

Comparta datos financieros con precaución Privacidad y seguridad para usuarios de aplicaciones 'fintech'



Cuando se utiliza con prudencia, la tecnología financiera o "fintech" puede ofrecer grandes beneficios. Con software móvil (aplicaciones) y herramientas en línea puede gestionar sus finanzas de forma más rápida, sencilla y cómoda. Fintech puede incluso ayudarle a alcanzar sus objetivos financieros.

La protección y seguridad de los usuarios es de gran importancia para la mayoría de las empresas fintech. Aun así, es importante desempeñar un papel activo para proteger su información personal y de su cuenta tomando algunas medidas sencillas pero eficaces a la hora de elegir y utilizar fintech.

Elija la tecnología financiera con prudencia

Aunque las atractivas utilidades y la comodidad le

llamen la atención, la seguridad de su información personal y de su cuenta debe ser su máxima prioridad a la hora de elegir una herramienta fintech.

Dondequiera que tenga una cuenta financiera (con bancos, prestamistas, emisores de tarjetas de crédito, empresas de inversión, la Administración del Seguro Social, etc.), es casi seguro que esa empresa o agencia ofrece su propia aplicación o plataforma en línea para permitirle acceder y gestionar su cuenta. Éstas suelen ser gratuitas, seguras y fáciles de usar, y cuentan con asistencia técnica en directo.

Las aplicaciones y herramientas fintech de terceros (que no se crearon para uso exclusivo con alguna institución financiera, agencia u otra entidad en la que usted tiene una cuenta) deben considerarse e investigarse más detenidamente ya que muchas piden su nombre de usuario y la contraseña de su cuenta bancaria. Aunque las herramientas fintech

independientes son fiables y seguras, debe compararlas e investigarlas antes de elegir, como lo haría con cualquier producto.

A continuación, algunos aspectos para tener en cuenta:

Política de privacidad y prácticas de seguridad:

Antes de descargar una aplicación fintech o abrir una cuenta, lea la divulgación de la empresa: acuerdo de usuario, política de privacidad, términos y condiciones, etc. para averiguar:

- Qué tipo de datos recoge.
- Cómo y durante cuánto tiempo se almacena la información.
- Si se vende o se comparte con otros, y con qué fines.
- Cuánto control tiene usted sobre lo que se recoge y cómo se utiliza o se comparte.
- Qué prácticas de seguridad se aplican para proteger sus datos.
- Quién es responsable si se produce una filtración de datos o si usted sufre pérdidas económicas.
- Cómo puede revocar el acceso a sus cuentas bancarias.
- Si ofrecen asistencia en directo en caso de necesitar ayuda.

Si no le gusta lo que lee, elija otra herramienta. (Aquí tiene algunos consejos sobre cómo leer una política de privacidad: <https://oag.ca.gov/privacy/facts/online-privacy/privacy-policy>.)

Compatibilidad y control: Si va a vincular la aplicación o herramienta que está considerando a sus cuentas bancarias, averigüe si la empresa fintech tiene un acuerdo con su banco que le permita a usted controlar a qué datos accede (o revocar el acceso por completo) directamente desde el tablero de su banco. (Puede consultar con su banco sobre cómo interactúa con cierta aplicación, pero de no poderlo determinar de antemano, tal vez tenga que registrarse y luego consultar el panel de “seguridad” de su banco, si lo tiene.) Intente también averiguar si la aplicación requiere que entregue las credenciales de acceso a su cuenta, o si el acceso se efectúa directamente con su banco. Si la aplicación solicita los datos de su cuenta (aunque en la pantalla aparezca lo que parece ser el logotipo de su banco), quiere decir que ésta o un proveedor de tecnología de terceros (llamado “agregador de datos”) está



almacenando sus datos de acceso al banco y los utiliza para entrar a su cuenta.

