02/01/2025

Golpe a la DGT con la nueva estafa masiva de nivel 4 de la multa de tráfico pendiente de pago

El organismo estatal alerta a la población ante estas prácticas por parte de los ciberdelincuentes



Las ciberestafas continúan abriéndose paso en la sociedad de manera alarmante. La cantidad de fraudes cibernéticos ha adquirido una categoría de problema de primer orden en casi cualquier aspecto de la vida, y el número de casos -y complejidad- aumenta exponencialmente.

En esta ocasión, las víctimas son, por un lado, la Dirección General de Tráfico (DGT) y por otro, los ciudadanos y contribuyentes, que ven cómo su información y datos personales se encuentran en peligro nuevamente.

Pero, ¿en qué consiste esta nueva estafa? Según informó el Instituto Nacional de Ciberseguridad (Incibe), se trata de uno de los más peligrosos de los que hay en la actualidad, ya que consiste en suplantar a la Dirección General de Tráfico con el objetivo de estafar y engañar a transportistas, camioneros, conductores autónomos y todo aquel que utilice su vehículo como forma de trabajo.

Para ello, consiguen replicar con total precisión la imagen y los métodos utilizados por la DGT para cobrar las multas, con la diferencia de que estas son falsas. Es tal la gravedad de esta estafa que desde el propio organismo estatal le dan una puntuación de importancia de 4 sobre 5.

Como otras muchas, este fraude se centra en el smishing (envío de mensajes de texto maliciosos) y phising (como correos electrónicos falsos) en los que se notifica a los conductores de una supuesta multa de tráfico que se encuentra pendiente de pago. Lo hacen de una forma que aparentemente procede de la DGT e incluyen enlaces a portales web similares a los oficiales.

Una vez llegado hasta aquí, a la víctima se le abre un formulario en el que se le pide que rellene los datos de información personal: número de DNI, dantos bancarios, etc. y todo ello en una interfaz idéntica a la oficial.

Para detectar estas posibles prácticas fraudulentas, desde Incibe han dado algunas claves que pueden servir como pistas para que las víctimas puedan darse cuenta de que están intentando ser estafadas.

Algunas de las que destacan son:

- Mensajes que aludan a urgencia desmedida: "Último recordatorio" o "en las próximas 24 horas"
- Faltas de ortografía: En muchas ocasiones, los estafadores cometen algunos errores ortográficos que, a todas luces, serían imposibles de encontrar en comunicados oficiales.

- URL sospechosas: Direcciones acortadas o dominios en los que no se especifique "dgt".

En el caso de que ya se hayan rellenado los datos, desde Incibe piden que se actúe rápidamente y se puede hacer de diferentes formas:

- Contactando con su banco para informar de lo ocurrido y que se proceda al bloqueo de la tarjeta
- Hacer capturas y recopilar todas las pruebas posibles (imágenes, enlaces...)
- Elevar una denuncia ante las autoridades competentes.

Pese a todo esto, tanto las autoridades, la DGT como Incibe, aseguran que son los autónomos los más susceptibles ante este tipo de prácticas y estafas ya que son aquellos que dependen fundamentalmente de su vehículo y utilizarlo con mayor frecuencia que otros.

Finalmente, destacan que se esté alerta especialmente en estas fechas, ya que los ciberdelincuentes intentan llevar a cabo estas prácticas fraudulentas con mayor asiduidad durante estas épocas, aunque no es la única época del año en el que estar pendiente, ya que pueden ocurrir en cualquier otro momento.

Fuente: https://www.huffingtonpost.es/

LINK DE LA NOTICIA