CincoDías
Cinco Días
España
12/05/20
Pr: Diaria
Tirada: 25.171
Dif: 17.439
Cod: 132309756
Pagina: 29
Secc: POLÍTICA - ECO Valor: 3.200,18 € Area (cm2): 180,8 Ocupac: 20,13 % Doc: 1/1 Autor: EFE MADRID Num. Lec: 38000

Hacienda alerta de un fraude en su nombre a empresarios

La Agencia Tributaria advierte de que no está pidiendo dinero a cambio de no cerrar negocios por el Covid-19

EFE
MADRID

Algunos empresarios han recibido un correo electrónico con el emblema de la Agencia Tributaria solicitándoles que descarguen y rellenen un documento para "evitar la suspensión" de su negocio, en el marco de las medidas económicas adoptadas durante el estado de alarma por la pandemia de coronavirus.

Se trata de un mensaje falso, que intenta suplantar a la Agencia Tributaria para sustraer datos de los usuarios. Este falso correo con medidas tributarias justifica su envío en lo dispuesto en el Real Decreto 15/2020 del 21 de abril, de medidas urgentes complementarias para apoyar la economía y el empleo, pero es un solo un anzuelo, según denunció ayer la Guardia Civil a través de su perfil oficial en Twitter.

Si el usuario pincha en el enlace con la indicación "Descargar", es remitido a una página web donde le piden que aporte sus datos personales. El correo también le indica que debe descargar, imprimir el archivo y enviarlo firmado en siete días.

La alerta de la Guardia Civil indica que este correo electrónico forma parte de una campaña de suplantación de la Agencia Tributaria con el objetivo de robar los datos personales de los usuarios que acceden a esa web, según esta alerta de la Guardia Civil.

El Instituto Armado, explicó ayer que el objetivo de este tipo de correos electrónicos es utilizar las supuestas ayudas económicas "como gancho" para robar credenciales a los empresarios. También recordó que la Agencia Tributaria no solicita información confidencial por correo electrónico.

El Instituto Nacional de Ciberseguridad (Incibe) ya emitió el 28 de abril una alerta de seguridad de importancia alta sobre esta campaña de envío de correos electrónicos "maliciosos", en la que recomienda a los empresarios que hayan accedido e introducido sus credenciales en esta web que cambien "lo antes posible" sus claves. Según detalla el Incibe en su aviso, los ciberdelincuentes que están detrás de este tipo de envíos utilizan una técnica llamada *spoofing* (del verbo inglés que significa parodiar o suplantar).