¿Cuáles son los fraudes más comunes?

A pesar de los numerosos beneficios que nos brinda Internet, características como el anonimato o la capacidad de interactuar desde cualquier parte del mundo, lo convierten en un entorno óptimo para poner en circulación diferentes tipos de fraudes, algunos de los cuales os citamos a continuación.

Es indudable que Internet proporciona muchísimas ventajas y oportunidades, sin embargo, no es oro todo lo que reluce, y es que en ocasiones nos podemos encontrar con situaciones no esperadas, en las que por ejemplo, podemos acabar siendo víctimas de algún fraude online. La mejor línea de defensa ante este tipo de situaciones, es conocer la forma de actuar de los ciberdelincuentes para ponerles freno y evitar así caer en sus redes. Por este motivo, a continuación listaremos los fraudes más comunes. ¡Esperamos qué os sea de utilidad!

Las compras online

Las principales características de este tipo de páginas son las siguientes:

1. Ofertan productos que son copias de originales.
2. Envían productos que nada tienen que ver con el que se ofertaba o con el que se solicitó.
3. Realizan cobros de cantidades mayores o superiores al importe indicado durante el proceso de compra.
4. No cumplen con los plazos de envío que ofertan en sus webs.
5. No cuentan con teléfono, dirección, etc., ofreciendo únicamente un formulario de contacto al cual nunca responden.

Por lo tanto, en nuestro afán de concienciar a los usuarios de los peligros que rodean a este tipo de compras online, exponemos una serie de consideraciones a tener en cuenta:

1. Cuando te des de alta en una página de compra online o vayas a realizar un pago, ésta deberá contar con certificado de seguridad, de tal manera que comience por "https" y que aparezca un candado en verde que indique que los datos viajan cifrados.
2. Si ves que tiene precios anormalmente bajos o todos los productos al mismo precio, debes sospechar.
3. Busca la información legal de la empresa. No te fíes si viene como único elemento de contacto un formulario o un correo webmail gratuito.
4. Analiza los tipos de pago que se permiten. Si en la página principal publicitan que se admite algún método como es PayPal, asegúrate de que te dan esa opción al pagar el pedido.
5. No realices nunca pagos a través de empresas como Western Union, MoneyGram, Ukash, etc., ya que no ofrecen garantías de recuperar el dinero en caso de fraude.
6. Antes de comprar, busca opiniones de otros usuarios. Puede darse el caso que un fraude de una página ya haya sido comentado por más gente en algún foro o red social.

El phishing

Se trata de la técnica más usada para el robo de información personal, credenciales de acceso a servicios online o información bancaria. Su funcionamiento se basa en envío de emails u otro tipo de mensajes suplantando la identidad de algún servicio o empresa conocido para que la víctima acceda a una página fraudulenta que simula ser la legítima. La finalidad es que el usuario introduzca todo tipo de información para que el ciberdelincuente pueda contar con ella.

1. Si recibes un archivo adjunto por email de alguien desconocido, o aun siendo conocido te resulta sospecho, elimínalo directamente y / o contrasta la información con el contacto antes de proceder a abrirlo. En cualquier caso, analízalo siempre con un antivirus antes de abrirlo para evitar una posible infección.
2. De igual modo, evita hacer clic en enlaces que te llegan al correo electrónico o por mensajería instantánea. Si necesitas acceder a un servicio conocido, hazlo escribiendo la dirección directamente en el navegador.
3. Sospecha de aquellos correos que presenten una escritura incorrecta o faltas gramaticales y de ortografía, también si tienen un tono impersonal comenzando los mensajes con un "Hola amigo" o "Estimado cliente".
4. La urgencia es parte fundamental de los mensajes de tipo phishing, generalmente siempre se piden hacer algo de manera inmediata. Es un indicio a tener en cuenta.
5. Si detectas un email de tipo phishing, avisa a tus contactos para que no caigan en el engaño.

Los falsos préstamos

La existencia y uso de las redes sociales permite a estos ciberdelincuentes, los que ofrecen supuestamente préstamos de dinero a bajo interés, anunciarse en cualquier perfil y llegar a una gran cantidad de personas a través de la viralización de sus anuncios. También puedes encontrarlos en foros, comentarios de artículos o en mensajes de correo electrónico.

