



Soluciones para fraudes y estafas

Lo que debe saber y a qué estar atento(a)

En 2024, las estafas se convirtieron en **la principal forma de fraude**, superando al fraude con pagos digitales

El porcentaje de fraudes relacionados con estafas aumentó un

56%

Fuente: PYMNTS, The State of Fraud and Financial Crime in the U.S. (La situación del fraude y los delitos financieros en EE. UU.), noviembre de 2024.



Su seguridad es la prioridad

En Wells Fargo, nos dedicamos a mantener sus cuentas seguras. Además de monitoreo de transacciones y protección contra el fraude proactivos las 24 horas del día, los 7 días de la semana, le ayudamos a detectar señales de advertencia de fraude y evitar las estafas más comunes.

Estas son algunas medidas y consejos que ayudarán a proteger a su familia y a usted.

Las estafas están en aumento

El creciente uso de la inteligencia artificial en las estafas

La inteligencia artificial (IA) está dificultando distinguir lo que es real de lo que no lo es. Los estafadores ahora utilizan la inteligencia artificial para crear voces, vídeos e imágenes falsos que parecen reales. Pueden utilizar estas falsificaciones en redes sociales, sitios web, mensajes de texto y correos electrónicos para engañarle y hacerle creer que está proporcionando su información a alguien en quien confía. Estas son algunas sugerencias para ayudar a protegerse:

- Deténgase antes de actuar. Muéstrese escéptico ante las peticiones y la fuente.
- Valide cualquier solicitud de información o dinero: pregunte a algún familiar o amigo por algo que solo ellos sepan.
- No se involucre en comunicaciones inesperadas.

Fraudes y estafas a personas mayores

Muchas estafas se centran en los adultos mayores porque constituyen un gran segmento de la población y a menudo tienen ahorros significativos.

Las estafas más comunes a tener en cuenta son las oportunidades de inversión, las emergencias familiares, los impostores del gobierno, y las estafas de asistencia técnica. Para ayudar a mantener su seguridad y la de sus seres queridos:

- No confíe en el identificador de llamadas.
- No le facilite el acceso a su dispositivo a nadie que se ponga en contacto con usted.
- Mantenga intactas sus conexiones sociales y consulte a un familiar o amigo de confianza sobre nuevas relaciones o situaciones sospechosas.
- No se deje presionar por nadie que se ponga en contacto con usted alegando que hay un fraude en su cuenta para que transfiera o envíe dinero. Una compañía legítima no le pedirá que haga eso.

Reconozca las señales de alerta de una estafa

Contacto imprevisto

Una persona o una compañía le contacta sin previo aviso por teléfono, mensaje de texto o correo electrónico, a menudo acerca de un fraude en su cuenta o un pedido, entrega, factura o cargo del que usted no tenía conocimiento. Puede que insistan en quedarse al teléfono. Cuelgue.

Todo es urgente

Los estafadores crean un falso sentido de urgencia y utilizan tácticas de presión como lenguaje rudo o insistente para que usted actúe de inmediato.



Situación emocional, manipuladora o amenazadora

Los estafadores juegan con sus emociones —miedo, amor, curiosidad— para captar su atención y conseguir que pague o facilite información sensible.

Solicitudes de pago inusuales

Los estafadores prefieren métodos de pago que dificulten o hagan que le resulte imposible recuperar su dinero. Tenga cuidado si alguien le pide que pague con tarjetas de regalo o prepagadas, criptomonedas, giros electrónicos o una app de pago. Estos métodos de pago equivalen a enviar efectivo. Recuerde que las solicitudes de pago con tarjetas de regalo casi siempre son una estafa.

Preste atención a las estafas comunes

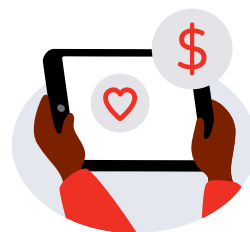
La estafa con cheques

Manténgase alerta si alguien le pide que cobre un cheque y envíe de vuelta una parte del depósito. Estos cheques usualmente son fraudulentos y puede tomar tiempo descubrir que son falsos.



La estafa de romance

Un nuevo interés amoroso le bombardea con palabras dulces, pero no quiere conocerle en persona. Inesperadamente, le pide que usted le envíe dinero para una inversión garantizada, dificultades económicas o una emergencia.



La estafa del familiar

Los estafadores juegan con sus emociones, identificándose como un amigo o familiar que llama o envía un mensaje de texto acerca de una emergencia. Podrían utilizar Inteligencia Artificial (IA) para clonar voces y convencerle de que se trata de una persona conocida.



