Guía para la Prevención del Fraude en Pagos | HSBC

Protege a tu empresa del fraude y del cibercrimen

HSBC

Fraude y estafas en pagos: protege a tu empresa

Actualmente, el fraude es una de las amenazas más comunes para las empresas

El fraude en pagos puede generar un impacto financiero negativo para las empresas, sin importar el tamaño de las mismas. Por tal motivo, se diseñó esta guía para proporcionar a tu equipo las herramientas necesarias para detectar tempranamente los intentos de fraude o de estafas, o bien tomar las acciones adecuadas en caso de ya haber sido víctima de los defraudadores.

USD $10.2bn

Costo global de estafas tipo Business Email Compromise (BEC) en 2022

Fuente: FBI Internet Crime Complaint Centre

Esta guía te ayudará a conocer algunas de las tipologías de fraude y estafas más comunes que podrían impactar a tu empresa. Así mismo, te proporcionará algunas medidas que puedes tomar para prevenir que tu empresa sea víctima de los defraudadores.

La educación y concientización de este tema por parte de todos los empleados dentro de una empresa permite tener una mejor protección para la misma. Esta guía además te proporcionará una serie de consejos que pueden compartirse entre tus equipos administrativos y aquellos que realicen pagos.

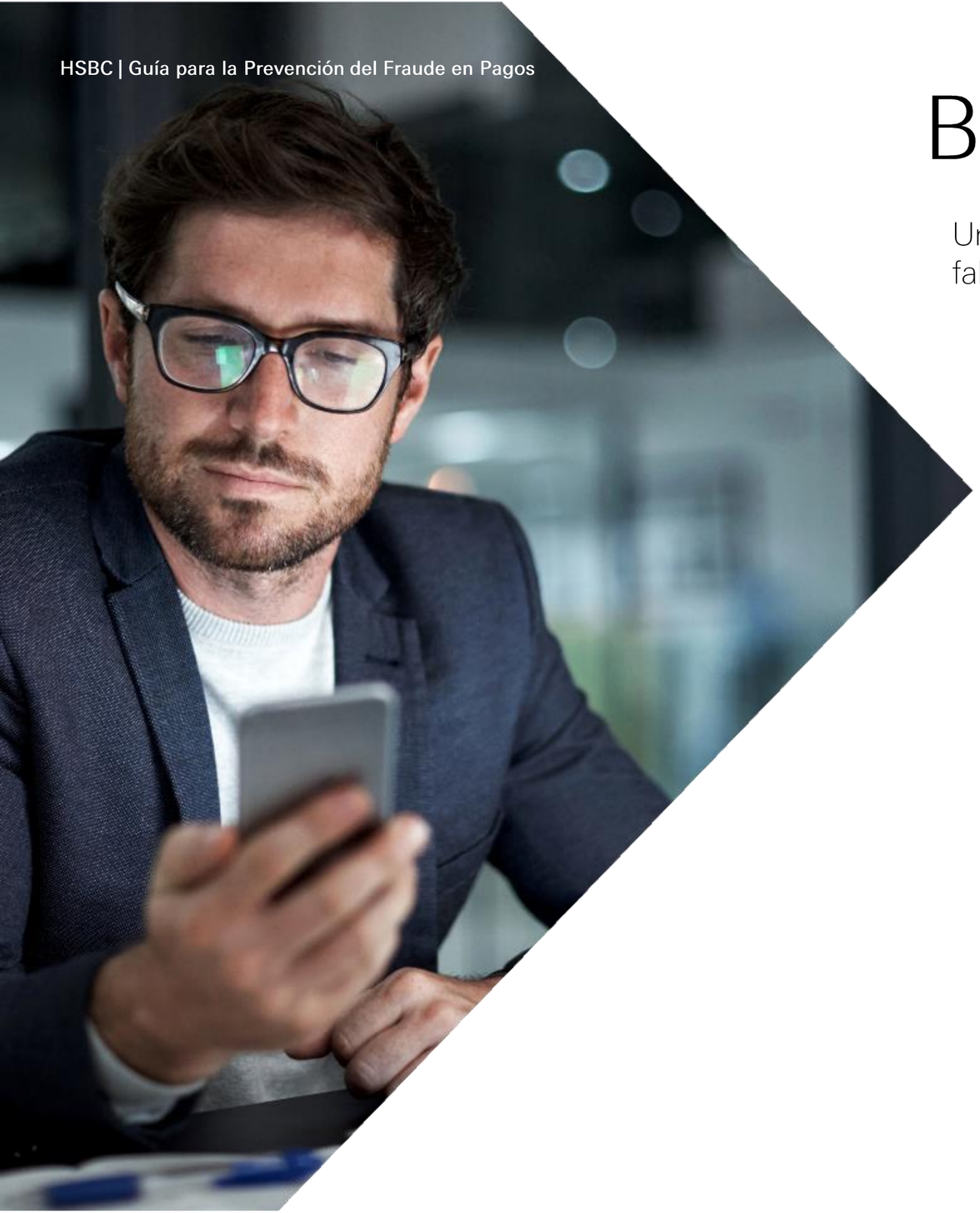
Tipos de fraude y estafas en pagos que podrían impactar a tu empresa

