MANUAL GENERAL DE PREVENCIÓN SOBRE EL DELITO DE FRAUDE A TRAVÉS DE INTERNET

Especialmente por páginas de venta por medio de Facebook.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

La plataforma de Facebook es muy grande y es utilizada de diversas formas, desde hace unos años se ha impulsado la plataforma Marketplace para realizar ventas en Internet, esto se hizo con el fin de que algunas personas buscan productos o servicios a través de publicaciones, lo cual ha causado que cada vez haya más víctimas de fraude

Para poder hablar de los fraudes por medio de la plataforma de Facebook, debemos saber que el Fraude Cibernético e Informático se define como el uso de dispositivos digitales con el objetivo de cometer actividades delincuenciales como suplantación de identidad, robos de contraseñas y datos, estafas, secuestros digitales, etc. También se refiere al fraude realizado a través del uso de una computadora o del Internet. La piratería informática (hacking) es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Estos fraudes electrónicos se llevan a cabo mediante el uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida. Los delincuentes pueden distorsionar los datos de diferentes maneras.

Una de las primeras causas que ha llevado en aumento los fraudes a través de la plataforma de Facebook hablando de las ventas, es la pandemia del COVID-19, el consecuente confinamiento y el cierre de negocios de manera física, las compras electrónicas por internet se dispararon en México y todo el mundo; sin embargo, con ello también las estafas y fraudes en sitios como Mercado Libre o redes sociales como Facebook y su famoso Marketplace.

Se ha dado más a través de Facebook ya que es una red social, un mercado enorme y como un mercado tradicional se ofertan todo tipo de bienes, además de servicios a través de esta red social. Pero esta red social tiene diferentes mecanismos para que los usuarios no sean víctimas de los diferentes delitos cibernéticos.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

TIPOS DE FRAUDES ELECTRÓNICOS

por medio de la plataforma Facebook:

TIPOS DE FRAUDES	DESCRIPCIÓN
GRUPOS DE FACEBOOK	Usuarios con diferentes intereses se agrupan con el objetivo de compartir experiencias y otras cosas, como ventas. Aunque los grupos no hayan sido creados con ese propósito en muchos de ellos se permite la venta entre usuarios. Tal es el caso de grupos cerrados cuyos objetivos son variados, pero en los que sus miembros hacen transacciones con bienes y servicios. Sin embargo, muchos defraudadores se valen de la confianza de los usuarios y los estafan.
ALQUILERES DE VIVIENDAS VACACIONALES	Tratan de engañar al usuario para alquilar un apartamento inexistente a un precio mucho más bajo de lo normal. Recomendaciones sé debe investigar los precios de alquileres de la zona, verificar si las imágenes del apartamento no sean sustraídas de otra web, ver en físico el inmueble, no debes pagar a través de servicios de envío de dinero de forma anónima, o por transferencia a un banco de diferente nacionalidad de la del presunto propietario.
COMPRAS ONLINE	Las tiendas online deben cumplir con unos requisitos legales, como información sobre la empresa y textos legales (política de privacidad, términos y condiciones, etc.). Se debe sospechar si no se encuentra esa información o si se nota que está mal redactada. De igual forma se debe buscar opiniones y comentarios de la tienda, tanto en la propia web como fuera de ella y en las redes sociales.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