Harán uso de la desesperación de la gente por obtener un crédito para intentar estafar y obtener un rédito económico o para hacerse con información personal de sus víctimas.

Las principales características que ofrecen este tipo de préstamos son las siguientes:

1. Ofrecen grandes cantidades de dinero a un interés inusualmente bajo.
2. Hacen uso de cuentas de correo gratuitas para los trámites y no trabajan nunca bajo una empresa reconocida o de prestigio.
3. Siempre piden dinero por adelantado, normalmente alegando gastos de gestión.
4. Piden hacer los envíos de los pagos a través de Western Unión o MoneyGram o transferencias a bancos extranjeros.

Para no caer en este tipo de engaños, recomendamos acudir a entidades de confianza u oficiales de crédito. También hacer búsquedas activas por Internet, los resultados te puedan dar pistas sobre si se está ante un fraude o no.

Encontrar pareja por Internet

En la gran mayoría de ocasiones, los ciberdelincuentes utilizarán este tipo de engaño para obtener, al igual que en los anteriores fraudes descritos, un beneficio económico.

Las principales técnicas de engaño que utilizan son la suplantación de identidad, la creación de perfiles falsos en redes sociales, o el uso de la conocida ingeniería social. Una vez ganada la confianza de la víctima, solicitarán envíos de dinero bajo cualquier excusa. También fotos y vídeos de contenido sexual o comprometedor que posteriormente utilizarán para exprimir económicamente a la víctima (sextorsión), o para desacreditarla en Internet.

Por lo tanto, sigue estos consejos para evitar convertirte en una víctima:

1. Configura tus redes sociales lo más restrictivas posible. No aceptes solicitudes de amistad de gente que no conozcas.
2. No facilites nunca información personal o bancaria a personas desconocidas.
3. Si recibes algún correo de alguien que no conoces, no lo abras, especialmente si contiene algún archivo adjunto o enlaces a páginas web.

4. Si al final decides quedar con una persona que únicamente conoces a través de redes sociales, hazlo en un lugar público y acude en compañía de alguien de tu confianza. Es importante dejar constancia a alguien más de dónde vas a ir y con quién.
5. No practiques sexting (fotos o vídeos sugerentes o con cierta connotación sexual), recuerda que una vez que envíes una foto o vídeo, perderás el control sobre ellos y podrían ser utilizados en tu contra.

Falsos alquileres o ventas de vehículos

Son estafas basadas en ofrecer alquiler de inmuebles con unas prestaciones muy buenas a precios que están fuera del mercado, anormalmente bajos en relación a la calidad del inmueble, su ubicación, su presencia interna, etc. Este síntoma debe ser suficiente para ponernos en alerta y sospechar que pueda tratarse de una estafa.

Esta misma casuística se está dando también con los automóviles. Se ofertan por diferentes páginas de ventas de segunda mano vehículos bien equipados a unos precios inusualmente bajos.

En ambos casos, el engaño suele ser similar: propietarios que se encuentran en el extranjero, y que no pueden salir del país en el que residen por el alto coste que supondría venir a realizar la operación de venta o alquiler. Además alegan que ya no volverán y por lo tanto no tienen interés en seguir residiendo o haciendo uso del bien en cuestión, y que por ese motivo lo alquilan o venden.

1. En el caso de los alquileres, utilizarán páginas de prestigio como AirBNB o TripAdvisor únicamente para conformar el engaño, ya que no serán utilizadas para nada más. De esta forma dotarán de mayor credibilidad a la operación.
2. Una característica común es que la venta o alquiler querrán cerrarlo en un periodo de tiempo muy corto y además, no pondrán reparos ante cualquier petición que se les haga, por muy extravagante que pueda ser.
3. En este tipo de fraudes, es muy importante buscar por la red para conocer opiniones de otros usuarios. En la gran mayoría de casos, esta búsqueda nos devolverá intentos anteriores de estafa y denuncia de usuarios alertando del fraude. Nos evitarán caer en su trampa.
4. También es una buena práctica, realizar una búsqueda en Google Street View o Google images para comprobar si las fotos que figuran en el anuncio se corresponden con la realidad o se tratan de imágenes