HSBC

Cómo podría contactarte un defraudador

- Las estafas Authorised Push Payment (APP) ocurren cuando una empresa es engañada para enviar dinero a un estafador que se presenta como un beneficiario genuino. Es importante entender cómo pueden ponerse en contacto los criminales contigo
- El Phishing es un componente común en muchas estafas APP. Se trata de los intentos de los defraudadores de engañar a los usuarios para que hagan clic en un enlace que, por ejemplo, descargará malware (software malicioso) o los dirigirá a un sitio web falso.
- Vishing - Si recibes una llamada telefónica inesperada solicitando dinero, existe una alta probabilidad de que se trate de una estafa. Los estafadores pueden hacerse pasar por una empresa o Autoridad reconocida en la que se confía (como algún banco o incluso la Policía). Puede que sepan detalles personales sobre ti o tu empresa e incluso pueden hacer que su número telefónico parezca auténtico utilizando una técnica llamada “suplantación de números” o “number spoofing”, en inglés.
- El Smishing se trata de una técnica a través de la cual los estafadores envían mensajes de texto falsos fingiendo ser tu banco u otra organización legítima. Su objetivo es hacerte responder con tus datos personales o financieros para que posteriormente puedan robar dinero de tu cuenta. Así mismo, el defraudador puede utilizar plataformas de mensajería comunes.

HSBC



Business Email Compromise

Una herramienta comúnmente utilizada por los estafadores es el envío de correos falsos:

Cuando tu empresa está a punto de realizar pagos a proveedores, es común que los delincuentes envíen correos electrónicos diseñados para aparentar ser un mensaje genuino de alguno de tus proveedores. A menudo, dentro del correo se indica que los datos bancarios del pago han cambiado, proporcionan nuevos datos bancarios y, finalmente, envían una solicitud de pago.

Estos correos electrónicos llegan a ser difíciles de detectar principalmente debido a que:

- Los atacantes en ocasiones usan la dirección de correo electrónico auténtica del proveedor, o una dirección de correo electrónico falsa que parece ser la dirección legítima;
- Las facturas pueden parecer auténticas;
- Puede que no haya diferencias perceptibles en la firma de correo electrónico del empleado de tu proveedor;
- El atacante tendrá acceso a la cadena de correo electrónico y podrá responder usando un lenguaje y tono similares;
- Tal vez lo más importante es que a menudo el pago que el defraudador solicita lo tienes pendiente con alguno de tus proveedores;
- Frecuentemente, la única diferencia es que los datos bancarios cambian.

¿Qué ocurre para que un correo electrónico se vea comprometido?

Apropiación del correo electrónico

- El atacante utiliza el hackeo, o las credenciales de la cuenta robada, para obtener acceso a una cuenta de correo electrónico corporativa.
- Los detalles de la cuenta pueden haberse obtenido a través de un ataque de phishing o una violación de datos.
- El criminal puede reunir información sobre los contactos del usuario, el estilo de correo electrónico y los datos personales para hacer sus mensajes más convincentes.

Suplantación de correo electrónico

- El criminal crea una cuenta con una dirección muy similar a la real.
- O puede utilizar un remitente (De: XXX) y encabezado (Asunto: XXX) falsos, esperando que el destinatario no se dé cuenta y le dé seguimiento o lo responda como si fuera un correo legítimo.

Fraude del CEO

Los delincuentes se hacen pasar por un ejecutivo o empleado de alto rango de la empresa.

- Envían un correo electrónico al Área de Finanzas solicitando que se realice un pago de monto alto de manera urgente. Podría incluso indicar que se trata de una transacción importante o para alguna adquisición de la empresa.
- A menudo, el empleado al que están suplantando se encuentra fuera de la oficina y se torna difícil verificar los detalles de la solicitud.
- La cuenta de correo electrónico pudo haber sido comprometida a través de phishing o alguna filtración de datos, y el defraudador la recopiló a través de sitios web de la empresa o redes sociales.

Otros tipos de ataque comunes:

Vishing y estafas telefónicas

Las estafas telefónicas, o vishing, ocurren cuando un estafador llama fingiendo ser tu banco u otra organización de confianza. Puede Incluso hacer que la llamada parezca venir de un número conocido y en el que confías; a esto se le conoce como suplantación de números de teléfono o spoofing.

Pueden sonar muy convincentes y tener, al momento, parte de tu información personal, como número de cuenta o domicilio. Si la llamada te hace sentir incómodo, o percibes que algo está mal, termínala inmediatamente.

Siempre puedes ponerte en contacto con tu banco a través de algún número conocido, tal como el que aparece en la parte posterior de tu tarjeta bancaria o bien contactar directamente a tu ejecutivo de relación.

Los estafadores pueden mantener la línea abierta e incluso suplantar un tono de marcado, por lo que es recomendable que uses un teléfono diferente o esperar, al menos 30 segundos, antes de hacer una nueva llamada.

Los ejemplos típicos incluyen:

- ‘’El banco” avisa que tu cuenta está en riesgo y es necesario transferir el dinero a una “cuenta segura” para mantenerlo a salvo;
- “El banco” necesita apoyo de tu empresa para investigar un fraude;
- Tu proveedor de Internet o telefonía celular llama para solucionar un supuesto problema técnico que no les has reportado.

Un banco jamás solicitará tus contraseñas, PIN, códigos token (código de seguridad de un solo uso) o códigos de acceso.

