

TGR denuncia nueva arremetida de correos maliciosos enviados a contribuyentes

- ***Quienes reciban estos mensajes falsos deben abstenerse de responderlos y de descargar archivos, para evitar el mal uso de sus datos personales.***

La Tesorería General de la República (TGR) está reportando una nueva arremetida de correos maliciosos, que envían sujetos anónimos, imitando los elementos distintivos e incluso valiéndose de los formatos de comunicación institucionales, para engañar a usuarios y contribuyentes, tratando que éstos caigan en el juego de entregar sus datos privados.

La advertencia es para que las personas que reciban estos mensajes fraudulentos, **no abran ni descarguen los links o direcciones de e-mails adjuntos**. El llamado a los contribuyentes es a tomar los resguardos correspondientes, primero, para identificar estos correos maliciosos, que en la jerga informática se conocen como *phishing*, y segundo, para que procedan a su inmediata eliminación en la bandeja de entrada de sus correos electrónicos.

Una forma de reconocer estas acciones fraudulentas es con el asunto del correo electrónico, el cual en esta ocasión tiene por título **“Segunda Alerta Urgente de Regularización”**.

Denuncia ante la Justicia

Debido a la gravedad de esta situación, la TGR realizó una denuncia ante el Ministerio Público para ubicar a los autores de estos envíos maliciosos y en lo posible, aplicar las sanciones que correspondan.

De forma complementaria, la TGR está trabajando con la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones (PDI), respecto a la prevención y advertencias de los tipos de delitos informáticos y cómo promover una cultura de ciberseguridad en el organismo, con foco en la difusión a los usuarios y contribuyentes.

La TGR aclara que, en el caso de establecer contacto con sus usuarios, **de ninguna manera solicita datos personales, o pide que los usuarios descarguen archivos** desde un mensaje de tipo masivo. Para ello, utiliza cuentas de correo institucionales debidamente identificadas, donde la información para el usuario se obtiene mediante el sitio tgr.cl, ingresando con su clave personal.

Recordamos que el sitio tgr.cl cuenta con altos niveles de seguridad para que los contribuyentes pueden efectuar pagos y hacer trámites, mediante el uso de sus claves secretas y personales, las cuales no se deben entregar por ningún motivo a terceros.

Orientación a los usuarios

A raíz de esta nueva arremetida de correos maliciosos, la plataforma Contact Center de la TGR ha recibido miles de llamadas durante estos días, dando respuestas oportunas a los usuarios, donde se les informa de los resguardos que deben tomar para evitar problemas posteriores.

Junto con lo anterior, se reitera que, en las comunicaciones oficiales de la TGR dirigidas a los usuarios, nunca se solicita descargar informes o dar acuse de recibo a través de e-mails, porque solo tienen como fin informar de las etapas del pago de los compromisos fiscales de año calendario.



Esta nueva embestida digital la están realizando delincuentes informáticos aprovechando la contingencia de la devolución masiva de excedentes de la Operación Renta 2018, por lo cual los contribuyentes deben tener especial cuidado y no tomar en cuenta estos emails, que claramente tienen un objetivo delictual.

Santiago, 10 de mayo de 2018

TESORERÍA GENERAL DE LA REPÚBLICA
Unidad de Comunicación Institucional TGR