Publicado en Ciudad de México el 12/07/2018

# [Los consumidores mexicanos necesitan fortalecer la seguridad en sus cuentas bancarias](http://www.notasdeprensa.es)

## Los ataques cibernéticos dirigidos a la industria financiera no siempre atacan a los bancos, sino que apuntan a sus clientes. Es por ello que Avast advierte a los usuarios que fortalezcan sus hábitos en línea para mantenerse protegidos, y con ello su dinero estará fuera del alcance de los ciberdelincuentes

 La semana pasada, autoridades mexicanas advirtieron a los bancos estar alertas ante posibles ataques cibernéticos y fortalecer los sistemas de seguridad. Los ataques cibernéticos dirigidos a la industria financiera no siempre atacan a los bancos, sino que apuntan a sus clientes. Es por ello que Avast (LSE: AVST), el líder mundial en productos de seguridad digital, advierte a los usuarios que fortalezcan sus hábitos en línea para mantenerse protegidos, y con ello su dinero estará fuera del alcance de los ciberdelincuentes. Los ciberdelincuentes se dirigen a los consumidores porque saben que la mayoría de las personas almacena información sensible y confidencial en sus dispositivos electrónicos y con esos mismos dispositivos realiza compras y operaciones bancarias en línea. También saben que los usuarios son un eslabón débil y que a menudo desconocen las mejores prácticas de seguridad. Luis Corrons, Evangelista de Seguridad de Avast, brinda 5 consejos para que los consumidores pueden combatir el delito cibernético. Tener cuidado con los Troyanos bancarios móvilesEl número de troyanos de banca móvil va en aumento. Los troyanos de banca móvil son aplicaciones que intentan engañar al usuario para que renuncie a los detalles de su cuenta bancaria haciéndose pasar por una aplicación bancaria legítima, generalmente imitan la pantalla de inicio de sesión o bien, proporcionan una pantalla genérica con el logotipo del banco en cuestión. Avast llevó a cabo recientemente una encuesta en la que pedía a los consumidores que compararan la autenticidad de las interfaces de aplicaciones bancarias oficiales y falsificadas. En México, el 68% identificó las interfaces reales de banca móvil como falsas y el 44% confundió las interfaces falsas de banca móvil con las reales. Estos resultados son alarmantes y demuestran que los consumidores pueden ser fácilmente víctimas de los troyanos bancarios. "Estamos viendo un aumento en la cantidad de aplicaciones maliciosas para dispositivos Android, mismas que pueden eludir las comprobaciones de seguridad en las tiendas populares de aplicaciones y llegar a los teléfonos de los consumidores. Estas aplicaciones a menudo se presentan como aplicaciones de juegos y estilo de vida, y usan tácticas de ingeniería social para engañar a los usuarios para que las descarguen", dijo Corrons. "Los consumidores pueden confiar, la mayoría de las veces, en las tiendas de aplicaciones como Google Play y App Store de Apple, para descargar aplicaciones bancarias. Sin embargo, también se recomienda una vigilancia adicional. Los usuarios deben confirmar que la aplicación bancaria que están utilizando es la versión verificada. Si la interfaz parece desconocida o sospechosa, los usuarios deben verificar con el equipo de atención al cliente del banco. Finalmente es importante que los usuarios usen la autenticación de dos factores, si está disponible, y asegurarse de tener instalado un antivirus para Android que detecte y sirva de escudo contra el codicioso malware", afirmó Corrons. Evitar la trampa de phishingLos usuarios también deben estar atentos al phishing, que es una técnica de ingeniería social que los ciberdelincuentes utilizan con el fin de engañar a las personas para que entreguen su información confidencial, como detalles de tarjetas de crédito y credenciales de inicio de sesión. La forma más común del phishing scam es mediante un correo electrónico diseñado para parecer que proviene de una organización legítima, por lo que es difícil de distinguir, e incluye enlaces o archivos adjuntos. Los enlaces en correos electrónicos de phishing