El Fraude Electrónico

A medida que el comercio electrónico se desarrolla y crece, el fraude se convierte cada vez más en uno de los obstáculos para su desarrollo en toda la cadena de comercio. El fraude electrónico, se considera un crimen, y es todo acto que infringe la ley y que se realiza violando la seguridad de algún medio de procesamiento electrónico de información. Según el último estudio de Cybersource en el 2009 se estimó que se perdieron US$ 3.3 billones por este concepto sólo en Estados Unidos, aunque las tasas de fraude como porcentaje de las ventas se ha mantenido relativamente constante, según se puede apreciar en la figura 1.

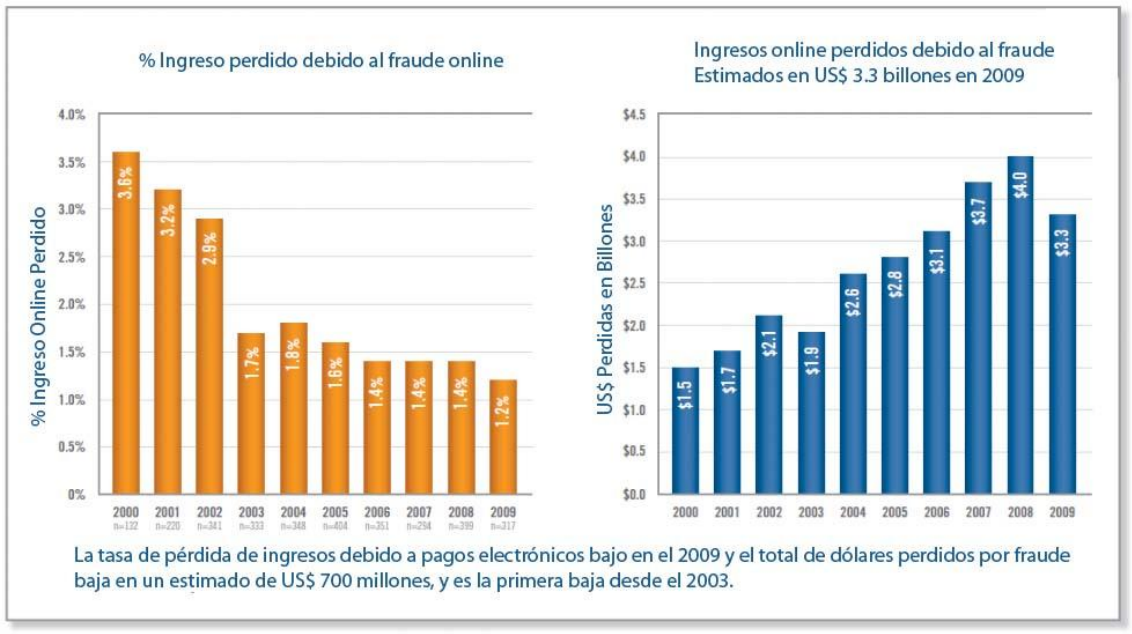

Figura 1: gráficos de fraude como % de ingreso y monto.

Según el último estudio WIP realizado por la Universidad Católica y la Cámara de Comercio de Santiago, en Chile el 3% de los usuarios de Internet que posee tarjetas de crédito declara haber sido víctima de uso fraudulento de la información de su tarjeta de crédito por esta vía, un porcentaje inferior en 2 décimas porcentuales al declarado tres años atrás. Esto indica una tendencia hacia el control de este problema, sin embargo, es necesario trabajar más para reducir las contingencias al mínimo.

Recordemos que los efectos de un fraude son multiplicativos y afectan a toda la cadena de aprovisionamiento en Internet. Con respecto a las operaciones bancarias, sólo el 1% de los usuarios e-banking manifiesta haber sido víctima de algún fraude al realizar operaciones con su Banco, un porcentaje muy menor, sin embargo es preocupante y es justamente en donde las entidades financieras deberán poner énfasis para reducir esto a cero en el corto plazo. A pesar de los números anteriores y pese a que muy pocos encuestados declaran haber sido víctimas de fraude online, persiste un fuerte temor al enfrentarse a los medios de pago y las operaciones online.

