BANCOPIANO

CANALES ELECTRÓNICOS

FRAUDES ELECTRÓNICOS: VISHING, SKIMMING, SMISHING

DICIEMBRE 2019

FRAUDES ELECTRÓNICOS

DEFINICIÓN
Es importante que conozcamos cuales son las amenazas y el fraude electrónico y como debemos protegernos.
El fraude electrónico no es más que es una manera de estafar a las personas a través de Internet o cualquier medio electrónico, con la finalidad de obtener información confidencial, especialmente de cuentas e instituciones bancarias.
Los delincuentes utilizan diferentes técnicas informáticas para atacar a los usuarios de los bancos. Lo que buscan es obtener los datos de las personas, ya sea información personal, de sus productos financieros (qué tarjetas de crédito tiene asociadas) o información de seguridad de sus cuentas (usuario y contraseñas de acceso).
Distintos tipos de amenazas y el medio en que podemos recibirlos:
Ingenieria social, phishing, ransomware, vishing, skimming, smishing, spyware, admare, malware, etc.

VISHING | SKIMMING | SMISHING

Es importante estar informados sobre los tipos de fraudes electrónicos más comunes y peligrosos para evitar caer en el engaño.

Vishing: El término deriva de la unión de dos palabras: “voice” (voz) y “phishing” (pesca), y se refiere al tipo de amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet. Por lo general, la víctima recibe una llamada con un mensaje de voz disfrazado como una comunicación de una institución financiera, donde se solicita que llame a un número e ingrese la información de su cuenta o PIN por razones de seguridad u otros fines oficiales, y cuando la víctima llama quien atiende es el ciberdelincuente.

Skimming: Se denomina de esta manera al robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc).

Smishing: Es una práctica en la que los delincuentes hacen uso de los mensajes de texto de los celulares y la ingeniería social para engañar a las personas y obtener información financiera para el robo de identidad. A través de envíos de mensajes SMS al celular intentan convencer a la víctima para que visite una web fraudulenta bajo alguna excusa con el objetivo final de obtener claves de usuario o información personal.

¿Cómo ocurre el vishing?
El cliente recibe una llamada telefónica donde le comunican que se realizó una compra extraña con la tarjeta de crédito, o con la excusa que se encuentran realizando una campaña para la que se requiere la actualización de la base de datos o registros para sorteos. Seguido a esto, los ciberdelincuentes solicitan algunos datos personales o bancarios, como por ejemplo: DNI, número de tarjeta de crédito, fecha de vencimiento, titular de la tarjeta.

Los delincuentes, normalmente, falsifican el origen de la llamada mediante la técnica “Caller ID Spoofing”, que permite a una persona hacerse pasar por otra, adulterando el número que aparece en la pantalla del identificador de llamadas del destinatario.

¿Cómo ocurre el skimming?
Los clonados de tarjeta se producen con un pequeño aparato llamado skimmer de bolsillo. El delincuente puede esconder este pequeño aparato en su pantalón y utilizarlo tras un mostrador o mientras camina hacia la caja al esconderlo en la mano cuando se le entrega la tarjeta pensando que se está solo abonando el consumo. El skimmer es un aparato que utiliza la tecnología usada por los cajeros automáticos para leer la banda magnética de las tarjetas. En este caso se realiza la lectura pasándola por una pequeña ranura y los datos quedan almacenados para transferirlos posteriormente a una PC. También se pueden copiar los datos al pasar la tarjeta por un cajero que haya sido manipulado para esconder el skimmer o si perdemos o nos roban la tarjeta.

¿Cómo ocurre el smishing?
Mediante el smishing los ciberdelincuentes envían un mensaje de texto o de whastapp sobre usos indebidos o compras sospechosas con la tarjeta de crédito. Por lo general, el texto brinda un número falso al que el cliente se debe comunicar para cancelar la compra y, de esa manera, es interrogado sobre su información personal.
Otra posibilidad, es que los mensajes contienen acceso a páginas webs fraudulentas que solicitan datos confidenciales como números de tarjeta de crédito, DNI, contraseña de banca por internet e incluso el código CVV, con el cual los delincuentes pueden realizar compras en línea.

Consejos que pueden ayudarlo a evitar ser víctima de este tipo de ataques:
VISHING
Nunca debe revelar datos como por ejemplo: DNI, número de tarjeta de crédito, fecha de vencimiento, titular de la tarjeta a nadie porque son la llave para autorizar las transacciones. Si recibe algún llamado con estar características debe colgar de inmediato y ponerse en contacto con el banco para denunciar lo sucedido El banco no se contactará por ninguna vía para solicitar información sensible y confidencial.

