LITORALPRESS

Fecha: 24-06-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: Cómo reducir el riesgo que corre cuando utiliza aplicaciones de finanzas personales

Pág. : 4
Cm2: 849,7

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Aumenta empleo de plataformas para administrar dinero:

Cómo reducir el riesgo que corre cuando utiliza aplicaciones de finanzas personales

Mientras más de ellas opere, mayor es el peligro de que su información se vea comprometida. Pero hay precauciones que puede tomar para protegerse.

TOMIO GERON
THE WALL STREET JOURNAL

Los consumidores están empleando cada vez más aplicaciones de finanzas personales para administrar su dinero, dependiendo de ellas para pagar, pedir préstamos, ahorrar, invertir y comprar. Si bien estos instrumentos pueden hacer que su vida sea más fácil, ¿es arriesgado dar a múltiples aplicaciones acceso a su información financiera?

Expertos en seguridad dicen que depende. Mientras más aplicaciones utilice, más alto es el riesgo de hackeos y filtraciones de datos. Pero hay cosas que los consumidores pueden hacer para protegerse.

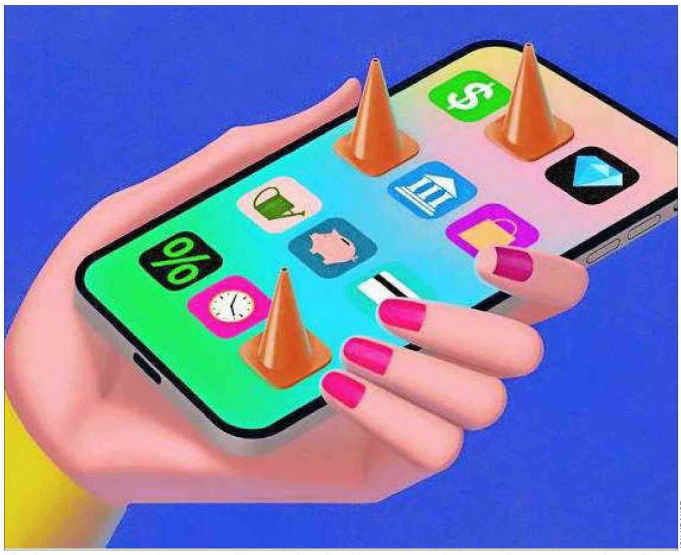
Los nuevos bancos que operan solo en línea, como también los instrumentos digitales como las aplicaciones de pago entre particulares, las de préstamos personales y las de ahorro y presupuesto se están volviendo más populares porque son convenientes y en algunos casos entretenidas de utilizar. Mientras tanto, los bancos y corretajes tradicionales están agregando opciones a sus aplicaciones para ayudar a los clientes a administrar mejor su cuenta corriente, de ahorro, tarjetas de crédito, hipotecas e inversiones.

Aunque las aplicaciones de finanzas no son especialmente vulnerables al hackeo, cualquier aplicación podría ser hackeada o violada, exponiendo los datos financieros de los usuarios o sus fondos. Y si lo inducen con engaños a revelar sus credenciales de acceso, los delincuentes podrían tener el mismo acceso fácil a sus fondos que el que usted tiene.

Existe también preocupación por los datos personales. Las aplicaciones pueden vender o compartir parte de su información con terceros, creando otro punto de vulnerabilidad.

"Aun cuando la aplicación original tenga sólidas medidas de seguridad, no pueden controlar totalmente las prácticas de seguridad de datos de sus asociados", señala Delicia Hand, directora sénior de mercado digital en Consumer Reports. "Si un tercero es víctima de una violación de datos, la información sensible de los usuarios podría quedar expuesta, lo que los pondría en riesgo de sufrir robo de identidad, fraude financiero o estafas específicas".

A continuación, una mirada más a fondo a algunas precauciones que puede tomar para utilizar aplicaciones de finanzas en forma más segura.



JON KRAUSE

El primer paso para protegerse es verificar que la aplicación que desea utilizar sea de una empresa de confianza.

Revisar y verificar

En primer lugar, verifique que la aplicación que quiere utilizar sea de una compañía respetable con políticas de seguridad y privacidad establecidas, y revise para ver si hay quejas al respecto en foros en línea, indica Meredith Fuchs, directora del equipo legal de la firma de tecnología financiera Plaid y exsubdirectora de la Oficina para la Protección Financiera del Consumidor.

RIESGO
Las aplicaciones pueden vender o compartir parte de su información con terceros, creando otro punto de vulnerabilidad.

Luego, baje la aplicación que desea directamente de la App Store o Play Store para tener la seguridad de que está obteniendo la que quiere y no una imitación. No baje una aplicación de un enlace o un sitio web, a menos que sea el sitio web de la compañía detrás de ella, dice Stuart Schechter, investigador de seguridad y comportamiento humano de la Universidad de Harvard.

