El Longino
Soy del Norte
Fecha: 02/04/2025 Audiencia: 10.800 Sección: LOCAL
Vpe: $319.605 Tirada: 3.600 Frecuencia: 0
Vpe pág: $515.658 Difusión: 3.600
Vpe portada: $515.658 Ocupación: 61,98%

Inicio de la Operación Renta 2025:

Cómo evitar posibles estafas digitales durante este proceso en Servicio Impuestos Internos

La asociación gremial que representa a las pequeñas, medianas y grandes empresas tecnológicas en nuestro país, Chiletec, advirtió que en los últimos años se han incrementado la mensajería que suplanta al Servicio de Impuestos Internos (SII) e hizo un llamado a adoptar una serie de medidas que eviten la ocurrencia de estos fraudes, que comúnmente buscan robar datos bancarios o personales.

Muchos usuarios han denunciado, en sus últimas declaraciones de renta, la circulación de correos electrónicos falsos que intentan suplantar la identidad del Servicio de Impuestos Internos (SII), aludiendo a problemas en la emisión de las boletas electrónicas o a la necesidad de modificar los datos de facturación. Desde la Asociación de Empresas Chilenas de Tecnologías (Chiletec) alertaron sobre los principales errores que cometen los chilenos ante este tipo de estafas masivas y advirtieron que es muy probable que estos ataques cibernéticos se incrementen en los próximos días debido al inicio de este proceso.

Según explicó Myriam Pérez, líder de la Mesa de Ciberseguridad de Chiletec, "uno de los errores más frecuentes incluyen el no verificar la autenticidad del remitente. Muchas asumen automáticamente que un correo electrónico, especialmente si parece provenir de una fuente legítima como el SII, es genuino. Otros errores incluyen hacer clic en enlaces o descargando archivos adjuntos sin la debida precaución, como pasar antes el cursor sobre ellos para verificar la URL de destino. Las personas también suelen pasar por alto las señales de alerta, como errores ortográficos o gramaticales y la solicitud de información personal o financiera a través de medios no seguros".

Respecto a los peligros que están asociados a este tipo de delitos, Pérez aseguró que "los usuarios se exponen a una serie de peligros, incluyendo el robo de identidad, acceso no autorizado a las cuentas bancarias, o la instalación de un malware en el dispositivo de la víctima. Esto último puede resultar en un control remoto del dispositivo y el robo de información personal y corporativa; y no me refiero solo a computadores, sino también en teléfonos móviles, que son cada vez más el objetivo de estos ataques debido a su uso masivo".

En este sentido, la especialista en seguridad de la información de Chiletec afirmó que "los estafadores también emplean técnicas como el phishing, a través de mensajes de WhatsApp o redes sociales como Instagram, donde envían enlaces maliciosos que, al ser clickeados, pueden instalar software dañino. Esta modalidad de estafa se ha vuelto particularmente atractiva para los ciberdelincuentes, dada la popularidad y la confianza que los usuarios depositan en esta plataforma. Este método permite a los estafadores personalizar sus ataques, haciendo sus engaños más convincentes y aumentando las probabilidades de éxito".

Respecto a la forma en cómo se puede prevenir este tipo de ciberataques, la líder de la Mesa de Ciberseguridad del gremio aseguró que "antes de interactuar con un correo electrónico, es crucial asegurarse de que el remitente sea legítimo e idealmente contactar a la entidad que envió el correo directamente por los canales oficiales. Además, es importante estar atentos a las advertencias del navegador sobre sitios web potencialmente inseguros o certificados de seguridad vencidos o inválidos. Estas alertas son un claro indicativo de que se debe proceder con precaución o, mejor aún, evitar completamente el ingreso a dicho sitio".

"También hay que evitar hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos sospechosos. Siempre utilizar soluciones de seguridad y mantener actualizado el software de antivirus y antimalware. Una buena práctica es habilitar la autenticación de dos factores (2FA), esto añade una capa adicional de seguridad a las cuentas en línea. Y por supuesto, mantenerse informado de las últimas técnicas de fraude y cómo evitarlas", agregó Pérez.