“CUIDADO SI LE LLEGA UN SMS AVISANDO DE LA ENTREGA DE UN PAQUETE, PUEDE SER UNA ESTAFA”

Recientemente varias personas se han puesto en contacto con esta Policía informando sobre la recepción de mensajes SMS o a través de Whatsapp con el que les comunican la entrega de un paquete: ¡cuidado, puede ser una estafa!

El timo consiste en recibir un mensaje en el móvil con el que avisan de la recepción de un envío suplantando a una empresa logística e invitan al receptor a instalar una app para saber dónde, supuestamente, está el paquete.

Si usted recibe un mensaje avisándole de que tiene un paquete pendiente de recoger, desconfíe, puede ser una estafa. El usuario recibe un SMS en el móvil que le avisa de que tiene un paquete pendiente de recoger. Ese mensaje contiene un enlace cuya consulta **desencadena la descarga de una aplicación maliciosa** destinada a acceder a los datos del terminal.

Por SMS, correo electrónico o mediante mensajería instantánea, las estafas online son el hecho delictivo más frecuente y van en aumento. Muchos delincuentes utilizan la reputación que generan **los logotipos y la imagen de marca** para idear mecanismos de engaño con los que ganarse la confianza de la víctima y conseguir sus credenciales bancarias e información de carácter personal.

Modalidades:

Una de estas estafas consiste en recibir un SMS en el que avisan de la recepción de un paquete suplantando a una empresa logística e invitan al receptor a instalarse una app para saber dónde, supuestamente, está el paquete. (Correos, FedEX, DHL, etc).

Una vez que este **troyano infecta los terminales**, se establece como aplicación por defecto para SMS para así poder controlarlo, acceder a la agenda de contactos y provocar el reenvío automático de mensajes de tipo SMS.

Los dispositivos que son infectados con este tipo de malware, envían sin que se percate el titular del teléfono, un SMS a todos los contactos de su agenda un mensaje simulando una empresa de paquetería con un enlace. Los receptores reciben el mensaje a su nombre (con el que figura en los contactos del infectado) y si proceden a **introducir los datos requeridos a través del enlace,** quedan también infectados, existiendo la posibilidad de que,

dependiendo del mensaje, los datos que ha introducido sean bancarios y sufran, a posteriori, algún cargo en tarjeta o accesos a su banca on line.

En otros casos, como el del actual software malicioso **«FLUBOT», la aplicación descargada contiene un troyano bancario que permite a los atacantes hacerse con el control del dispositivo y visionar los datos de cuentas bancarias, tarjetas y aplicaciones de pago por teléfono.**

Estos ataques no son muy diferentes de los correos de spam recibidos a diario, pero el mensaje dirigido al teléfono o WhatsApp, ha demostrado ser más efectivo al ser más personal.

A pesar de las advertencias y las campañas de prevención, este tipo de fraude es muy popular debido al éxito que tienen. La mayoría de los internautas están acostumbrados al spam y a no prestar atención a los correos que ofrecen oportunidades o chollos, pero nuestro teléfono es más personal, y recibir un SMS e indica que, como mínimo, el remitente tiene nuestro número. Eso puede despertar una falsa confianza en el atacante, cuando en realidad conseguir un número de teléfono es cada vez más fácil gracias a servicios de compra-venta efectuada.

Consejos para evitar ser víctima de phishing (suplantación de identidad):

Además de preguntar a las empresas por esos SMS, hay varios pasos que puedes seguir para saber si ese mensaje tan tentador que has recibido es phishing. Una de las cosas en las que puedes fijarte es en cómo está escrito, ya que si incluye faltas de ortografía o frases sin sentido es muy probable que no sea un mensaje real.

Siga estas recomendaciones para evitar este timo:

Fíjate bien en el teléfono que te los envía. Consulta ese mismo número de teléfono en Internet antes y comprueba que es legítimo. Si no lo es, es posible que veas advertencias en la Red sobre posibles fraudes o de otros usuarios estafados.

Mire la dirección de la web a la que le redirige. Normalmente este tipo de notificaciones vienen con un link en el que te piden que introduzcas tus datos. Si la dirección web de esta página web no es de la empresa legítima, ojo porque puede ser similar pero nunca el mismo: incluirá guiones, números, alguna letra más, palabras como «online», «compra» que lo hagan parecerse al original. Vete a la web original y compara las direcciones de dominio.

Si una institución, supuestamente, se está poniendo en contacto contigo por teléfono, solicítales que te manden un correo personal con esa misma

información, diles que les atenderás más tarde y consulta el teléfono en Internet. En todo caso, ninguna empresa o institución debe pedirte datos personales o bancarios por teléfono si tú no has sido quien haya solicitado el servicio a la empresa verdadera.

Contraste con las fuentes antes de dar sus datos. Estos mensajes transmiten urgencia para que no te dé tiempo a reaccionar. Tómate tu tiempo para hacer las comprobaciones personales oportunas, los servicios que te requieran algo, siempre te darán un tiempo para ello. Si algo es urgente, sospecha.

Ante cualquier sospecha que tenga de que ha podido sufrir una estafa de este tipo:

Cambie las contraseñas.-

Si has clicado en los enlaces maliciosos y has introducido tus datos, te recomendamos que rápidamente cambies tus credenciales de acceso a tus cuentas bancarias.

Informe a sus contactos.-

Para prevenir que tus contactos accedan a los enlaces de cualquier página fraudulenta, infórmales sobre el mensaje que has recibido y así evitarás que tus contactos sufran el mismo ataque de phishing.

Contacte con su entidad Bancaria.-

Envía información sobre el correo electrónico o SMS que suplanta a atención al cliente de tu entidad bancaria.

Denuncie la estafa.-

Recaba y documenta toda la información posible sobre el engaño y denúncialo ante la Policía o Guardia Civil.