Account Takeover o apropiación de cuentas

Los estafadores se comunican con sus víctimas potenciales por teléfono, a menudo desde números telefónicos “falsificados” que muestran el número telefónico de HSBC o el de la empresa que aparentan ser,

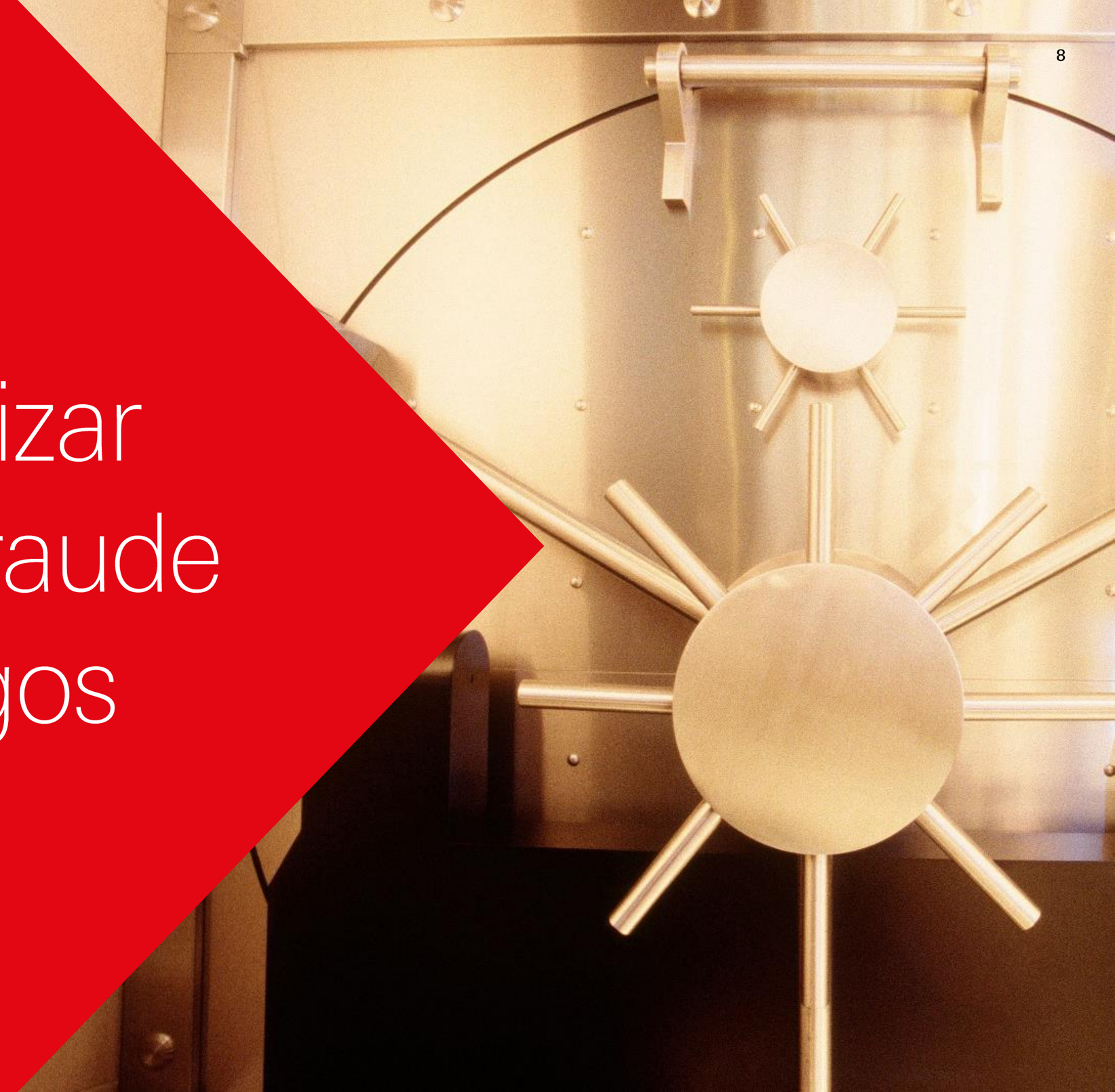
Los estafadores conocen las prácticas de tu empresa y se apegarán a los pasos que generalmente lleva a cabo la misma, con la finalidad de ganar tu confianza.

Posteriormente, utilizarán varios métodos para engañarte con la finalidad de obtener detalles de seguridad tales como nombres de usuario, contraseñas, códigos de un solo uso, entro otros. Los estafadores podrán usar esta información para apropiarse de la cuenta de tu empresa y, finalmente, transferir fondos fuera de su banco.

Recuerde:

- HSBC nunca le solicitará contraseñas, NIPs de sus tarjetas o valores token (códigos de seguridad de un solo uso);
- Nunca reveles códigos de seguridad a nadie;
- HSBC nunca te solicitará transferir tu dinero de una cuenta a otra (“cuenta segura”);
- HSBC nunca te pedirá que descargues software de acceso remoto para detener un pago.
- HSBC nunca te solicitará una actualización en línea de tu banca por Internet.

Cómo minimizar el riesgo de fraude al realizar pagos



HSBC

Minimiza el riesgo de fraude en pagos

Hay medidas que todas las empresas pueden tomar para minimizar el fraude en pagos y el riesgo de estafa las cuales no necesariamente deben ser complicadas o costosas. Todos pueden poner de su parte y jugar un papel en la prevención del fraude.

