Proteger Sus Cuentas en Línea

As a medida que la tecnología financiera ha evolucionado, ha dado a los consumidores la capacidad de comprar, ahorrar e invertir en línea utilizando sus teléfonos celulares, tabletas y computadoras. Estas comodidades financieras modernas, sin embargo, vienen con riesgo. Los estafadores siempre buscan nuevas formas de entrar en el bolsillo de un consumidor, electrónicamente o de otra manera. Los inversores deben ser cautelosos en la forma en que utilizan las comodidades que ofrecen las tecnologías financieras nuevas y en evolución, especialmente a medida que se han utilizado más ampliamente durante la pandemia de COVID-19. Tener precaución a puedes mantener una distancia virtual entre los estafadores y su dinero.

Bancos, cooperativas de crédito, firmas de corretaje, asesores de inversiones, planes de jubilación de empleadores, cuentas personales de jubilación y más, ofrecen a los consumidores acceso electrónico sus cuentas a través de sitios web y aplicaciones móviles. Los inversores minoristas pueden tomar decisiones financieras importantes, de día o de noche, desde sus teléfonos móviles. No hacer mucho tiempo, este tipo de acceso a los mercados financieros era el reino de la ciencia ficción. Ya no más. La tecnología nos permite comprar valores, enviar dinero y pagar facturas con solo deslizar un dedo. Desafortunadamente, estas comodidades no se contrarrestan con protecciones comparables contra el fraude o el abuso.

Cuentas en Línea, Compras Virtuales, y el Riesgo para Sus Información Financiera

Cuanto más se comparta la información financiera a través de aplicaciones, sitios web y otros medios digitales, más en riesgo estará. Los estafadores pueden acceder a información privada de diferentes maneras y usar esa información para perjudicarlo financieramente. Aquí hay algunos ejemplos:

Brecha de Datos. Una brecha de datos es un incidente que expone información confidencial o protegida, que generalmente involucra la pérdida o el robo de datos privados que pueden ser utilizados por los delincuentes para robar las identidades y activos de los consumidores. Las brechas de datos ocurren a negocios, universidades, hospitales, gobiernos e incluso agencias de informes de crédito y monitoreo datos. Los datos se pueden vender través de mercados negros en línea que trafican con información malversada.

Phishing. El phishing implica que los estafadores utilicen correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentas para hacerse pasar por personas y entidades legítimas para engañar a los consumidores para que den su información personal. El estafador finge ser un negocio conocido, un empleador o alguna otra persona o entidad en la que el consumidor confía. Luego, el estafador utiliza la presunta confianza de una persona para solicitar datos personales que pueden usarse de manera fraudulenta venderse en el mercado negro en línea.

Skimming. Skimming (*robo electrónico)* implica el uso de tecnología instalada fraudulenta-mente en un lector de tarjetas de débito o crédito, con frecuencia en una bomba de gasolina o un cajeoro automático. Cuando un consumidor inserta su tarjeta para pagar a gasolina o retirar dinero de su cuenta,"el desviador" copia o "desvía" información de la tarjeta, lo que permite al estafador hacer versiones falsificadas de la tarjeta para uso fraudulento.

Estafas de Wi-Fi. Muchos negocios y espacios públicos ofrecen Internet inalámbrico gratuito para que el público lo use cuando realice su vida diaria. El Wi-Fi público no seguro es una mina de oro para los estafadores que buscan robar información financiera personal de personas que usan estas redes públicas para comprar en línea o acceder a información personal que se vuelve visible para cualquiera que quiera ver.

Estos no son las únicas formas en que los estafadores intentan obtener acceso a su dinero, pero son algunas de las formas más comunes en que los malos actores intentan usar la nueva tecnología parajugar viejos trucos, dejando a los consumidores e inversores con una bolsa vacía.

Emitido febrero de 2021

Para aprender mas, póngase en contacto la Oficial de Servicio en la Division de Valores:
Arizona Corporation Commission
1300 W. Washington St., Phoenix AZ 85007| teléfono: 602-542-0662 o número gratuito 1-866-837-4399| facsímil: 602-388-1335| correo electrónico: ValoresDiv@azcc.gov | sitio web: azcc.gov/azinversor

Cómo Protegerse y *Su Información Financiera*

Supervisar Sus Reportes del Crédito. En los estados unidos, los consumidores pueden visitar el sitio web en inglés, annualcreditreport.com. Además, visitar el sitio web usa.gov/espanol/credito para aprender sobre la importancia de verificar sus reportes del crédito de las tres principales agencias delos reportes del crédito de forma gratuita.

Si una entrada no parece familiar, los consumidores deben hacer un seguimiento de inmediato. Disputar entradas que sean fraudulentas. Los consumidores interesados en una mayor tranquilidad podrían considerar suscribirse a un servicio de monitoreo de crédito.

Tener Cuidado con la Conexión Wi-Fi Pública. Las redes Wi-Fi públicas—especialmente las redes públicas no seguras, con llevan enormes riesgos. Evitar las compras en línea y el acceso a datos financieros u otros datos personales en redes Wi-Fi públicas. Esperar hasta que pueda acceder a una red privada cifrada para ingresar su número de tarjeta de crédito o ingresar la información de inicio de sesión de la cuenta.

Comprobar Sus Reportes de Crédito. En los estados unidos, los consumidores pueden visitar el sitio web en inglés, annualcreditreport.com. Además, visitar usa.gov/espanol/credito para aprender sobre la importancia de verificar sus reportes del crédito de las tres principales agencias de reportes del crédito de forma gratuita. Si una entrada no parece familiar, los consumidores deben hacer un seguimiento de inmediato. Disputar entradas que sean fraudulentas. Los consumidores interesados en una mayor tranquilidad podrían considerar suscribirse a un servicio de monitoreo del crédito.

Tener Cuidado con Tarjetas Débitos. Las tarjetas de débito ofrecen menos protecciones contra el fraude que las tarjetas de crédito y dejan su cuenta bancaria vulnerable a los estafadores que obtienen información de la cuenta bancaria o falsifican su tarjeta. Las tarjetas de crédito ofrecen mejores protecciones contra el fraude que las tarjetas de débito, y los consumidores deben considerar el uso de una tarjeta de crédito en lugar de una tarjeta de débito cada vez que compran en línea o dan un número de tarjeta para pagar algo por teléfono.

Alzar Su Voz Si Algo es Mal. Si como un inversor sospecha que algo es mal con su statu de cuenta o informe de crédito, debe hacer un seguimiento con su institución financiera y las principales agencias de informes de crédito para asegurarse de que la entrada del cargo o informe de crédito sea precisa. Disputar transacciones y anotaciones de crédito que no son legítimas.

La *Conclusion*

Tener cuidado al divulgar información personal en línea y evitar hacerlo en un entorno público a toda costa. Usar métodos de pago más seguros que vengan con una protección contra el fraude mejorada si es posible, verifique los estados de cuenta regularmente. Antes de que invierte, comprobar y preguntar con el Oficial de Servicio en la División de Valores del Arizona Corporation Commission por correo electrónico a ValoresDiv@azcc.gov, o por teléfono local al 602-542-0662 o número gratuito en Arizona, 1-866-837-4399 antes de realizar cualquier inversión, si sospecha fraude de inversión.