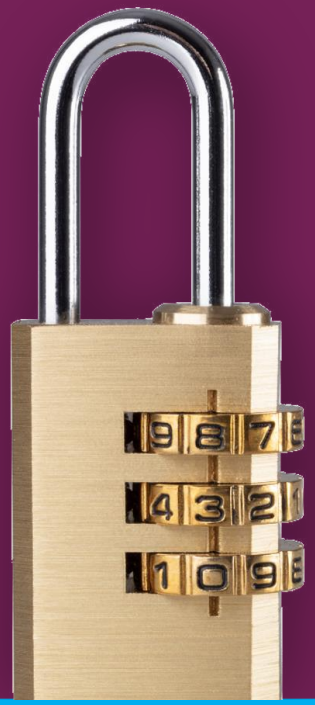
Fraude y Ciberseguridad:
Cómo proteger su organización

Barclays Bank México

Agosto 2025

BARCLAYS



Temas importantes

Haga de la prevención del fraude y la seguridad cibernética una prioridad

- Los estafadores están trabajando tan duro como usted. Tome medidas para asegurarse de que su organización se mantenga un paso por delante de los ciberdelincuentes.

Educar y reforzar procesos

- La prevención del fraude y la seguridad cibernética son responsabilidad de todos. Capacite al personal en todos los niveles, realice actualizaciones durante todo el año y refuerce los procesos.

Capacite a su fuerza laboral

- Un liderazgo fuerte y una cultura abierta pueden facilitar que las personas hablen y comprendan su papel en la protección del negocio.

Sea consciente de lo que comparte

- Los estafadores investigan los canales de redes sociales y los sitios web de las empresas para saber a quién dirigirse y cuándo dirigirse.

Sospeche y no sucumba a las tácticas de presión

- Los estafadores presionarán y pueden falsificar direcciones de correo electrónico y números de teléfono para que parezcan provenir de una fuente genuina, incluido alguien de su propia organización. Con los avances en la tecnología, todo se puede falsificar, incluidas las personas.

Mejores prácticas

Realice siempre controles verbales

Siempre que sea posible, debe realizar una llamada para validar una solicitud. Use un número de confianza que tenga registrado y no uno incluido en la instrucción para comunicarse con la persona o empresa.

Puntos de contacto únicos

Considere establecer puntos de contacto únicos con las empresas a las que paga regularmente.

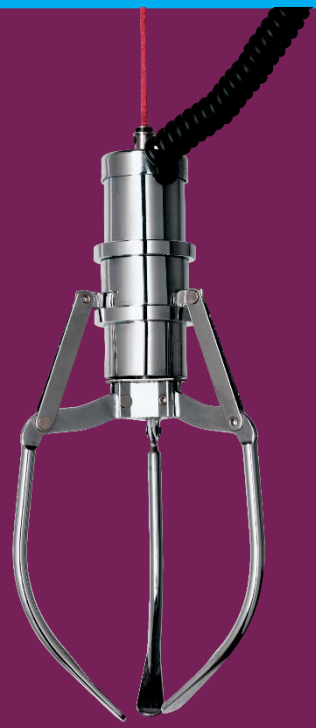
Aplique este mismo principio tanto interna como externamente.

Siga la diligencia debida

Realice auditorías en sus cuentas de forma regular.

El personal debe escalar cualquier sospecha utilizando puntos de contacto únicos.

Ingeniería social



BARCLAYS

Ingeniería social: el kit de herramientas de un estafador

Sentido de autoridad

Tendemos a cumplir con la autoridad en lugar de seguir nuestra conciencia.

Sentido para evitar situaciones negativas

Tendemos a ser reacios a las pérdidas y buscaremos evitar una consecuencia negativa.

Sentido de urgencia

Tomamos peores decisiones bajo estrés y presión de tiempo.

Búsqueda de lucro

Es dificil resistirse a abrir un archivo adjunto de correo electrónico que promete posibles recompensas.

