Nota de prensa

THADERCONSUMO
Federación Murciana de Asociaciones de Amas de Casa, Consumidores y Usuarios

Tras el inicio de la crisis con el Covid- 19, se ha observado un aumento de la criminalidad en determinadas áreas, como las estafas sanitarias o bancarias.

Murcia, 26 de marzo de 2020.- La Guardia Civil está trabajando para prevenir e investigar los posibles delitos que pudieran cometerse a través de la red, como son los relacionados con los fraudes. Para ello, el Grupo de Delitos Telemáticos de la UCO ha habilitado un canal para recibir información de los ciudadanos relacionada con las ventas fraudulentas y posibles estafas que utilizan el Covid-19 como gancho. Esta cuenta es **ciberestafas@guardiacivil.org**

Se han detectado casos de **phising** tan llamativos como el de ofrecer suscripciones gratuitas durante cinco años a plataformas de música digital, o de contenido multimedia como Netflix, HBO o Spotify, suplantaciones a instituciones como Unicef o la propia Organización Mundial de la Salud; todas ellas solicitando datos personales con motivo de alguna campaña relacionada con el coronavirus.

De la misma manera, se han detectado varios casos de intentos de **estafa a farmacias** y empresas relacionadas con el sector, en los que se les ofrece grandes cantidades de mascarillas y productos muy demandados a consecuencia de esta crisis sanitaria, y debemos de estar alerta, pues ni las propias instituciones publicas están a salvo:, es el caso del Govern catalán, que ha presentado una denuncia ante los Mossos d'Esquadra por una posible estafa al intentar adquirir batas de protección y mascarillas para el Instituto Catalán de la Salud (ICS) ante el déficit de material sanitario para combatir el virus. La cuantía del contrato, supuestamente estafa, asciende a 35 millones de euros.

Algunos ejemplos de **ciberdelitos** comunes que usan el gancho del Covid-19 son"*spams"*[envíos masivos de correos electrónicos], emails falsos con adjuntos maliciosos,"*ransomware"*[secuestrador de datos] o e-shops [tiendas virtuales]. Son un fraude, donde al comprar clonarán la tarjeta o"*apps"*maliciosas para Android. Esto ocurre porque la gente es más vulnerable en esta situación y puede bajar la guardia para conocer las últimas noticias de la pandemia o comprar mascarillas, entre otros productos.

Uno de los fraudes detectados es un"*gusano"*(una subclase de virus informático que realiza copias de sí mismo hasta colapsar los equipos que

infecta) que llega mediante un mensaje de **móvil SMS** donde se ofrece una aplicación con la que conseguir mascarillas sanitarias. El enlace lleva también a una página falsa donde comprarlas que sirve para robar los datos de la tarjeta del usuario engañado. Una vez se hace clic en el enlace, el mensaje se reenvía a todos los contactos de la agenda

La Guardia Civil investiga una nueva estafa en la que los autores se hacen pasar por la Agencia Estatal de Administración Tributaria (AEAT) para **cobrar facturas falsas a las empresas**. Los estafadores aprovechan la confusión generada en muchas empresas tras los ERTE presentados para reclamar facturas irreales en nombre de la **AEAT**. La reclamación se produce vía correo electrónico, y los estafadores redactan un mismo asunto en los emails: 'Denuncia de facturas no declaradas'. Los ciber delincuentes usan el conocido método del phising, consistente en el robo de información personal mediante correos electrónicos fraudulentos que solicitan que aportes tus datos personales, financieros o de seguridad para llevar a cabo la ciberestafa. Los investigadores han comprobado que el dominio de la dirección de correo del remitente -que se visualiza en el apartado 'from'- es el mismo que utiliza la AEAT, @correo.aeat.es.

Asimismo, desde **Thaderconsumo** hemos observado **repuntes en la Región de estafas**, que a través de mensajes de texto o correos electrónicos, se hacen pasar por tu propia entidad bancaria, informando de cambio de condiciones en tu cuenta. Dicho correo suele llevar un archivo adjunto o un link pinchable: al acceder o abrir el archivo, se descarga malware en la terminal y es ahí donde se inicia el robo de datos, entre otros.

Recomendaciones para no caer en estafas:

- Verificar el nombre de la persona o compañía que le ofrece artículos médicos, o modificaciones de las condiciones de sus servicios, llamando a la compañía para que sea esta quien por teléfono nos informe de ellas y nos las mande por escrito al domicilio, si así fuese.
- Verificar la autenticación de la página donde ingresa.
- Hacer una búsqueda de la empresa, buscando entre otras las posibles denuncias que pueda tener.
- Tener cuidado si se pide realizar un pago a una cuenta bancaria alojada en un país diferente al de la empresa. Utilizar siempre en las webs las plataformas de pago de las mismas, ya que el pago externo exime de responsabilidad a la empresa que aloja el servicio fraudulento.
- Si cree que fue víctima, avise al banco para suspender el pago y póngase en contacto con la guardia civil a la mayor brevedad.
- No haga clic en enlaces ni abra archivos que no pensaba recibir, aun cuando parezcan ser oficiales.

Más información: 670 31 29 07

968 20 32 46 (WhatsApp)