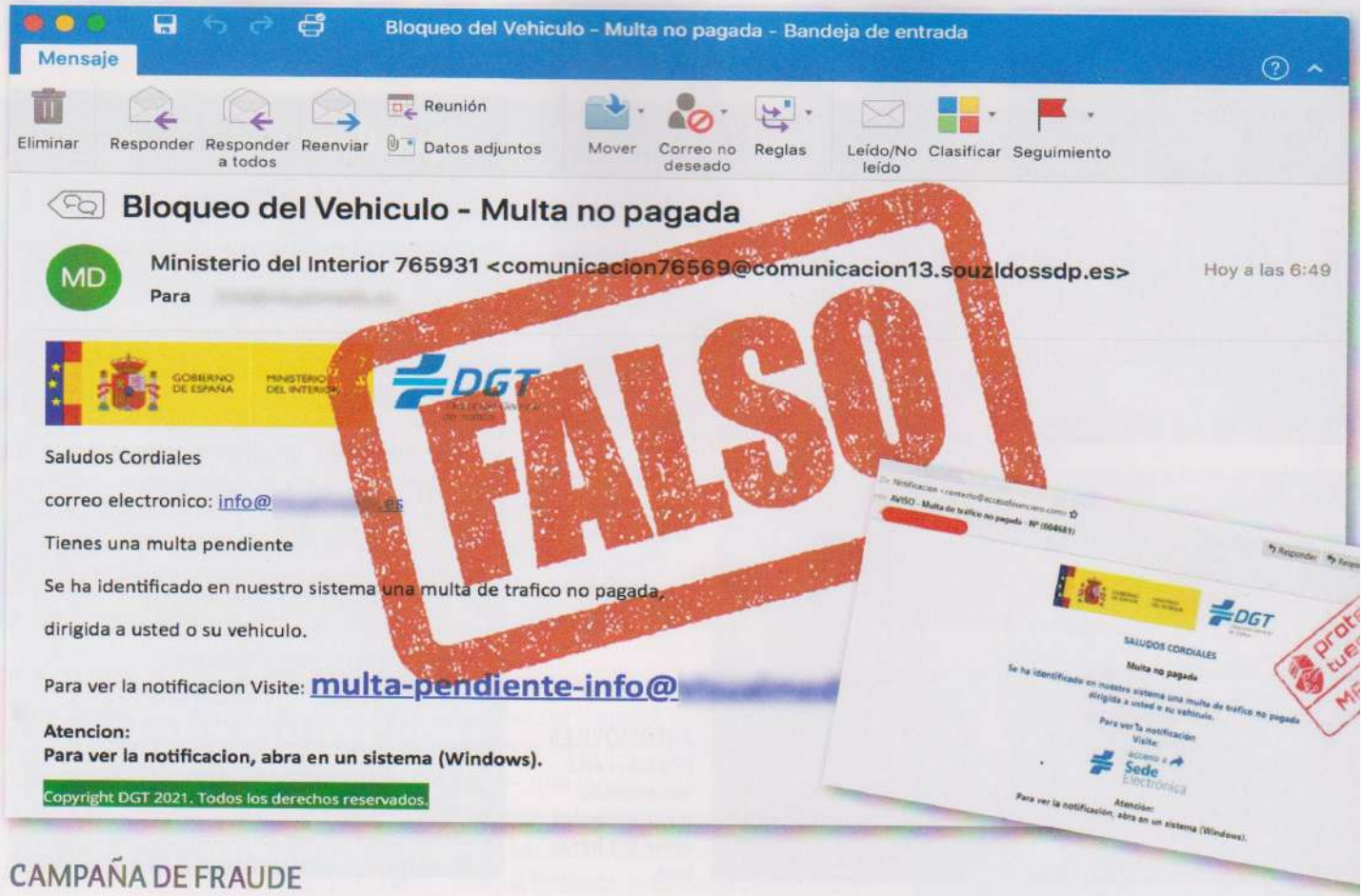

CAMPAÑA DE FRAUDE

La DGT nunca notifica multas a través de correo electrónico

Cada cierto tiempo se producen envíos masivos de avisos de multas de tráfico por correo electrónico. Se trata de un fraude (*phising*) que busca instalar un software malicioso. Pero la DGT **NUNCA** notifica sus multas a través de correo electrónico: **siempre lo hace por correo postal certificado o Dirección Electrónica Vial.**

• J. M. M.