La estafa del impostor

Los estafadores se hacen pasar por representantes de Wells Fargo, el Servicio de Impuestos Internos (IRS, por sus siglas en inglés), algún servicio público u organizaciones reconocidas para convencerle de que proporcione su información financiera personal. Podrían presionarle para que envíe dinero por giro electrónico, retire efectivo o que use tarjetas prepagadas o de regalo para resolver un problema con una cuenta o pagar una factura falsa.



Mantenga su seguridad con estas sugerencias

Proteja su información

No comparta su contraseña, número de identificación personal (PIN, por sus siglas en inglés) ni códigos de acceso por única vez. Los estafadores pueden hacerse pasar por un empleado de Wells Fargo y pedirle esta información privada por un “problema” con su cuenta. Nunca comparta con nadie la información de inicio de sesión de su cuenta.

No confíe en el identificador de llamadas

Los estafadores pueden imitar el identificador de llamadas para que sus llamadas parezcan legítimas.

Tenga cuidado cuando envíe dinero

No se deje presionar para enviar dinero sin verificar cuidadosamente que la solicitud sea legítima y la información que se le ha dado esté correcta.

Nunca permita el acceso remoto a su computadora

Los estafadores podrían comunicarse con usted para ofrecerle un reembolso o ayudarlo a eliminar un virus. Si les permite acceder a su computadora, podrían engañarle y lograr que usted les envíe dinero o comparta su información de inicio de sesión.

Evite interactuar

No haga clic en enlaces, descargue archivos adjuntos ni llame a números de teléfono que vengan con comunicaciones inesperadas.

Comuníquese con nosotros directamente

Cuando tenga dudas, cuelgue el teléfono o no lo conteste y llámenos usando el número de teléfono que aparece al dorso de su tarjeta o en wellsfargo.com/es. También puede comunicarse con nosotros usando la app de Wells Fargo Mobile®¹.

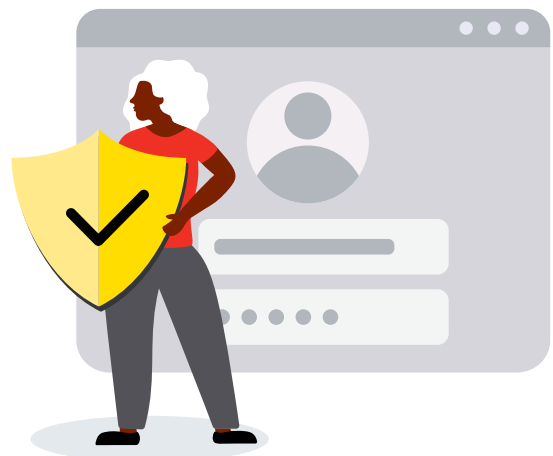
Tome medidas

Visite el Centro de Seguridad en nuestra app de Banca Móvil

Averigüe en qué condición se encuentra la seguridad de su cuenta para revisar y añadir rápidamente funciones con la finalidad de ayudar a proteger sus cuentas. También puede visitar por Internet el Centro de Seguridad, en wellsfargo.com/seguridad.

Active las alertas para cuentas²

Las alertas por notificaciones push, correos electrónicos y mensajes de texto son una manera fácil de recibir notificaciones de actividad en su cuenta, para que pueda comunicarse rápidamente con nosotros si algo no está bien.



Agregue opciones de seguridad mejoradas

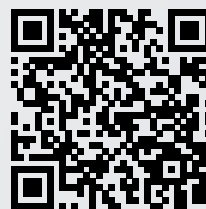
Considere usar la verificación de dos pasos, la autenticación biométrica en la app, una llave de acceso o el reconocimiento de voz. Estos servicios nos ayudan a comprobar que es usted.

Preste atención a los cambios en su reporte de crédito

[Inscríbase en el servicio Credit Close-Up®](#) para recibir alertas de monitoreo de crédito, ver su informe de crédito de Experian® y mucho más, y así ayudar a detectar robos de identidad.³

Obtenga acceso al Centro de Seguridad y mucho más con la app de Wells Fargo Mobile®

Escanee el código QR con la cámara de su dispositivo, o visítenos en wellsfargo.com/es/mobile-online-banking/apps/ o en su tienda de apps.



