CENTRO CIBERNÉTICO POLICIAL

Boletín de análisis en CIBERSEGURIDAD FINANCIERA


Imagen tomada de: http://abrirconta.com/qual-melhor-cartao-de-credito

Fraude con tarjetas débito y crédito
CARDING - SKIMMING

El Centro Cibernético Policial hace un llamado a los tarjetahabientes y usuarios de pagos electrónicos acerca de una modalidad delictiva que se ha estado expandiendo recientemente, se trata del "Skimming" (clonación de tarjetas débito y crédito), que se lleva a cabo en cajeros electrónicos, establecimientos comerciales y estaciones de gasolina principalmente. Una actividad que se ha popularizado y extendido geográficamente, causando importantes afectaciones económicas a miles de usuarios.

Sin embargo, no existe un registro centralizado de este tipo de ataques, que en muchos casos pudieron evitarse mediante la aplicación de medidas preventivas.

Estadística de esta modalidad 2014 – 2017

A través de esta modalidad se han recibido un total de **7.117 denuncias** discriminadas, así:

2014: 1.938
2015: 1.699
2016: 2.163
2017: 1317

Afectando en delitos como acceso abusivo a un sistema informático, violación de datos personales, hurto por medios informáticos y trasferencia no consentida de activos.

CENTRO CIBERNÉTICO POLICIAL

Boletín de análisis en
CIBERSEGURIDAD FINANCIERA

Carding - Skimming

Es un tipo de fraude que facilita el duplicado de tarjetas de crédito y débito copiando los datos de la banda magnética, para su posterior uso de manera fraudulenta, realizando transacciones y retiros sin autorización del titular de la cuenta.

Esta modalidad delictiva puede ocurrir tanto en cajeros automáticos como en establecimientos comerciales de todo tipo, como restaurantes, estaciones de gasolina, salones de belleza, entre otros. Los delincuentes pueden cargar consigo un dispositivo conocido como "skimmer" que les permite leer la banda magnética con tan solo deslizarla por una ranura, o simplemente instalan el dispositivo sobre el lector del cajero automático. Una vez conseguida la información, la graban en una tarjeta nueva y obtienen su contraseña por medio de cámaras que instalan en los cajeros automáticos, o a través de una persona que simula ser un cliente del cajero y observa cuando la víctima digita su clave.

Skimmer

Dispositivo electrónico que realiza una copia de los datos contenidos en la banda magnética de una tarjeta de crédito o débito.

El Centro Cibernético Policial sugiere las siguientes recomendaciones de ciberseguridad para evitar ser víctima de este tipo de fraude:

En cajeros automáticos

1.Antes de utilizar un cajero, verifique que no exista ningún aparato o dispositivo extraño instalado, especialmente en la ranura de ingreso de la tarjeta o cerca del teclado numérico.

2. Cuando realice pagos con su tarjeta nunca la pierda de vista y cuando se la devuelvan, verifique que los datos en ella sean los suyos.

CENTRO CIBERNÉTICO POLICIAL

Boletín de análisis en
CIBERSEGURIDAD FINANCIERA

3. Nunca acepte ayuda de extraños al realizar transacciones en cajeros automáticos.
4. Revise frecuentemente el saldo de sus cuentas bancarias.
5. No confíe en la amabilidad de extraños al momento de realizar transacciones.
6. En lo posible, trate de ocultar su clave mientras la digita, podría haber micro cámaras instaladas.
7. Si detecta alguna anomalía en el cajero, informe de inmediato a su entidad bancaria o a la línea de emergencias de la Policía Nacional 123.

En restaurantes o estaciones de gasolina

1. Realice la operación personalmente, no entregue su tarjeta a terceros.
2. Cubra el teclado cuando digite la clave.
3. Nunca olvide firmar el comprobante de pago.
4. Cerciórese de que su tarjeta sea deslizada una sola vez y por un sólo dispositivo; cuando se la devuelvan verifique que sea la suya.
5 No arroje a la basura los comprobantes de pago en los cuales estén registrados sus datos (firma, teléfono, número de tarjeta o número de cédula).

¿Qué hacer si ya se cometió el fraude y usted es la víctima?

Ante cualquier inquietud acerca de la clonación de tarjetas débito o crédito "Skimming", el Centro Cibernético Policial está presto las 24 horas del día para brindarle una orientación oportuna a través de sus redes sociales, como son: Twitter @CaiVirtual , Facebook CaiVirtual, el portal de servicios con chat interactivo 24/7 caivirtual.policia.gov.co, el correo electrónico caivirtual@correo.policia.gov.co ó a través de la línea telefónica, en la ciudad de Bogotá, +57 1 5159700.

caivirtual

@CaiVirtual