



BOLETÍN DE NOTICIAS DEL CONSUMIDOR DE LA FLORIDA

Una Publicación del Departamento de
Agricultura y Servicios al Consumidor

Diciembre 2025

ES LA TEMPORADA... PARA ESTAFAS



¡La temporada festiva está aquí! Estamos hablando de fiestas navideñas, pasar tiempo con familiares y amigos, dar y recibir regalos y disfrutar de todas las decoraciones navideñas. Aunque es un momento de celebración y alegría, no olvide estar atento cuando se trata de estafas. Con un mínimo esfuerzo, puede evitar ser víctima de una de estas estafas navideñas.

El Better Business Bureau (BBB) ha reunido la siguiente lista de las principales estafas navideñas y cómo evitarlas.

1. Anuncios Engañosos en las Redes Sociales:

Con frecuencia recibe anuncios de productos en sus redes sociales y algunos parecen muy atractivos. Sin embargo, ¡investigue la empresa / producto antes de comprar! BBB afirma que las personas han denunciado artículos que nunca aparecen a pesar del pago puntual o de recibir falsificaciones o artículos que de ninguna manera coinciden con la descripción de lo que se anunció. A otros se les ha facturado por esa prueba "gratuita" a la que nunca accedieron. El Informe de riesgo de BBB Scam Tracker de 2024 indica que las compras en línea fueron la cuarta estafa más arriesgada reportada por los consumidores.

CONSEJO: Antes de realizar el pedido, consulte el perfil comercial y las reseñas en línea en sitios web independientes.

2. Aplicaciones Con Temas Festivos:

Google Play y la App Store de Apple tienen cientos de aplicaciones con temas navideños donde los niños emocionados pueden chatear por video en vivo con Santa, encender la menorá, ver a Santa alimentar a los renos reales, rastrear el trineo en Nochebuena o leerle sus listas de deseos.

CONSEJO: Tenga cuidado con las aplicaciones gratuitas: la mayoría contienen más publicidad que otras aplicaciones que cobran una pequeña tarifa y pueden contener programa maligno. Verifique las políticas de privacidad de cerca para determinar qué información se recopilará y siempre lea las reseñas.

www.FloridaConsumerHelp.com

1-800-HELP-FLA(435-7352) • Mon-Fri, 8a.m. – 5p.m., EST • 1-800-FL-AYUDA(352-9832)

3. Intercambios de Regalos en las Redes Sociales:

¿Has oído hablar de los intercambios de regalos de “Secret Sister” (Hermana Secreta) o “Secret Santa Dog” (Cachorro Secreto de Santa)? De lo contrario, es probable que haya oído hablar de este esquema en el que proporciona su dirección de correo electrónico, prometiendo enviar un regalo a otro en la lista, reenviar a su familia y amigos para que hagan lo mismo, y otros harán lo mismo por usted. El problema con esto es que cualquiera que participe ha compartido su información personal con el embaucador y le ha enviado un regalo, y todos los involucrados han violado la ley por participar en un esquema piramidal.

CONSEJO: Solo compre regalos de minoristas confiables para aquellos que están cerca y son queridos.

4. Tarjetas de Regalo Gratis:

A todos nos gusta “GRATIS”. Sin embargo, a veces “gratis” viene con más de lo que queremos. Los estafadores se aprovechan de la emoción por la posibilidad de gratis enviando correos electrónicos de phishing, creando anuncios emergentes o enviando mensajes de texto, solicitando información personal a cambio de tarjetas de regalo gratis.

CONSEJO: Si ha recibido un correo electrónico de este tipo, márkelo como spam o correo no deseado y elimínelo. Elimine también cualquier texto similar no solicitado.

5. Hablando de Tarjetas de Regalo:

Si una agencia gubernamental, empresa u otra entidad se comunica con usted ofreciéndole cualquier cosa a cambio de una tarjeta de regalo, es una estafa. Ninguna empresa legítima le pedirá que compre una tarjeta de regalo para pagarles. Las solicitudes pueden venir como una llamada telefónica, correo electrónico, mensaje de texto o mensaje de redes sociales, y algunas indicarán que es urgente. Las instrucciones pueden incluir una tienda específica para obtener la tarjeta de regalo. Sin embargo, todas las instrucciones le indicarán que proporcione el número de la tarjeta de regalo y el PIN, ya sea verbalmente o con una foto.