1. La disponibilidad podría verse afectada por el área de cobertura de su proveedor de telefonía móvil. Es posible que se apliquen tarifas por servicio de mensajería y datos de su proveedor de telefonía móvil.
2. Es posible que se requiera inscripción. La disponibilidad podría verse afectada por el área de cobertura de su proveedor de telefonía móvil. Es posible que se apliquen tarifas por servicio de mensajería y datos de su proveedor de telefonía móvil.
3. Usted debe ser el titular de una cuenta al consumidor de Wells Fargo elegible con una Puntuación FICO® Score disponible y estar inscrito en la banca por Internet Wells Fargo Online. Las cuentas al consumidor de Wells Fargo elegibles incluyen las cuentas de depósito, de préstamo y de crédito, si bien otras cuentas al consumidor también podrían ser elegibles. Comuníquese con Wells Fargo para obtener detalles. La disponibilidad podría verse afectada por el área de cobertura de su proveedor de telefonía móvil. Es posible que se apliquen tarifas por servicio de mensajería y datos de su proveedor de telefonía móvil.

Tenga en cuenta que la puntuación proporcionada en este servicio tiene fines educativos y es posible que no sea la puntuación usada por Wells Fargo para tomar decisiones de crédito. Hay muchos factores que Wells Fargo analiza para determinar sus opciones de crédito; por lo tanto, una Puntuación FICO® Score o clasificación de crédito de Wells Fargo específicas no garantizan una tasa de préstamo específica, la aprobación de un préstamo o una mejora de categoría en una tarjeta de crédito.

Wells Fargo y Fair Isaac no son organizaciones de reparación de crédito, según lo definido en virtud de las leyes federales y estatales, incluida la Credit Repair Organizations Act (Ley de Organizaciones de Reparación de Crédito). Wells Fargo y Fair Isaac no ofrecen servicios de reparación de crédito ni asesoramiento o asistencia con la reconstrucción o la mejora de su registro de crédito, historial de crédito o clasificación de crédito.

FICO es una marca comercial registrada de Fair Isaac Corporation en Estados Unidos y en otros países.

Estamos aquí para ayudar

Comuníquese con nosotros de inmediato si ha sido víctima de fraude, robo de identidad o una estafa, y notifique a la policía y a la Comisión Federal de Comercio (FTC, por sus siglas en inglés) para apoyo y denuncia adicionales.

- Tarjetas o cheques perdidos o robados.
- Compras, retiros o transacciones sospechosas o no autorizadas.
- Robo de identidad.

Aceptamos todas las llamadas de retransmisión, incluso del 711.

Cuentas personales
1-800-869-3557

Cuentas para empresas
1-800-225-5935

Tarjetas de crédito
1-800-642-4720

Si ha experimentado cambios de perfil no autorizados, actividad sospechosa o fraude con servicios provistos por la banca por Internet Wells Fargo Online® o en la app de Wells Fargo Mobile®, comuníquese con nosotros al **1-866-867-5568** (en inglés).

Ayúdenos a luchar contra los impostores que se hacen pasar por empleados de Wells Fargo

Suplantación de identidad (phishing) a través de correos electrónicos o mensajes de texto

- Si hizo clic en un enlace sospechoso, abrió un archivo adjunto, proporcionó códigos por única vez o cualquier información de su cuenta personal, llame de inmediato al **1-866-867-5568** (en inglés).
- Si no contestó, envíe el correo electrónico/mensaje de texto a reportphish@wellsfargo.com.²

Llamadas telefónicas sospechosas

- Si recibió una llamada, envió un pago o proporcionó códigos de acceso por única vez o información de su cuenta personal a alguien que dijo ser de Wells Fargo, llámenos de inmediato al **1-800-869-3557**.

Fraude a personas mayores

Si usted o una persona mayor o dependiente ha experimentado actividad sospechosa o fraude, llámenos de inmediato al **1-800-869-3557** o hable con un empleado de la sucursal.

También puede llamar a la línea directa nacional contra el Fraude a los Adultos Mayores al **1-833-FRAUD-11 (1-833-372-8311)**.

Para obtener más información, visítenos en wellsfargo.com/estafas

Es posible que la banca por Internet Wells Fargo Online® y la app de Wells Fargo Mobile® no estén disponibles en español para todos los clientes y que algunos productos, servicios y comunicaciones solo se ofrezcan en inglés.

1. La disponibilidad podría verse afectada por el área de cobertura de su proveedor de telefonía móvil. Es posible que se apliquen tarifas por servicio de mensajería y datos de su proveedor de telefonía móvil.
2. Tenga en cuenta que, por motivos técnicos, es posible que algunos mensajes de correo electrónico reenviados a reportphish@wellsfargo.com sean rechazados por nuestro servidor. Si esto ocurre, elimine el correo electrónico o mensaje de texto sospechoso. Wells Fargo trabaja en forma regular para detectar correos electrónicos y sitios Web fraudulentos. Gracias por tomar medidas para proteger su información personal y financiera.