SIM swapping: como evitar esta estafa

A evolución das estafas na actualidade fai que calquera usuario poida ser obxecto delas. Se ademais trátase dunha vinculada aos dispositivos móbiles, é máis probable que poida chegar a sucedernos. Neste artigo profundaremos sobre o SIM swapping e como debemos actuar para evitar esta fraude.

A penetración da tecnoloxía móbil en España é unha realidade. Así o demostra o feito de que máis do 99% dos fogares españois conta con teléfono móbil e o 57,5% dispón de tablet segundo datos da Enquisa sobre equipamento e uso de tecnoloxía de información e comunicación (https://www.ine.es/prensa/tich_2021.pdf) nos fogares 2021, publicado polo Instituto Nacional de Estatística.

A importancia da presenza deste tipo de dispositivos vese acrecentada polo feito de que os cidadáns recorren preferente aos mesmos para acceder a Internet. Así o demostra o recente estudo da Asociación para a Investigación de Medios de Comunicación (AIMC) (https://www.aimc.es/otros-estudios-trabajos/navegantes-la-red/), onde o 92,5% dos enquisados afirman usalo, seguido polo 72% que recoñece facelo mediante computador portátil e, un 47,5% a través de tablet. En consonancia con estes datos, segundo o estudo Dixital Report España 2022 (https://wearesocial.com/es/blog/2022/02/digital-report-espana-2022-nueve-de-cada-diez-espanoles-usan-las-redes-sociales-y-pasan-cerca-de-dos-horas-al-dia-en-ellas/) de Hootsuite e de We Are Social, é o 90,4% dos usuarios os que acceden a través de smartphone.

Neste contexto, e tras comprobar como os dispositivos móbiles han aumentado a súa presenza na sociedade española e o seu uso como medio de pago, imos analizar un pouco máis en detalle o SIM swapping, unha estafa cuxo funcionamento xa explicamos en 2019 (https://www.osi.es/es/actualidad/blog/2019/09/26/por-que-un-ciberdelincuente-le-interesa-duplicar-tu-tarjeta-sim).

VÍDEO

https://www.youtube.com/watch?v=fIaodow_nxw&t=3s

Lembremos que ante un SIM swapping, os ciberdelincuentes tentan duplicar de forma fraudulenta a tarxeta SIM do dispositivo móbil dunha persoa. Para iso suplanta a súa identidade a fin de conseguir un duplicado da mesma. Posteriormente, unha vez que a vítima queda sen servizo telefónico, accede á súa información persoal e toma o control das súas aplicacións, suplantándolle nas súas redes sociais, contas de correo electrónico ou banca dixital, utilizando os SMS de verificación que chegan ao número de teléfono. Desta forma o ciberdelincuente pode recuperar as mensaxes de texto de confirmación coas claves e realizar algún ciberdelito con estas credenciais, como pode ser realizar unha operación bancaria e suplantacións de identidade.

A pesar dos esforzos da Forzas e Corpos de Seguridade do Estado, en concreto da Policía Nacional (https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=11102#), para tentar acabar coas organizacións criminais que fan uso deste método, é unha fraude que segue en vigor motivado por esa presenza masiva dos móbiles nos fogares españois e polas novas técnicas dos ciberdelincuentes, por exemplo suplantando a entidades bancarias (https://www.osi.es/es/actualidad/avisos/2022/03/aumentan-los-envios-de-sms-fraudulentos-que-suplantan-entidades-bancarias) mediante SMS fraudulentos ou aos servizos de atención ao cliente (https://www.osi.es/es/actualidad/avisos/2021/12/detectadas-llamadas-fraudulentas-que-se-hacen-pasar-por-el-servicio-de) mediante chamadas telefónicas.

Para evitar ser vítima desta fraude, desde a OSI recomendamos:

- Se detectas que o teléfono queda sen cobertura sen un motivo lóxico, contacta coa operadora de telefonía para notificalo e comprobar que ocorreu.

- Implementa no teu dispositivo a autenticación en dous pasos (https://www.osi.es/es/actualidad/blog/2022/05/04/protege-el-acceso-tus-cuentas-activando-la-autenticacion-en-dos-pasos), como medida adicional ao contrasinal coa que poderás dificultar que alguén sen autorización acceda ás túas contas. Podes utilizar aplicacións como Microsoft Authenticator ((https://www.osi.es/es/actualidad/blog/2021/01/13/aplicaciones-para-verificacion-en-dos-pasos-google-authenticator-y), Google Authenticator (https://www.osi.es/es/actualidad/blog/2021/01/13/aplicaciones-para-verificacion-en-dos-pasos-google-authenticator-y) como método alternativo de dobre factor.
- Actualiza as opcións de recuperación da conta (https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar), por se conseguisen acceder á túa información.
- Se cauteloso coa información que compartes nas redes sociais (https://www.osi.es/es/actualidad/blog/2019/03/20/consideraciones-tener-en-cuenta-al-publicar-en-redes-sociales) e, no seu caso configurar adecuadamente os axustes de privacidade e seguridade, de forma que só os teus contactos poidan ver a información que se publica nelas.
- Non abras hipervínculos da internet que se sexan sospeitosos nin arquivos adxuntos recibidos por correo electrónico ou SMS, dado que ás veces os ciberdelincuentes suplantan a identidade dos nosos destinatarios.
- Evita proporcionar información persoal (https://www.osi.es/es/actualidad/blog/2021/01/20/protege-tu-movil-ios-y-android-con-5-consejos) por correo electrónico ou por teléfono cando che chamen, especialmente se non podes contrastar que realmente son quen di ser.
- Actualiza os contrasinais de forma periódica e asegúrache de que son robustas (https://www.osi.es/es/actualidad/blog/2019/02/20/tipicos-errores-que-cometemos-al-usar-nuestras-contrasenas-y-como).
- Non introduzas información sensible, como contrasinais e datos bancarios, se o dispositivo está conectado a wifi públicas (https://www.osi.es/es/wifi-publica).
- Non descargues aplicacións de tendas non oficiais (Google Play ou Apple Store) e, no seu caso, revisa os permisos que concedes para non dar acceso aos teus datos

persoais (.https://www.osi.es/es/campanas/dispositivos-moviles/acepto-no-acepto).

Finalmente, se consideras que fuches vítima do SIM swapping, garda todas as evidencias que poidas (https://www.osi.es/es/actualidad/blog/2022/01/26/testigos-online-y-obtencion-de-pruebas-te-explicamos-su-utilidad), pono en coñecemento do teu banco, da operadora de telefonía móbil e denúnciao ante as Forzas e Corpos de Seguridade do Estado (https://www.osi.es/es/reporte-de-fraude).

Fonte: Oficina de Seguridad del Internauta (OSI