- Implementa gestiones de vigilancia para áreas de tu empresa que pudieran ser vulnerables;
- Educa y concientiza a tus colaboradores acerca de los riesgos de estafas, incluyendo de qué forma pueden identificarlas y, por tanto, evitarlas. Asegúrate de que conozcan las políticas y procedimientos de seguridad de tu empresa;
- Cuestiona cualquier solicitud inusual de pagos;
- Es fundamental que se verifiquen los datos de cualquier beneficiario nuevo o los detalles de las cuentas.

Revisa la dirección de correo electrónico

Los estafadores se harán pasar por personas de buena reputación.

- Si el nombre que aparece en el correo electrónico resulta familiar (de alguien conocido o con el que existe una relación habitual), asegúrate de confirmar que **el correo electrónico coincida**;

- Si se trata de un colega, su dirección de correo electrónico debería estar listado en el directorio de la compañía (en caso de que existe alguno);
- Asegúrate de que el nombre del dominio esté escrito correctamente. Habitualmente, los estafadores crean dominios falsos que se asemejan mucho al real, pero alteran una o dos palabras esperando que los destinatarios no se den cuenta. Por ejemplo, J@rnbusiness.com vs J@mbusiness.com.
- Ten en cuenta que el nombre que se despliega en el correo podría estar ocultando la dirección real del remitente.

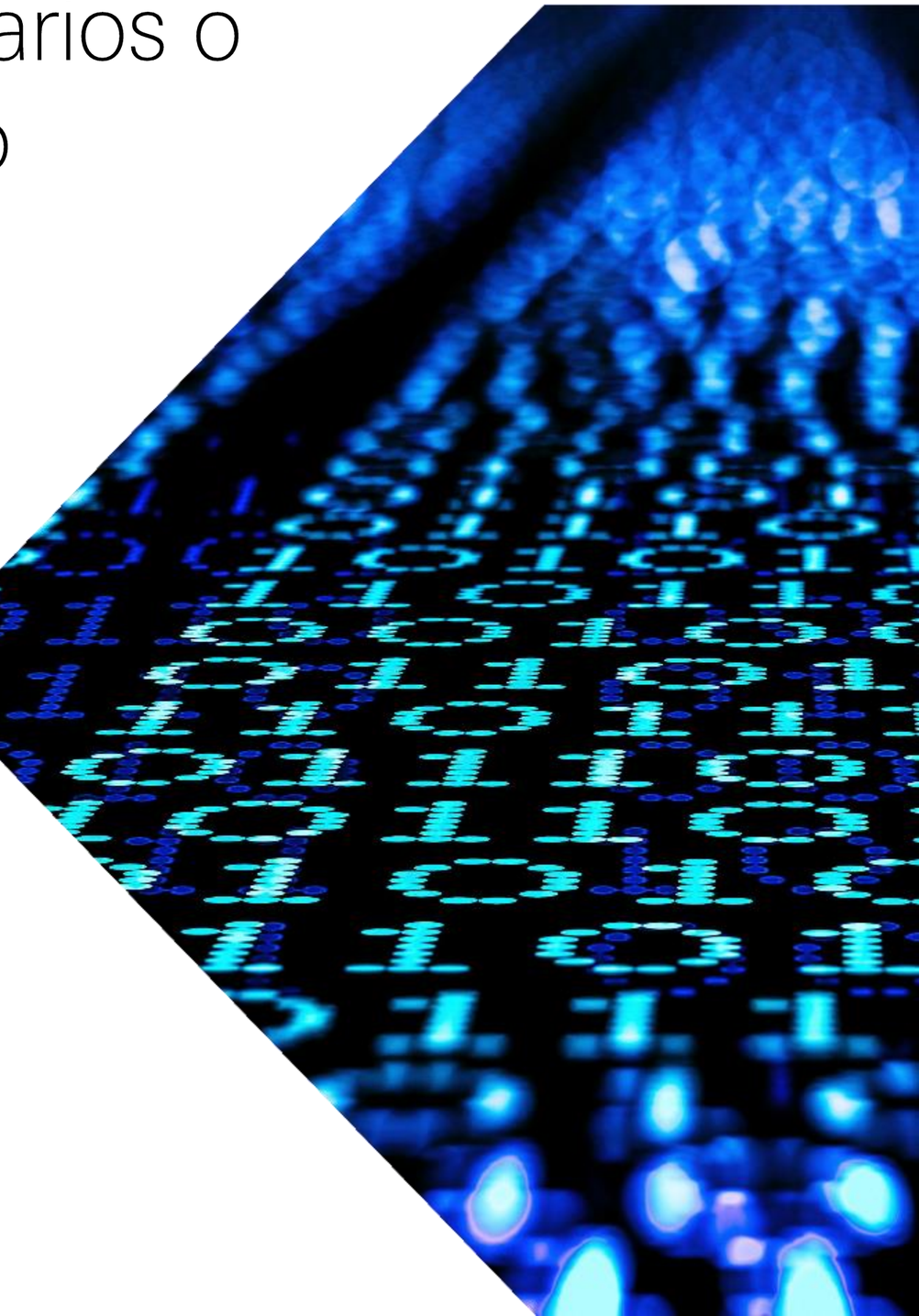
Revisa el correo electrónico a fondo

Si el correo electrónico está redactado con un sentido de urgencia para realizar un pago, ¡Cuidado! Esto es una señal de alarma.