CONSEJO: Si tiene alguna duda sobre si es o no una estafa, pregúntese: “¿Es alguien en quien confío?” Si no, es una estafa. Cuando compre una tarjeta de regalo para un regalo real, siempre guarde una copia de la tarjeta y el recibo de la tienda para informar cualquier estafa a la compañía de tarjetas de regalo y solicitar que le devuelvan su dinero.

6. Organizaciones Benéficas Falsas:

Los días festivos son un momento para donaciones caritativas, pero tenga cuidado con las organizaciones benéficas fraudulentas y los estafadores. Evite las donaciones espontáneas a organizaciones desconocidas. Las organizaciones confiables agradecerán sus donaciones mañana tanto como lo hacen hoy.

CONSEJO: Verifique que las organizaciones benéficas estén registradas en Florida en [Check-A-Charity](#). Si es posible, haga donaciones a través del sitio web de la organización benéfica con su tarjeta de crédito.

7. Estafas de Mascotas:

Si está pensando en agregar un miembro de cuatro patas a la familia estas vacaciones, tenga cuidado con las estafas. Según el Better Business Bureau, hasta el 80% de los anuncios de mascotas en línea son falsos.

CONSEJO: Antes de tomar la decisión de comprar, asegúrese de ver al animal en persona.



TENGA CUIDADO AL COMPRAR EN LÍNEA

En lo que puede ser la época más ocupada del año para algunos, comprar en línea ciertamente puede hacernos la vida más fácil. En lugar de ir de tienda en tienda, examinando los estantes, puede elegir el regalo perfecto con solo unos pocos clics. A veces sabe exactamente lo que está buscando y dónde encontrarlo, pero otras veces ve un anuncio en las redes sociales o recibe un correo electrónico, y el producto está a solo un enlace de distancia. Antes de hacer clic en ese enlace, considere si el sitio web es legítimo.

- **Evalúe la Barra de Dirección de los Minoristas.** Los estafadores a menudo usarán una URL que está cerca de la URL de un minorista legítimo, pero no exactamente igual. ¿La dirección comienza con “https”? La “s” indica seguro, y si lo ve, indica que el protocolo del sitio web es seguro. Busque un icono de candado en la barra de direcciones. Cuando haga clic en ese icono, debería ver información del sitio, como un SSL válido, las cookies en uso y si su información está segura cuando se envía al sitio.
- **Evalúe el Sitio Web.** ¿El sitio web utiliza la gramática y la ortografía adecuadas? ¿Hay una página de contacto con un número de teléfono y una dirección física válidos? ¿Qué pasa con la política de privacidad del sitio web? Si respondió “no” a cualquiera de estos, puede que no sea legítimo.

- **Reflexione Sobre la compra.** Antes de realizar una compra en un sitio web con el que no está familiarizado, investigue la empresa. Consulte las reseñas en otros sitios para obtener reseñas de la empresa e informes de estafas o calificaciones de confianza.
- **Rechaza la Oferta.** Si encuentra una oferta más barata que la suciedad que no puede ser cierta, probablemente no lo sea. Verifique los costos de envío y manejo, las tarifas de envío, etc. Si ve alguna señal de alerta, es probable que sea una estafa.
- **Resiste la Compra Impulsiva.** Una vez más, la investigación es clave. Los anunciantes, legítimos y fraudulentos, tienen la capacidad de rastrear sus comportamientos de compra a partir de anuncios en redes sociales y adaptarán los anuncios que ve. No actúe por capricho: siempre investigue la empresa y el producto antes de comprar para evitar a los estafadores.
- **Considere la Tarjeta de Crédito.** Las compañías de tarjetas de crédito permiten disputas de cargos fraudulentos, lo que es posible que no pueda hacer si compra un artículo con una tarjeta de débito o de regalo. Si se le pide que pague con una tarjeta de regalo prepagada o una aplicación de billetera digital, como Zelle, Venmo o PayPal, podría ser una estafa.



ALERTA AL CONSUMIDOR DE LA FCC

La FCC publicó recientemente la siguiente [alerta al consumidor](#) con respecto a los estafadores que ofrecen servicios de cable y transmisión con descuento.