Reputación y capacidad de respuesta: No descargue una aplicación si no procede de una fuente de confianza. Lea los comentarios sobre la herramienta que esté considerando y verifique que el desarrollador es legítimo y que los usuarios están satisfechos con la funcionalidad de la herramienta y la forma en que la empresa maneja los datos de clientes y resuelve problemas. Busque en internet el nombre de la empresa o la herramienta junto con la palabra “reviews” (reseñas) o “ratings” (calificaciones) para encontrar opiniones de miembros del mismo sector (de compañías como CNET, PCMag.com y TechCrunch), opiniones de usuarios y noticias. Haga una búsqueda también con el nombre de la herramienta fintech y la palabra “breach” (brecha de seguridad) para obtener información sobre sus prácticas de seguridad, si alguna vez sufrió una brecha o infracción de seguridad y, de ser así, cómo respondió. Sin embargo, hasta las aplicaciones más conocidas y las que reciben críticas favorables utilizan agregadores de datos para almacenar su información de acceso al banco y podrían tener políticas distintas a las que



usted conoce. Por lo tanto, debería seguir los consejos de privacidad y seguridad que se ofrecen a continuación.

Consejos de privacidad y seguridad

Muchas empresas fintech están comprometidas a proteger la información personal y las cuentas de sus usuarios, pero la privacidad y la seguridad en línea es una responsabilidad compartida. A continuación, presentamos algunos consejos sobre cómo usted, como consumidor de fintech, puede ayudar a reducir los posibles riesgos:

Reduzca la exposición: En aras de limitar quién tiene acceso a sus datos y en cuántos lugares se almacenan (corriendo peligro de sufrir una infracción de datos), tiene sentido inscribirse en pocas herramientas fintech, lo justo para satisfacer sus necesidades.

Lea la divulgación de servicios de la empresa: Debe responder a todas las cuestiones indicadas en la lista de viñetas anterior.

Genere contraseñas seguras: Utilice una combinación de al menos ocho números, letras mayúsculas y minúsculas y símbolos. Nunca use la misma contraseña para todas sus cuentas.

Aproveche las funciones de seguridad adicionales: Si tiene la opción, active medidas de seguridad como

la autenticación de dos factores (o multifactores), en la que el usuario proporciona dos o más elementos de verificación (su contraseña más las respuestas a las preguntas de seguridad, un código enviado a su teléfono móvil, o su huella digital, por ejemplo).

Utilice el panel de control de su banco (u otros recursos) para gestionar el acceso a fintech: Si tiene cuenta en uno de los muchos bancos que ofrecen una plataforma para gestionar determinadas aplicaciones desde un panel de control, utilícelo para descubrir qué aplicación recopila datos y qué datos recopila; para limitar el acceso a determinadas cuentas o a determinados tipos de información; o, incluso, para revocar por completo el acceso a una aplicación. Comuníquese con el banco si tiene preguntas sobre los datos recopilados de sus cuentas, o si necesita ayuda sobre seguridad.

Opte por recibir notificaciones de su banco y de sus herramientas fintech: Así se mantendrá informado sobre las corrientes amenazas de seguridad, las actualizaciones de software (con parches de seguridad), los cambios en la política de privacidad u otras condiciones de la empresa, y de cierta actividad en su cuenta con señas de fraude (por ejemplo, la notificación de una transferencia desde una de sus cuentas que no fue hecha por usted).

Bloquee aplicaciones que ya no utiliza: Aunque siempre es conveniente eliminar las aplicaciones fintech que ya no utiliza, esto no es suficiente para evitar que sigan accediendo a los datos de su cuenta. La forma más eficaz de hacerlo es cambiar el nombre de usuario y la contraseña de sus cuentas financieras. Una vez realizado el cambio, proporcione el nombre de usuario y la contraseña nueva sólo a aquellas aplicaciones y herramientas con las que quiere seguir tratando. (Verifique también si su banco habilitó esa función en su panel de seguridad.)

Supervise sus cuentas: Ya sea que use fintech o no, es prudente verificar sus cuentas financieras con regularidad para poder detectar cualquier actividad sospechosa.