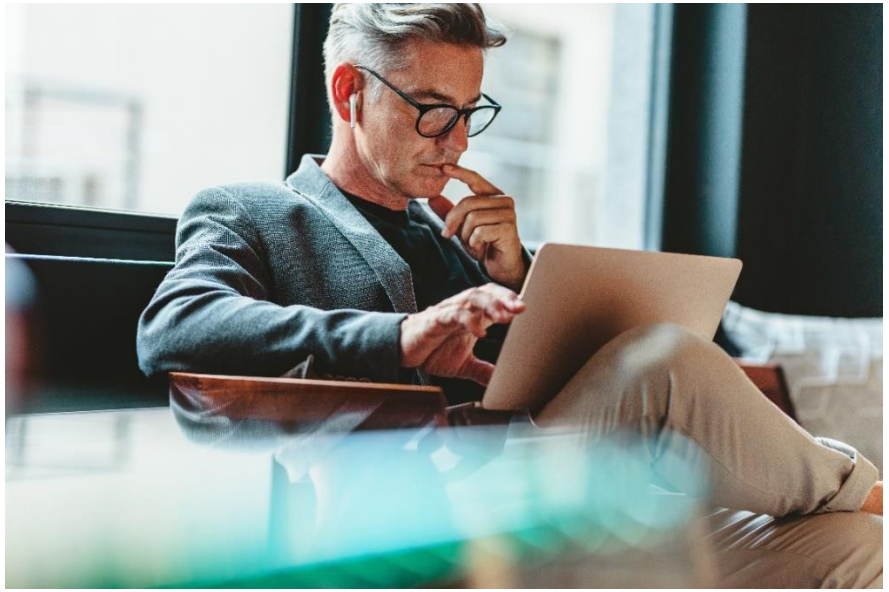
Amenazas clave de fraude y estafa

BARCLAYS

Fraude en instrucción de pagos: un caso práctico

Definición

El fraude de pagos es cuando un estafador envía una factura falsa o notifica a su empresa que los detalles de pago del proveedor han cambiado y proporciona detalles alternativos para defraudarlo.



Ejemplo

Una empresa recibe un correo electrónico que pretende ser de un proveedor conocido que informa un cambio en los detalles de la cuenta bancaria. De acuerdo con su proceso, un miembro del personal llama al proveedor a través del número proporcionado en el correo electrónico para validar la solicitud y los detalles de la cuenta bancaria proporcionados.

¿Qué pasa después?

La persona que contesta el teléfono confirma que tanto la solicitud como los detalles de pago proporcionados son genuinos. Como resultado, la empresa realiza una serie de pagos por un total de 20,000,000 de pesos a la cuenta.

Resultado

El proveedor genuino se pone en contacto con la empresa para consultar la no recepción del pago adeudado. El proveedor les informa de que no han cambiado sus datos bancarios, y el cliente se da cuenta de que validó la instrucción con un estafador.

Acción - Detener y desafiar

Siempre realice verificaciones verbales utilizando los detalles que se encuentran en el archivo y no los contenidos en la instrucción de pago.

BARCLAYS

Fraude sobre actualización de contactos de pago: un caso práctico

Ejemplo
Una empresa recibe un correo electrónico de un proveedor conocido que informa de un cambio en los datos de contacto (número de teléfono/punto de contacto/dirección de correo electrónico). Un mes después, la empresa recibe un correo electrónico del mismo proveedor con respecto a una factura, informando de un cambio en los detalles de la cuenta.
De acuerdo con su proceso, un miembro del personal llama al proveedor utilizando los datos de contacto archivados que se actualizaron un mes antes.

¿Qué pasa después?
La persona que atiende la llamada confirma la solicitud y que los datos de pago proporcionados son correctos, y la empresa realiza un pago por más de MXN 20,000,000

Resultado
El cliente recibe una llamada de su equipo de relaciones informando que el banco receptor ha informado de la cuenta como sospechosa. En una investigación adicional, se descubre que la solicitud de actualizar los datos de contacto es fraudulenta, lo que los ha llevado a pagar el dinero adeudado a la cuenta de un estafador.

Acción - Detener y desafiar
Siempre realice verificaciones verbales en todo tipo de comunicación, incluidas las solicitudes para modificar los datos de contacto.

Fraude de suplantación de CEO: un caso práctico

Definición

El fraude del CEO es cuando los estafadores se hacen pasar por un alto directivo, a menudo el CEO, para persuadir a un empleado de que realice un pago.

Ejemplo

Un miembro del personal recibe varios correos electrónicos que pretenden ser del director general de la empresa, pidiéndoles que realicen pagos por un total de MXN 14,800,000.

¿Qué pasa después?

Los pagos se ingresaron en el sistema.

Cuando se retienen los pagos para los controles de seguridad, el miembro del personal informa al banco que está convencido de que las solicitudes de pago son genuinas.

