25/03/2020

La UCO crea un canal contra el fraude online por el Covid-19: desde suscribirse a la OMS a plataformas de música

Desde el comienzo de la situación sanitaria vivida en España los ciberdelincuentes han intensificado las campañas de phishing con el objetivo de hacerse con los datos personales y credenciales de los ciudadanos



El Grupo de Delitos Telemáticos de la Unidad Central Operativa (UCO) de la Guardia Civil ha creado un canal de comunicación ciudadana para rastrear el fraude online aprovechando el estado de alarma por el Covid-19. Se han detectado desde **falsas suscripciones a organizaciones como la OMS o Nacional Unidas**, como a plataformas musicales, así como estafas a farmacias a las que se promete material sanitario. El objetivo es perseguir el delito relacionado con los fraudes, la instalación de programas maliciosos (malware) o la desinformación. Para ello, ha habilitado el correo electrónico ciberestafas@guardiacivil.org, para recibir información de los ciudadanos relacionada con las ventas fraudulentas y posibles estafas que utilizan el Covid-19 como gancho.

Desde el comienzo de la situación sanitaria vivida en España los **ciberdelincuentes han intensificado las campañas de phishing** con el objetivo de hacerse con los datos personales y credenciales de los ciudadanos. Es muy importante estar alerta y tomar precauciones, recomienda la UCO, que pide prestar atención al remitente de los emails recibidos y las páginas webs que se visitan.

Ejemplos de estafas

Solo a modo de ejemplo, se han detectado casos de phishing tan llamativos como el de ofrecer suscripciones gratuitas durante cinco años a plataformas de música digital, o suplantaciones a instituciones como Unicef o la propia Organización Mundial de la Salud (OMS), todas ellas solicitando datos personales con motivo de alguna campaña relacionada con el coronavirus. De la misma manera, ha concluido, también 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 similares muy demandados como consecuencia de esta crisis sanitaria.

Entre los consejos que adoptar, los especialistas dicen que se debe evitar los documentos y archivos adjuntos sobre el Covid-19 en los correos electrónicos que se reciban y recelar de solicitudes de datos de salud por internet, procedimiento normalmente ajeno a las administraciones sanitarias. Además, la Guardia Civil recomienda **no descargar e instalar aplicaciones no oficiales** que tengan que ver con el Covid-19 y, ante la menor sospecha de haber sido objeto de una estafa de este tipo, comunicar a las entidades bancarias esta circunstancia.

Teletrabajo y bulos

En relación con el teletrabajo que muchas empresas han adoptado para hacer frente a la situación actual, la UCO ha tildado de muy recomendable que se adopten medidas para garantizar la seguridad en los dispositivos utilizados. Entre las mismas, ha recomendado que el sistema operativo y las aplicaciones estén correctamente actualizados; **cambiar periódicamente las contraseñas y no utilizar una única para todo**; implementar un doble factor de autenticación a los usuarios que realicen teletrabajo; disponer de un antivirus y firewall activos y no olvidar cerrar la sesión al terminar de trabajar.

Asimismo, en todas las situaciones y más en una como la actual, el instituto armado califica de vital que la información que se comparta sea veraz y contrastada, ya que la desinformación y los bulos son otro enemigo a batir. En este sentido piden no difundir información que no provenga de medios y fuentes oficiales; no contribuir a la difusión de contenido no contrastado; no compartir mensajes que puedan genera alarma en la población; y no olvidar que la creación y difusión de fake news puede tener consecuencias penales.

Fuente: Infolibre

https://www.infolibre.es/noticias/politica/2020/03/20/la_uco_crea_canal_contra_fraude_online_por_covid_desde_suscribirse_oms_plataformas_