SMISHING
No hacerle caso a los mensajes que solicitan realizar una llamada, una operación, o brindar datos. No proporcionar datos sobre tarjetas de crédito y similares a través de SMS aunque parezca provenir desde una entidad bancaria confiable. Hay que poner especial atención a los números sospechosos y recordar que el único número de la banca por teléfono de la Entidad es el que figura en la página web del banco.

SKIMMING
Al introducir la tarjeta en algún cajero automático, verifique que no posea algún tipo de elemento extraño. No pierda de vista la tarjeta en el momento de llevar a cabo una transacción. Exija que la transacción en la máquina lectora se haga en presencia tuya. Si su tarjeta es pasada más de una vez por la máquina lectora, exija la destrucción del comprobante y la cancelación de la operación anterior.

BANCOPIANO

CANALES ELECTRÓNICOS

FRAUDES ELECTRÓNICOS: PHISHING

SEPTIEMBRE 2019

FRAUDES ELECTRÓNICOS - DEFINICIÓN

Es importante que conozcamos cuales son las amenazas y el fraude electrónico y como debemos protegernos.
El fraude electrónico no es más que es una manera de estafar a las personas a través de Internet o cualquier medio electrónico, con la finalidad de obtener información confidencial, especialmente de cuentas e instituciones bancarias.
Los delincuentes utilizan diferentes técnicas informáticas para atacar a los usuarios de los bancos. Lo que buscan es obtener los datos de las personas, ya sea información personal, de sus productos financieros (qué tarjetas de crédito tiene asociadas) o información de seguridad de sus cuentas (usuario y contraseñas de acceso).
Distintos tipos de amenazas y el medio en que podemos recibirlos:
Ingeniería social, phishing, ransomware, vishing, skimming, smishing, spyware, admare, malware, etc.

PHISHING

Es importante estar informados sobre los tipos de fraudes electrónicos más comunes y peligrosos para evitar caer en el engaño.
El ‘phishing’’ es un método fraudulento mediante el cual se busca conseguir información privada como contraseñas o información de tarjetas de crédito a los clientes de un banco.
El ataque de ‘phishing’ viene por medio de un correo electrónico en el que se pide al cliente sus datos de cuenta y clave de acceso, simulando la página legítima de la entidad para que los usuarios brinden claves personales o información sobre tarjetas de crédito.

El estafador se hace pasar por representante de una entidad bancaria, intenta persuadir a los clientes para que envíen sus datos a través de correo electrónico (‘phishing’) es una de las técnicas que más han proliferado en el mundo de la ciberdelincuencia. ¿Cómo ocurre el phishing?
En cualquier momento el cliente puede recibir un correo electrónico de su entidad bancaria explicando que por razones de seguridad, mantenimiento, mejora del servicio, confirmación de identidad, advertencia de fraude o cualquier otro motivo, el cliente debe actualizar los datos de su cuenta.
El correo de fraude también puede decir que se bloqueará la cuenta si no se actualiza la información en un período de tiempo determinado. Por lo general, dichos correos imitan el diseño (logotipo, firma, etc.) que utiliza el banco para comunicarse regularmente con el cliente. El mensaje puede tener un formulario para enviar los datos, aunque lo más habitual es que incluya un enlace a una página para actualizarlos allí y de esa manera capturarlos para cometer fraude.

El objetivo es robar nuestros datos bancarios. Proveer información es como darles a los estafadores la llave de nuestra cuenta bancaria.

Consejos que pueden ayudarte a evitar ser víctima de este tipo de ataques:

- No responder nunca los correos electrónicos que soliciten dinero, envíos de giros, datos bancarios, contraseñas o datos de tarjetas de crédito.
- No hacer clic en los enlaces de estos mensajes. Si cree que el mensaje puede ser verdadero y que proviene, por ejemplo, de su banco, ingrese al sitio web de la institución escribiendo la dirección directamente en la barra del navegador, para evitar ingresar en alguna página web realizada por el atacante.
- En caso de recibir mensajes de promociones de alguna tienda o comercio, se debe corroborar siempre con la entidad y verificar llamando a los números oficiales establecidos por ésta.
- No responder mensajes sospechosos o de remitentes desconocidos.
- Si se recibe una llamada que provenga supuestamente de Banco Piano, verificar la legitimidad de la misma. Si no es así, reportar el caso al ejecutivo de cuentas.
- No revelar a un tercero, ni por mensajes ni por correo electrónico, claves de ningún tipo como pin, contraseñas, nombres completos, número de documento.
- Las compañías, entidades bancarias u operadores de tarjeta no solicitan información personal a sus clientes o verificación de sus cuentas vía e-mail.
- Si se recibe un correo electrónico que provenga supuestamente de Banco Piano, verificar la legitimidad del mismo observando la dirección que aparece como remitente. Debe corresponder siempre al dominio @piano.com.ar. Si no es así, reportar el caso al ejecutivo de cuentas enviando el 'mail' original y luego eliminándolo.
- No acceder a Banco Piano a través de enlaces recibidos vía correo electrónico o sitios desconocidos o sospechosos. Para acceder de manera segura, la recomendación es que lo hagas a través del sitio institucional al cual se accede escribiendo https://www.bancopiano.com.ar .
- En el navegador se puede verificar y confirmar que se está en el sitio seguro de Banco Piano observando que la barra de dirección tiene un candado y la identificación del Banco.
- No ingresar el usuario y clave de Banca Online sin haber verificado la autenticidad del sitio accedido.
- Evitar acceder a Banca Online desde lugares públicos, tales como: cibercafés, accesos públicos a WiFi o desde cualquier lugar que se considere de riesgo.

