
NOTA DE PRENSA

AVACU insiste en ser precavidos ante varios intentos de estafas a través del correo electrónico

Valencia, 19 de febrero de 2021. En las últimas semanas venimos advirtiendo desde la Asociación Valenciana de Consumidores y Usuarios un incremento en el número de intentos de estafas a través de correos electrónicos, ya no solo mediante la técnica de *phishing* (mensajes que intentan conseguir nuestros datos personales y bancarios, contraseñas...) sino también intentos de "secuestro" de nuestro ordenador o dispositivo móvil, solicitando una cantidad de dinero para "liberar" el mismo.

Desde AVACU creemos que es importante advertir a los usuarios sobre estos correos ya que, si bien se trata de mensajes claramente identificables y que debemos desechar, con el tiempo se han ido perfeccionando y podrían llegar a confundir y engañar al consumidor, acabando por conseguir bien sus datos o bien el pago de un importe económico.

En primer lugar, hay que recordar que se entiende por *phishing* aquella estafa que tiene como objetivo conseguir datos privados del usuario, para poder acceder a sus cuentas o tarjetas bancarias. En estos casos, el usuario recibe un correo electrónico en el que se le indica que su cuenta o tarjeta ha sido desactivada por un intento de *hackeo* o bien solicitándole una confirmación de sus datos o de un pago y que debe volver a introducir sus datos y contraseña en el enlace que se le adjunta. Estos correos presentan la apariencia y logo de la entidad bancaria, por lo que el usuario puede llegar a pensar que es la propia entidad quien le está solicitando dichos datos.

Asimismo, también hemos detectado en los últimos días varios intentos de un tipo de *ransomware*, es decir, el secuestro de nuestro dispositivo y bloqueo a los datos del mismo (imágenes, documentos, correos electrónicos, datos personales y bancarios...), solicitando el pago de un importe para liberarlo. El usuario recibe un correo en el que se le informa de que se ha instalado un software en su dispositivo y se ha accedido al control del mismo (programas, cámara, micrófono...), indicándole además, en muchos casos, que se está en posesión de vídeos o imágenes de contenido sexual del usuario y se le amenaza con difundirlas entre sus contactos. Para evitarlo, se le indica que debe pagar una cantidad de dinero a cambio de devolverle el control de su dispositivo y no difundir dichas imágenes.

¿Qué debemos hacer si recibimos alguno de estos correos?

- Nunca se deben responder ni enviar información personal o nuestros datos bancarios a este tipo de correos, ni abrir los posibles archivos adjuntos que incluyan.

- En muchos intentos de *phishing* el usuario ni siquiera tiene cuenta en la supuesta entidad bancaria que le está advirtiendo de un problema en su cuenta o tarjeta, por lo que debemos ignorar ese correo. En caso de que se tratara de nuestra entidad bancaria, hay que tener presente que nunca nos van a solicitar dichos datos a través de un correo electrónico, por lo que también debe ignorarse esa solicitud.
- No pagar el rescate que nos solicitan.
- Proteger correctamente el acceso a nuestro WiFi.
- Tener actualizado nuestro sistema operativo y el antivirus y realizar copias de seguridad periódicas para poder restaurar los archivos
- No usar la misma contraseña para diferentes accesos y cambiarlas cada cierto tiempo. En este sentido, desde la Oficina de Seguridad del Internauta aconsejan utilizar un gestor de contraseñas (aplicación en la que podemos almacenar nuestras diferentes credenciales de forma segura).

¿Qué hacer en caso de ser víctima de *phishing* o si nos roban o secuestran nuestros datos?

Si hemos respondido a uno de estos correos facilitando nuestros datos personales o bancarios, lo primero que debemos hacer es ponernos en contacto con nuestra entidad bancaria y comunicarlo, de manera que tomen las medidas oportunas.

También debemos pasar el antivirus por nuestro dispositivo, para que detecte y limpie cualquier problema que encuentre. Además, debemos cambiar la contraseña que podamos haber facilitado de acceso a correos electrónicos, plataformas de compras, bancos, redes sociales...

Para cualquier consulta, recuerde que puede ponerse en contacto con nosotros en avacu@avacu.es o en nuestros teléfonos de atención 96 351 66 44 y 96 352 68 65.