- Considera como sospechoso cualquier correo relacionado con pagos si tiene un lenguaje de urgencia o proporciona excusas para no poder comunicarse por teléfono con el remitente;

- Algunos correos electrónicos de phishing podrían estar mal escritos. Incluso si la ortografía es correcta, a menudo su redacción es deficiente. Extrema precauciones con los correos externos, especialmente aquellos que contengan vínculos o archivos adjuntos. Ten en cuenta que la Inteligencia Artificial Generativa facilita a los atacantes crear correos electrónicos maliciosos convincentes;
- Si no esperas alguna comunicación y/o no reconoces al remitente, **no abras vínculos o archivos adjuntos**.

Valida los datos de nuevos beneficiarios o cambios en las cuentas de depósito



Confirma la veracidad de la solicitud a través de los contactos habituales y validados

- Cuando sea posible, intenta hablar con alguien que te sea conocido. Por ejemplo, si recibes una solicitud para un cambio en las cuentas beneficiarias por parte de algún colaborador de tu compañía, valida por teléfono que dicha solicitud sea genuina. Si se trata de algún proveedor, comunícate con tu contacto habitual al número telefónico que ya has utilizado previamente.

- No respondas el correo electrónico ni uses los datos de contacto contenidos en el mismo.

- En ocasiones, los ciberdelincuentes envían correos electrónicos de suplantación de identidad (phishing) a personas que figuran en la lista de contactos del correo comprometido. Puede que reconozcas al remitente debido a que la dirección de correo es exacta. Sin embargo, el mensaje puede contener elementos que te parezcan sospechos. Llamar a tu contacto, te permitirá validar que la solicitud de pago es genuina y, en caso de que la cuenta de correo electrónico se haya visto comprometida, ayuda a alertar a las víctimas.

Minimiza el riesgo de fraude en pagos

El fraude puede ocurrirle a cualquier tipo de empresa de distintas maneras. Afortunadamente, hay medidas que puedes tomar para ayudar a proteger a tu empresa contra el fraude y el cibercrimen. Aquí se mencionan algunos de los mejores consejos y checklists útiles que puedes usar para ayudar a mitigar el riesgo de fraude:

Crea e incorpora procedimientos de seguridad que sean claros para los equipos de tu empresa que realicen pagos. La más importante para prevenir el fraude es asegurarse de que todos los pagos sean validados. Crea un procedimiento para evitar que los equipos de pago autoricen pagos a cuentas nuevas, o con datos modificados, sin una validación adecuada. Apegarse a lo anterior, ayudará a que no se retiren recursos de las cuentas basándose únicamente en instrucciones telefónicas o por correo electrónico no verificadas, incluso aunque parezcan auténticas. Alienta a tu equipo a ponerse en contacto directamente con los beneficiarios, previo a girar la instrucción de pago.

Sensibiliza a tus colaboradores

Es importante capacitar a tus colaboradores. Ser conscientes de cuáles son los riesgos de fraude es responsabilidad de todos dentro de una empresa. Crea una cultura basada en el riesgo e implementa un proceso para que los colaboradores escalen cualquier preocupación a la alta dirección. Los colaboradores deben sentirse cómodos para cuestionar cualquier solicitud de pago.

Alienta a los colaboradores a revisar antes de dar clic

Está bien hacer clic en enlaces de sitios web de confianza. Sin embargo, hay que evitar hacer clic en enlaces dentro de correos electrónicos y mensajes SMS no verificados. Si se posa el ratón sobre un enlace, se podrá ver la URL oculta y verificar su legitimidad. Revisa las direcciones de correo y busca errores ortográficos y gramaticales antes de hacer clic en enlaces o abrir archivos adjuntos.

Haz que tus contraseñas sean más fuertes

Haz uso de administradores de contraseñas seguros o utiliza una frase de contraseña (una cadena de palabras que suele ser más larga que una contraseña tradicional). Las frases de contraseña son fáciles de recordar pero muy difíciles de descifrar. Alienta a tus colaboradores a elegir tres palabras al azar y seleccionar una mezcla de caracteres alfanuméricos y símbolos.

Deberás saber cómo actuar en caso de un evento de fraude o un ciberataque

Si tú o tu empresa son víctimas, es importante actuar con rapidez. Además, es importante reportar cualquier sospecha o incidente de ciberseguridad confirmado. Es recomendable ponerse en contacto con tu institución financiera.

Checklist: alta dirección de la empresa

La forma más efectiva de reducir el impacto por fraude en pagos es, en primer lugar, evitar que este ocurra. Con la finalidad de evitar ser víctima de fraude, se diseñó la siguiente lista que proporciona algunos consejos para la seguridad de su empresa:

- ☐ ¿Su empresa cuenta con procedimientos para la validación de solicitudes de pago nuevas o para las cuales se solicitó un cambio en cuentas? ¿Saben sus colaboradores en dónde encontrar los datos de contacto ya validados?
- ☐ ¿Tienes protocolos sobre cómo, quién y por qué medios tu personal puede solicitar que se realicen pagos? Además, en caso de que exista alguna preocupación o duda sobre la solicitud de pago, ¿cómo se puede validar?
- ☐ ¿Las contraseñas de su empresa son robustas? Por ejemplo, de una longitud mínima de caracteres y con caracteres alfanuméricos y símbolos. ¿Has pensado en utilizar un administrador de contraseñas o hacer obligatorio el uso de “frases de contraseña”?
- ☐ ¿Has considerado y aplicado la autenticación de dos factores siempre que sea posible?
- ☐ ¿Saben tus colaboradores qué hacer en caso de que se haya enviado un pago fraudulento?
- ☐ ¿Tienes un plan de respuesta ante incidentes cibernéticos por ejemplo un correo electrónico comprometido?
- ☐ ¿Discutes regularmente los riesgos potenciales de fraude con los colaboradores que envían pagos?
- ☐ ¿Se cuenta con un antivirus reconocido y adecuado para las funciones de su empresa en todos sus dispositivos?