Resultado

Cuando el miembro del personal menciona más tarde los pagos a su CEO, el CEO informa que no los solicitó, momento en el que ya era demasiado tarde.

Acción - Detener y desafiar

Realice verificaciones verbales y siga la política de la empresa al realizar pagos: no espere hasta que sea demasiado tarde.

Fraude en solicitudes de líneas de crédito: un caso práctico

Definición

El fraude de solicitudes crediticias es cuando un estafador roba información de la empresa para solicitar una línea de crédito a nombre de la empresa, sin embargo, los fondos se pagarán en otro lugar. Esto a menudo se solicita virtualmente.

Ejemplo

Un proveedor recibe una solicitud de financiación de activos con documentación de respaldo a nombre de una empresa genuina, junto con facturas por el activo.

¿Qué pasa después?

El proveedor realiza verificaciones de diligencia debida, pero estas no incluyen una verificación verbal con la empresa utilizando un número de contacto verificado.

Después de esto, el proveedor realiza un pago de MXN 2,300,000 a los detalles de la cuenta proporcionados.

Resultado

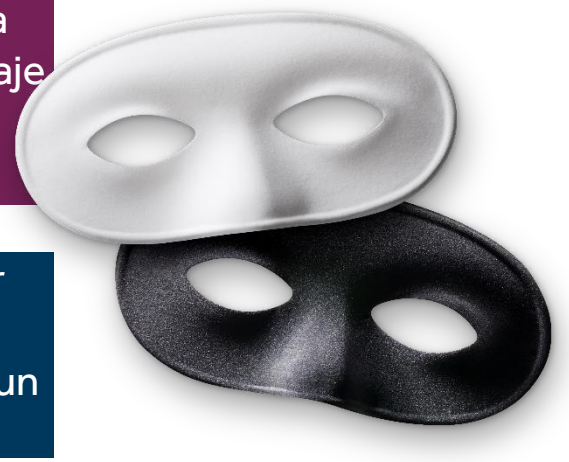
El fraude se descubre cuando hay problemas para cobrar el primer reembolso y el proveedor se comunica con la empresa genuina solo para descubrir que no había solicitado la financiación. Como resultado, toman medidas para revisar sus procesos para hacerlos más sólidos.

Acción - Detener y desafiar

Descartar procesos sólidos y la debida diligencia para obtener ganancias potenciales podría resultar en una pérdida financiera sustancial.

Fraude de suplantación de identidad bancaria

El fraude de suplantación de identidad bancaria es cuando el estafador se pone en contacto con la víctima haciéndose pasar por su banco. A menudo comienza con una llamada telefónica o un mensaje de texto, donde el estafador puede afirmar que ha habido fraude en la cuenta de la víctima o un problema con una transacción.



Para ayudar con esto, pueden afirmar que necesitan tomar el control de la computadora, transferir dinero a una cuenta "segura" para proteger los fondos o usar la firma digital para eliminar transacciones fraudulentas o retenidas. Es posible que se le pida que descargue software o utilice un chat web.

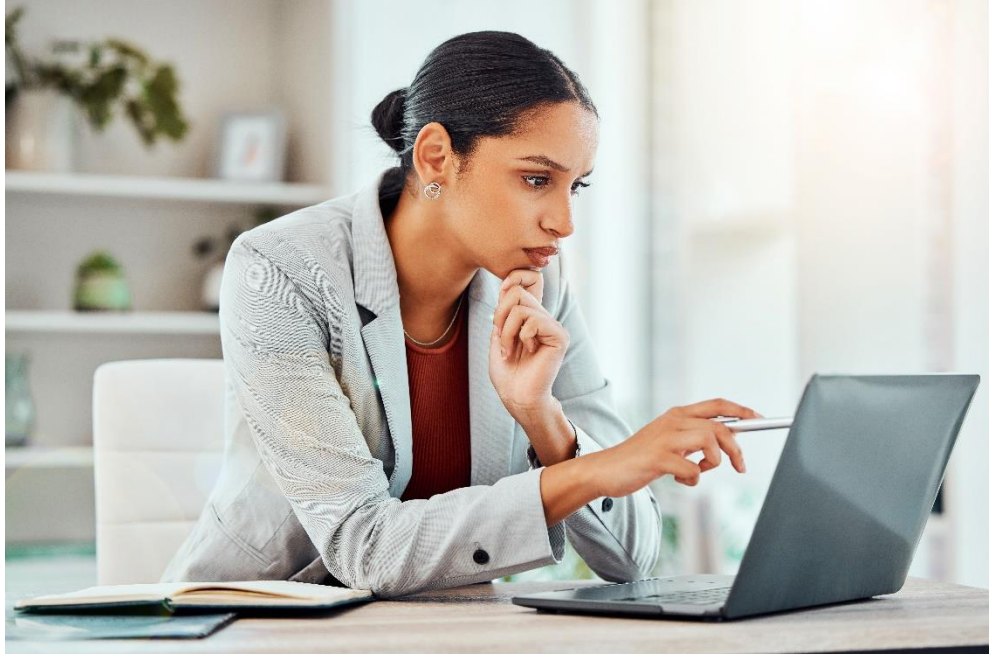
Al usar el 'chat web' o descargar software, esto le da al estafador acceso remoto a su dispositivo, donde su pantalla puede volverse negra, o se le pedirá que apague su pantalla para ayudar con el proceso.

