FDIC

Diciembre 2, 2022

FEDERAL DEPOSIT INSURANCE CORPORATION

consumer news


# Evite estafas al comprar ofertas en línea

## *Protéjase y conozca las señales*

Durante la temporada navideña, tendemos a hacer muchas más compras en línea para viajes y regalos, por lo que es especialmente importante estar atento a la protección de su dinero. Estas son algunas de las estafas más comunes a tener en cuenta:

### Sitios web y aplicaciones falsas

Los estafadores a menudo crean sitios web falsos que son tan similares a los sitios de minoristas populares que engañan fácilmente a los consumidores para que proporcionen información de pago. Los estafadores toman su información y su dinero, pero usted nunca recibe los productos. Los estafadores también han desarrollado aplicaciones falsas que contienen malware. Cuando descarga la aplicación, el malware roba información personal de su dispositivo o la bloquea, y la retiene para pedir un rescate hasta que pague a los estafadores. Otros tipos de aplicaciones fraudulentas le piden que inicie sesión usando sus redes sociales o cuentas de correo electrónico que podrían exponer su información personal para que los estafadores la roben.

Tenga cuidado con las aplicaciones o los sitios web que solicitan permisos sospechosos, como otorgar acceso a sus contactos, mensajes de texto, contraseñas almacenadas o información de tarjetas de crédito. Además, la mala gramática o las palabras mal escritas en la descripción de una aplicación o en un sitio web son una señal de alerta de que no es legítimo.

### Enlaces de correo electrónico

Evite hacer clic en enlaces en correos electrónicos no solicitados o correos electrónicos de fuentes desconocidas. Los enlaces pueden conducir a un sitio web ilegítimo que intente que ingrese su tarjeta de crédito u otra información personal. Algunos enlaces pueden descargar malware (software malicioso, como virus informáticos) en su computadora cuando hace clic en ellos que pueden robar su información bancaria, incluida la identificación de inicio de sesión, contraseñas y números de tarjetas de crédito o débito. Estos correos electrónicos suelen ser muy similares a los enviados por minoristas, bancos y otras entidades conocidas.

Esté atento a los correos electrónicos que tengan errores tipográficos u otros errores obvios. Además, sea escéptico con los archivos adjuntos de correo electrónico descritos como cupones, reembolsos o formularios de pago, ya que podrían incluir malware. Y evite las ofertas por correo electrónico que parezcan "demasiado buenas para ser verdad". Si un correo electrónico promete artículos populares gratis o a un precio sorprendentemente bajo, probablemente sea una estafa.

### Hacer pagos en sitios no seguros

Antes de pagar una compra en línea, asegúrese de que el sitio web en el que se encuentra tenga "https" al comienzo de su URL con un símbolo de candado:


Esto significa que el sitio tiene una conexión de red protegida. Los sitios web con "http" al comienzo de la URL sin "s" son más vulnerables a los ataques de estafadores que roban información de tarjetas de crédito al monitorear el tráfico de la red. También tenga en cuenta las ventanas emergentes que aparecen mientras está en un sitio web y le solicitan la información de su tarjeta de crédito para recibir cupones o ganar artículos gratis. Las empresas legítimas no solicitan su información personal para esos fines.

### Uso de wifi público para comprar o acceder a información confidencial

La conectividad inalámbrica, también conocida como wifi, permite que su computadora portátil, PC o dispositivo móvil se conecte a Internet sin una conexión física por cable. Muchos restaurantes, hoteles, bibliotecas y otros lugares ofrecen wifi público gratuito, lo cual es conveniente cuando estás en movimiento. Sin embargo, es posible que estas redes no sean seguras (ya que no requieren una contraseña o brindan la misma contraseña genérica a todos los clientes para acceder) y pueden exponer su información personal y bancaria a estafadores que buscan robar nombres, números de seguro social y datos bancarios. números de cuenta

Evite usar wifi público para realizar compras en línea, iniciar sesión en sus cuentas financieras o acceder a otros sitios que tengan información confidencial sobre usted. También es una buena idea quedarse con los sitios web que tienen encriptación "https" (discutido anteriormente) cuando se encuentran en lugares públicos.

### Estafas de confirmación de entrega de paquetes

Esta estafa es especialmente popular durante las festividades cuando las personas reciben regalos por correo que pueden no estar esperando.

Los estafadores llaman o envían un correo electrónico afirmando ser del Servicio Postal de los EE. UU. o de una importante empresa de envíos y afirman que usted tiene un paquete en espera de entrega. Para asegurarse de que el paquete es para usted, se le pide que proporcione información personal, que los estafadores roban para usarla para abrir cuentas de crédito a su nombre. En respuesta a esta estafa, el Servicio Postal de EE. UU. explicó que no llama a las personas para pedir información personal si hay un problema con una entrega. Visite https://www.uspis.gov/news/scam-article/fake-usps-phone-calls (en inglés) para obtener más información.

Los estafadores también utilizan correos electrónicos y mensajes de texto en sus esquemas. Lea más https://www.fdic.gov/resources/consumers/consumer-news/documents/2020/2020-10-esp.pdf.

No permita que estas estafas empañen su espíritu navideño. En cambio, aquí hay precauciones que puede tomar para proteger su dinero mientras compra en línea:

- En general, utilice siempre contraseñas únicas y difíciles de adivinar en cada cuenta.
- Si está utilizando aplicaciones de compras, céntrese únicamente en las aplicaciones oficiales del minorista que se encuentran en el sitio web del minorista o en un mercado de aplicaciones de confianza, que ofrecen mayor seguridad.
- Nunca proporcione la información de su tarjeta de crédito a menos que esté en un sitio seguro, mostrando "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 proporcione dos pruebas al iniciar sesión en una cuenta. Presenta una capa adicional de seguridad para que sea más difícil para alguien que no es usted iniciar sesión en su cuenta. Para obtener más información, visite https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication (en inglés)
- Controle las facturas de las tarjetas de crédito y los extractos bancarios, así como las aplicaciones y otras transacciones en línea en busca de compras o retiros no autorizados. Póngase en contacto inmediatamente con su banco si ve algo sospechoso. Además, es posible que desee considerar suscribirse a los servicios de alerta. Muchos emisores de tarjetas de crédito, bancos y proveedores de aplicaciones móviles ofrecen servicios que le notifican sobre ciertas actividades de la cuenta, como inicios de sesión recientes desde dispositivos no reconocidos.

**Recursos adicionales:**

Comisión Federal de Comercio (FTC por sus siglas en inglés): Compras en internet https://consumidor.ftc.gov/articulos/compras-en-internet

FTC: ¿Compra en línea? Conozca a su distribuidor y sus derechos (en inglés) https://consumer.ftc.gov/consumer-alerts/2021/06/shopping-online-know-your-retailer-your-rights

CFPB Estudio detalla el rápido crecimiento de los préstamos "Compre ahora, pague después" (en inglés) https://www.consumerfinance.gov/about-us/newsroom/cfpb-study-details-the-rapid-growth-of-buy-now-pay-later-lending/

Cybersecurity & Infrastructure Security Agency (CISA, por sus siglas en inglés): Compras seguras en línea https://www.cisa.gov/uscert/ncas/tips/ST07-001

Para más recursos para el consumidor, visite FDIC.gov/español o vaya al FDIC Knowledge Center. También puede llamar gratuitamente a la FDIC al **1-877-275-3342 #9 para español**. Envíe sus comentarios o ideas para artículos a ConsumerNews@fdic.gov. ¡Suscríbase a esta y otras publicaciones gratis de la FDIC para mantenerse informado!

FDIC