Checklist: Procesamiento de Pagos – 1 de 2

Es importante ser conscientes de cuáles son las áreas de su empresa con más probabilidades de ser vulneradas. La siguiente lista fue diseñada para apoyar a los responsables del área de pagos y tiene como finalidad crear una cultura sobre los riesgos potenciales de fraude:

☐ Cuestiona si la solicitud es inusual o está fuera de contexto, ¿Hace sentido?

Cualquier correo electrónico en el que se hable de pagos y/o cuentas y que haya sido redactado con un sentido de urgencia o, en el cual se den excusas para no poder contactarse con su remitente, debe ser tratado con mucho cuidado. Si no esperabas dicha comunicación y/o no reconoces al remitente, no hagas clic en ningún vínculo ni abras los archivos adjuntos.

☐ Comprueba que la dirección de correo electrónica sea legítima

Si el nombre desplegado en el correo resulta familiar (de algún conocido), asegúrate de confirmar que la dirección y dominio coincidan. Los defraudadores se harán pasar por personas que conoces, incluyendo a tus colaboradores; se esperaría que dichas direcciones de correo estuvieran disponibles en un directorio de la empresa (en caso de tenerlo). Es importante asegurarse de que el dominio esté escrito correctamente ya que, en ocasiones, los defraudadores crearán dominios falsos que se asemejan al real alterando tan solo una o dos letras para que el destinatario no lo note. Por ejemplo, J@rnbusiness.com vs J@mbusiness.com. Ten en cuenta que el nombre que se despliega en el correo podría estar ocultando la dirección real del remitente.

☐ Cuestiona la solicitud de pago incluso si viene de la alta dirección de la empresa

Los defraudadores saben que si las solicitudes de pago provienen de la alta dirección de la empresa, hay una probabilidad menor de que haya un cuestionamiento. Tomando en cuenta lo anterior, no confíes en solicitudes vía correo electrónico a pesar de que aparente venir de un alto ejecutivo de la empresa o de un socio. Los defraudadores a menudo usan las plataformas más comunes de mensajería para facilitar el fraude.

⚠ Recuerda, el defraudador podría tener acceso al correo electrónico con el cual has tenido comunicaciones previas.

Checklist: Procesamiento de pagos – 2 de 2

La validación de los detalles de pago es vital para limitar el impacto de los fraudes y estafas. Además de llevar a cabo llamadas a los beneficiarios, existe una serie de consideraciones adicionales para asegurarse de minimizar el riesgo:

☐ Valida <u>todas</u> las solicitudes de cambio de cuentas y/o los datos de nuevos beneficiarios

Confirma que la solicitud sea auténtica a través de los medios a través de los cuales se comunican habitualmente. Cuando sea posible, hable con la persona responsable de los cambio para realizar los pagos. Si se trata de un proveedor, habla con la persona de contacto habitual y pide que confirmen el cambio **vía telefónica**. Recuerda, el defraudador pudiera tener acceso a la bandeja de correo de tu proveedor por lo que la respuesta, por este medio, podría venir del propio delincuente.

- No respondas el correo electrónico ni utilices los detalles contenidos en el mismo. Si los defraudadores se apoderaron de la cuenta de correo de alguien más, podrían modificar los detalles de contacto y, finalmente, podrías terminar hablando con el defraudador.
- Habla vía telefónica con quien está solicitando el pago. Los defraudadores saben que estas llamadas son parte del proceso por lo que podrían intentar primero comunicarse contigo.

⚠ Recuerda que una vez que se ha procesado un pago, no siempre es posible recuperar los fondos

Qué hacer si eres víctima de un evento de fraude

HSBC

En caso de haber sido víctima de un fraude:

Toma acciones inmediatas para minimizar el riesgo de pérdida de los fondos; si actúas de manera rápida, existe mayor posibilidad de recuperar los fondos

- **Detén cualquier** comunicación con el defraudador.
- **Alerta a cualquier parte relevante** (empleados, clientes e instituciones financieras). Es extremadamente importante contactar a tu banco con la finalidad de iniciar el proceso de una posible recuperación de fondos. El dinero se mueve muy rápido y puede tornarse difícil recuperarlo una vez que salen de las cuentas bancarias.
- **Reporta el fraude** a las autoridades correspondientes.
- **Revisa tus estados de cuenta para identificar cualquier transacción no reconocida o actividad inusual.**
- **Guarda toda la documentación** relacionada al fraude, incluyendo correos, facturas y cualquier correspondencia adicional.
- **Revisa y actualiza tus políticas y procedimientos de seguridad.**

Reportar un evento de fraude a HSBC

Es importante seguir las siguientes recomendaciones con la finalidad de tomar las acciones correspondientes e intentar tener una posible recuperación de recursos:

1. ACTÚA RÁPIDO: Entre más rápido se notifique al equipo de prevención de fraude, las posibilidades de que el pago sea detenido en el sistema y/o que los fondos sean devueltos son más altas;
2. RECOLECTA INFORMACIÓN: recopila toda la información pertinente relacionada con el fraude;
3. REPORTA A LAS AUTORIDADES: guarda evidencia de todas las comunicaciones y reporta a la Autoridades correspondientes.