Esto les permite iniciar transacciones sin su conocimiento donde le pedirán que ingrese su PIN, comparta un código de validación o use su dispositivo biométrico para completar el proceso. Al hacerlo, está autorizando los pagos establecidos por el estafador.

Fraude interno: un caso práctico

Definición

El fraude interno, se lleva a cabo desde el interior de una organización por su propio personal. Aunque solo lo comete una minoría, puede tener un gran impacto en una empresa y puede tomar muchas formas, desde fraude de pagos y recibos, hasta fraude de viajes y adquisiciones.



Ejemplo

Una investigación interna llevada a cabo por un cliente descubrió que un empleado había manipulado facturas para que contuvieran los detalles de su propia cuenta y conocidos.

El empleado había enviado facturas manipuladas al departamento de pagos, que había procedido a seguir las instrucciones y pagarlas.

¿Cuál fue el costo del fraude?

Duranteun período de 8 años, se realizaron un total de 117 pagos por más de MXN 15,300,000 a varias cuentas bancarias mantenidas en varios bancos.

El cliente denunció el fraude a la Policía y al banco.

Se contactó a los bancos receptores para investigar, donde solo quedaban 150,000 pesos para recuperar.

BARCLAYS

Cómo prevenir el fraude interno

Con el fraude interno, el perpetrador puede actuar solo, en connivencia con otro colega o con alguien ajeno a la empresa. Puede pasar desapercibida durante muchos años, causando daños a las finanzas, el bienestar del personal y la reputación de una empresa.

Consideraciones de alto riesgo

Los empleados de alto riesgo generalmente incluyen a cualquiera:

- En un puesto de responsabilidad o con mucha autonomía
- Con una queja actual o histórica
- Elaborar su aviso porque están a punto de irse
- En condiciones de influir en los sistemas financieros de la empresa.

Si su empresa tiene una alta rotación de personal, podría estar particularmente en riesgo de fraude interno.

Manténgase al tanto del pulso: para proteger a su organización del fraude interno, debe considerar los riesgos en cada etapa del empleo, esto incluye la contratación, el empleo y el abandono del negocio. Siempre que sea posible, segregar los controles para que ninguna persona sea responsable de cada etapa de un proceso

Promover el bienestar: asegúrese de que existan medidas para apoyar a los colegas en tiempos difíciles, dificultades financieras o problemas con las drogas, el alcohol o el juego, y que sepan cómo acceder a estas medidas.

Denuncia de irregularidades: es importante facilitar que el personal plantee sus inquietudes o sospechas al tener políticas claras y promoverlas regularmente dentro de su fuerza laboral.

Fraude con transacciones no autorizadas: un caso práctico

Definición

La negociación fraudulenta de trasacciones no autorizadas es la ocultación, manipulación y/o falsificación deliberada de operaciones o registros relacionados con la negociación de productos financieros, para evitar la detección y/o apoyar la elusión de los controles atenuantes, lo que conduce a una pérdida o ganancia por fraude.

Ejemplo

Un operador deshonesto en una empresa tomó una posición larga no autorizada y sin cobertura en los futuros del índice EURO STOXX 50 y S&P 500, que alcanzó una exposición máxima de 240 billones de pesos. En lugar de recortar inmediatamente la exposición, la aumentó deliberadamente y utilizó tácticas engañosas para ocultar la exposición.

