Ciudad de México, a 28 de marzo de 2018
INAI/084/18

RECOMIENDA INAI A USUARIOS DE INTERNET TENER PRECAUCIÓN PARA EVITAR SER VÍCTIMAS DE *PHISHING*

- **El *Phishing* es uno de los ataques más utilizados en Internet, es una forma de engaño que utilizan los ciberdelincuentes para obtener información personal, bancaria o usurpar la identidad de algún individuo, empresa u organización**
- **En México 65.5 millones de personas usan Internet, de acuerdo con el INEGI**

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emite recomendaciones de seguridad a los usuarios de Internet para la protección de su privacidad y evitar ser víctimas de *Phishing*.

El órgano garante hizo hincapié que el manejo responsable de los datos personales disminuye la exposición a riesgos como la usurpación de identidad, el secuestro y la extorsión.

El *Phishing* es uno de los ataques más utilizados en Internet, es una forma de engaño que utilizan los ciberdelincuentes para obtener información personal, bancaria o usurpar la identidad de alguna persona, empresa u organización.

El *Phishing* puede consistir en mensajes engañosos, o bien en la falsificación de sitios web (*clonados*), imitando a los portales oficiales de organizaciones, empresas, personajes públicos, entre otros.

Existen distintos modelos de distribución de *Phishing*, las más comunes son:

- *Phishing tradicional*: Implica el envío de correos o mensajes engañosos de manera masiva, sin estar dirigidos a un destinatario específico.
- *Phishing dirigido* (*Spear Phishing*): Consiste el envío de correos electrónicos o mensajes personalizados para un grupo específico, o incluso a un individuo en particular.

A su vez, los *ciberdelincuentes* pueden valerse de distintas técnicas para ejecutar estos ataques. Una de estas técnicas es el uso de *enlaces web acortados,* los cuales originalmente se pensaron para compartir direcciones electrónicas a través de redes sociales, sin embargo, un atacante se vale de dichas direcciones cortas para “esconder” referencias a sitios, donde se distribuyen programas maliciosos (*malware*) o dedicados a realizar estafas.

Por ejemplo, la dirección electrónica “www.soyunadireccionmaliciosa.com.mx”, puede “disfrazarse” con una herramienta como *bit.ly* o *Google URL Shortener*, para

verse de la siguiente forma: “goo.gl/aUIbkja”. Este formato, además de ser más fácil de compartir por mensajería instantánea o redes sociales, no permite al usuario inferir que el contenido del sitio puede ser peligroso.

Además del correo electrónico, los atacantes pueden realizar *Phishing* a través de distintos servicios de mensajería, por ejemplo los mensajes de texto SMS *(Smishing)*. En esta modalidad, los *ciberdelincuentes* se hacen pasar por entidades bancarias u otra organización conocida, y envían un mensaje de texto al teléfono de la víctima solicitando datos personales para verificar un supuesto fraude, o indicando que ha ganado un premio. Para recabar la información bancaria o los números de las tarjetas de crédito, los atacantes incluso cuentan con falsos centros de atención telefónica.

A través de redes sociales, el *Phishing se* manifiesta a través de mensajes o publicaciones con enlaces a sitios con contenido malicioso o fraudulento.

En este contexto, el INAI recomienda algunas medidas preventivas para evitar ser víctima de *Phishing*:

1. Verificar que en los navegadores de Internet se encuentren habilitadas las funciones de *bloqueo de contenido*, del apartado de *seguridad y privacidad*. Por ejemplo: “Protegerte a ti y a tu dispositivo contra sitios peligrosos” (*Google Chrome*), “Protege mi PC contra las descargas y los sitios malintencionados con el filtro Smart Screen” (*Microsoft Edge*) y “Bloqueo de contenido peligroso o engañoso” (*Mozilla Firefox*).
2. Desconfiar de las supuestas notificaciones de empresas proveedoras de servicios, instituciones bancarias u otras organizaciones, con mensajes genéricos como “Estimado usuario” o “Estimado cliente”, sin algún tipo de personalización.
3. Tener precaución con los mensajes de texto, correos electrónicos o notificaciones que recibas, toma en cuenta que, aunque el mensaje incluya cierta información personal, no es una prueba de que es genuino.
4. Evitar la descarga de los archivos adjuntos y dar clic en los enlaces de correos o mensajes no solicitados.
5. Verificar los enlaces acotados con algún servicio en línea, por ejemplo: *Unshorten o URL XRAY*
6. No ingresar a sitios web a través de enlaces que recibes por correo electrónico, servicios de mensajería o publicaciones en redes sociales. En su lugar, teclea la dirección directamente en el navegador.
7. Ser precavido con las solicitudes de amistad o agregar como contactos a personas desconocidas.
8. No proporcionar información personal, en especial financiera o bancaria, a través de correo electrónico, portales de Internet o llamadas telefónicas, sin la seguridad de que la persona o entidad que la solicita está autorizada para ello. Se recomienda hacer una llamada o enviar un correo electrónico directamente al banco o empresa con la que tengamos la relación y a nombre de quien se realiza el contacto, para verificar que el correo electrónico, llamada telefónica o la comunicación sean auténticos.
9. Revisa de manera periódica los movimientos de tus cuentas de servicios y bancarias en busca de anomalías.

10. Cambia tus contraseñas frecuentemente, si sospechas que has sufrido de *Phishing*, cámbialas de inmediato.

En México 65.5 millones de personas usan Internet, de acuerdo con la última Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2016 (ENDUTIH-2016), que realizó el Instituto Nacional de Estadística y Geografía (INEGI).

La encuesta reportó un incremento en las transacciones electrónicas respecto a los resultados de la encuesta anterior; éstas pasaron del 12.8 por ciento en 2015 al 14.7 por ciento en 2016.

De acuerdo con datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios (CONDUSEF), de enero a septiembre de 2017, se registraron 4.8 millones de reclamaciones por posible fraude con tarjeta de crédito y débito; es decir, 28% más que en 2016.

Además, la CONDUSEF mencionó que el 49% de los fraudes con tarjetas fue en el comercio electrónico, y con mayor frecuencia mediante técnicas de suplantación de identidad como *Phishing* .

El INAI reafirmó la importancia de la protección de los datos personales en el uso de Internet para evitar consecuencias negativas.

-o0o-