Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Ciudad de México, a 12 de enero de 2021
INAI/013/21

ALERTA INAI DE FRAUDES A TRAVÉS DE *PHISHING O* SUPLANTACIÓN DE IDENTIDAD

- Se deben tomar las precauciones necesarias para no ser víctimas de ciberdelincuentes.

El *phishing* es la técnica utilizada por ciberdelincuentes para obtener información de cuentas bancarias y/o de seguridad social, contraseñas, entre otros datos, enviando mensajes para suplantar a una entidad legítima como puede ser un banco, una red social, un servicio o una entidad pública.

Ante tal situación, el Instituto Nacional de Transparencia, Acceso de la Información y Protección de Datos Personales (INAI) recomienda lo siguiente:

1. Antes de ingresar los datos personales en un formulario o página web, revisar si cuenta con una política o aviso de privacidad para saber el uso que se dará a la información solicitada.

2. Evitar ingresar a sitios web a través de enlaces que se reciben por correo electrónico, servicios de mensajería o publicaciones en redes sociales. En su lugar, teclear la dirección del sitio directamente en el navegador.

3. Comprobar que la dirección de la página web comience con https:// e incluya un pequeño candado cerrado en la barra de estado del navegador.

4. Establecer filtros de correo no deseado y fraudulento.

5. Prestar atención en la redacción, faltas de ortografía o signos extraños de los sitios y mensajes en línea.

6. Si el mensaje obliga a tomar una decisión de manera inmediata, se recomienda verificar directamente con el servicio que lo solicita para corroborar la autenticidad de la solicitud.

7. Evitar descargar archivos de fuentes no confiables o remitentes desconocidos.

8. Revisar de forma periódica los estados de cuenta bancarios y departamentales, con la finalidad de identificar cualquier transacción o movimiento irregular.

9. Evitar proporcionar datos personales o información confidencial a través de llamadas telefónicas o en sitios que parezcan sospechosos o de los cuales se desconfíe.

10. Cambiar contraseñas frecuentemente.

11. En caso de haber sido víctima de phishing, recopilar toda la información que sea posible: correos, capturas de conversaciones mediante mensajería electrónica, documentación enviada.

El Instituto señala que otras variedades de *phishing* son el *smishing* que consiste en mensajes alertando a la persona de que ha sido ganador de un "premio", comúnmente la víctima responde con alguna acción como llamar a un número telefónico, hacer *clic* en un enlace en donde se le solicitarán datos personales, de cuentas bancarias, contraseñas o incluso números de tarjetas; el *vishing,* práctica que consiste en el uso de la línea telefónica convencional y técnicas sociales para engañar a las personas y obtener información confidencial, datos personales, contraseñas o información útil para el robo o suplantación de identidad.

Seguir estas recomendaciones contribuirá a evitar ser víctimas de los ciberdelincuentes.

El INAI invita a la sociedad a visitar el micrositio #IdentidadSegura, que proporciona información y herramientas sobre cómo proteger sus datos personales y así reducir el riesgo de que su identidad sea robada y, en caso de haber sido víctimas, conocer qué hacer y ante quién acudir https://micrositios.inai.org.mx/identidadsegura/.

-o0o-