Ponte en contacto con la Línea de Prevención de Fraudes de HSBC México:

Líneas de contacto

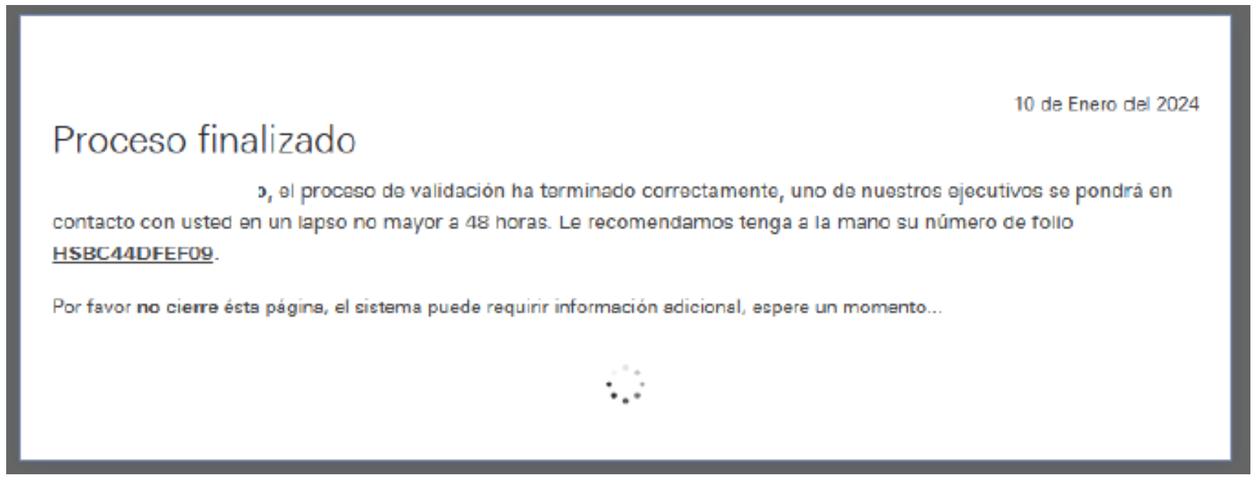
Desde México 55 5721 3388
Desde el Extranjero +52 55 5721 3388

Si sufres un ciberataque:

- **Desconecta los dispositivos afectados** de la conexión a Internet para evitar la propagación del malware y/o de los accesos no autorizados;
- **Cambia las contraseñas** de todas las cuentas afectadas, incluyendo correo electrónico, la red y cualquier otra cuenta que pudiera verse comprometida;
- Contrata una firma de seguridad reconocida para que **lleve a cabo una auditoría** de todos tus sistemas con la finalidad de identificar cualquier vulnerabilidad o brecha de seguridad.
- **Alerta a cualquier parte involucrada**, tal como empleados, clientes y autoridades regulatorias, proporcionándoles cualquier información necesaria;
- **Detecta cuál fue la fuente del ataque** y toma las medidas pertinentes para prevenir ataques similares en el futuro.

¡Cuidado! A continuación se muestran algunos ejemplos de pantallas falsas:

HSBC no enviará este tipo de pantallas, ni solicitará una supuesta actualización de datos en ventanas emergentes

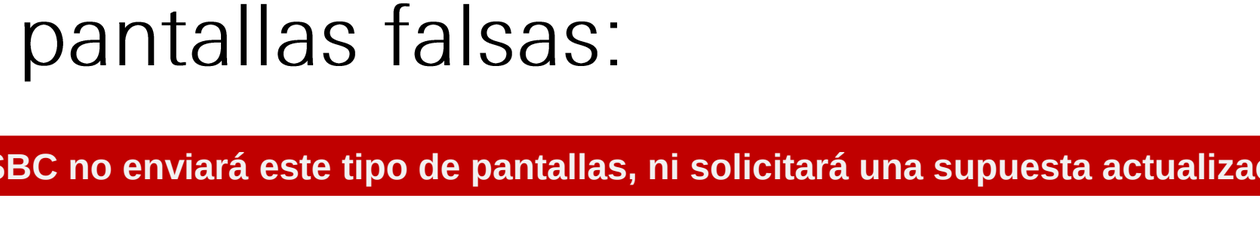


10 de Enero del 2024

Proceso finalizado

, el proceso de validación ha terminado correctamente, uno de nuestros ejecutivos se pondrá en contacto con usted en un lapso no mayor a 48 horas. Le recomendamos tenga a la mano su número de folio HSBC44DFEF09.

Por favor **no cierre** ésta página, el sistema puede requerir información adicional, espere un momento...



12 de Enero del 2024

Información requerida

estamos comprometidos a mantenerte informado sobre todos los movimientos realizados en el servicio, por lo que es necesario verificar tu información de contacto.

Un ejecutivo se está comunicando, por favor tenga a la mano su Teléfono Movil.