Para ocultar el riesgo y manipular las pérdidas y ganancias que generaba una posición tan excesiva, el operador utilizó muchos métodos de ocultación diferentes, incluida la reserva de operaciones falsas, la reserva tardía de operaciones reales y la retención de ganancias de las pérdidas y ganancias informadas oficialmente, solo para filtrarlas con el tiempo.

¿Cuál fue el costo del fraude?

El fraude resultó en una pérdida de $ 40.6 billones de pesos y, en última instancia, condujo a la renuncia del CEO de la empresa, así como de los codirectores del negocio. El operador fue acusado y condenado por dos cargos de fraude y fue sentenciado a siete años de prisión.

Importancia de los controles verbales

BARCLAYS

Seguir los pasos a continuación puede ayudar a proteger a su organización de estafas en la gestión de pagos, como el fraude de instrucción de pagos y CEO:

Sí

- Siempre realice verificaciones verbales por teléfono con instrucciones de pago nuevas o modificadas
- Siempre realice verificaciones verbales en todo tipo de comunicación, incluidas las solicitudes para modificar los datos de contacto
- Utilice los datos de contacto que tiene archivados y aplique los mismos principios a las solicitudes de su organización
- Pídale a su contacto que le lea los datos bancarios del beneficiario. Esto confirmará si coinciden con los detalles que se le proporcionaron en las instrucciones

No

- Nunca confíe en una llamada entrante para obtener confirmación
- No use un número incluido en la solicitud, ya que esto podría resultar en que hable con el estafador
- Nunca se sienta presionado a tomar una decisión

Cómo los estafadores se dirigen a usted y a su empresa

Correo electrónico (Phishing)

El phishing es el uso fraudulento de correos electrónicos para manipular a los objetivos para que revelen contraseñas e información confidencial o transfieran dinero a otras cuentas. Los mensajes a menudo contienen enlaces a sitios web falsos que solicitan información de contraseña y cuenta o instalan virus en sus dispositivos. **Las direcciones de correo electrónico se pueden falsificar para que parezcan provenir de una dirección de correo electrónico genuina y ocultar al verdadero remitente.**

El compromiso del correo electrónico empresarial (BEC) es un tipo más sofisticado de phishing en el que los delincuentes logran obtener acceso a la cuenta de correo electrónico genuina de una persona y enviar correos electrónicos desde la cuenta haciéndose pasar por una persona de confianza, para tratar de engañarlo para que envíe dinero o divulgue información confidencial.

Los mejores consejos para proteger a su organización del phishing:

1. Nunca haga clic en enlaces ni abra archivos adjuntos en correos electrónicos de remitentes no verificados, ni ingrese información personal o de seguridad en un sitio al que se acceda a través de un enlace de correo electrónico no verificado
2. Recuerde: nunca nos comunicaremos con usted para pedirle su PIN, contraseñas completas o detalles completos de la cuenta. Tampoco le pediremos que realice un pago o solicite acceso a sus sistemas o PC
3. Informar a todo el personal sobre los riesgos de los correos electrónicos de phishing, especialmente las estafas de pago, e informarles cómo responder si son atacados. Considere adoptar un complemento 'Phish me/Report Phishing' en su Outlook e intente tener una opción de vista previa si es posible
4. No asuma que un remitente es genuino solo porque conoce información sobre usted o su empresa, o porque la dirección de correo electrónico le resulta familiar. Los estafadores son expertos en recopilar información y pueden crear direcciones de correo electrónico falsas, que pueden parecer de su propia organización.

Cómo los estafadores se dirigen a usted y a su empresa

Mensajes de texto (SMS de Smishing)

El smishing es una forma de ingeniería social que explota los mensajes cortos y los servicios de mensajería (SMS). Esta es una práctica similar a las llamadas telefónicas que usan SMS. El remitente del mensaje puede ser falsificado para que parezca genuino y los mensajes a menudo contienen enlaces a páginas web, direcciones de correo electrónico o números de teléfono que, cuando se hace clic en ellos, abren automáticamente una ventana del navegador, un mensaje de correo electrónico o incluso marcan un número. Esto a menudo lleva a que se le pida a la víctima que divulgue información personal.

Las tendencias recientes de smishing incluyen mensajes que se hacen pasar por empresas de entrega que incluyen un "enlace de seguimiento" o un enlace para pagar una "tarifa de envío" adicional.

