



SIM swapping

The background features a close-up, slightly blurred view of several SIM cards. A prominent red rectangular overlay is centered on the page, containing the title and descriptive text. The title 'SIM swapping' is rendered in white, with 'SIM' in a bold, solid font and 'swapping' in a white outline font. Two white curved arrows originate from the right side of the 'SIM' text and point towards the 'swapping' text, indicating a process or flow. The overall design is clean and modern, with decorative elements like a grid of dots in the top-left and bottom-right corners.

Es un tipo de ataque cibernético que permite al atacante suplantar tu identidad con el propósito de obtener una tarjeta SIM con tu mismo número de teléfono.

Tu número celular es comúnmente utilizado para recibir códigos de verificación, o validar el ingreso a ciertas plataformas, y lo que buscan los delincuentes es acceder a estos códigos para robar nuestras cuentas digitales: **banca online, correo electrónico, redes sociales, etc.**

El delincuente obtiene los datos personales de las víctimas (fotos, copias de identidad, etc) buscando en redes sociales, phishing, aplicaciones maliciosas, etc



Con esta información el delincuente comienza a realizar el plan para hacer pasar por la víctima ante la compañía telefónica.

¿Cómo funciona el **SIM** swapping?

La víctima notará primero que el celular perdió cobertura y que no tiene acceso a sus cuentas de correo, redes sociales, o banca electrónica.


El delincuente engaña a la compañía telefónica para que le cambien o dupliquen la tarjeta SIM.


El delincuente ahora puede hacer llamadas, enviar mensajes de texto, y así tratar de conseguir acceso a cuentas de correo, redes sociales e incluso, banca electrónica.


Consejos para prevenir el **SIM** swapping?


Si sospechas que eres víctima de Sim Swapping


Contacta tu compañía móvil para bloquear tu número de teléfono, luego contacta a tu banco y gestiona el cambio de credenciales de tu banca online

 No publiques información personal como tu número de celular en redes sociales

 No ingreses información personal en links de páginas sospechosas que recibas por correos electrónicos o aplicaciones de mensajería.

 Utiliza doble factor de autenticación como medida extra de seguridad

 No compartas tus contraseñas con nadie, ni las guardes en las notas de tu celular

 No abras enlaces sospechosos que recibas por correo o de personas desconocidas

La principal forma para averiguar si su SIM card está siendo clonada es si tu celular se queda sin línea y dejan de funcionar distintos servicios como las llamadas y los datos móviles.



¡QUE NO TE ENGAÑEN!



Si no compartes el usuario
y contraseña de tu
banca en línea, es
IMPOSIBLE
que te hagan fraude

Reporta cualquier intento al



2280-1010

**DAR TU INFORMACIÓN BANCARIA,
ES DAR ACCESO A TU DINERO**

Visita www.bancatlan.hn para más consejos de seguridad