Cada cierto tiempo, redes de malhechores ponen en marcha campañas de fraude a través del correo electrónico, en un tipo de intento de estafa conocido como *phising* (pesca en inglés). Y, claro está, las multas de tráfico son un 'gancho' muy llamativo para sus intentos de fraude.

De hecho, a finales de marzo el INCIBE (Instituto Nacional de Ciberseguridad) lanzó una alerta al haber *"detectado una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar a la Dirección General de Tráfico (DGT) con el propósito de difundir malware"* (software malicioso). De hecho, en dicha campaña, se envía un correo al usuario suplantando al Ministerio del Interior, con el asunto «Bloqueo del Vehículo – Multa no pagada». En el cuerpo del mensaje se indica al usuario que tiene una multa pendiente y que puede acceder a la notificación desde el enlace que figura en el correo. Este enlace dirige al usuario a una web externa, desde donde se descarga un archivo comprimido en formato .zip que simula ser la multa y que contiene *malware*.

El timo del carné caducado

También se han detectado –y denunciado públicamente– correos electrónicos en los que se avisa de la presunta caducidad del permiso de conducir y se solicitan datos tales como fotografía de las dos caras del DNI, del permiso de conducir e incluso una foto. Se trata, también, de un intento de fraude. La DGT ha alertado, a través de sus redes sociales, de que no se proporcione *"ningún dato ni pinches en ningún enlace"* en caso de recibir estos correos. *"Elimínelos directamente"*, concluye en sus redes sociales.

LA DGT NO COMUNICA MULTAS POR E-MAIL. Al margen de recordar los consejos que facilita INCIBE para identificar correos peligrosos y evitar engaños: no abrir correos de origina desconocido, desconfiar y no abrir archivos adjuntos, ver la dirección real de envío…, hay que destacar que la DGT nunca co-

MINISTERIO DEL INTERIOR

DGT

Centro de Tratamiento de Denuncias Automatizadas
Apartado de Correos 505, 24080-LEON

VELOCIDAD
NOTIFICACION DE INICIACIÓN DE EXPEDIENTE

Nº EXPEDIENTE:

FECHA Y HORA DE LA INFRACCIÓN: 03/03/2021 - 16:14h

IMPORTE TOTAL DE LA MULTA: 300.00€
IMPORTE CON 50% DE REDUCCIÓN: 150.00€
IMPORTE ABONADO: 0.00€
MATRÍCULA:
CLASE: TURISMO
MARCA:
MODELO:

DATOS DEL INTERESADO

NT80147016168200000 3852

LUGAR DE LA INFRACCIÓN

LUGAR: Vía A-2 P. Klm.: 272.9
sentido: D-DECRECIENTE 2

FOTOGRAFÍA DEL VEHÍCULO DENUNCIADO:

PRECEPTO INFRINGIDO

Art. 21 LTSV
Art. 48.1 REGLAMENTO GENERAL DE CIRCULACION

PÉRDIDA DE PUNTOS

Esta infracción lleva aparejada la pérdida de 2 PUNTOS.
Puede consultar su saldo de puntos en www.dgt.es

HECHO DENUNCIADO:

CIRCULAR A 159 KM/H, TENIENDO LIMITADA LA VELOCIDAD A 120 KM/H. EXISTE UNA LIMITACION GENERICA EN VIA INTERURBANA. CINEMOMETRO 2334 MULTANOVA ANTENA 2334 QUE HA SIDO SOMETIDO AL CONTROL METROLOGICO LEGALMENTE ESTABLECIDO ART. 83.2 LTSV.).

Ha sido Vd. identificado como el conductor del vehículo reseñado en el momento de cometerse la infracción que se notifica. Dicha infracción fue captada en el lugar, fecha y hora señalados, a través de medios de captación y reproducción de imágenes que permiten la identificación del vehículo, lo que impidió notificar la denuncia en el acto (art. 89.2.c LTSV). La imagen del vehículo y el certificado del cinemómetro utilizado se remiten adjuntos a este documento.

ESTA, SÍ

La DGT solo comunica sus sanciones a través de correo certificado en comunicaciones como la de la imagen. En caso de fallar esta notificación (por ejemplo, el conductor ha cambiado su residencia y no lo ha notificado a la Jefatura de Tráfico) se comunica a través del TAU o del TESTRA o de los boletines oficiales o, si lo han solicitado, a través de la Dirección Electrónica Vial.

munica sus multas por correo electrónico, sino siempre lo hace a través de cartas certificadas o, cuando esta notificación falla, a través de boletines oficiales, tablón de anuncios municipal o el Tablón Edictal de Sanciones de Tráfico (TESTRA) o en el Tablón Edictal Único (TEU).