Alerta de la FCC: Estafadores que Ofrecen Servicios de Cable y Transmisión con Descuento. Los consumidores informan llamadas automáticas y mensajes de voz que afirman que “el 50% de descuento en su factura mensual está a punto de caducar” y los instan a devolver la llamada de inmediato.

La Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) está alertando a los consumidores sobre llamadas y mensajes de texto fraudulentos que afirman ofrecer un 50% de descuento en las facturas de Comcast, Spectrum o Prime. Los consumidores están denunciando llamadas automáticas y mensajes de voz que reclaman. Por ejemplo, una persona que llamó dijo:

“Hola. Esto es Comcast Xfinity. Estamos revisando tu cuenta y parece que tienes 50

El porcentaje de descuento en su factura mensual vence hoy. Para confirmar y asegurar sus ahorros, llame al número que aparece en su identificador de llamadas de inmediato. Esta oferta no puede ser extendido. Gracias”.

Las quejas presentadas ante la FCC informan que a los consumidores que devuelven la llamada al número a menudo se les anima a actuar rápidamente para asegurarse de mantener el “descuento”. El estafador también afirmará que la única forma de asegurar el descuento es pagar por adelantado varios meses de servicio con una tarjeta de regalo. La presión para actuar rápidamente y solo aceptar tarjetas de regalo como pago son signos seguros de estafa.

Si tienes preguntas sobre tu factura de cable o suscripciones y descuentos de transmisión, llama o envía un correo electrónico a tu proveedor de servicios al número oficial de servicio al cliente o a la dirección de correo electrónico que figura en tu factura. Muchos servicios también ofrecen la oportunidad de chatear con el servicio de atención al cliente en su sitio web oficial o en el portal de su cuenta.

Qué Hacer Si Ha Sido Estafado

Si cree que es víctima de una estafa, debe:

- Repórtelo a la policía local lo antes posible.
- Póngase en contacto con la compañía de tarjetas de regalo. Es posible que puedan ayudarlo a recuperar su dinero.
- [Presente una queja ante la FCC](#). Lea las preguntas frecuentes del Centro de quejas de la FCC para obtener más información sobre el proceso informal de quejas de la FCC, incluido cómo presentar una queja y qué sucede después de presentar una queja.

Para obtener más información sobre todo tipo de estafas y fraudes, visite [Scams and Fraud / Consumer Resources / Home - Florida Department of Agriculture & Consumer Services](#).



“LEY LIMÓN” PARA MASCOTAS DE FLORIDA

Si su familia está considerando agregar una nueva mascota, conocer sus derechos antes de realizar la compra puede brindarle cierto alivio en caso de que algo salga mal.

La Ley de Mascotas de Florida, [Sección 828.29, Estatutos de Florida](#), proporciona requisitos de salud estandarizados para perros y gatos vendidos dentro de Florida. Los comerciantes de mascotas tienen prohibido tergiversar deliberadamente la salud de cualquier perro o gato dentro del estado. La ley de Florida define a un comerciante de mascotas como cualquier persona que venda más de dos camadas o 20 perros o gatos al público por año. La Ley de Mascotas de Florida no se aplica a los criadores aficionados, las instalaciones de control de animales del condado o municipales, ni las organizaciones humanitarias sin fines de lucro registradas.

