¡Cuidado con el Skimming!

Es una palabra poco conocida para ustedes. Pero hace referencia a la **clonación de tarjetas**. Es frecuente en cajeros electrónicos y en establecimientos que no tienen todas las garantías que quisiéramos.

Sucede mientras se realiza un pago, en el que utilizan un dispositivo para clonar la tarjeta e incluso hasta **recopilar la información del código PIN**.

El *skimming* también está presente en el comercio electrónico, una gran cantidad de páginas web han sido afectadas con un *malware*. Este código malicioso está presente en páginas de todo tipo de comercios, algunas relacionadas con compra de vuelos o entradas a eventos, compra de ropa, etc. Lo que hace básicamente es leer la información del pago que realizan los usuarios.

¡Siga estas recomendaciones y manténgase alerta!

- ***Antes de usar el cajero,* busque signos de alteración.** Verifique si hay características sospechosas. Intente mover partes de la máquina, que tengan apariencia de no estar colocadas con firmeza al dispositivo, *como el lector de las tarjetas, teclado numérico o la parte superior de la pantalla.*
- **Mantenga *su* tarjeta a la vista**. En los comercios, asegúrese de que su tarjeta solo se use en un dispositivo *y al momento de recibir verificar los datos*.
- **Sea discreto y no comparta su PIN**. No comenté con nadie su PIN, no lo anote en ningún lado, no guardes una copia junto con su tarjeta *y cubra el teclado al digitar su PIN.*
- **Verifique el extracto de su tarjeta de crédito**. Es un buen hábito puede identificar transacciones fraudulentas tan pronto como sucedan, y reportar al banco de forma oportuna.
- **Notifica a tu banco cuando vayas al extranjero**. Informar *con el fin de que el banco pueda hacer el correcto seguimiento a todas las transacciones de tu tarjeta de crédito.*
- **Dentro de compras virtuales,** es importante manejar contraseñas de acceso robustas para acceder a las tiendas. En lo posible, se debe habilitar un doble factor de autenticación.

Les contamos qué es el *sim swapping*

Imagen tomada de: https://www.redeszone.net/2019/02/09/ataques-sim-swapping-evitarlos/

En esta técnica los delincuentes intentaran clonar la SIM de su teléfono celular, esto lo logran reuniendo tanta información como sea posible de las redes sociales de la víctima con otra técnica denominada ingeniería social.

Los delincuentes llaman al operador de telefonía móvil, se hacen pasar por la victima indicando haber perdido o dañado la tarjeta SIM. Seguido a esto le piden a la persona de servicio al cliente que active una nueva tarjeta SIM en posesión del delincuente. Esto traslada el número de teléfono al dispositivo del delincuente que contiene una SIM diferente. O indicando necesitar ayuda para cambiar a un nuevo teléfono.

¿Cómo logran superar los filtros de las preguntas de seguridad? Ahí es donde los datos que han recopilados a través de correos de *phishing*, *malware*, la web oscura o la ingeniería sociales cobran valor.

¿Cómo obtienen tu dinero? Es posible que configure una segunda cuenta bancaria a su nombre en el banco y realizar transferencias entre esas cuentas y no generar ninguna alarma.

¿Cómo evitar que clonen la SIM de su teléfono?

- Conducta *online*: Esté muy atento con los correos electrónicos de *phishing* y otras maneras en las que los delincuentes pueden intentar obtener su información personal.
- Códigos PIN: si su proveedor de telefonía lo permite, establezca un código de acceso o PIN para las comunicaciones.
- ID: Evite crear su autenticación de seguridad e identidad únicamente alrededor de su número de teléfono.
- Aplicaciones de autenticación: puede usar aplicaciones de autenticación como Google Authenticator, que brindan autenticación de dos factores, está se vinculará a su dispositivo físico en lugar de al número de teléfono.