RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/12145 **07/05/2020** **27304**

AUTOR/A: BELTRÁN VILLALBA, Ana María (GP); VÁZQUEZ BLANCO, Ana Belén (GP); ROJAS GARCÍA, Carlos (GP); JIMÉNEZ-BECERRIL BARRIO, María Teresa (GP); SANTAMARÍA RUIZ, Luis (GP); MONTESINOS AGUAYO, Pablo (GP); ÁLVAREZ FANJUL, Beatriz (GP); BORREGO CORTÉS, Isabel María (GP); HISPÁN IGLESIAS DE USSEL, Pablo (GP); MATEU ISTÚRIZ, Jaime Miguel (GP)

RESPUESTA:

En relación con la pregunta formulada, se informa que según la información aportada por el INCIBE-CERT, desde el inicio del dispositivo especial de ciberseguridad con motivo de la pandemia de COVID-19, se han registrado hasta la actualidad un total de 91 modalidades de correos fraudulentos, que se tratarían de campañas de correo electrónico en las que se presentarían casos de phishing, spam, suplantaciones, etc., con el fin de robar información de carácter personal y otra información sensible a sus víctimas aprovechando las circunstancias actuales. Este porcentaje se correspondería con un 45,96% de los incidentes detectados por ese equipo de respuesta a incidentes de seguridad(CSIRT).

En la actualidad, las principales medidas de protección ante ataques de phising o smishing se basan en el desarrollo de políticas de navegación segura e higiene digital. Es una tendencia criminal que va actualizando el engaño al entorno del perfil de la víctima mediante campañas en determinadas ventanas temporales.

Por ello se considera fundamental actualizar la casuística y difundir esa información entre los usuarios. A este respecto, el Gobierno sustenta su política de información especializada en dos pilares:

- El primero es el Instituto Nacional de Ciberseguridad (INCIBE), el cual ofrece su respuesta, a través de la Oficina de Seguridad del Internauta (OSI) ,donde constantemente se actualiza la información de campañas de phising/smishing.

- El segundo, las Fuerzas y Cuerpos de Seguridad (FCSE), estas informan sobre las últimas tendencias, ya sea bien con material propio elaborado fruto de la propia experiencia, bien siendo eje de trasmisión de información aportada por otros cuerpos y agencias policiales a nivel nacional e internacional.

Cabe indicar que las FCSE están siendo muy activas en materia de información y concienciación sobre esta amenaza a la ciudadanía. En este sentido, son continuos los mensajes informando sobre campañas en las cuentas y perfiles corporativos en redes sociales, donde además de aportar contenidos propios, se hace eco de otros elaborados por agencias internacionales como INTERPOL o EC3-EUROPOL.

Madrid, 11 de junio de 2020