



• Información relevante en materia de Protección de Datos Personales

PHISHING

¡FELICIDADES!
SE GANÓ \$ 100 000 000 000

EL PHISHING REGULARMENTE SE DA POR MEDIO DE

- LLAMADAS: ¡Acaba de ganar un vehículo!
- CORREOS ELECTRÓNICOS: ¡URGENTE! Si eres usuario de google.com, estómalo cliente. Para verificar su identidad ingresa los siguientes datos: <http://www.inai.org.mx>
- MENSAJES DE TEXTO: DESCONOCIDO +01 (246) 7693. Si quieres participar en el sorteo ALBERCADA, para registrarse <http://www.inai.org.mx>

PARA RECONOCER UN MENSAJE DE PHISHING, EL INAI RECOMIENDA HACERTE LAS SIGUIENTES PREGUNTAS

- ¿El contenido, redacción u ortografía del mensaje es sospechoso?
- ¿El mensaje se dirige de forma genérica al destinatario?
- En caso de contar con un hipervínculo, ¿este se direcciona a un sitio seguro?
- ¿El mensaje solicita realizar una acción determinada de forma inmediata, como por ejemplo la actualización de datos, cambio de contraseña o efectuar el pago de un servicio?
- ¿El mensaje ofrece algún cupón, premio, concurso u oferta sospechosa?
- ¿El mensaje proviene de un correo electrónico que no pertenece a la entidad que dice ser?

Telinai
www.telinai.org.mx
800 835 4324

¡NO PONGAS EN RIESGO TUS DATOS PERSONALES!

MENSAJES INFORMATIVOS CON ENLACES MALICIOSOS
Remiten a información o recomendaciones sobre COVID-19, buscan la atención del usuario para que visite sitios maliciosos que solicitan información personal.

RANSOMWARE
Archivos adjuntos de correo electrónico o mensaje de texto que contienen un programa malicioso que puede infectar, cifrar o tomar el control de nuestros equipos, y afectar la confidencialidad y disponibilidad de nuestros datos personales y de la información almacenada.

MENSAJES DE SOLIDARIDAD
Aprovechan la situación de emergencia sanitaria para engañar y solicitar apoyo destinado al personal de salud. Algunos piden datos personales o donaciones económicas.

MENSAJES PHISHING
Comparten la dirección electrónica de un sitio que suplanta la identidad de otro conocido o de interés del usuario. A través de este engaño, el atacante roba la información o datos personales ingresados por la víctima en el sitio falso.

MENSAJES SMISHING
Mensajes SMS que suplantan la identidad de una institución oficial, con la finalidad de compartir un enlace en el que solicitan datos personales.

BENEFICIOS DE PROGRAMAS SOCIALES
Mensajes que suplantan la identidad de instituciones públicas y ofrecen apoyo económico, a través de supuestos programas sociales, para lo cual solicitan datos personales y en algunos casos dinero.

OFERTAS DE TRABAJO
Mensajes que comparten falsas ofertas de empleo y que, para registrarse en las supuestas listas de vacantes, solicitan datos personales.

SOPORTE TÉCNICO FRAUDULENTO
Servicios falsos a través de llamadas o mensajes que aprovechan la situación de trabajo a distancia para obtener datos personales del usuario, incluyendo sus contraseñas.

SERVICIOS GRATUITOS
Mensajes falsos que ofrecen promociones, descuentos o cupones para tener acceso gratuito a servicios de entretenimiento y que, para hacerlos válidos, solicitan datos personales.

FRAUDES MÁS UTILIZADOS EN LA EMERGENCIA SANITARIA POR COVID-19

#TusDatosValen
#INAIteDefiende

Fuente: <https://www.inai.org.mx/actualidad/blog/2020/03/27/top-10-fraudes-que-utilizan-covid-19-para-esparar-las-señales>

Para proteger tu vida, tenes que preguntar #AcércatealINAI

INGRESA DATOS PERSONALES SEGUROS COVID 19

inai www.inai.org.mx





inai  **PROTECCIÓN DE DATOS PERSONALES durante el trabajo a distancia**

Como parte de las medidas de control adoptadas para evitar la propagación de COVID-19, las organizaciones e instituciones del Sector Privado y Público, en los casos que así lo permitan, adoptarán esquemas de trabajo a distancia también llamado teletrabajo.

Para proteger los datos personales y la información que será utilizada en este esquema temporal de trabajo, el INAI comparte las siguientes recomendaciones:

Correo electrónico:

- Cumplir con las políticas de la organización relacionadas con el uso de correo electrónico.
- Usar las cuentas de correo electrónico de trabajo en lugar de cuentas personales para correos electrónicos relacionados con actividades laborales que traten datos personales.
- Si es estrictamente necesario utilizar cuentas de correo electrónico personal para enviar datos personales o información confidencial adjunta, ésta deberá estar cifrada.
- Evitar incluir datos personales o información confidencial en el asunto del correo electrónico.
- Antes de enviar un correo electrónico verificar que la dirección del destinatario sea correcta, especialmente en casos donde se envíen datos personales y/o sensibles.
- Verificar que el entorno donde se utilice el correo electrónico sea seguro, para evitar que personas no autorizadas tengan acceso a datos personales o información.