conducen a sitios web maliciosos casi idénticos al sitio web que están imitando y solicitan a los usuarios que ingrese información personal. "Los archivos adjuntos en los correos electrónicos de phishing descargan malware directamente o usan ingeniería social adicional para, por ejemplo, ajustar la configuración para luego descargar el malware. Si un correo electrónico que dice ser una institución bancaria parece sospechoso, podría tratarse de phishing y los usuarios deberían consultar con su banco para asegurarse de que el correo electrónico sea realmente de ellos", comentó Corrons. Cuidar las contraseñas, porque son la clave de acceso a la bóvedaEl uso de contraseñas sólidas y únicas para cada cuenta en línea, así como cambiarlas regularmente, es un paso importante que los usuarios deben seguir para mantener seguras sus cuentas en línea, especialmente las bancarias. "Recomendamos usar un administrador de contraseñas, como Avast Passwords, para gestionar sus contraseñas, ya que la mayoría de los usuarios tienen más de 20 cuentas en línea, lo que les dificulta crear y recordar contraseñas sólidas y únicas para cada una de sus cuentas", dijo Corrons. Los administradores de contraseñas usan cifrado seguro y generan contraseñas híper seguras para todas las cuentas, con lo que los usuarios no tienen que recordar contraseñas largas y pueden cambiarlas fácilmente con frecuencia. Cambiar las contraseñas de las cuentas de manera regular es extremadamente necesario, ya que las empresas no siempre detectan las infracciones de datos, lo que quiere decir que los ciberdelincuentes pueden tener acceso a las credenciales de inicio de sesión sin que nadie se dé cuenta y por lo tanto, comenzarán a cometer fraude. Instalar una red de seguridadLa instalación de un software antivirus en cualquier dispositivo, ya sea Mac, Windows o Android, es imprescindible. El software antivirus protege a los usuarios contra una gran cantidad de amenazas, incluyendo spyware, ransomware, keyloggers y troyanos. "Independientemente de cuán cuidadosos sean los usuarios, los ciberdelincuentes siempre están descubriendo nuevas formas de acceder a las cuentas de los usuarios. El antivirus actúa como una red de seguridad, protegiendo incluso a los usuarios más cautelosos en segundo plano en todo momento, para que puedan usar sus dispositivos sin tener que preocuparse", dijo Corrons. Mantener la banca en línea solamente en dispositivos propios"Por último, recomendamos que los usuarios nunca lleven a cabo transacciones financieras desde una computadora o dispositivo móvil que no les pertenece, ya que no se puede estar seguro de quién lo usó antes y qué tipo de software se está ejecutando en el dispositivo. Lo mismo ocurre con las redes Wi-Fi; los usuarios deben evitar realizar transacciones financieras cuando estén conectados a redes Wi-Fi públicas, ya que los hackers pueden espiar las actividades de la red. Si es absolutamente necesario, los usuarios deben usar una VPN cuando realicen operaciones bancarias en línea utilizando Wi-Fi público", finalizó Corrons. Avast Antivirus y Avast SecureLine VPN para PC, Mac, iOS y Android pueden descargarse en www.avast.com. Acerca de AvastAvast (LSE: AVST) es el líder global en productos de seguridad digital. Con más de 400 millones de usuarios en línea, Avast ofrece productos bajo las marcas Avast y AVG que protegen a las personas de las amenazas en internet y el escenario en evolución de amenazas de Internet de las Cosas. La red de detección de amenazas de la compañía está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital de Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros. Avast cuenta con el respaldo de las firmas globales líderes de capital privado CVC Capital Partners y Summit Partners. Visitar: www.avast.com.

**Datos de contacto:**

Flor Carreno

Agencia de Relaciones Públicas

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/los-consumidores-mexicanos-necesitan\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Nacional E-Commerce Software Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)