WORLD COMPLIANCE ASSOCIATION



10 fraudes que utilizan el coronavirus para engañar a los usuarios

Mensajes de solicitud de ayuda, ataques phising, cadenas de WhatsApp fraudulentas o supuestos servicios gratuitos

La crisis sanitaria debido al brote de coronavirus por todo el mundo ha supuesto también la proliferación de ciberataques y fraudes online que aprovechan la situación de vulnerabilidad de los usuarios para obtener un beneficio económico.

Desde las instituciones públicas como la Guardia Civil alertan a la ciudadanía diariamente de este tipo de estafas y por esta razón **la Oficina de Seguridad del Internauta (OSI) ha elaborado un decálogo de los fraudes más habituales** de los ciberdelincuentes sobre el coronavirus.

1. Mil y un consejos para “frenar” el coronavirus (WhatsApp)

¿Te ha llegado un mensaje por WhatsApp donde te recomiendan una solución para el coronavirus? ¿Te redirige a una página web? ¿Y has recibido un mensaje que por esa red social sobre una ampliación de los datos de Internet por motivo de la cuarentena?

Circulan cientos de mensajes de este tipo donde supuestos expertos ofrecen recomendaciones para tratar el virus. Gran parte de esos mensajes contienen enlaces web maliciosos. Otros buscan desinformar por completo. Por esta razón, evita este tipo de cadenas y sigue siempre la información de fuentes oficiales como el Gobierno, el Ministerio de Sanidad, la Organización Mundial de la Salud, la Guardia Civil o la Policía Nacional.

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

Otro tipo de fraude que está circulando por redes sociales como Twitter, Facebook o Instagram es la que **solicita una ayuda o colaboración para los profesionales sanitarios**, aprovechándose de esta situación de emergencia sanitaria.

En estos casos nos solicitarán información personal relevante y que realicemos alguna donación económica. **No confíes en estos mensajes, sobre todo si son fuentes que desconoces.** Además el mensaje suele ser: Manda ayuda al teléfono/email XXX.

Esto no quiere decir que las iniciativas solidarias que vemos estos días por redes sociales sean falsas o un fraude. Primero revisa quien difunde la información y contrástala para evitar problemas.

3. Corona-phising (correo electrónico)

El phising es una técnica bastante utilizada por los delincuentes en Internet y se basa en **suplantar la identidad de instituciones, bancos u organismos públicos, incluso de la OMS, para robar información personal** como el número de cuenta bancaria.

Aprovechando la preocupación global sobre el coronavirus están proliferando estos ataques que tratan de ganarse nuestra confianza **para hacerse con el control de datos personales o infectarnos con un malware.**

Por ejemplo, podríamos recibir un correo procedente de un supuesto hospital que nos informa de que podemos ser de los primeros en hacernos el test de diagnóstico pero que para ello debemos hacer clic en un enlace muy sospechoso. **Para averiguar si se trata de un phising algunos consejos son:**

- Sospechar si hay errores gramaticales o una mala redacción del texto.
- Si el mensaje te obliga a tomar una decisión inminente es mala señal.

- Comprueba la dirección del remitente.
- Si recibes comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”, es un indicio que te debe poner en alerta.
- Ninguna institución, banco u organismo público te va a pedir datos personales por correo electrónico, y menos tu número de cuenta.
- Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la ecuación: solicitud de datos bancarios + datos personales = fraude.

4. Corona-smishing (SMS)

Un fraude muy habitual es el envío de un SMS haciéndose pasar por algún ministerio, la Comunidad de Madrid o alguna otra institución pública para compartir un enlace donde nos solicitan datos personales.

Como siempre, duda de cualquier mensaje que solicite datos personales. Siempre suelen ser fraudes. Ante cualquier duda contacta con las autoridades.

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. Estafas en compras online

Los ciberdelincuentes están aprovechando la situación para beneficiarse con productos relacionados con la enfermedad como mascarillas o guantes. **Se han identificado ya varias estafas relacionadas con esta venta online.**

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.

6. Coronaware (ransomware)

Otra estafa que se ha extendido estos días está relacionada con el malware llamado coronavirus. **Un malware es un programa o software malicioso dañino para el sistema de nuestro smartphone o PC que intenta controlar, dañar o deshabilitar las funciones del dispositivo.** Su objetivo es obtener un beneficio económico mediante el robo o cifrado de los datos personales.

¿Te ha llegado algún archivo de vídeo o un documento donde se incluyen instrucciones o alertas sobre cómo protegernos contra el coronavirus? Pues esta es la trampa. No debemos fiarnos de todo lo que recibimos, sobre todo si la fuente es desconocida, ya que los archivos adjuntos pueden contener malware. Es algo muy común en el correo electrónico aunque también por WhatsApp y redes sociales.

Siempre que quieras informarte sobre estos aspectos acude a la página web oficial de los organismos especializados como la Organización Mundial de la Salud (OMS) o el Ministerio de Sanidad, ya que tienen guías exhaustivas sobre todo esto.

7. Corona-cheques

De acuerdo con la OSI, muchos usuarios están recibiendo a través de WhatsApp un mensaje de supuestamente un Ministerio en el que **se les indica que el Gobierno regala una cantidad de X euros para sobrellevar mejor las consecuencias de esta crisis.**

Para recibirlos nos indica que hagamos clic en un enlace adjunto. Esta información es totalmente falsa. El Gobierno no va a regalar dinero de esta forma y menos para compartirlo por una aplicación de mensajería instantánea.

Confirma si la fuente es fiable y accede a los canales de comunicación oficiales del Ministerio en redes sociales o página web. Recuerda que todos los mensajes o avisos que te lleguen (SMS, WhatsApp, Internet, RRSS...) sobre un supuesto regalo de dinero, megas...etc, suelen ser estafas.

8. Ofertas de trabajo fraudulentas

Un fraude habitual pero que ahora toma el matiz sanitario. **Circulan ofertas de empleo para fabricar material sanitario.** Para acceder a ellas tenemos que compartir nuestra información personal e incluso hacer algún pago adelantado para el envío de material.

Si recibes una oferta así, revisa los detalles del anuncio y contrasta la información. Descarta la oferta si proviene de algún remitente o usuario desconocido y mucho más si no has solicitado nada por ninguna web de empleo.

9. Soporte técnico fraudulento (teléfono)

Muchos ciberdelincuentes están aprovechando esta situación de cuarentena para dirigir sus ataques a un sector de la población vulnerable: las personas mayores. **Las supuestas llamadas de soporte técnico estos días suelen ser estafas que quieren que nos instalemos algún software malicioso** alegando que nuestro dispositivo (teléfono, router...) está averiado. El soporte técnico no nos va a llamar sino notificamos nosotros antes una incidencia.

10. Servicios gratuitos para la cuarentena (falsos cupones)

¿Has recibido una promoción, suscripción gratuita a Netflix o descuentos? Hace unas semanas ya se alertó que estaban dando pases o cupones gratuitos para Netflix que los recibías en tu correo electrónico. Es totalmente falso.

Un ejemplo de mensaje: Disfruta de todos nuestros servicios de streaming de películas y series de forma totalmente gratuita". Los ciberdelincuentes buscarán que rellenemos algunos formularios con nuestros datos personales o que paguemos una pequeña cantidad bajo cualquier excusa.

Lo primero que debemos hacer es revisar la URL, y si no estamos seguros, ir a la fuente oficial para confirmar o desmentir. Si existe alguna suscripción o promoción los canales de información de estas plataformas lo colgarán en su web o redes sociales.

Fuente: *20 minutos*