AMCDC
Asociación Mexicana Contra Delitos Cibernéticos

EL ROBO DE IDENTIDAD	En este caso los estafadores asumen la identidad de otra persona, a veces de formas realmente sofisticadas, y con fines varios. En el caso podemos encontrarnos con consumidores que utilizan una tarjeta de crédito a otro nombre y realizan compras con una identidad que no es la suya.
FRAUDE POR TRIANGULACIÓN	Consiste en cliente compra un producto en una tienda pirata que ha adquirido ilegalmente numeración de tarjetas robadas, la tienda utiliza una tarjeta robada para comprar el mismo producto en una tienda legal y le hace llegar el producto al cliente. El usuario no sabe que ha sido víctima de una estafa., por la complejidad y la cantidad de capas que implica, es un fraude difícil de detectar.
PHISHING	Este término hace alusión a la idea de *«pescar al usuario»* (del inglés fishing=pescar). Este tipo de fraude se basa en engañar al usuario para poder hacerse con usuarios/contraseñas y datos bancarios, utilizando webs falsas. Por eso es importante asegurarse siempre de que la URL a la que se nos remite es la verdadera y cuenta con un certificado de seguridad.
PHARMING	Es similar a un tipo de Phishing más sofisticado. En este caso el estafador trata de modificar las direcciones DNS para que el usuario acceda a una web idéntica a la original e incluso con una URL creíble, y así poder acceder a nuestros datos para fines varios. En el caso de una entidad bancaria, por ejemplo, acceder a nuestro dinero.
EL TICKET DEL OXXO	Cuando se vende un artículo por medio de Facebook y Marketplace, generalmente el vendedor y el comprador llegan a un acuerdo para entregar el producto en un punto medio. Sin embargo, la estafa consta en que el

	Comprador señala que no puede asistir al lugar de encuentro. En su estrategia afirma que enviará a un familiar de confianza y que, para que confíen en él, envía una foto de un ticket de transferencia falso con la cantidad que el vendedor ha puesto a su producto. Pese a que el vendedor argumente que aún no llega el depósito a su cuenta bancaria, el comprador comenta que la transferencia puede tardar un poco en reflejarse ya que se realizó a través de Oxxo.
TIENDAS DE ARTÍCULOS BARATOS	Si se encuentra publicidad de tiendas con ofertas exageradas, es un gran motivo para desconfiar y no hacer clic en la publicación. Sin embargo, si todavía tiene deseos de entrar en dicha oferta, debes observar si la página que visita empieza por “https” y si tiene un candado verde. También si ofrece diferentes métodos de pago seguro, que sean conocidos por usted, y si tiene buenas críticas en internet. Otro motivo de desconfianza es que la tienda no tenga un contacto real con teléfono y dirección.
FAKE NEWS	Se identifican por el contenido fraudulento con el objetivo de ser engañoso, y compartido con la intención de afectar procesos públicos. Existen distintos tipos como son la parodia que no causa mayor daño, contenido engañoso es aquel en que la información es distorsionada, el contexto falso es la información real con un contexto falso, el contenido impostor es cuando una persona suplanta la identidad real, el contenido manipulado es la información o imágenes manipuladas para engañar a los demás y el contenido fabricado está recién fabricado con el objetivo de causar daños, y engañar. Algunas de estas Fake News tienen enlaces que te redirigen a portales “malware” con el fin de infectar nuestro dispositivo.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

LOS FRAUDES POR MEDIO DEL COMERCIO y las redes sociales

Tienen cosas buenas y cosas malas, una de las malas es que cualquier persona puede llegar a ser víctima de estos delitos, pero la buena es que este tipo de acciones ilegales pueden prevenirse y combatirse, y todo ello empieza por conocer qué tipos de fraude digital son los más habituales, principalmente en las plataformas más conocidas como lo es Facebook.

¿COMO DETECTAR UNA PÁGINA DE Facebook es falsa?

Hay varios tipos de páginas falsas con intereses ilegales las más comunes son páginas de venta de artículos.

Si se quiere saber cómo poder identificar a estas páginas, antes debemos conocer muy bien cuáles son las reglas y opciones que nos ofrece la plataforma. Una de las formas más fácil de identificar la autenticidad de una página es comprobando si tiene insignia de verificación azul, significa que Facebook ha comprobado que esa página es real y corresponde a una marca o personaje público.

¿CÓMO IDENTIFICAR UN PERFIL falso en Facebook?

El perfil de la persona cuenta con las siguientes normalizaciones

- Una sola fotografía de perfil. Puede ser una cuenta fraudulenta o, simplemente, una persona celosa de su intimidad.
- Una fotografía de perfil que no corresponde con un humano. Dibujos,

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

fotografías de paisajes o de personajes de televisión son algunas de las fotografías de perfil preferidas para los perfiles falsos o, de nuevo, los celosos de su privacidad.