Debido a lo anterior la gestión de fraude en línea sigue siendo un costo considerable y creciente para los comercios de todos los tamaños. Los que enfrentan acciones ligadas a la detección, prevención y manejo de fraude en línea.

Hoy los comercios han centrado sus esfuerzos en la conversión de las ventas y la reducción de las tasas para el rechazo, debido a la sospecha de fraude. Otros resultados del estudio indican que muchos comerciantes han conseguido aumentar su tasa de aceptación de la orden con poco o ningún aumento en las tasas de fraude. Situación que permite impulsar el círculo virtuoso del comercio.

Tipos de fraude electrónico

1. Phishing: se conoce como "Phishing" a la estafa o fraude que utiliza medios electrónicos con el objetivo de suplantar la identidad. Gracias a esta práctica, el estafador puede obtener información privilegiada, como datos bancarios o contraseñas, entre otros. Etimológicamente, el término Phishing procede del inglés "fishing", que significa "pesca". Se entiende que el delincuente "pesca" a un usuario mediante engaños para obtener su información. La persona que practica Phishing es conocida como *phisher*. El Phishing es una práctica englobada en el movimiento conocido como Ingeniería Social. En el ámbito informático, la Ingeniería Social es un concepto que se refiere a obtener información confidencial recurriendo al engaño del usuario del sistema de cómputo. En general los bancos son blanco de las estafas más recurrentes, hoy en día hay varias que apuntan a cuentas de Facebook y otros servicios.

2. El Pharming: modifica los mecanismos de resolución de nombres sobre los que el usuario accede a las diferentes páginas web tecleando la dirección en su navegador. Esta modificación provoca que cuando el usuario introduce en el navegador la dirección del sitio web legítimo, automáticamente es dirigido hacia una página web fraudulenta, este caso de fraude es el más difícil de detectar, porque para el usuario la interfaz es la misma. En la figura 2 se muestra una de las advertencias de Banco Itaú para alertar de una posible estafa de este tipo.

Figura 2: Alerta de pharming banco Itaú

3. SMiShing: en este caso el gancho es un mensaje SMS utilizado para el engaño y su funcionamiento es similar al del Phishing. Aprovecha las funcionalidades de navegación web de los terminales de telefonía móvil para que el usuario acceda de manera inmediata a la página web falsa y proporcione allí sus datos.

4. **El Scam:** utiliza también el correo electrónico para la divulgación de la página web falsa, pero el contenido del mensaje no intenta suplantar a ningún tercero sino que ofrece cantidades de dinero a conseguir fácilmente después de proporcionar cierta información personal y/o bancaria.

5. Spam: el Spam es una estrategia que consiste en enviar correos electrónicos sin la autorización previa del destinatario. A estos correos se les conoce también como "correos no deseados" o "correos basura". El Spam se realiza con fines publicitarios o de ingeniería social y en muchos países está penado por la ley. El envío masivo de correos basura es la estrategia utilizada por los phishers para propagar sus falsos mensajes. Los mensajes enviados son amigables y atractivos para conseguir que el usuario los lea y acceda a sus contenidos. Las empresas hoy se encuentran reemplazando el Spam por el permission marketing, de manera de asegurar los envíos a sus clientes o potenciales clientes.

6. Fraude telefónico o vishing: en los fraudes de vishing, los estafadores envían correos electrónicos falsos en los que se les pide a los clientes que llamen a un número de teléfono. El número de teléfono puede diferenciarse de un número de teléfono verdadero de alguna compañía por sólo un dígito o puede ser completamente diferente. En cualquiera de los dos casos, los estafadores esperan agarrar desprevenido a un cliente de esta compañía enfatizando, por lo general, la urgencia en el texto del correo electrónico. Si el cliente marca el número de teléfono, se le solicitará que ingrese su información confidencial a través de la marcación de los dígitos del teléfono o por voz. La información se recopila a fin de utilizarla para actividades fraudulentas.

