MEDIDAS DE SEGURIDAD PARA OPERAR SEGURO EN LA WEB

American Express nunca solicita datos confidenciales de usuario, claves o números de Tarjeta por correo electrónico o en ventanas emergentes (pop-ups) en Internet. Nunca ingrese su clave en un lugar que no sea la Página Web de American Express.

Para consultas telefónicas, conozca los números de contacto telefónico haciendo click aquí.

¿QUÉ HACER ANTE UN CORREO FRAUDULENTO?

En caso de recibir un mensaje que le resulte sospechoso, no haga clic en sus vínculos. Si lo hizo, cierre la página lo antes posible. Ante la duda, no ingrese datos personales. Infórmenos de inmediato, llamando a los números de teléfono disponibles haciendo click aquí, para que podamos prevenir un posible fraude. Puede reportar cualquier caso las 24 horas del día, los siete días de la semana.

¿QUÉ DEBE HACER SI HA MANIFESTADO INFORMACIÓN SENSIBLE A TRAVÉS DEL TELÉFONO A UNA PARTE SOSPECHOSA?

Si usted ya ha respondido a una llamada sospechosa con la información de su cuenta de American Express y cree que es fraudulento, por favor póngase en contacto con American Express de inmediato reportando su caso a través de los números de teléfono que figuran en nuestra página de contacto.

¿CUÁLES SON LOS CASOS MÁS COMUNES DE FRAUDE?

ROBO DE IDENTIDAD: El robo de identidad ocurre cuando alguien utiliza su nombre o información personal, como su número de DNI, número de licencia de conducir, número de Tarjeta de Crédito, número de teléfono y otros números de cuenta, sin su permiso. Los estafadores utilizan esta información para abrir cuentas de Crédito, cuentas bancarias, cuentas de servicios telefónicos, y hacer compras importantes, todo en su nombre.

PHISING: consiste en recibir un correo electrónico no solicitado en nombre de una institución financiera u otra empresa. Estos mensajes piden al usuario que haga clic en un link que conduce a una página que imita a la real, en la que se pide al Socio que ingrese nombre de usuario y clave. En general, estos e-mails fraudulentos mencionan algunas consecuencias para quienes ignoren el mensaje (bloqueo de fondos, cargos extra, etc.). Recuerde que American Express nunca le solicitará por email sus datos personales ni números de su Tarjeta.

SPOOFING: son empresas que se hacen pasar por empresas verdaderas. Estos e-mails engañan a los Socios y lo fomentan a responder, o a hacer clic en un enlace que direcciona una página web fraudulenta que le pedirá información personal, como su número de tarjeta de Crédito, número de Seguro Social o contraseña de la cuenta. También puede estar constituido por llamadas telefónicas o ventanas emergentes (pop-ups) que dirigen al usuario a un sitio falso.

Estos correos electrónicos fraudulentos a menudo son difíciles de identificar, pero American Express le recomienda algunos tips para darse cuenta si usted se encuentra frente a uno de estos casos:

E-MAIL SALUDOS: American Express recomienda a sus Socios, siempre desconfiar de los e-mails que le piden datos de su cuenta y que no lo saludan por su nombre. Si bien no es imposible, es más difícil

y costoso para los phishers asociar una dirección de correo electrónico con el nombre del propietario. Debido a esto, los phishing e-mails más a menudo se abordan de forma genérica como "Estimado Socio". American Express jamás solicita información confidencial o datos personales por email.

ENLACES EN CORREOS ELECTRÓNICOS: Casi todos los e-mails comerciales de hoy contienen un "vínculo a un sitio web", o la dirección web (URL). American Express utiliza enlaces en sus comunicaciones online para ayudar a sus Socios a encontrar fácilmente la información que están buscando. Los phishers también utilizan enlaces para atraer a Socios a "falsas páginas web" o sitios web "simulados". American Express le recomienda que si usted sospecha de un email, no haga clic en ningún enlace del mismo. Busque las señales de advertencia descritas anteriormente (saludos genéricos, sentido de urgencia, nombre del enlace). PHISING TELÉFONO (TAMBIÉN LLAMADO "VISHING"): Es otra forma por la cual los estafadores tratan de recopilar información confidencial de usted. En este tipo de fraude, se contactan con usted por teléfono o por email y le piden que por favor se comunique por teléfono. American Express le recomienda que si alguna vez sospecha que no es American Express quién se ha puesto en contacto con usted, se comunique de inmediato al teléfono que está en el dorso de su Tarjeta. Le pedirán que ingrese su número de Tarjeta y le harán algunas preguntas acerca de su fecha de cumpleaños, domicilio de facturación y últimas compras realizadas, entre otras.

DUMPSTER BUCEO: se produce cuando los estafadores buscan entre sus residuos papeles que pueden servirles para realizar algún tipo de fraude. La gente suele tirar a la basura facturas de servicios públicos, y otros tipos de correspondencia. Por lo general, estos archivos contienen su nombre, dirección y, a veces, los números de cuenta. Los estafadores pueden utilizar esta información para acceder a las cuentas existentes o crear y abrir otras nuevas. American Express le recomienda destruir todos los documentos que contengan información confidencial antes de arrojarlos a la basura.

AMERICAN EXPRESS LE RECOMIENDA CONSEJOS PARA GARANTIZAR SU SEGURIDAD:

ELIJA SU PROPIO NOMBRE DE USUARIO Y CONTRASEÑA: Cuando usted se registra en Servicios Online, para acceder a su cuenta desde nuestra página Web, American Express le permite crear su propio nombre de usuario y contraseña. Esta información es cifrada durante la transmisión con tecnología de 128 bits de encriptación. Una vez que ya está registrado, para iniciar sesión sólo necesita ingresar su nombre de usuario y contraseña. No le solicitaremos su número de Tarjeta.

SITIO WEB SEGURO PARA MANTENIMIENTO DE SU CUENTA: American Express utiliza 128-bit Secure Sockets Layer (SSL). Esto significa que cuando usted está en nuestro Sitio Web, los datos transferidos no podrán ser vistos en ninguna otra parte.
El ícono del candado que aparece en la parte inferior de los navegadores indica que un Sitio es seguro. La dirección, a su vez, debe comenzar con https://.

TIEMPO DE ESPERA: Luego de 10 minutos de inactividad, la sesión de su cuenta terminará automáticamente. Para continuar utilizando el sistema en línea, usted tendrá que volver a introducir su nombre de usuario y contraseña.

RECOMENDACIONES EN EL USO DE CLAVES:

• Utilice claves diferentes en todos los servicios.

• Cambie sus claves periódicamente.

• Evite claves que sean fácilmente identificables como fechas de nacimiento, teléfonos, su documento de identidad o nombres de familiares.

• Nunca revele las claves por ningún motivo.

• No anote sus claves, se recomienda memorizarlas.

• Asegúrese de no ser observado al ingresar la clave.

• Desconéctese de la sesión antes de dejar el equipo.

• Nunca modifique su clave desde locutorios o PC ajenas.

• No utilice el servicio desde locutorios o PC ajenas: pueden existir programas o dispositivos para capturar sus datos confidenciales.

• Evite compartir su computadora o acceder a nuestro portal desde máquinas de uso público. No envíe información sobre sus cuentas por correo electrónico.

• Al recibir correo electrónico recomendamos abrir solamente los de procedencia conocida y tener especial cuidado con los archivos adjuntos (incluso de procedencia conocida), ya que pueden contener virus o troyanos. American Express no envía emails con adjuntos.