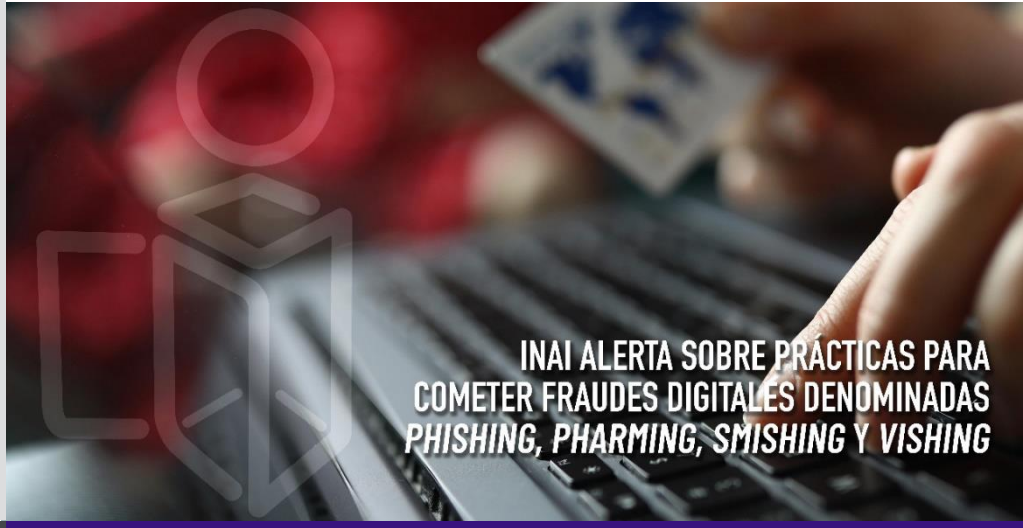
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL Y DIFUSIÓN

COMUNICADO • **INAI/449/21**



Ciudad de México.
28 de diciembre de 2021

www.inai.org.mx

- **Los ciberdelincuentes engañan a las personas usuarias para obtener sus datos personales, mediante sitios web falsos, correos electrónicos, mensajes de texto o llamadas**
- **El INAI emite recomendaciones para evitar que las personas sean víctimas de estos tipos de fraude**

INAI ALERTA SOBRE PRÁCTICAS PARA COMETER FRAUDES DIGITALES DENOMINADAS *PHISHING, PHARMING, SMISHING* Y *VISHING*

Los ciberdelincuentes buscan obtener ilegalmente datos personales y cometer fraudes o estafas, a través de diversas prácticas, como el *phishing, pharming, smishing y vishing*, alerta el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

El *phishing* consiste en usurpar la identidad de una empresa u organización gubernamental. Se hacen llegar correos electrónicos a la víctima con un enlace a una página aparentemente legal, pero en realidad es duplicada, en donde piden datos personales para después cometer el fraude.

Dos variantes del phishing son el *vishing* y el *smishing*; en el primer caso se utilizan mensajes de texto SMS fraudulentos para obtener datos personales de la víctima y, en el segundo, llamadas telefónicas o mensajes de voz.

A su vez, el *pharming* es la práctica de suplantar el dominio de un sitio web. En este caso se dirige al usuario a un sitio falso, con apariencia prácticamente igual al que es de su interés acceder, en el que se captura la información confidencial de la víctima.

A fin de que las personas extremen precauciones en el cuidado de su información confidencial y eviten ser víctimas de alguno o varios de estos tipos de fraude, el INAI hace las siguientes recomendaciones:

- No acceder a *links* o vínculos contenidos en correos electrónicos o mensajes de texto que provengan de un remitente desconocido.

- Cerrar cualquier ventana emergente que pueda abrirse al navegar.

- Verificar que la dirección del portal de un banco o del sitio donde se requiera realizar alguna compra e ingresar datos bancarios, inicie preferentemente con el ícono de un candado cerrado y con https, ya que la "s" implica que los datos ingresados se transmitirán de forma cifrada.

- Evitar el uso de computadoras públicas para acceder a la información personal y/o realizar operaciones de banca en línea; de ser necesario, recordar limpiar el historial al terminar la navegación.

- Por ningún motivo proporcionar datos personales bancarios por correo electrónico, mensajes o llamadas.

- No dar *clic* en los hipervínculos donde se solicite actualizar datos bancarios.

- En caso de recibir una notificación por correo electrónico en la que se informe que la cuenta fue bloqueada, reportar esta situación al banco mediante la línea de atención telefónica y no a través de los teléfonos recibidos en dicha notificación. Si aún quedara duda del correo, llamar o asistir al banco y verificar los hechos.

- Evitar responder mensajes de texto en los que soliciten visitar un sitio web o llamar a un número telefónico para resolver problemas financieros.

- Nunca revelar el número de la tarjeta de crédito o el código de seguridad de ésta como respuesta a una llamada, mensaje o correo electrónico.

- Desconfiar de llamadas de números desconocidos o con una numeración sospechosa.

- Elegir en todo momento la opción de "NO" recordar las contraseñas, que suele aparecer en una ventana emergente del navegador.

- Cambiar con regularidad las contraseñas y claves de acceso. Una contraseña segura debe contener más de seis caracteres, combinando letras mayúsculas, minúsculas y distintos signos.

-o0o-

VER FOTOGRAFÍA