7. Cartas Nigerianas: el usuario recibe un correo electrónico donde le ofrecen el acceso a una gran suma de dinero, previo pago de un anticipo que el timador justifica bajo la necesidad de liberar una fortuna en alguna divisa extranjera o país en conflicto, y ofrece una pequeña parte de la misma una vez haya sido liberada.

8. Estafa Piramidal: Normalmente llega a través de un correo electrónico que ofrece un trabajo basado en la promoción de productos y en la captación de nuevos empleados. Al contactar con la presunta empresa, nos comunican que los nuevos miembros deben abonar una tasa de iniciación. Una vez incluidos en la organización, se descubre que los beneficios obtenidos no vienen tanto por la venta o promoción de los productos sino por la captación de nuevos miembros.

9. **Mulas**: un correo electrónico ofrece al usuario la posibilidad de quedarse con un porcentaje de una transacción electrónica por el simple hecho de realizar otra transferencia del importe recibido, menos la comisión acordada, a otra cuenta que se le indica. Este caso no sólo se corresponde con un fraude, sino que además la persona se convierte en colaborador de un delito de blanqueo de dinero.

Hoy en día 9 de cada 10 correos electrónicos enviados son fraudulentos o "spam". Los ataques de phishing, los correos electrónicos falsos y las formas de fraude online están aumentando a tasas del orden del 20% mensual. Mensualmente se crean 60.000 nuevos sitios web fraudulentos y 35.000 campañas de phishing.

Un 78% de los ataques incluye un componente financiero. Los ciberdelitos podrían incluso superar los ingresos del tráfico de drogas internacional. Las tarjetas de crédito son el objetivo principal: 32% de los casos.

La información de cuentas bancarias representan el 19% de todos los bienes anunciados para su venta.

Algunos actores de la organización y división del trabajo en el crimen Cibernético

- "Spammers" envían los correos electrónicos de phishing
- “ScriptKidders”: Crackers jóvenes e inexpertos que recopilan equipos víctima (denominados "roots“ y zombies) para realizar sus ataques o estafas.
- Diseñadores web: crean sitios web malintencionados
- “CashOuts”: Responsables de retirar fondos de una tarjeta de crédito o una cuenta bancaria
- "Droppers": una especie de repartidores, se encargan de recibir los artículos comprados.

Qué es lo que intercambian las organizaciones de delitos informáticos

- Números de tarjetas de crédito: incluido el CVV2 (número verificador de tres dígitos que se encuentra en la parte posterior de la tarjeta)
- Acceso administrador de los servidores: estos servidores pirateados, se utilizan para alojar sitios web de phishing u otros fraudes.
- Listas de emails: para el envío de spam y para buscar víctimas de estafas.
- Cuentas en línea: cuentas de servicios de pago en línea, como e-gold y WMZ.
- Cuentas de Western Union: para enviar fondos.

No se puede eliminar a los delincuentes, pero se les puede poner mayores obstáculos para mitigar el riesgo. El fraude no desaparece, pero migra a los lugares de menor resistencia por lo tanto es necesario preparase, protegerse, aprendiendo y educando a los usuarios.

Los usuarios, al menos tienen que desconfiar de todo lo que llegue por correo, tener los últimos parches y actualizaciones del sistema operativo y del navegador de Internet. Mantener las contraseñas seguras y a salvo, usar algún software de seguridad como Firewall y Antivirus. Revisar los estados bancarios regularmente, proteger la información personal, sobre todo de aquellas ofertas que parecen demasiado buenas para ser ciertas, porque normalmente no lo son.

