en:

- Alerta ciudadana de la SSC, disponible en: https://www.ssc.cdmx.gob.mx/blog/post/policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-nueva-modalidad-de-fraude-denominada-sim-swapping-o-duplicacion-de-sim
- “Guía para PREVENIR el robo de identidad” de INAI, disponible en: http://inicio.inai.org.mx/Guias/Gu%C3%ADa_Prevenir_RI.pdf
- Micrositio de Ciberseguridad de IFT, disponible en: https://ciberseguridad.ift.org.mx/
- Micrositio #Identidad Segura de INAI, disponible en: https://micrositios.inai.org.mx/identidadsegura/
- “Modalidad de fraude también conocido como SIM Swapping” de CONDUSEF, disponible en: https://www.gob.mx/condusef/articulos/modalidad-de-fraude-tambien-conocido-como-sim-swapping?idiom=es