Revise la política de privacidad de la aplicación para ver cómo recopila y maneja los datos del cliente. La venta de datos en general ha caído en desgracia, según Hand, pero algunas aplicaciones comparten datos de los usuarios —entre ellos nombres, correos electrónicos y números de teléfono, o datos financieros como el historial de transacciones o saldos de cuenta— con asociados como proveedores de servicios, empresas afiliadas y asociados de márketing.

Busque políticas en las que la compañía solo tenga acceso a datos que realmente necesita para proporcionar un servicio, en vez de recolectar todo lo que pueda. "Mientras menos datos haya recopilado realmente una compañía sobre usted, menor va a ser el daño final que se pueda hacer si esos datos son robados", indica Brian Callahan, director de Rensselaer Cybersecurity Collaboratory en Rensselaer Polytechnic Institute.

Revise cómo la aplicación maneja los cargos o transacciones no autorizados, si es pertinente. Hand señala que algunas aplicaciones puede que tengan protecciones más firmes que otras o procesos de disputa y resolución más simplificados.

Contraseñas y claves

Cuando configure una aplicación, utilice una contraseña sólida o un administrador de contraseña y active una autenticación de dos factores, la que verifica la identidad cuando inicia sesión en una aplicación.

Para una seguridad incluso más firme, algunas aplicaciones permiten que los usuarios suban una foto o un video actual para verificar la identidad. Algunas también permiten el uso de una clave de acceso, un *software* especial que está ligado a su teléfono o a otro dispositivo, o una llave de seguridad física que se conecta a su teléfono o a otro dispositivo para verificar su identidad. Esta última proporciona una seguridad muy sólida —mientras no la pierda— pero puede que no sea necesaria para todos los usuarios.

Fuera de las aplicaciones, no olvide mantener seguros sus dispositivos y cuentas de correo electrónico. Por ejemplo, los consumidores podrían querer activar el reconocimiento facial —como Face ID en los dispositivos Apple— de modo que cuando un banco o aplicación envíe un código de acceso sea seguro. Igualmente es fundamental que utilice contraseñas resistentes y permita la autenticación de dos factores en las cuentas de correo electrónico que se utilizan para acceder a las cuentas financieras, precisan expertos.

Gavin Reid, jefe de seguridad de información de la compañía de ciberseguridad Human Security, utiliza dos cuentas de correo electrónico —una para uso diario y otra que es solo para cosas como cuentas financieras— además de una llave de seguridad física. Igualmente aconseja borrar cualquier aplicación que no esté utilizando, para reducir riesgos.

"La cosa más importante que un consumidor puede hacer es asegurarse de guardar las cosas que son privadas para sí mismo; privadas para sí mismo", sostiene Jess Turner, vicepresidenta ejecutiva y jefa global de banca abierta y API de Mastercard. "Por lo tanto: no compartir información de credenciales, contraseñas o nombres de usuario, apoyarse en cosas como la biometría".

Limitar los enlaces

Conectar las aplicaciones de finanzas a sus cuentas de banco y de otras instituciones financieras es algo que a menudo se requiere si desea hacer pagos, pedir préstamos o administrar el gasto y la inversión. Muchas aplicaciones y bancos utilizan servicios intermediarios como Plaid, Mastercard, MX Technologies u otros para hacer esto. Por ejemplo, cuando un consumidor quiere conectar una cuenta bancaria a una aplicación de pago, Plaid puede abrir una ventana y pedir la aprobación para vincular las cuentas y describir qué datos se compartirán antes de hacer la conexión.

Estos servicios intermediarios tienen establecidas muchas medidas de seguridad. Sin embargo, la conexión de aplicaciones puede presentar riesgos al aumentar la exposición potencial de datos financieros a través del intermediario o las otras aplicaciones involucradas, explica Reid, jefe de seguridad de información de Human Security.

"Debería limitar ese tipo de intercambio tanto como sea posible para reducir su huella de riesgo", agrega. "Entender quién tiene sus datos y qué pueden hacer con ellos es fundamental".

Por supuesto, cuando diversas aplicaciones están compartiendo información entre ellas, como también con terceros asociados, puede ser difícil hacer un seguimiento y controlar cómo se están utilizando sus datos personales. Para ayudar con esto, Consumer Reports tiene una aplicación gratuita, llamada Permission Slip, que muestra a los consumidores qué tipos de datos están recopilando las empresas de y sobre ellos. La aplicación también enviará solicitudes en nombre de los consumidores, pidiendo a las empresas que dejen de vender sus datos personales o que los borren por completo.

Los consumidores también podrían obtener pronto cierta ayuda en esta área de las autoridades reguladoras. Se espera que la Oficina para la Protección Financiera del Consumidor emita normas finales este año en la Sección 1033 Dodd-Frank, la que, entre otras cosas, unificaría cómo se comparten los datos entre instituciones financieras y otorgaría a las personas el derecho a revocar el acceso a sus datos o a exigir que se borren, además de prohibir el mal uso de los datos para cosas como publicidad orientada.

Artículo traducido del inglés por "El Mercurio".