

La suplantación de empresas de paquetería por SMS

RESUMEN: Los ciberdelicuentes continúan suplantando la identidad de empresas con nombre conocido, para hacer un envío masivo de SMS con fines criminales, como es la apropiación indebida de datos.

CATEGORÍAS: CIBERSEGURIDAD

Nº HIPERVINCULOS: 2

¿Alguna vez has recibido un SMS diciéndote que tu paquete está a punto de llegar cuando resulta que no has pedido nada? Pues esto tiene una explicación. Hace unos meses, aunque perduran y continúan a día de hoy, algunas empresas de paquetería como [Correos](#) y Correos Express han sido suplantadas por mensajes de SMS.

Este ciberataque se conoce como smishing. Consiste en el envío de un SMS a gente aleatoria, haciéndose pasar por Correos o Correos Express, incluso cualquier otra empresa consolidada que genere confianza; para que los usuarios pinchen en el enlace y de esta forma, obtener todos sus datos de carácter personal sin permiso. Si recibes un mensaje de texto de algo que no has pedido o que le ves con un aspecto fraudulento, no lo abras.

¿Cómo evitar ser víctima de fraudes como smishing?

Lo primero y más importante es que bajo ningún concepto abras el mensaje, ni lo contestes; lo mejor es eliminarlo de tu bandeja de entrada.

Debes de ser muy cauto ante el uso de los SMS, porque muchas veces, como mencionábamos anteriormente, se esconden bajo el nombre de una empresa reconocida, como puede ser: Correos, Coca-Cola, Mercadona, etc.

Si lo consideras fiable y entras, procura asegurarte que la URL pertenece a la página oficial; de no ser así, no facilites ningún tipo de información, ni mucho menos tus datos de carácter personal. Los ciberdelicuentes procuran dejarlo todo con un aspecto muy similar al de la web oficial para que "caigan sus presas".

Y ante la duda de saber si es verdadero el mensaje o no, ponte en contacto con la propia empresa; ella te resolverá la duda o en caso contrario, les ayudarás a que estén informados de que están sufriendo ciberataques.

¿Qué hago si he "caído en la trampa" y he pagado los gastos de envío que me pedían?

Hay ocasiones en las que vamos con prisas o no nos fijamos, y por error entramos en la espiral del ciberdelicuyente. En este caso, en cuanto seas consciente de ello, ponte en contacto con tu entidad bancaria para contarla lo sucedido y que cancele el pago o si estáis a tiempo que no lo permita. Y si a parte de haber pagado has ofrecido tus datos personales, procura estar muy atento a los medios digitales para que no hagan un uso indebido de los mismos.

Y por último, no olvides denunciarlo a las [Fuerzas y Cuerpos de Seguridad del Estado](#) (FCSE), para que hagan un parte de lo ocurrido e investiguen para que no le ocurra a nadie más.