Confirmar

12 de Enero del 2024

Actualización de Datos

en **HSBCnet** queremos brindarte el mejor servicio, por ello, constantemente desarrollamos nuevas funcionalidades para que tu experiencia en nuestra banca electrónica sea satisfactoria. Además de estar mejor informado de tus movimientos y nuestras promociones proporcionanos tus datos para estar en contacto contigo.

Nombre Completo *

Teléfono *

(No incluir prefijo 044 o 045)

Número de celular *

Número de celular asociado a tu cuenta. (No incluir prefijo 044 o 045)

Correo electrónico:

Correo electrónico asociado a su cuenta.

Confirmar

En caso de identificar una pantalla inusual en su sesión de banca por Internet, favor de contactar al equipo de **Prevención de fraudes** de HSBC al teléfono **55 5721 3388**

Diccionario técnico

HSBC

Términos de fraude y ciberseguridad que debes conocer

- **Anti-Virus** – un programa informático utilizado para prevenir, detectar y a veces eliminar software malicioso.
- **Bring Your Own Device (BYOD) o <Traiga su propio dispositivo> en español** – política implementada por las empresas que permite a un empleado utilizar sus propios dispositivos electrónicos personales con fines de trabajo.
- **Common Vulnerabilities and Exposures (CVE)** – es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente..
- **Cripto moneda** – monedas digitales que se negocian como una mercancía.
- **Ciberataque** - ataques maliciosos de sistemas informáticos, redes, infraestructuras o dispositivos.
- **Ciber incidente** – violación de la política de seguridad de un sistema para afectar su integridad o disponibilidad y/o el acceso no autorizado o el intento de acceso a un sistema o sistemas.
- **Dark web o Web obscura**– parte del Internet que no está indexado por los motores de búsqueda y al cual solamente se accede con permisos especiales o software.
- **Huella digital** – rastro de información que deja el uso del Internet. Puede incluir información pasiva tales como cookies, o información que ha sido activamente compartida en Internet, tales como publicaciones en redes sociales.
- **Encriptación** – el proceso de codificación matemática de los datos. Estos datos se pueden cifrar en reposo, como los datos guardados en un disco duro, o en tránsito, como los datos enviados a través de HTTPS entre el navegador web y el servidor del banco. El cifrado de datos no los hace invisibles para los cibercriminales; sin embargo, los convierte en texto incomprensible sin posible uso para los criminales.
- **Firewall**– un sistema de seguridad de red que monitorea y controla el tráfico de información entrante y saliente, según un conjunto de reglas..
- **Hacker** – una persona involucrada en una amplia gama de explotación de redes informáticas; los hackers de "sombrero negro" generalmente conducen un manejo malicioso de la información, mientras que los hackers de "sombrero blanco" actúan en beneficio de la ciberdefensa.
- **Malware** – se trata de un término general para una amplia variedad de códigos maliciosos que dan acceso remoto, cargan o eliminan malwares adicionales, roban información bancaria, cifran y niegan el acceso a los datos, o secuestran los dispositivos para que no puedan ser utilizados.
- **Patching** – proceso de actualización de un software o hardware existentes para corregir errores y vulnerabilidades.
- **Penetration testing (Pruebas de penetración)** – se trata de un proceso utilizado por las organizaciones para poner a prueba su propia seguridad con tácticas utilizadas por cibercriminales, y que son llevadas a cabo por “red teams” o equipos de hackers de sombrero blanco profesionales.

- **Phishing** – usualmente se lleva a cabo por correo electrónico; se trata de un mensaje diseñado para engañar al receptor y obtener información sensible, que dé clic en vínculos maliciosos y/o que abra algún archivo malicioso. El phishing comúnmente es usado para lograr acceder a un dispositivo o red.
- **Ransomware** – un tipo de software malicioso que bloquea o restringe el acceso a los datos bajo la promesa de que la restricción se eliminará una vez que se haya pagado un rescate.
- **Smishing** – un mensaje de phishing via SMS/mensaje de texto.
- **Ingeniería social** – es la manipulación a un individuo para que lleve a cabo alguna acción, usualmente para obtener su información personal.
- **Spear phishing** – un tipo de mensaje de phishing dirigido a alguna persona en específico o a un grupo selecto de personas.
- **Troyano** – malware diseñado para aparentar ser un archivo o programa inofensivo y el cual tiene como finalidad convencer a la víctima potencial de que puede ser abierto/instalado de manera segura. Los troyanos son muy comunes y frequentemente llegan a los dispositivos via correo electrónico u otro tipo de malware llamados “loaders”.
- **Autenticación en dos fases (2FA)** – un proceso de autenticación en el que se requiere que un usuario tenga dos factores, como una contraseña y un código de acceso único (OTP). Generalmente, estos factores se clasifican como algo que usted conoce (contraseña), algo que usted es (huella digital), o algo que usted tiene (tarjeta de claves).
- **Red Privada Virtual (VPN, por sus siglas en inglés)** – permite conexiones privadas seguras a través de la infraestructura pública, desarrollada originalmente para que las organizaciones autenticaran al empleado en redes internas tales como servidores de correo electrónico o carpetas compartidas. En la actualidad, las VPN son cada vez más utilizadas para crear conexiones encriptadas a un servidor VPN para conectarse a otros recursos de internet.
- **Vishing** – un intento de phishing por teléfono con un fuerte uso de ingeniería social.
- **Vulnerabilidad de día cero** – fallo de seguridad de software descubierto recientemente para el que aún no existe un parche porque los desarrolladores de software desconocían su existencia.