

OFICINA DE PROTECCION AL CONSUMIDOR

Los días festivos traen más que tiempos festivos...También Traen Estafadores

Noviembre 2, 2020

Los días de las fiestas estarán aquí pronto. Mientras que la pandemia creó muchos giros nuevos en viejas estafas, las vacaciones también sacarán los criminales. Tarjetas de regalo vacías, solicitudes de caridad falsas, ciberataques, y ladrones que roban paquetes de su porche no solamente aparecen durante esta temporada. Pero dado que los consumidores están abrumados en 2020, y que dependen en gran medida de las transacciones y comunicaciones en línea, puede ser más fácil ser víctima de estafas este año. Aquí hay algunos consejos que debe seguir para mantenerse a salvo en esta temporada de fiestas:

Compras en línea

Según la Comisión Federal de Comercio, es [más seguro](#) pagar con tarjeta de crédito, que proporcionan protección adicional para la mayoría de las compras en línea. Las tarjetas de crédito también proporcionan procedimientos de disputa y beneficios para devoluciones o cambios. Las tarjetas de débito, incluso aquellas con logotipos de Visa o Mastercard, no proporcionan las mismas protecciones y procedimientos de disputa que las tarjetas de crédito.



*Asegurando Integridad
en nuestro Mercado*



Si ha sido víctima de una estafa, o si tiene alguna disputa sobre las actividades de un comerciante, comuníquese con la Oficina de Protección al Consumidor.

100 Maryland Avenue
Suite 3600
Rockville, MD 20850
Main: 240.777.3636
Tip Line: 240.777.3681
Fax: 240.777.3768
Consumer@MontgomeryCountyMD.gov

También puede **presentar una queja** en línea haciendo clic [AQUI](#)



Si compra en Craigslist, Facebook Marketplace, Letgo, u otros mercados de terceros, tenga en cuenta que [los estafadores utilizan](#) estos sitios para defraudarlo. Los delincuentes utilizarán fotos de archivo, o fotos de otras transacciones reales, para vender bienes [inexistentes](#) e alquilar propiedad inexistente. Si el trato parece demasiado bueno para ser verdad, y no puede verlo antes de enviar un pago digital o una tarjeta de regalo, es una señal de que usted puede estar tratando con una estafa. Si usted es el vendedor, el estafador puede querer pagarle por cheque y por una cantidad mayor de la que busca. Esto se hace generalmente con la necesidad de *que escriba* un buen cheque para reembolsar la diferencia en uno malo. Eso es una señal de una estafa de fraude de cheques.

Finalmente, en este año hemos visto un aumento de sitios web minoristas falsos que venden bienes inexistentes—muchos utilizan Shopify como plataforma y publicidad en las redes sociales. Estos comerciantes venden productos falsificados o no tienen bienes para vender. Pueden enviarle sobres vacíos para obtener una prueba de entrega para combatir los gastos de devolución o disputas a través de su banco. Según la revista *Forbes*, una característica distintiva de la estafa es encontrar el mismo anuncio, imágenes, y se ocupa de numerosos diferentes compañías con nombres que suenan extraños, por ejemplo, Predictfuture vende el mismo equipo de ejercicios al mismo precio reducido como Geoghost.store.

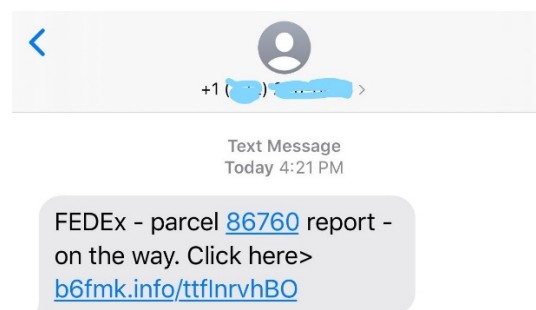
Tarjetas de regalo

Estas tarjetas son regalos geniales y fáciles, pero también son las favoritas de los delincuentes que saben que las tarjetas de regalo son prácticamente imposibles de rastrear. Si alguien se comunica con usted sobre facturas impagadas y exige el pago