- Una fotografía de perfil falsa. ¿A qué nos referimos por falsa? Es aquella que quiere hacernos creer que es la persona detrás del perfil, pero, en realidad, es una fotografía de sacada de la red.
- Si te vas a “Fotos” en el menú del perfil sospechoso, puedes encontrar:
- Ninguna fotografía. De nuevo, nos surgiría la duda entre una persona concienciada con su privacidad y un posible perfil falso.
- Fotografías falsas. Podemos pensar que, por el hecho de tener fotografías, esa persona es la que se esconde detrás del perfil. Nada más lejos de la realidad: las fotografías pueden ser “robadas” de otro perfil o directamente de Internet.

La nueva modalidad delictiva se produce cuando delincuentes se contactan a través de las redes sociales, principalmente Facebook, haciéndose pasar por clientes para comprar o vender algún objeto, pactando un encuentro con el vendedor. Muchas de las estafas económicas se hacen prometiendo un servicio y pidiéndole al comprador que haga una transferencia previa para apartado.

MEDIDAS DE PREVENCIÓN

- Se recomienda que, ante todo, no se reciba ninguna transferencia bancaria y se entregue con el comprador con quien se realizó el trato.
- Hay que evitar pactar ventas de bienes a través de las redes sociales y nunca informar datos privados sobre la cuenta bancaria.
- También se recomienda no comprar objetos en comercios no autorizados y menos aún si el precio de venta está por debajo de su valor de mercado.
- Siempre hay que exigir la factura o ticket al realizar una compra.
- No hagas transferencias a menos que estés seguro de la compra y de la

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

persona que se lo está vendiendo.

- Siempre solicita que sea pago contra entrega. En caso de que sea transferencia, puedes pedir una identificación oficial, asegurándote de que sea el nombre de la cuenta a la que lo harás, pero recomendamos evitarlo.
- En ventas, revisa la reputación del vendedor.
- En Facebook Marketplace, si vemos un producto y damos clic en el perfil del vendedor podemos ver cómo ha sido calificado por otros usuarios de la plataforma. Esto hace que sea la mejor forma para realizar negocios en Facebook. En algunos grupos incluso se pueden pedir referencias de los vendedores para estar seguros de que no es una estafa.
- Asegúrate de que el vendedor del producto que buscas sea de confianza, y que no pida información personal de ningún tipo.
- Una de las recomendaciones centrales que da Facebook es que debemos desconfiar de cualquier persona “que te pida trasladar la conversación fuera de las plataformas donde sucedió el contacto inicial, a un lugar menos público o seguro, como un correo electrónico o un sitio no confiable”. De esta forma, se pueden realizar distintos fraudes, y es una señal de alerta. Si alguien quiere mover la negociación incluso en persona, toma tus precauciones.
- Revisa lo mejor que puedas, de acuerdo con Facebook, cualquier persona se registra en Messenger con un número de celular, así que podemos revisar ese número para saber si es de la locación de la que asegura ser el “vendedor”. Esa es sólo una forma en la que nos podemos asegurar de la identidad de una persona, o si es confiable.
- Evita los perfiles que casi no tienen amigos o que parecen nuevos, o que parece que tienen fotografías falsas. De igual forma, si un servicio parece informal y te hace sentir incómodo, evítalo.
- Suena un poco exagerado (ya que no todas las personas tienen ortografía y redacción perfecta) pero se recomienda desconfiar de las publicaciones que incluyan esos errores, ya que por lo general los sitios de ventas o los vendedores se esfuerzan por tener una comunicación óptima. En el comercio informal lo podemos ver más, pero aun así es buen motivo para desconfiar.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

- Si una persona pide datos personales, si no tiene demasiada información en su perfil, si te pide una transferencia, o cualquier otra cosa que te haga sentir sospecha, lo mejor es dejarlo de lado. Si insiste en ofrecerte el producto incluso si ya te rehusaste, es mayor motivo de sospecha.