Tenga en cuenta lo siguiente cuando reciba un mensaje de fuentes conocidas o desconocidas, ya que podrían ser fraudulentos:

- Atraer al destinatario para que haga clic en los enlaces incrustados en el mensaje
- Podría incluirse en conversaciones genuinas o hilos de texto
- Los contactos genuinos pueden ser suplantados
- Errores gramaticales y/u ortográficos: estos se pasan por alto fácilmente y pueden indicar que es fraudulento

Oficina de correos: tiene un paquete en espera de entrega debido a una tarifa de envío impaga. Paga aquí: https://postoffice-billing.com

Ha recibido un nuevo mensaje de voz: http://agci.top/e/?/p7uokh1j

BARCLAYS: No tenemos actividad inusual en su cuenta. Para evitar que se coloque un bloqueo, visite: http://secure.global-auth1202.com/barclays

NHS: Es elegible para solicitar un Pase Covid que demuestre que ha sido vacunado contra COVID-19. Puede solicitarlo aquí: http://nhs-uk.digital-passform.com

Cómo los estafadores se dirigen a usted y a su empresa

Llamadas a teléfonos fijos/móviles (vishing) y mensajes de texto (Smishing)

El vishing (phishing de voz) y el smishing (phishing por SMS) implican recibir llamadas o mensajes de texto fraudulentos que dicen ser de una organización o contacto conocido, la policía, un proveedor o incluso un miembro interno del personal.

Los mejores consejos para proteger su negocio del vishing y el smishing:

1. Nunca asuma que la persona que llama es genuina porque conoce información sobre usted, su empresa o sus colegas. El identificador de llamadas puede ser falsificado, así que no confíe en esto como indicador de legitimidad
2. Si recibe una llamada sospechosa, finalice la conversación inmediatamente y llame a un contacto de confianza de la organización en cuestión. Use un teléfono diferente, ya que el estafador puede mantener abierta la línea original
3. Su banco nunca enviará mensajes de texto que enlacen a páginas de inicio de sesión de banca en línea, ni solicitará confirmación de detalles de cuenta o seguridad
4. Los estafadores a menudo crean un sentido de urgencia para convencer a los empleados de que actúen rápidamente sin pensar adecuadamente en las implicaciones de sus acciones. Siempre date tiempo para detenerte y pensar.

Amenazas de Fraude más importantes a nivel mundial

BARCLAYS

Malware

Los ciberdelincuentes utilizan malware (abreviatura de "software malicioso") para interrumpir los sistemas informáticos y acceder a información confidencial. El malware se puede instalar fácilmente en su computadora o dispositivo móvil haciendo clic en un enlace o abriendo un archivo adjunto de correo electrónico. Incluso se puede ocultar dentro de otros archivos, como descargas de software.

Cinco tipos de malware

Ransomware
Deshabilita el acceso al sistema hasta que se pague un rescate

Spyware
Supervisa en secreto los dispositivos en busca de datos de actividad del usuario

Troyanos
Malware oculto en software deseable

Rootkits
Da a los hackers control remoto sobre los dispositivos infectados

Registradores de teclas
Supervise las pulsaciones de teclas para obtener datos confidenciales y credenciales