BANCO PIANO	**RED LINK**
0810-122-2770	**(011) 4319 – LINK**
info@piano.com.ar	**(5465)**

BANCOPIANO

CANALES ELECTRÓNICOS

FRAUDES ELECTRÓNICOS: INGENIERÍA SOCIAL

DEFINICIÓN

Es importante que conozcamos cuales son las amenazas y el fraude electrónico y como debemos protegernos.
El fraude electrónico no es más que es una manera de estafar a las personas a través de Internet o cualquier medio electrónico, con la finalidad de obtener información confidencial, especialmente de cuentas e instituciones bancarias.
Los delincuentes utilizan diferentes técnicas informáticas para atacar a los usuarios de los bancos. Lo que buscan es obtener los datos de las personas, ya sea información personal, de sus productos financieros (qué tarjetas de crédito tiene asociadas) o información de seguridad de sus cuentas (usuario y contraseñas de acceso). Distintos tipos de amenazas y el medio en que podemos recibirlos:
Ingeniería social, phishing, ransomware, vishing, skimming, smishing, spyware, admare, malware, etc.

INGENIERÍA SOCIAL

La ingeniería social es una acción destinada a conseguir información de terceros a través de prácticas y técnicas relacionadas con la comunicación. Esto es, aprovecharse mediante engaños, y artimañas de la persona para lograr que esta nos brinde información voluntariamente.

Los ingenieros sociales son expertos en la técnica y ciencia de manipular a la gente haciéndola proveer información sensible como direcciones, teléfonos, números de tarjetas, etc. a través de la construcción de relaciones y aprovechando la tendencia natural de la gente a confiar y ser útil.

Medios: Celulares, Teléfonos, Internet (Phishing, Redes Sociales, etc.), Persona a Persona.

Objetivo: Obtener información suficiente que permita perpetrar un fraude en nombre de terceros.

Tipo de Fraudes: Usurpación de Identidad, Uso de cuentas de terceros, Secuestros virtuales, Uso de tarjetas de terceros, y cualquier tipo de manipulación de la persona para obtener un determinado fin.

Aquí hay algunos de los trucos que emplean habitualmente:

Llamar para decir que has ganado un premio o una suma en efectivo. Solo deberías pagar por el “envío” o un “gasto administrativo”.

Decir que son de tu compañía de Tarjetas de Crédito y pedirte que confirmes tus datos.

Decir que son de otra compañía de Tarjetas de Crédito, te prometen una oferta especial o tasas de interés bajas si transferís el saldo de tu tarjeta a esa compañía.; para hacer esto necesitan tu número.

Decir que representa a un importante centro de beneficencia y pedir por una donación. Este tipo de fraude es a menudo cínicamente empleado en las repercusiones de grandes desastres tales como el tsunami o el fenómeno del niño. También es con frecuencia llevado a cabo vía correo electrónico.

La forma más eficaz de protegerte frente a estas amenazas es mantenerte informado: saber cuáles son los peligros, qué se debe evitar y con qué hay que tener cuidado.

Consejos que pueden ayudarte a identificar las estrategias usadas en la ingeniería social y por tanto a evitar ser víctima de este tipo de ataques:

Nunca reveles por teléfono o e-mail datos confidenciales (como claves de acceso, números de Tarjetas de Crédito, cuentas bancarias, etc.).

Nunca hagas click en un enlace a una página web que te llegue a través de un e-mail en el que te piden datos personales.

Desconfié de cualquier mensaje de e-mail en el que se te ofrezca la posibilidad de ganar dinero con facilidad.

Si sos usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web datos de acceso, asegúrate de que la dirección de la web es correcta.

No confíes en las direcciones de los remitentes de e-mail o en los identificadores del número llamante en el teléfono: pueden falsearse con suma facilidad.

Utiliza el sentido común y pregúntate siempre que recibas un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que te solicitan.

Se puede prevenir que tales planes tengan éxito si se sigue una regla muy simple. Nunca se debe dar información personal a alguien que llame salvo se verifique 100% la identidad de la persona.