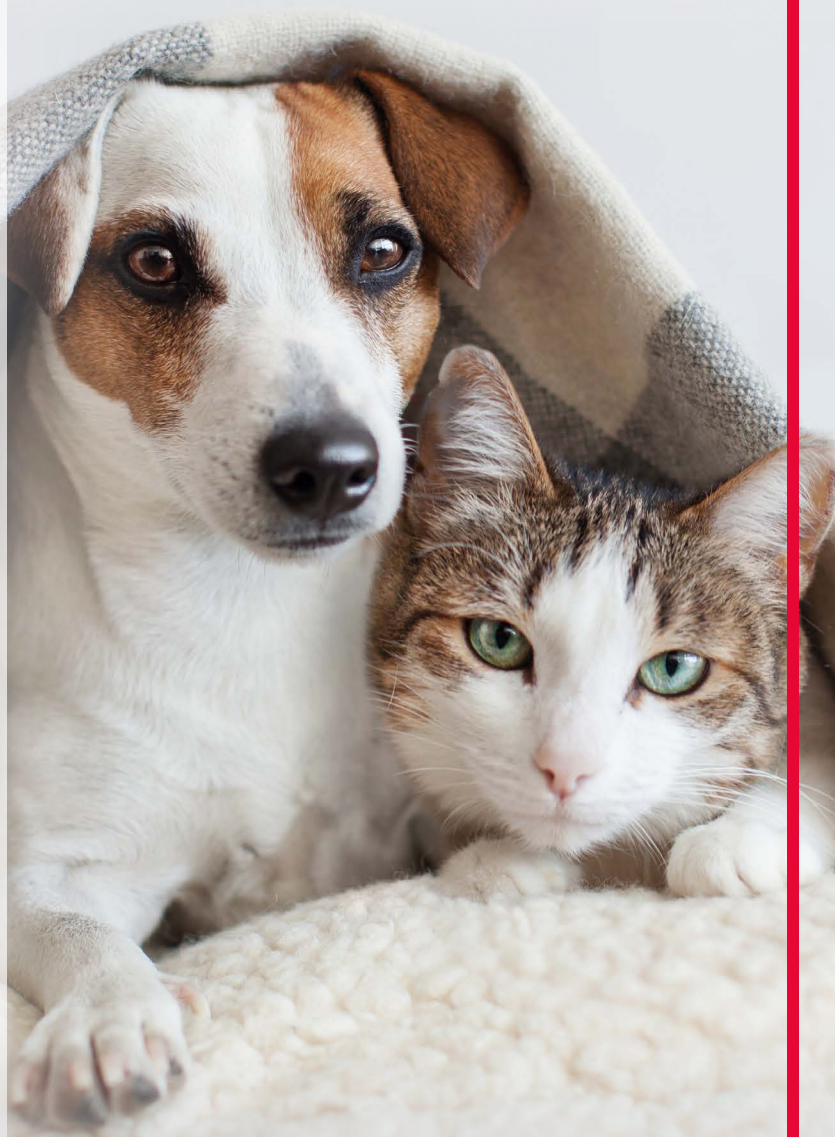
Los comerciantes de mascotas están obligados por ley a proporcionar al consumidor un aviso por escrito que detalle los derechos del comprador, junto con un certificado oficial de inspección veterinaria, que acredite la raza, el sexo, la edad, el color y el historial de salud de la mascota, incluida una lista de vacunas. Si el concesionario no está familiarizado con este requisito o se niega a proporcionar cualquiera de los documentos, tenga cuidado.

Al comprar la mascota, la ley proporciona a los nuevos propietarios períodos de tiempo específicos dentro de los cuales se deben completar ciertas acciones. Cualquier enfermedad contagiosa o infecciosa debe ser documentada por un veterinario dentro de los 14 días; Los defectos congénitos o hereditarios, o las tergiversaciones en cuanto a la raza, el sexo, la edad o el color, deben documentarse en el plazo de un año. Al tener conocimiento de cualquiera de los anteriores, el consumidor tiene dos días para notificar al distribuidor de los hallazgos y tres días para proporcionar la documentación escrita.

Tras la notificación, el consumidor tiene tres opciones:

- El consumidor puede devolver la mascota al distribuidor para obtener un reembolso completo y el reembolso de los costos veterinarios.
- El consumidor puede cambiar la mascota por otra de igual valor y se le reembolsarán los gastos veterinarios.
- El consumidor puede optar por quedarse con la mascota, y el distribuidor será responsable de los costos veterinarios razonables para tratar o curar al animal.

Los problemas relacionados con el certificado de salud deben dirigirse al Departamento de Agricultura y Servicios al Consumidor de Florida al (850) 410-0950.



CLONACIÓN DE VOZ DE IA

El mes pasado, discutimos el creciente uso de la inteligencia artificial o IA. Existen numerosas formas en que se utiliza la IA en la vida diaria, como asistentes de voz (piense en Alexa o Siri), recomendaciones de música o películas en su servicio de transmisión o chatbots de servicio al cliente; La lista tanto en nuestra vida personal como en la industria se expande diariamente. Sin embargo, como con cualquier nueva tecnología, se ha adaptado para su uso en estafas. Este mes, vamos a ver en detalle las estafas de clonación de voz de IA.

