Edición No. 7 – junio 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

TOP de los 10 fraudes que utilizan con Covid-19 para engañar a los usuarios

Ante la pandemia de COVID-19, es de esperar que haya quien quiera *aprovecharse y sacar un beneficio económico* de la situación. Los ciberdelincuentes no descansan y siempre encuentran nuevas formas de llevar a cabo sus estafas y fraudes online.

A más de uno se le colapsa el celular con mensajes, noticias y cadenas sobre el **coronavirus** o **COVID-19**. El uso de las redes sociales también se ha disparado, generando y compartiendo contenido sin cesar, aunque **no siempre es información verificada**. A continuación, repasaremos algunos de los ***fraudes más utilizados en estos momentos de crisis sanitaria*** para que tengamos los ojos bien abiertos y no caer en el engaño.

1. Mil y un consejos para "frenar" el Coronavirus (WhatsApp

Circulan cientos de mensajes con enlace a una gran variedad de páginas web, donde supuestos "expertos" ofrecen sus recomendaciones y soluciones ante el virus. Mucha atención pues una gran parte de estos mensajes contienen enlaces maliciosos o buscan desinformar. Incluso hay algunos que buscarán una compensación económica o nuestros datos a cambio de ofrecernos su supuesta ayuda.

2. Manda "Ayuda" al teléfono/email XXXX (redes sociales)

Otro tipo de estafa muy común es aprovecharse de la labor de los profesionales de la salud, pidiendo que colaboremos para agradecer todo su trabajo y esfuerzo.

En muchos casos nos pedirán que ingresemos algunos datos personales o incluso que realicemos alguna donación económica. Es una forma de recolectar información personal de un gran número de usuarios. No significa que todas las iniciativas solidarias que circulan por Internet sean un fraude, pero sí habrá que ser cautos y contrastar la información para evitar problemas.

3. Corona Phishing (Correo Electrónico)

En este fraude el ciberdelincuente suplanta la identidad de una institución, como puede ser la OMS o cualquier otra, que, aprovechándose de la preocupación global sobre el COVID-19, trata de ganarse nuestra confianza para hacerse con el control de determinados datos personales, como los datos bancarios o incluso infectarnos con un malware.

4. Corona Smishing (SMS)

Un fraude muy popular es el envío a través de SMS haciéndose pasar, por ejemplo, por el Ministerio de Trabajo, compartiendo un enlace donde se nos solicitarán una serie de datos personales. Aparentemente serán necesarios para tramitar una "solicitud de baja temporal en relación con el coronavirus". Se debe prestar mucha atención, ya que su carácter urgente puede confundirnos y hacernos caer en una trampa.

5. Estafa en la venta de material sanitario (compras online)

Una vez más los estafadores tratan de beneficiarse con los productos "estrella" relacionados con el coronavirus. Se han identificado varias estafas principalmente relacionadas con la venta online de mascarillas.

Por ejemplo, el vendedor asegura disponer de mascarillas especialmente preparadas para protegernos del virus, pero las víctimas, tras realizar la compra, no llegan a recibir lo que han comprado o, en su defecto, solo una parte o en unas condiciones muy distintas de las anunciadas.

Edición No. 7 – junio 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

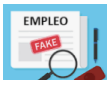
6. Coronaware (ransomware)

Otro fraude muy extendido es el basado en un malware llamado "Coronavirus". ¿Quién no abriría un archivo de vídeo o un documento donde se incluyen instrucciones y alertas sobre cómo protegernos contra el COVID-19? Pues aquí está la trampa, pues no debemos confiarnos de todo lo que recibimos, ya que los archivos adjuntos pueden contener malware que termine por infectarnos y tomar control de nuestros equipos y la red de nuestra institución, Es muy común a través del correo electrónico

7. El gobierno reparte "Corona-cheques"

Muchos usuarios están recibiendo a través de sus aplicaciones de mensajería instantánea un mensaje supuestamente se les indica que el Gobierno regala una cantidad ¨X¨ de dinero para sobrellevar mejor las consecuencias de la actual crisis sanitaria por el COVID-19. Para recibirlos, deberemos hacer clic en el enlace que viene adjunto. Mucho cuidado pues a día de hoy esta información es falsa.

Antes de hacer clic sobre cualquier enlace, se debe confirmar si la fuente es fiable, podemos comprobarlo mediante sus canales de comunicación oficiales, en las redes sociales o en las webs oficiales de las distintas entidades.



8. Ofertas de trabajo fraudulentas

Circulan falsas ofertas de empleo aprovechándose de esta difícil situación, los ciberdelincuentes tratarán de hacernos creer que nos encontramos ante una oferta de trabajo real para que compartamos con ellos nuestros datos personales e incluso que realicemos algún pago por adelantado por algún concepto. Ante una oferta de estas características, lo mejor es revisar todos los detalles del anuncio, contrastar la información y si algún detalle nos llama la atención o nos resulta raro, descartar la oferta, especialmente si proviene de un usuario desconocido o sin haberlo solicitado a ningún portal web de ofertas de trabajo.

9. Soporte técnico fraudulento (teléfono)

Los ciberdelincuentes, aprovechando la situación de cuarentena y teletrabajo, están poniendo en práctica algunas de sus engaños más clásicos. Recientemente se han notificado denuncias de usuarios que afirmaban haber recibido llamadas de un supuesto "soporte técnico" para colaborar mientras duren estas semanas de teletrabajo. Lamentablemente, tras seguir sus indicaciones, el ciberdelincuente acaba por conseguir nuestras credenciales o que instalemos algún software malicioso sin darnos cuenta.

10. Lleva mejor la cuarentena con estos "servicios gratuitos"

En este momento, donde la mejor solución para vencer al virus es quedarnos en casa, es cuando aparecen los fraudes sobre supuestas promociones y suscripciones gratuitas o con descuentos. Un ejemplo de mensaje que podemos recibir es el siguiente: "Disfruta de todos nuestros servicios de streaming de películas y series de forma totalmente gratuita". Los ciberdelincuentes buscarán que digitemos algunos formularios con nuestros datos personales o que paguemos una pequeña cantidad bajo cualquier excusa.

Ante situaciones de crisis, ***¡mucho cuidado!.*** Presta atención a los mensajes que recibimos a través de Internet y **con ayuda de nuestro sentido común y reportando al personal de seguridad de nuestras instituciones** seremos capaces de detectar y ponerle freno a este tipo de fraudes.

Fuente: Oficina de Seguridad del Internauta (OSI).