Tipos de fraude y seguridad en el E-commerce.

Tipos de Fraude en el E-commerce.

Se conoce como FRAUDE **CIBERNÉTICO** a aquellas estafas que utilizan la red, para realizar transacciones ilícitas.

Muchas veces las personas que realizan este tipo de fraudes, se aprovechan del desconocimiento o del poco cuidado que las personas tienen al utilizar los servicios financieros en línea, convirtiéndose en un blanco fácil para los estafadores.

Dentro de estas actividades es común encontrar: **correo basura, smishing, pishing y pharming,**

- **Correo basura:** También conocido como SPAM, se trata de un mensaje enviado a varios destinatarios que usualmente no lo solicitaron, con fine publicitarios o comerciales.

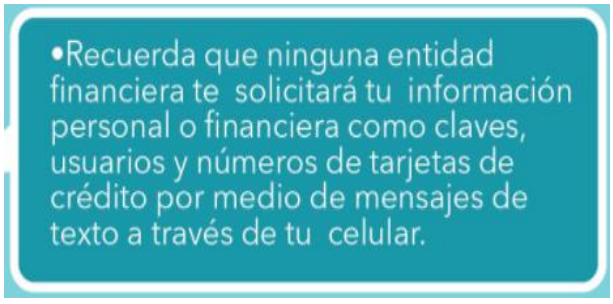
La información de dicho correo te invita a visitar una página o descargar algún archivo que por lo general es un virus que roba la información de tu dispositivo.

¿Cómo evitarlo?

1. Instala en tu computadora o dispositivo móvil un buen antivirus.
2. No des "clic" o abras vínculos sospechosos.
3. Si descargas aplicaciones, realízalo por medio de las tiendas y desarrolladores oficiales

- **Smishing:** En este tipo de fraude, te envían mensajes SMS a tu teléfono móvil con la finalidad de que visites una página web fraudulenta. Esto con el fin de obtener tu información bancaria, para realizar transacciones en tu nombre.

¿Cómo evitarlo?



- **Phishing:** También conocido como suplantación de identidad, en este tipo de fraude el objetivo es que al hacerse pasar por una Institución Financiera, con un mensaje indicándote un error en tu cuenta bancaria, y al ingresar tus datos, obtienen tu información confidencial como: números de tus tarjetas de crédito, claves, datos de cuentas bancarias, contraseñas, etc.

Si caes en la trampa, con tus datos pueden hacer compras o solicitar créditos a tu nombre, realizar transferencias y hasta vaciar tus cuentas.

Recuerda que las personas que realizan este tipo de fraudes son hábiles y te engañan con tácticas alarmistas o solicitudes urgentes para preocuparte y evitar que pienses bien la situación.

También existe el phishing telefónico, en donde los delincuentes simulan ser empleados de alguna institución y generalmente te convencen al decirte que tus cuentas están registrando cargos irregulares o que requieren alguna información, evita proporcionarles tus datos y llama directamente a la Institución Financiera para corroborar la información.

1. Llega en correos masivos.
2. Utilizan la imagen oficia de alguna Institución Financiera.
3. Te dicen que hay algo mal con tu cuenta y que requieres actualizar tu información.
4. Hay una liga que te dirige al sitio falso.
5. Te solicitan tus datos personales y financieros.
6. A veces llegan a pedirte los dígitos de tu clave.

¿Cómo evitarlo?

1. Nunca entregues tus datos por correo electrónico.
2. Las empresas y bancos **NUNCA** te van a solicitar tus datos financieros o números de tarjetas de crédito por teléfono o internet, cuando no seas tú quien inicie una operación.
3. Si aún te queda duda del correo, llama o asiste a tu banco y verifica los hechos.

- **Pharming:** Consiste en redirigirte a una página de internet falsa mediante ventanas emergentes, para robar tu información.

Suelen mostrar leyendas similares a esta: ***¡Felicidades, eres el visitante un millón, haz clic aquí para reclamar tu premio!***

¿Cómo evitarlo?

1. No des clic a páginas sospechosas o respondas mensajes de correo que te dicen haber ganado un premio, viaje o sorteo, ya que generalmente solicitan antes tus datos personales para otorgarte el supuesto premio.
2. Verifica que el sitio en el que navegas cuente con el protocolo de seguridad "https://" y un candado cerrado en la barra de direcciones.

Seguridad a la hora de realizar una compra en sitios E-commerce.

Para disminuir los riesgos asociados a los pagos con tarjeta en comercio electrónico existen sistemas de seguridad que validan la información impresa de la tarjeta.