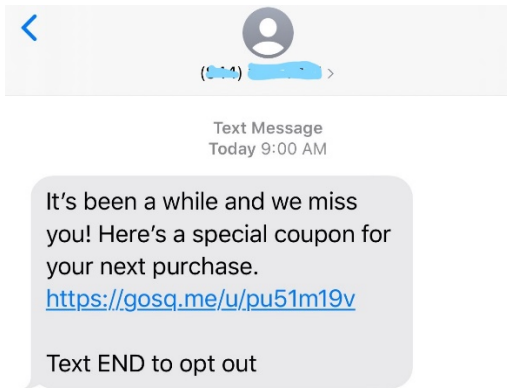
mediante una tarjeta de regalo o una tarjeta prepagada, o incluso una transferencia bancaria, es una bandera roja que una estafa está en marcha. Al comprar tarjetas de regalo, asegúrese de que el embalaje no se ha visto comprometido. No compre tarjetas de regalo que tengan un empaque que muestre el código de barras en la parte posterior. Según una encuesta de AARP informada por CNBC, uno de cada cinco consumidores dice que las tarjetas de regalo que recibieron estaban vacías. Los delincuentes recogen y registran el número de tarjetas de regalo vacías, esperan la notificación de activación y drenan rápidamente el valor de la tarjeta, a veces incluso antes de que se presente como regalo. CNBC también informa que las tarjetas de regalo vendidas a través de sitios de subastas en línea a menudo son robadas. Consulte nuestro sitio web para obtener más información sobre el uso de [tarjetas de regalo](#).

Ciberseguridad

Los ciberataques a través de phishing y smishing comenzaron a principios de otoño con mensajes falsos sobre el envío retrasado:



o cupones de comerciantes no identificados que buscan obtener su negocio de nuevo:



Al revisar estos mensajes, ¿tiene sentido la dirección del remitente? ¿El USPS le envía un correo electrónico desde una dirección de correo electrónico biz o .net? ¿El texto lo dirige a FedEx pero con una dirección web que no suena como el sitio web real de FedEx? No haga clic en correos electrónicos, mensajes de texto o chats no solicitados a través de las redes sociales u otras plataformas de aplicaciones de comunicación. Lo involucrarán en una estafa, o descargarán programas de virus o malware que mantendrán su cuenta y la información de acceso al correo electrónico para cometer un robo de identidad en el futuro. Visite nuestro sitio web para obtener más información sobre [phishing, smishing y pharming](#).

Los piratas del porche

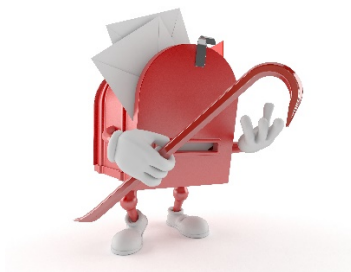
Los piratas del porche son la [nueva forma de hurto](#). En lugar de robar mercadería en las tiendas, estos delincuentes se la robarán de la entrada. Según un [informe](#), el 36% de los consumidores en 2019 informaron haber tenido al menos un envío robado.



Para combatir la piratería en los porches, realice un seguimiento de sus paquetes en línea para que puedan recuperarse rápidamente, considere la posibilidad de enviar paquetes a su dirección de trabajo o utilizar recogidas en la tienda cuando esté disponible, o instalar una cámara de seguridad en la puerta principal, un foco o una caja de seguridad, a los ladrones no les gustan las cámaras. Si los artículos son robados, presente inmediatamente una reclamación con el comerciante y el proveedor de envío.

Merodeadores del correo

Durante las fiestas, los residentes pueden utilizar su buzón de correo para enviar tarjetas navideñas, con cheques o tarjetas de regalo. Sin embargo, tenga en cuenta que una bandera levantada en ese buzón indica a los ladrones de correo que hay correo para robar.



Los delincuentes [robarán su correo](#). "lavarán cheques" cualquier cheque y volver a escribir a sí mismos, o incluso imprimir cheques falsificados utilizando la información de su cuenta. Coloque su correo en los buzones azules o llévelos directamente a la oficina de correos.

Donaciones

Las organizaciones y campañas benéficas aumentan durante la temporada navideña. Antes de donar a una organización benéfica, asegúrese de que sea una organización benéfica y no un [PAC](#) fraudulento y que estén registrados en el Secretario de Estado de [Maryland](#).



Luego investigue para asegurarse de que usan el dinero que reciben para el trabajo y no para contratar centros de llamadas para obtener más dinero. [Charity Navigator](#), [Guidestar](#), [Charity Watch](#), y [Give.org](#) son solo algunos lugares para ayudarlo a ser su investigación.

Conclusión

Para mantenerse seguro esta temporada de navideña se requiere una diligencia adicional. Consulte nuestro sitio web para obtener más información y consejos sobre [compras navideñas](#) u otros temas relacionados, como el uso de aplicaciones de pago [digital](#) en lugar de [tarjetas de crédito o débito](#), o la ley de Maryland sobre [devoluciones y cambios](#).