Bloquee su dispositivo y aplicaciones: Configure sus dispositivos móviles (y su computadora) para que requieran una contraseña o número PIN para iniciarse o despertarse. (Aprenda a hacerlo en dispositivos Apple [<https://support.apple.com/es-us/HT204060>] y Android [<https://support.google.com/android/answer/9079129>]). Cierre sesión en sus cuentas o aplicaciones cuando no las esté usando. Active funciones o instale

aplicaciones que puedan localizar, bloquear o borrar su dispositivo a distancia en caso de pérdida o robo.

Cuando algo va mal

Aunque muchas empresas fintech le dan prioridad a la protección de datos de los usuarios, las fintech operan mayormente sin regulación. Esto significa que no están obligadas a aplicar las estrictas medidas de seguridad que debe utilizar el sector financiero. Por lo tanto, existe una ambigüedad sobre quién es responsable cuando algo va mal.

Cuando usted comparte su nombre de usuario y contraseña con cualquiera, incluso con una empresa fintech, le está entregando las llaves de su cuenta.

He aquí algunos consejos para evitar y resolver problemas:

- Envíe dinero a través de aplicaciones de pago por móvil "peer-to-peer" (entre pares o P2P) (por ejemplo, Venmo y Cash App) y a través de servicios de transferencia de dinero bancarios (como Zelle) sólo a personas que conozca y en las que confíe. Estos pagos se procesan de forma instantánea, como si se tratara de dinero en efectivo, por lo que no hay forma de recuperar su dinero si lo estafan o si accidentalmente envía el dinero a alguien con el mismo nombre que su destinatario.
- Si algo va mal (cree que fue estafado, que envió dinero a la persona equivocada, o que envió una

cantidad errónea) póngase en contacto con su banco y con la empresa de pagos por móvil para saber si se puede hacer algo. Algunas P2P pueden mediar en una disputa (pero no le reembolsarán si la otra parte no acepta devolverle el dinero). Su banco puede ayudarlo de forma similar u ofrecerle asesoramiento.

- Cambie las contraseñas tanto de su cuenta bancaria como de la cuenta de fintech tan pronto como note cualquier actividad inusual o no autorizada. Si aún desea utilizar la herramienta fintech después de que se haya investigado y resuelto el problema, puede volver a vincular las cuentas.
- Si su problema no puede resolverse directamente, presente una queja ante la oficina federal Consumer Financial Protection Bureau (CFPB) (<https://www.consumerfinance.gov/es/enviar-una-queja/>). Esta oficina remitirá su queja a la empresa para que usted reciba una respuesta. También puede presentar una queja ante el Better Business Bureau (BBB) (<https://www.bbb.org/consumer-complaints/file-a-complaint/get-started>); las empresas acreditadas por la organización BBB están obligadas a responder a las quejas de los consumidores.

Para entender cómo funciona fintech, incluyendo por qué, cómo y cuándo las aplicaciones y herramientas acceden a la información de su cuenta financiera, lea la guía complementaria de Consumer Action,

Comparta datos financieros con precaución: Lo que debe saber sobre cómo funcionan las aplicaciones 'fintech' (https://consumer-action.org/spanish/articles/fintech_apps_sp).

Visite nuestra página web sobre cómo compartir datos financieros con precaución, **Share financial data with care** (<http://bit.ly/fintech-privacy>), para ver un breve video y encontrar más información sobre cómo controlar y proteger su información financiera cuando utiliza aplicaciones que requieren acceso a sus cuentas bancarias y otras cuentas financieras.

Acerca de Consumer Action

www.consumer-action.org

A través de educación y defensa, Consumer Action promueve derechos y políticas sólidas a favor del consumidor que impulsan equidad y prosperidad financiera para los consumidores subrepresentados en todo el país.

Asesoramiento y asistencia al consumidor:

Envíe quejas sobre asuntos del consumidor a: www.consumer-action.org/hotline/complaint_form/ o al 415-777-9635. (Las quejas en español pueden presentarse a: <https://complaints.consumer-action.org/forms/spanish-form/>.)

Nuestra línea directa acepta llamadas en chino, inglés y español.

© Consumer Action 2021

Acerca de esta guía

Esta guía se creó como parte del proyecto educativo Share Financial Data with Care de Consumer Action, con aportaciones de The Clearing House.