Proteger su negocio contra el malware

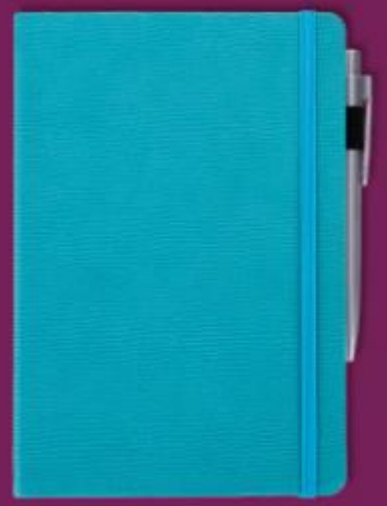
Cómo prevenir el malware

- **Software y dispositivos de seguridad:** considere usar protección antivirus y ejecute análisis regulares en todos los dispositivos. Instale últimas actualizaciones para sus firewalls, software de seguridad y navegadores de Internet, y asegurese de que los dispositivos móviles estén actualizados al último sistema operativo.
- **Archivos de copia de seguridad:** Realice copias de seguridad periódicas de los archivos críticos. Almacene copias de seguridad sin conexión en una ubicación diferente de su red y sistemas, o en un servicio en la nube diseñado para este propósito.
- **Fuentes confiables:** solo descargue archivos y software de fuentes confiables.
- **Aplicaciones móviles:** asegúrate de que las aplicaciones móviles que descargue tengan valoraciones positivas y de que solo utilices mercados oficiales, como Google Store o App Store.
- **Códigos QR:** tenga cuidado y nunca escanee un código QR que crea que podría haber sido manipulado, en su lugar, use su navegador o tienda de aplicaciones para encontrar lo que necesita.
- **Correos electrónicos y mensajes de texto:** asegúrese de que todos los correos electrónicos o mensajes de texto que reciba provengan de fuentes legítimas antes de abrir cualquier enlace o archivo adjunto, especialmente si lo presionan para que tome medidas urgentes.
- **Contraseñas:** use contraseñas complejas y autenticación multifactor para dificultar que los delincuentes accedan a sus cuentas.
- **Plan de recuperación ante desastres:** pruebe y ensaye su plan de recuperación ante desastres para asegurarse de que su empresa esté preparada para un ataque.

Qué hacer si eres víctima

- **Actúe de inmediato:** si su computadora o dispositivo se infecta con malware, tome medidas inmediatas para limitar el riesgo de infección y busque asistencia profesional. Desconecte los cables de red y desactive las conexiones Wi-Fi y Bluetooth.
- **Mantenga su dispositivo encendido:** no apague su dispositivo, ya que es posible que no pueda volver a acceder a él. Borre de forma segura los dispositivos infectados y vuelva a instalar el sistema operativo.
- **Guarde la evidencia:** conserve cualquier evidencia en coordinación con las autoridades que investigan el ataque.
- **Restablecer credenciales:** cuando sea seguro hacerlo, restablezca sus credenciales, incluidas las contraseñas, pero asegúrese de no bloquearse de los sistemas necesarios para la recuperación.
- **Rescates:** Pagar los rescates exigidos por los ciberdelincuentes solo fomenta nuevos ataques. No hay garantía de que obtenga resultados.
- **Busca asesoramiento:** consulta los datos de contacto de la Policía Cibernética en México:
  - Portal de la Policía de Ciberseguridad,
  - Portal de informes de delitos cibernéticos,
  - Email de la Policía Cibernética: policia.cibernetica@ssc.cdmx.gob.mx

Controles internos



BARCLAYS

Lista de verificación de concientización sobre el fraude

Apoyo	Capacitación	Revisión
Asegúrese de que sus equipos tengan acceso a capacitación y soporte en sus procesos financieros. Establezca "lo que es normal" para el negocio a través de una simple lista de verificación.	Aproveche las oportunidades de formación en prevención del fraude y compruebe que todos los compañeros están al tanto de las últimas tendencias en materia de fraude.	Emita recordatorios regulares a su equipo sobre la importancia de seguir los procesos. Revise y pruebe regularmente los métodos internos de prevención para asegurarse de que sean sólidos.
Acceso/Privilegios	**Malware/Descargas**	**Proteger**
Asegúrese de que los empleados solo tengan acceso a los sistemas y privilegios necesarios para su función. Esto debe revisarse periódicamente.	Evalúe su seguridad cibernética. Evite que el personal descargue aplicaciones a través de Internet y edúquelos sobre los riesgos y las señales de alerta.	Garantice que las solicitudes de pago se introduzcan, verifiquen y autoricen siguiendo los procesos y controles internos adecuados.

Aviso Legal

Grupo Financiero Barclays México, S.A. de C.V., Barclays Bank México, S.A., Institución de Banca Múltiple, Grupo Financiero Barclays Grupo México y Barclays Capital Casa de Bolsa, S.A. de C.V., Grupo Financiero Barclays México, (en conjunto, "Barclays") son entidades debidamente constituidas y autorizadas para operar de conformidad con las leyes de México, y sujetas a la supervisión de la Comisión Nacional Bancaria y de Valores y del Banco de México, entre otras autoridades financieras.

Barclays es un nombre comercial y una marca comercial de Barclays y sus subsidiarias.

Las llamadas pueden grabarse por seguridad y otros fines.

Se hizo todo lo posible para garantizar que la información proporcionada sea precisa. Sin embargo, ni Barclays ni ninguno de sus empleados hacen ninguna representación o garantía (expresa o implícita) en relación con la exactitud, confiabilidad o integridad de cualquier información o suposición en la que se pueda basar este documento y no se hace responsable de ningún error. Barclays (o cualquiera de sus filiales) no acepta ninguna responsabilidad por cualquier pérdida (ya sea directa o indirecta) que surja del uso de la información proporcionada.