FDIC

Noviembre 19, 2018

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer **news**


PHOTO: GETTY IMAGES

¿Compra en línea durante las vacaciones?

Proteja su dinero de las estafas

Durante la temporada festiva tendemos a hacer muchas más compras de viajes y regalos en línea, por lo que es especialmente importante estar atento a la hora de proteger su dinero. He aquí algunas de las estafas más comunes a las que debe estar atento:

Aplicaciones y sitios web falsos. Los estafadores a menudo crean sitios falsos que son tan parecidos a los de comerciantes populares que engañan fácilmente a los consumidores para que les den su información de pago. Los estafadores toman su información y dinero, pero usted nunca recibe los productos. Los estafadores también han desarrollado aplicaciones falsas que contienen malware. Cuando usted baja una aplicación, el malware le roba su información personal o la bloquea, secuestrándola hasta que le paga un rescate a los estafadores. Otros tipos de aplicaciones fraudulentas le piden que inicie sesión usando sus cuentas de medios sociales o correo electrónico que podría exponer su información personal para que los estafadores la roben.

Tenga cuidado con las aplicaciones o los sitios web que le solicitan permisos sospechosos, como otorgar acceso a sus contactos, mensajes de texto, contraseñas almacenadas o información de su tarjeta de crédito. Además, la mala gramática o las palabras mal escritas en la descripción de una aplicación o sitio web son una señal de advertencia de que estos no son legítimos.

Enlaces en el correo electrónico. Evite dar clic en los enlaces que vienen en los mensajes no solicitados o de fuentes desconocidas. Los enlaces le pueden llevar a un sitio ilegítimo que puede intentar obtener su tarjeta de crédito u otra información personal. Algunos enlaces podrían bajar malware (software malicioso, como virus informáticos) a su computadora cuando hace clic en ellos para robar su información bancaria, incluyendo su identificación de inicio de sesión, contraseñas y los números de sus tarjetas de crédito o débito. Estos mensajes de correo electrónico suelen ser muy similares a los enviados por los comerciantes, bancos y otras entidades conocidas.

Esté atento a los mensajes de correo electrónico que contienen errores tipográficos u otros errores obvios. Además, desconfié de los archivos adjuntos que se describen como cupones, reembolsos o formularios de pagos, ya que podrían incluir malware. Y evite las ofertas por correo electrónico que parezcan "demasiado buenas para ser verdad". Si un mensaje de correo electrónico le promete artículos populares gratis o un precio sorprendentemente bajo, probablemente es una estafa.

Hacer pagos en sitios no seguros. Antes de pagar una compra en línea, asegúrese de que el sitio en el que está tenga "https" al inicio de la URL con un símbolo de candado:

Esto significa que el sitio tiene una conexión de red protegida. Los sitios con "http" al inicio de la URL sin la "s" son más vulnerables a los ataques de los estafadores que roban información de tarjetas de crédito monitoreando el tráfico de la red. También tenga cuidado con las ventanas emergentes que aparecen cuando está en un sitio pidiéndole la información de su tarjeta de crédito para que reciba cupones u obtenga artículos gratis. Las compañías legítimas no le piden su información personal para esos fines.

Usar Wi-Fi público para hacer compras o acceder a información confidencial. La conectividad inalámbrica, también conocida como Wi- Fi, le permite a su computadora portátil, computadora de escritorio o dispositivo móvil conectarse a Internet sin una conexión por cable física. Muchos restaurantes, hoteles, bibliotecas y otros lugares ofrecen Wi-Fi público gratuito, que es conveniente cuando usted está fuera de casa. Sin embargo, estas redes podrían no ser seguras (ya que no requieren una contraseña o proporcionan la misma contraseña de acceso genérica a todos sus clientes) y podrían exponer su información personal y bancaria a los estafadores que buscan robar nombres, números de seguro social y cuentas bancarias.

Evite usar el Wi-Fi público para hacer compras en línea, ingresar a sus cuentas financieras o acceder a otros sitios que tienen su información confidencial.

También es buena idea sólo usar sitios que tienen una encriptación "https" (descrita anteriormente) cuando esté en lugares públicos.

Estafas de confirmación de entrega de paquetes. Esta estafa es especialmente popular durante los días festivos cuando la gente recibe regalos por correo que podrían no estar esperando.

Los estafadores llaman o envían un mensaje de correo electrónico diciendo ser empleados del Servicio Postal de los Estados Unidos o de una importante compañía de envíos y le dicen que usted tiene un paquete listo para su entrega.

Para asegurarse de que el paquete le pertenece, se le pide que dé su información personal, la que los estafadores roban para abrir cuentas de crédito a su nombre. En respuesta a esta estafa, el Servicio Postal de los Estados unidos explicó que ellos no llaman ni envían correo electrónico pidiendo información personal si hay un problema con una entrega. Visite https://postalinspectors.uspis.gov para obtener más información.

No deje que estás estafas le arruinen su espíritu festivo. En cambio, he aquí algunas precauciones que puede tomar para proteger su dinero cuando hace compras en línea:

- En general, siempre utilice contraseñas que sean únicas y difíciles de adivinar para cada cuenta.
- Si usa aplicaciones de compra, utilice sólo las aplicaciones oficiales de los comerciantes que se encuentran en su sitio web o en un mercado de aplicaciones confiable, ya que ofrecen mayor seguridad.
- Nunca proporcione la información de su tarjeta de crédito a menos que esté en un sitio seguro, que muestre
- "https" al comienzo de la URL y el símbolo de candado.
- Piense en implementar la autenticación de dos factores en sus cuentas. La autenticación de dos factores requiere que usted proporcione dos pruebas cuando ingresa a su cuenta. Presenta una capa de seguridad adicional para que sea más difícil para alguien que no sea usted ingresar a su cuenta. Para obtener más información, visite https://www.nist. gov/itl/tig/back- basics-multi-factor- authentication
- Monitoree las facturas de sus tarjetas de crédito y sus estados de cuenta bancarios, así como las transacciones hechas a través de aplicaciones u otras transacciones en línea para detectar compras y retiros no autorizados. Contacte de inmediato a su banco si advierte algo sospechoso. Además, es posible que desee considerar registrarse para recibir servicios de alerta. Muchos emisores de tarjetas de crédito, bancos y proveedores de aplicaciones móviles ofrecen servicios que le avisan de ciertas actividades relacionadas con sus cuentas, como inicios de sesión recientes desde dispositivos no reconocidos.

Para obtener más ayuda o información, vaya a **www.fdic.gov** o llame a la FDIC gratis al **1-877-ASK-FDIC (1-877-275-3342)**. Envíe sus ideas para historias o comentarios a Asuntos del Consumidor a **consumeraffairsmailbox@fdic.gov**

FDIC