Por ellos es de suma importancia tomar en cuenta los siguientes puntos antes de confiar en una venta:

- Personas que no conozcas y que te pidan dinero
- Personas que te pidan que les envíes dinero o tarjetas de regalo a cambio de préstamos, premios u otras ganancias.
- Desconfía de las personas que te pidan una suma de dinero a fin de postularte para un empleo.
- Desconfía de páginas que representen a empresas grandes, organizaciones o figuras públicas y no estén verificadas.
- Desconfía de las personas que te pidan seguir conversando por un canal distinto de Facebook que sea menos público o seguro (por ejemplo, otro correo electrónico).
- Desconfía de las personas que afirmen ser amigos o familiares en situaciones de emergencia.
- Desconfía de las personas que dan información falsa respecto de su ubicación. Si una persona se registra en Messenger con su número de teléfono celular, puedes consultar a qué país corresponde ese número. Si crees que una página tal vez te esté estafando, puedes consultar su ubicación.
- Desconfía de mensajes o publicaciones con faltas de ortografía o errores gramaticales.
- Desconfía de las personas o cuentas que te dirigen a una página para conseguir un premio.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

CONCLUSIONES

Los delitos cibernéticos que han ido surgiendo al pasar de los años, han ido cambiando en la forma de cometerse y por ellos se ha ido convirtiendo en un problema a la hora de combatirse, pero si se puede prevenir y gestionar, para evitar este tipo de prácticas delictivas por medio de la plataforma de Facebook donde se pueda gestionar y dotar a la plataforma de ventas de un sistema de pago seguro que sea capaz de reconocer y bloquear operaciones sospechosas y al mismo tiempo, ser lo suficientemente inteligente para no bloquear innecesariamente aquéllas operaciones y usuarios que no representan ninguna amenaza.

Nos queda claro que el Internet es una herramienta que nos proporciona muchos beneficios desde varios puntos de vista. Nos facilita la realización de muchas acciones, nos permite el acceso a la información de una forma rápida y nos proporciona la posibilidad de podernos comunicar entre nosotros de una forma sencilla y económica independientemente del lugar en el que nos encontramos. Sin embargo, como hemos podido comprobar, el uso de Internet también puede tener sus inconvenientes, ya que los delincuentes aprovechan este instrumento para cometer diversos delitos.

Cuando hablamos de los tipos de fraudes cometidos a través de Facebook por medio de las ventas se puede observar los diferentes modus operandi de los delincuentes al hacer la acción de las ventas. Los ciudadanos que utilizan las tecnologías a veces creen que es de forma segura, pero, así como avanza la tecnología avanzan las nuevas formas de delinquir con diversos riesgos y consecuencias por cada delito cibernético.

El delito cibernético más frecuente es el fraude ya que es una problemática por la que la sociedad está en continuo riesgo, ya que los delincuentes han encontrado diversas formas de cometer esta conducta, afectando la economía de las personas generando grandes pérdidas.

Canal de Miramontes 2063, Col el Centinela, Coyoacán CDMX. CP 04450.
www.amcdc.org.mx delitosciberneticos@amcdc.org.mx

La AMCDC considera que el incremento de los delitos cibernéticos como es el fraude a través de las distintas redes sociales se debe a diversos motivos:

I. las personas que cometen estas conductas delictivas han ido encontrando nuevas modalidades de cometer estas acciones ilícitas.

II. Las personas que usan estas redes sociales confían de más al realizar compras desde la comodidad de su casa y con ello va acompañado de un constante desarrollo tecnológico lo que hace que cada vez haya un número elevado de herramientas para la comisión de estos delitos y una mayor disponibilidad de estas para los delincuentes.

III. Por último la AMCDC considera que las personas que utilizan esta herramienta del internet y en especial la plataforma de Facebook, además de aplicar las medidas preventivas que se ha expuesto en el presente manual, debe estar mejor informados de los riesgos a los que se expone al conectarse a la red, ya que por sentido común es el único que puede evitar, en primera instancia, ser víctima de estos delitos.

Autor Lic. Viviana Montecinos Carrera Centro Universitario de América