Al comprar con una tarjeta de crédito, la página donde realizas tu compra te pedirá como primer paso la siguiente información:

1. **Número de tarjeta**
2. **Fecha de caducidad**
3. **Nombre del titular de la tarjeta**
4. **Código de seguridad**

A fin de mejorar los mecanismos de seguridad en comercio electrónico, actualmente se están desarrollando nuevas herramientas por parte de los titulares de marca: Visa, MasterCard, American Express, entre otros. Estos servicios los ponen a disposición de sus clientes respectivos, los bancos emisores y los bancos adquirentes que dan el servicio de recepción de pagos con tarjetas a los comercios.

Estos desarrollos tecnológicos permiten brindar mayor seguridad en tus pagos en comercio electrónico, si sigues las recomendaciones de los bancos que te dan estos servicios.

Tal es el caso de servicios como 3D Secure con los que cuentan las tarjetas Visa y MasterCard.

¿Cómo funciona el 3D Secure?

3D Secure es un procedimiento de seguridad que permite una mejor identificación del tarjetahabiente en sus compras en sitios de comercio electrónico. Consiste en el registro de su tarjeta de crédito para poder hacer uso de este servicio. Durante el registro, el Tarjetahabiente genera una contraseña a través de aplicaciones provistas por el emisor de la tarjeta. Dicha contraseña se le solicitará al tarjetahabiente cuando realice compras en sitios de comercio electrónico. Una vez que el

Tarjetahabiente proporciona la contraseña, su banco emisor valida que corresponda con los registros de generación correspondientes.

Este sistema disminuye los fraudes en compras en línea, sin embargo no ha sido de fácil uso para los Tarjetahabientes y friccionaba las compras en comercio electrónico. Por lo anterior, los titulares de marca, han realizado algunas modificaciones al proceso de validación de contraseñas, para hacerlo más amigable y de fácil uso para los tarjetahabientes. Te recomendamos acercarte con tu banco para conocer las mejoras que se han realizado a este servicio.

El sistema de Visa se conoce como "Verified by Visa", mientras que el de MasterCard se conoce como "SecureCode". El funcionamiento y efectividad de ambas herramientas es similar.

El servicio no tiene costo para los tarjetahabientes y es indispensable que el comercio electrónico donde se realice la compra esté afiliado al servicio (a través de su banco adquirente) para poderlo utilizar durante el proceso de pago con tarjeta.

Antes de hacer una compra, deberás registrar tu tarjeta de crédito o débito MasterCard o Visa en la Entidad Financiera que la emitió, para generar su "Secure Code".

Segundo paso

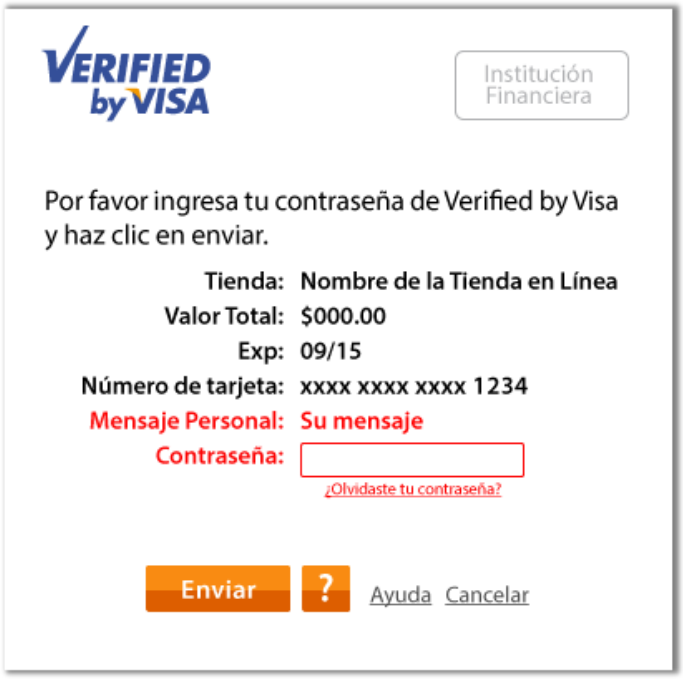
Una vez que realices tu compra y hayas introducido los datos del primer paso de tu tarjeta, al dar clic en "ENVIAR" o "COMPRAR" para concluir el pedido, se abrirá la casilla "Secure Code" de manera automática.

El formato de pedido del comercio en el que realizarás tu compra, solicitará los datos del "Secure Code" (código de Seguridad) que puede ser:

El NIP que usas en el Cajero Automático.

Un código alfa-numérico que es enviado en el momento a tu teléfono celular

Tu número telefónico o algún dato adicional que se encuentre registrado en tu tarjeta.



Referencias:

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2017). Tipos de fraude en el E-commerce. 2018, de CONDUSEF Sitio web: http://www.condusef.gob.mx/gbmx/?p=tipos-de-fraude

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2017). Medidas de seguridad en el E-commerce. 2018, de CONDUSEF Sitio web: http://www.condusef.gob.mx/gbmx/?p=medidas-de-seguridad