Las herramientas de clonación de voz habilitadas por IA se están utilizando maliciosamente para imitar voces y luego defraudar a las víctimas. Algunas de las diversas tácticas utilizadas son las siguientes:

- **Fraude del CEO:** el CEO de su empresa se comunica con usted con una solicitud urgente: debe pagar un pedido de la empresa de inmediato. Desafortunadamente, el CEO no tiene su tarjeta de compra disponible. Quieren que use su cuenta personal y transfiera dinero para completar la transacción y la compañía le reembolsará. ¿Qué harías?
- **Estafa de abuelos:** su nieto lo llama y le pide ayuda. Está en problemas y necesita dinero de inmediato o la situación podría empeorar mucho. ¿Cómo se dice que no?
- **Suplantación de identidad del gobierno y de las fuerzas del orden:** el IRS acaba de comunicarse con usted para decirle que su declaración de impuestos más reciente fue errónea, pero puede evitar una auditoría, multas y tiempo en la cárcel pagando la diferencia mediante transferencia bancaria por teléfono. ¿Deberías estar de acuerdo?

Es probable que cada una de estas estafas tenga múltiples señales de alerta en común. Aquí hay cosas que debe buscar si se enfrenta a una situación similar.

- Información de contacto inusual. Probablemente no reconozca el número desde el que se realiza la llamada.
- Hay una urgencia en la llamada, y la persona que llama no se deja disuadir por sus preguntas, insistiendo en que debe enviar los fondos AHORA sin consultar a otros ni verificar su solicitud.
- Manipulación emocional. La persona que llama usa sus emociones para obtener una respuesta de usted. El CEO puede decirle que sus acciones resultarán en una gran promoción, su nieto puede llorar y suplicar, y el empleado del gobierno puede amenazarlo con acciones legales.
- Métodos de pago inusuales. La persona que llama solicita tarjetas de regalo, transferencias bancarias o criptomonedas.
- Falta de sonidos humanos normales. La voz de la persona que llama es plana y no tiene variación en el tono, o la cadencia está apagada. No hay ruidos de relleno como un suspiro o un carruaje de garganta.
- Falta de ruidos de fondo o ruidos de fondo extraños. Es posible que no haya ruido de fondo que normalmente escucharías, como otros hablando o el tráfico, o que el ruido sea extraño, como un eco electrónico.
- Repetición. No importa lo que digas, la persona que llama repite las mismas frases o frases similares.

¿Cómo puede protegerse si los estafadores están usando una voz familiar y tácticas emocionales para aprovecharse? Puede proteger su seguridad financiera con solo unos sencillos pasos.

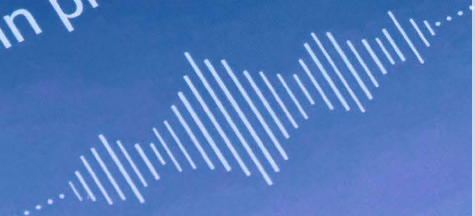
- Minimice el contenido disponible públicamente en línea. Si hay muy poco contenido de voz en línea, es más difícil para el estafador obtener muestras para clonar su voz y la de sus seres queridos y colegas.
- Siempre verifique. Cree una palabra de seguridad familiar para usar en tales situaciones. Si la persona que llama no puede proporcionarlo, probablemente sea una estafa. Las empresas deben emplear un riguroso proceso de verificación que descubra tales actividades, con capacitación obligatoria para los empleados. Consulte a una persona de confianza para obtener asesoramiento.
- Haz preguntas. Si la llamada es de un número extraño, pero usted conoce a la persona que llama, hágale una pregunta a la persona que llama para la que solo él o ella sabría la respuesta.
- Véalo por escrito. Para los suplantadores del gobierno o de las fuerzas del orden, pida verlo todo por escrito. Ninguna agencia gubernamental lo obligará a realizar un pago por teléfono, y definitivamente no con una tarjeta de regalo.

Aunque estos escenarios suenan inquietantes, si mantienes la calma, buscas las pistas y das algunos pasos adicionales con seguridad, puedes evitar convertirte en una víctima.

El próximo mes, continuaremos la serie sobre estafas de IA y cómo evitarlas.



Voice Cloning
in progress....



