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

DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL Y DIFUSIÓN

COMUNICADO • **INAI/385/22**

Ciudad de México.
26 de diciembre de 2022

www.inai.org.mx

- **Con esta práctica, se infringen las medidas de seguridad de instituciones o empresas para acceder a sistemas informáticos y obtener información de manera ilícita**

- **De acuerdo con datos de la Asociación Mexicana de Ciberseguridad, México registró 85 mil millones de intentos de ciberataques en el primer semestre de 2022**

EMITE INAI RECOMENDACIONES PARA PROTEGER DATOS PERSONALES ANTE UN *CRACKEO* O CIBERATAQUE

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emite una serie de recomendaciones que deberán seguir las personas ante un *crackeo* o ciberataque, ya sea a instancias públicas o privadas, con el fin de proteger sus datos personales.

En el mundo digital, el *crackeo* o ciberataque se ha convertido en una práctica cada vez más común, con la cual se infringen las medidas de seguridad de instituciones o empresas para acceder a sistemas informáticos y obtener información de manera ilícita, entre la que puede haber datos de carácter personal.

De acuerdo con datos de la Asociación Mexicana de Ciberseguridad (AMECI), México registró 85 mil millones de intentos de ciberataques en el primer semestre de 2022.

Ante un crackeo o ciberataque a instancias públicas o privadas que, por alguna razón, posean nuestros datos personales, el INAI recomienda lo siguiente:

- Al recibir correos electrónicos de instituciones conocidas, como tu banco, verifica que la dirección de correo del remitente sea válida, pues generalmente, para robar información (*phishing*) o infectar con un *malware*, utilizan correos similares a los originales.

- No proporciones información personal al responder algún correo electrónico, mensaje de texto o llamada; mejor, entra en contacto con la institución o empresa por los canales oficiales y cuentas verificadas.

- Evita abrir archivos adjuntos de correos electrónicos no verificados, ya que pueden contener virus; si hay duda, consulta el origen de éstos.

- Cambia y actualiza tus contraseñas cada cierto tiempo, debido a que todas pueden ser descifrables en determinado momento; sin embargo, al modificarlas, de manera constante, las posibilidades disminuyen.

- Utiliza contraseñas robustas que contengan mínimo 12 caracteres, dentro de los cuales haya números, letras y símbolos, evitando formar palabras disponibles en un diccionario.

- Implementa la autenticación de doble factor en los servicios en los que esté disponible este control de seguridad; para agregar una capa extra de seguridad a tus cuentas, es decir, un paso adicional al iniciar la sesión, a fin de impedir que otras personas puedan entrar, aunque tengan acceso a tu contraseña.

- Practica el *egosurfing* cada cierto tiempo; esta acción consiste en utilizar las redes sociales y los buscadores de Internet para localizar información sobre nosotros mismos en la red, con el fin de constatar que no existan perfiles falsos o actividades sospechosas.

En caso de que el *crackeo* o ciberataque sea directamente a tus cuentas de redes sociales, el INAI sugiere emprender las siguientes acciones:

- Cambia tu contraseña; esto se debe hacer tanto en el servicio que ha sufrido el ataque como en otros donde se haya utilizado la misma contraseña o una parecida.

- Avisa a todos tus contactos y solicita que no den *clic* a ninguna publicación o contesten mensajes que provenga de tu perfil.

- Verifica todo tu perfil, pues suelen manipularlo, por ejemplo, colocando *links* que, en realidad, son un medio de difusión de *malware*.

- En caso de estar disponible en la aplicación de la red en cuestión, implementa el control de autenticación de doble factor.

- Bloquea tus cuentas bancarias en caso de que estén vinculadas, de alguna manera, con tu red social.

- Configura la privacidad de tus cuentas en redes sociales; es recomendable que algunos contenidos solo estén disponibles para amigos y familiares más cercanos, y no para el público en general.

- Actualiza siempre tus dispositivos móviles y computadoras, protégelas con un antivirus; al actualizar los sistemas operativos y aplicaciones, se despliegan parches de seguridad.

El acceso no autorizado a tu información personal vulnera tu derecho a la protección de datos personales y puedes denunciarlo ante este Instituto. La queja puede enviarse al correo atencion@inai.org.mx.

-o0o-

VER FOTOGRAFÍA