Los comerciantes deben conocer bien su negocio y a sus clientes, ponerse en contacto con ellos cuando sea posible, utilizar sistemas de autenticación de la transacción, para esto se pueden monitorear y analizar los patrones de la operación, como el país de emisión de la tarjeta, el origen de la compra, el IP del lugar de entrega, modificaciones sospechosas, cambios de tarjeta, teléfonos, direcciones, mails. Así como análisis del producto y la fecha de entrega que podrían generar algunas ventas inusuales. Para todo esto existen herramientas automáticas de monitoreo y alertas.

Ejemplo de un Fraude en línea en España

En una cuenta de email, se recibe un correo simulando provenir del Banco Santander de España (Figura 3), pudiendo o no la persona tener cuenta en ese banco. El asunto de correo es: *"Banco Santander! Activación de la cuenta!"* e incluye links hacia una página fraudulenta que imita el diseño de la página real. El objetivo de los ciberdelincuentes es obtener información de acceso a las cuentas para robar el dinero.

Figura 3: Captura del correo

Dependiendo de la estafa, muchas veces el diseño está muy bien logrado y es una réplica casi perfecta del sitio original. Si sólo es phishing en la barra de navegación aparecerá otra dirección diferente al sitio oficial del banco, en algunos casos son muy parecidas.

.

Figura 4: Captura de página fraudulenta

Los usuarios que caen en la trampa del correo y completan este formulario verán un mensaje que advierte un error durante el proceso de acceso, a su vez y sin que ellos lo detecten la información ingresada es enviada a los estafadores.

El sitio debe ser denunciado y algunos navegadores como FireFox y Explorer ya han incorporado advertencias sobre sitios fraudulentos al ingresar a ellos.

Dada la naturaleza de estas estafas, los bancos han tomado cartas en el asunto y han agregado numerosas advertencias para comunicar a los usuarios sobre los e-mails fraudulentos y además

proporciona algunas recomendaciones de seguridad que también pueden ser aplicadas para cualquier otra institución financiera:

- Su usuario, contraseña, pin de tarjeta, firma, etc. son datos de carácter personal y estrictamente confidenciales, solo deben ser usados para el acceso a los servicios propios de Santander.

- Desconfíe de cualquier toma de datos personales realizada a través de Internet, en nombre de Santander, y **fuera de su sitio web seguro**. Ante cualquier duda de la veracidad de los datos pedidos o autenticidad de las páginas visitadas, rogamos contacten de manera inmediata con Santander por los canales establecidos. Ninguna Empresa del Grupo Santander le requerirá información que ya deba estar en su poder.

- No dé nunca información personal o financiera en respuesta a un e-mail.

- No utilice los enlaces incorporados en e-mails o páginas Web de terceros.

Conclusiones

A partir de la creciente demanda del comercio electrónico, se han generado un gran número de formas de fraude electrónico, un gran número de nuevas presentaciones en las que los estafadores logran aprovecharse de los incautos compradores, y más aún de los que no conocen un solo método para poder protegerse contra estos timadores.

Mientras mayor es el número de servicios que diferentes instituciones ofrecen sobre Internet, cada vez el fraude y los delitos aumentarán en complejidad. Estos son otra representación de la realidad en el mundo virtual, los robos, estafas y otros. Como usuarios tenemos que asimilar que para lo mismo que nos protegemos en el mundo real, tenemos que hacerlo en Internet.

Referencias

1. Cisneros, Héctor. “Análisis de los distintos métodos de seguridad para evitar el fraude en los pagos que se realizan en los sitios de comercio electrónico.”, Instituto tecnológico de Durango, México.

2. Cybersource, “Online Fraud Report”, 11th Annual edition 2010.

3. CENTRO DE ESTUDIOS DE LA ECONOMÍA DIGITAL, “La economía digital en Chile”, Edición 2009.

4. Phishing del Banco Santander, http://blog.segu-info.com.ar/2008/03/phishing-del-banco-santander.html#axzz1LXkhw1gs. 4 de marzo 2008, accedido 6 de mayor de 2011.