LA NUEVA ESTAFA: GHOST TAPPING (TOQUE FANTASMA)

Cuando sus brazos están llenos de compras navideñas, ¿no es conveniente cuando puede tocar su tarjeta de crédito para pagar? Aunque es conveniente, también es objeto de una nueva estafa. Aprenda a mantener su tarjeta de crédito a salvo del Toque Fantasma.

El Better Business Bureau (BBB) emitió recientemente una alerta por una nueva estafa: el ghost tapping (toque fantasma). La nueva estafa involucra tarjetas de pago y billeteras móviles. La tecnología tap-to-pay (pago-a-pago) utiliza Near Field Communication (NFC), lo que permite que los dispositivos intercambien datos a muy corta distancia. Si bien NFC es en gran medida seguro, los estafadores pueden explotarlo, especialmente en multitudes o situaciones de distracción (como compras festivas).

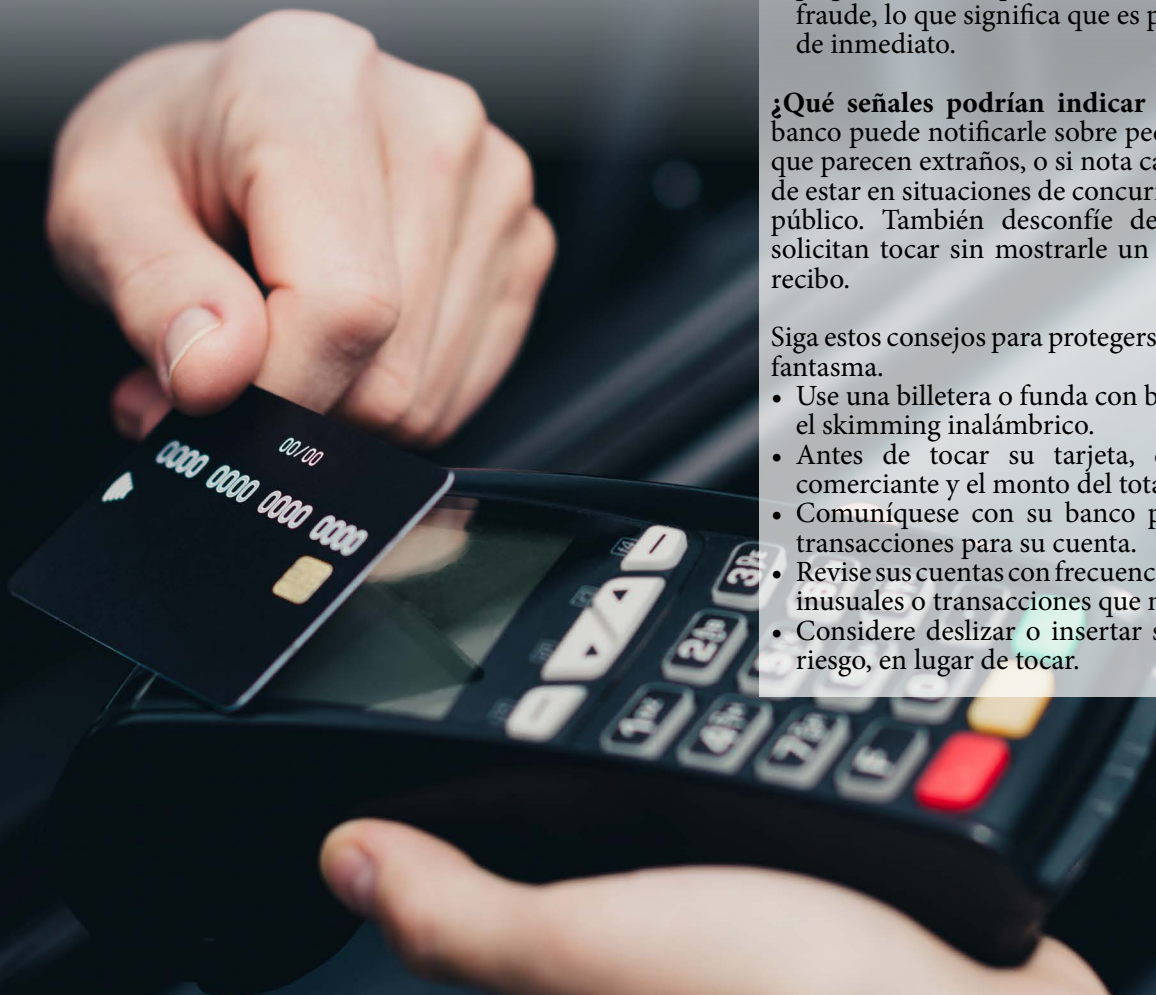
El ghost tapping (toque fantasma) no necesita el contacto físico requerido con estafas anteriores con tarjetas de débito y crédito. Los estafadores solo necesitan un dispositivo de escaneo y estar cerca de usted. Tenga en cuenta las siguientes situaciones:

