A través de la cuenta ciberestafas@guardiacivil.org los ciudadanos pueden comunicar posibles estafas y ventas fraudulentas relacionadas con el Covid-19 como gancho. El cibercrimen está aprovechando para lanzar campañas de phishing y obtener datos personales y bancarios, o como gancho para cometer ciberestafas o fraudes relacionados con productos sanitarios.

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, la instalación de programas maliciosos (malware) o la desinformación. 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 COVID19 como gancho. Esta cuenta es ciberestafas@guardiacivil.org.

Desde el comienzo de la situación sanitaria vivida en nuestro país, los ciberdelincuentes han

intensificado las campañas de phishing con el objetivo de hacerse con los datos personales y credenciales de los ciudadanos. Por este motivo, es muy importante estar alerta y tomar precauciones como las siguientes:

- Â Â Â Se recomienda prestar especial atención al remitente de los emails recibidos.
- Â Â Â Evitar abrir los documentos y archivos adjuntos sobre el COVID-19 en los correos electrónicos que se reciban.
- Â Â Â Recelar de solicitudes de datos de salud por internet, procedimiento normalmente ajeno a las administraciones sanitarias.
- Â Â Â No descargar e instalar aplicaciones no oficiales que tengan que ver con el COVID-19.
- Â Â Â Ante la menor sospecha de haber sido objeto de una estafa de este tipo, comunicar a las entidades bancarias esta circunstancia.

Teletrabajo

Por otro lado, en relación con el teletrabajo que muchas empresas han adoptado para hacer frente a la situación actual, es muy recomendable que se adopten medidas para garantizar la seguridad en los dispositivos utilizados durante el teletrabajo, tales como:

- Â Â Â Se recomienda que el sistema operativo y las aplicaciones estén correctamente actualizados.
- Â Â Â Cambiar periódicamente las contraseñas y no utilizar una única para todo.
- Â Â Â Implementar doble factor de autenticación a los usuarios que realicen teletrabajo.
- Â Â Â Disponer de un antivirus y firewall activos.
- Â Â Â No olvidar cerrar la sesión al terminar de trabajar.

Bulos

Asimismo, en todas las situaciones, y más en una como la actual, es vital que la información que compartamos sea veraz y contrastada, por ello, la desinformación y los bulos son otro enemigo a batir. En este sentido es muy importante:

- Â Â Â No difundir información que no provenga de medios y fuentes oficiales.
- Â Â Â No contribuir a la difusión de contenido no contrastado.
- Â Â Â No compartir mensajes que puedan generar alarma en la población.

- Â Â Â No olvidar que la creación y difusión de “fake news” puede tener consecuencias penales.

Sólo a modo de ejemplo, se han detectado casos de phishing tan llamativos como el de ofrecer subscripciones gratuitas durante 5 años a plataformas de música digital, suplantaciones a instituciones como UNICEF o la propia Organización Mundial de la Salud, todas ellas solicitando nuestros datos personales con motivo de alguna campaña relacionada con el Coronavirus.

De la misma manera, también se hanÂ 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 a consecuencia de esta crisis sanitaria.

* Texto remitido en el que se respeta el contenido íntegro, la redacción y la ortografía, con excepción del titular y de la entradilla del artículo
Â