Esto solo tiene una excepción: que previamente se haya inscrito usted de forma voluntaria en la Dirección Electrónica Vial (DEV) –un buzón electrónico en el que puede darse de alta para recibir las comunicaciones y notificaciones que haya que hacerle de manera telemática y que tiene los mismos efectos jurídicos que una notificación en papel por carta certificada–. En este caso sí podría recibir el aviso de que existe una notificación por SMS o a través del correo electrónico que usted previamente haya habilitado en el que se le solicitará que entre en la página de la Dirección Electrónica Vial y, tras identificarse (con DNI electrónico o Certificado Digital), accederá a la notificación de multa.

COMPROBAR LA MULTA. En cualquier caso –y además de recomendar no descargar ni abrir correos sospechosos o sus adjuntos–, cualquier ciudadano puede entrar al TESTRA y sin certificado de ningún tipo ni DNI electrónico, solo introduciendo el número del DNI, NIE o CIF comprobar si existe alguna multa de aquellas sanciones cuya notificación por correo mediante carta certificada haya fallado (por ejemplo, por haber cambiado de domicilio y no haberlo notificado a la jefatura de Tráfico correspondiente). ◆

Alarma: americanismos y faltas de ortografía

Hay varias señales de alarma para identificar un posible fraude. En primer lugar, el usuario real que envía el correo. Son sospechosas direcciones como @comunicacion13.souzldossdp.es, que aparecen cuando se pulsa sobre el nombre del remitente. También lo son el uso de americanismos (como tránsito en vez de tráfico) o incluso faltas de ortografía.

Pistas para evitar el fraude

El envío de presuntas multas de tráfico por correo electrónico es la punta del iceberg de la ciberdelincuencia. Es muy habitual –en concreto el fraude con multas de la DGT– la suplantación de identidad a través de correo electrónico (*email spoofing*). Según el Instituto Nacional de Ciberseguridad (INCIBE), *"se envían correos con remitente falso para enviar spam, difundir malware o llevar a cabo ataques de* phishing *y suplantar la identidad de directivos de la empresa, proveedores, clientes, etc"*. Y la relajación de las medidas de seguridad imprescindibles debido a la multitud de tareas para las que a diario se usa el correo electrónico, con prisas y rutinas, la utilizan los ciberdelincuentes para sus engaños.

Consejos ante un correo sospechoso:

1 No abrir correos de usuarios desconocidos, o que no haya solicitado, y eliminarlos directamente.

2 No contestar en ningún caso a estos correos.

3 Revisar los enlaces antes hacer clic, aunque sean de contactos conocidos.

4 Desconfiar de los enlaces acortados.

5 Desconfiar de los ficheros adjuntos, aunque sean de contactos conocidos.

6 Tener siempre actualizados sistema operativo y antivirus (y que esté activo).

7 Asegurarse de que las cuentas de usuario utilizan contraseñas robustas y no tienen permisos de administrador.

Es importante, ante la mínima duda, analizar detenidamente el correo. Si ya se ha descargado y ejecutado el archivo, escanee todo el equipo con el antivirus y siga las instrucciones marcadas por el mismo para eliminar el malware.

Señas de distinción

- Los métodos cada vez más depurados de los ciberdelincuentes hacen complicado distinguir un correo legítimo de otro que no lo es. En los encabezados de los correos hay, oculta pero visualizable con un par de clics, información que puede dar pistas sobre si se trata de un correo 'peligroso'. (En este enlace, el INCIBE explica cómo acceder a esa información en función del sistema operativo y el programa que utilice para acceder al correo electrónico).
- En la información de las cabeceras, con herramientas como MessageHeader, hay indicios de que se trata de un correo legítimo. Por ejemplo, que el correo se entregue en 1 segundo («Delivered after 1 sec»): un tiempo de entrega excesivo o el paso por muchos servidores antes de ser entregado (en el último campo se ven los servidores por los que pasa el correo hasta ser entregado) es indicativo de correo fraudulento. Otro buen indicio es que el dominio (campo «From:») desde el que se envía coincida con el emisor del mensaje recibido (no hay suplantación). La no coincidencia, por el contrario, es mala señal.
- También son 'pistas' de que el correo puede ser fraudulento el uso de americanismos (por ejemplo, tránsito en vez de tráfico) o incluso se han detectado algunos con faltas de ortografía.