VIGI PRENSA: 2015

Skimming

Asegure sus Tarjetas Bancarias

El Cai Virtual en compañía de Incocredito realiza la publicación de las recomendaciones que se deben tener en cuenta al momento de ejecutar alguna transacción con tarjetas de crédito y/o débito tanto para el cliente como para el vendedor, así:

TRANSACCIONES PRESENCIALES:

- En una transacción con tarjeta siempre debe haber presencia del titular de la tarjeta, la tarjeta de crédito y el documento de identidad.
- Solicite y verifique el documento de identidad y la tarjeta de crédito antes de la transacción.
- Revise las características de seguridad tanto del documento de identidad como de la tarjeta.
- Confronte los datos del documento de identidad contra los de la tarjeta.
- Valide en el comprobante diligenciado los 4 últimos números de la tarjeta, fecha de vencimiento, tipo de tarjeta, franquicia o marca.
- Verifique que la firma en el comprobante coincida con la firma registrada en el panel de la tarjeta.

- Verifique que el número de cédula en el comprobante coincida con el del documento de identidad.
- Cuando en su establecimiento se requiera el mantenimiento de los dispositivos de tipo datáfono, tenga presente que sólo las personas autorizadas por Credibanco o Redeban Multicolor pueden tener acceso a la terminal, para lo cual se deben contactar a los números telefónicos autorizados para confirmar la identidad del funcionario.
- Lleve un control de las visitas realizadas para el mantenimiento de datáfonos. No permita que personas extrañas manipulen o abran las terminales o que estas sean retiradas temporalmente del establecimiento así sea por corto tiempo.
- Mantenga al personal de su establecimiento capacitado.

VENTAS NO PRESENCIALES (INTERNET):

1. No utilice computadores públicos para efectuar operaciones bancarias por Internet.
2. Nunca descargue ni baje software de sitios desconocidos. Los programas gratuitos pueden contener programas espía mediante los cuales pueden robar información confidencial como usuario y contraseña.
3. No utilice enlaces que se encuentran dentro de un correo electrónico para ingresar a una página Web. Ingrese al sitio Web escribiendo la dirección usted mismo.
4. Absténgase de llenar formas de texto en correos electrónicos que solicitan información financiera personal. Evite comunicar información confidencial como números de tarjeta de crédito o información de cuentas vía correo electrónico.
5. Utilice un software Antivirus y manténgalo actualizado: Casi la totalidad de los códigos maliciosos enviados en archivos adjuntos de correos electrónicos son detenidos por los programas antivirus comerciales.
6. Instale un Firewall personal.
7. La página Web del comercio debe ser una página segura certificada por una empresa idónea y reconocida.
8. La información de la tarjeta habiente debe viajar por un canal dedicado (VPN) o Red privada virtual (Virtual Prívate Network).
9. La información debe ser encriptada con software de alto nivel y reconocimiento, la norma PCI DSS exige la utilización de Triple DES o AES.
10. Se recomienda certificarse con los sistemas de tarjetas para realizar transacciones seguras por Internet.
11. Se sugiere hacer validaciones con el cliente vía telefónica.

12. Se recomienda contar con un servicio de atención telefónica 7 x 24 y una línea nacional para atender las inquietudes del cliente.
13. Es importante que en el establecimiento se tengan definidas políticas de facturación, cambios, reembolsos y cancelaciones.
14. Es recomendable contar con antivirus para evitar la instalación de troyanos o virus que faciliten el robo de información.

RECOMENDACIONES EN SERVICIO DE DOMICILIOS:

- Se recomienda asignar un datáfono exclusivo por cada domiciliario.
- Desarrollar e implementar un proceso diario de validación del inventario de datáfonos asignados al punto de venta.
- Garantizar la custodia de estos dispositivos en horarios no hábiles.

RECOMENDACIONES EN EL CONTROL DE LA INFORMACIÓN:

- La administración de la información de los tarjetahabientes debe estar en áreas seguras.
- Es importante realizar seguimiento estricto al manejo y control de información en servidores y equipos de cómputo.
- No se debe almacenar información Financiera de tarjetahabientes o bases de datos que puedan comprometer al comercio como punto de compromiso por fuga de información.
- Cumplir con estándares de seguridad información como PCI.

RECOMENDACIONES ANTE UN POSIBLE FRAUDE:

- Verifique la autenticidad de la tarjeta y el documento de identidad.
- Ante alguna irregularidad de aviso al jefe inmediato y/o personal de seguridad del almacén.
- Si tiene certeza absoluta de la irregularidad contacte al Centro de información de INCOCREDITO.
- Una vez confirmado el fraude INCOCREDITO coordinará con la autoridad la captura y judicialización.

VIGI PRENSA: 2015

EN ESTABLECIMIENTOS COMERCIALES

- Realice la operación personalmente.
- Tape el teclado cuando digite la clave.
- Firme siempre el comprobante de pago.
- No pierda de vista la tarjeta al efectuar sus transacciones en caso de ser necesario solicite un datáfono inalámbrico.
- Verifique que su tarjeta sea deslizada una sola vez y cuando se la devuelvan verifique que sea la suya.
- Si su tarjeta tiene chip, solicite al comercio que realice la transacción por este medio.
- No arroje a la basura los comprobantes de pago en los cuales estén registrados sus datos (firma, teléfono, número de tarjeta, número de cédula).

EN CAJEROS AUTOMÁTICOS

- Verifique que no haya ningún objeto extraño adherido al cajero.
- Antes de introducir la tarjeta en la ranura, verifique que esta no tenga objetos extraños adheridos a esta.
- No haga caso a avisos impresos pegados en el cajero que le indican cómo hacer sus operaciones.
- Nunca acepte ayuda de un extraño cuando use un cajero automático.
- Párese cerca al cajero automático y use su cuerpo y sus manos como escudo para asegurarse de que nadie lo vea ingresar su clave.
- No se deje distraer, intimidar o apurar en hacer su transacción en el cajero automático.
- Tape el teclado cuando digite la clave.
- Si usted no ha terminado su transacción y es abordado por un tercero, presione el botón Cancelar, recoja su tarjeta y retírese.
- Revise frecuentemente los saldos de sus cuentas bancarias.

ASIGNACIÓN DE CLAVES

- No utilice claves que sean fácilmente identificables como fechas de nacimiento, secuencias o caracteres repetidos.
- Procure no utilizar la misma clave para múltiples sistemas, cuentas de correo o acceso a las Entidades Financieras donde tiene sus productos.
- No utilice la opción recordar clave en los navegadores.

VIGI PRENSA: 2015

- No anote sus claves, memorícelas.
- Si su tarjeta se lo permite, cambie periódicamente sus claves secretas.
- No utilice las mismas claves para sitios web desconocidos y que para entidades con un alto nivel de seguridad.
- Cuide la privacidad de su clave secreta, evite compartirla con terceros.

Fuente: Centro Cibernético Policial
http://www.ccp.gov.co/ciberseguridad/recomendaciones/skimming