- Contacto cercano en lugares públicos: los estafadores pueden intentar chocar “accidentalmente” con usted y cargar en secreto su tarjeta de crédito o billetera móvil habilitada para tocar.
- Comerciantes falsos: En varias ferias, mercados o festivales, los estafadores pueden hacerse pasar por vendedores y especificar pagos a domicilio, cobrándole mucho más que los artículos insignificantes que están vendiendo.
- Fraude de caridad: los estafadores pueden pedir una pequeña donación, pero luego cargar a su tarjeta por mucho más.
- Apresurar una compra: Especialmente durante la temporada navideña, los estafadores esperan que no preste atención y toque su tarjeta sin verificar el nombre comercial o el monto de la transacción.
- Comenzando poco a poco. En algunos casos, se realizan pequeños retiros para eludir los sistemas de detección de fraude, lo que significa que es posible que no note el robo de inmediato.

¿Qué señales podrían indicar un toque fantasma? Su banco puede notificarle sobre pequeños cargos de “prueba” que parecen extraños, o si nota cargos sospechosos después de estar en situaciones de concurrencia o asistir a un evento público. También desconfíe de los proveedores que le solicitan tocar sin mostrarle un total o proporcionarle un recibo.

Siga estos consejos para protegerse de ser presa de golpecitos fantasma.

- Use una billetera o funda con bloqueo RFID para detener el skimming inalámbrico.
- Antes de tocar su tarjeta, confirme el nombre del comerciante y el monto del total en la pantalla de pago.
- Comuníquese con su banco para promulgar alertas de transacciones para su cuenta.
- Revise sus cuentas con frecuencia para detectar actividades inusuales o transacciones que no reconoce.
- Considere deslizar o insertar su tarjeta en áreas de alto riesgo, en lugar de tocar.



ACERCA DE LA DIVISIÓN FDACS DE SERVICIOS AL CONSUMIDOR

FDACS es la agencia estatal de protección al consumidor de Florida responsable de manejar las quejas de los consumidores y regular muchas industrias que afectan directamente a los consumidores de Florida. FDACS maneja más de 400,000 quejas y consultas de los consumidores, supervisa más de 500,000 dispositivos regulados, entidades y productos como bombas de gas y básculas de comestibles, realiza más de \$30,000 análisis de laboratorio en productos como gasolina y fluido de freno, realiza casi 9,000 inspecciones de paseo justo y devuelve más de \$2.8 millones a los consumidores a través de mediaciones con empresas.



La División de Seguridad Alimentaria supervisa los alimentos desde el punto de fabricación y distribución a través de las ventas al por mayor y al por menor para garantizar al público productos alimenticios seguros, saludables y debidamente representados.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD



La Comisión de Seguridad de Productos de Consumo proporciona información sobre la retirada de productos de consumo como parte de la misión de la agencia de proteger a los consumidores y a las familias de los productos peligrosos.

OPRIMA EN EL ICONO ANTERIOR PARA VER LO RETIRADO, LOS RETIROS DEL MERCADO Y LAS ALERTAS DE SEGURIDAD.

El Departamento de Agricultura y Servicios al Consumidor de Florida es el centro de intercambio de información del estado para quejas, protección e información de los consumidores. Los consumidores que deseen información sobre la presentación de una queja contra una empresa o que crean que se ha producido fraude pueden visitarnos en línea en FloridaConsumerHelp.com o ponerse en contacto con la línea directa de información y protección al consumidor del departamento llamando al 1-800-HELP-FLA (435-7352) o al 1-800-FL-AYUDA (352-9832) en español.