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

Ciudad de México, a 20 de julio de 2018
INAI/210/18

# *PHISHING*, PRÁCTICA FRECUENTE PARA OBTENER INFORMACIÓN CONFIDENCIAL DE INTERNAUTAS Y COMETER ILÍCITOS, ALERTA INAI

- **El Instituto emite una serie recomendaciones de seguridad a los usuarios de Internet para proteger su privacidad y evitar ser víctimas de este método de fraude**

El *phising* se ha convertido en una de las principales prácticas de ciberdelincuentes para obtener información confidencial de usuarios de Internet, de manera ilegal, y cometer ilícitos como la usurpación de identidad, el secuestro y la extorsión, alerta el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Esta práctica consiste en el envío de mensajes engañosos o en la clonación de portales oficiales de organizaciones, empresas, personajes públicos, entre otros.

Existen dos modalidades, el *phishing tradicional*, que implica el envío de correos o mensajes engañosos de manera masiva, sin destinatario específico, y el *phishing dirigido,* que se refiere al envío de correos o mensajes personalizados.

Otra técnica frecuente 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 estos vínculos para “esconder” referencias a sitios, en los que se distribuyen programas maliciosos (*malware*) o dedicados a estafar.

En las redes sociales, la práctica se da a través de mensajes o publicaciones con enlaces a sitios con contenido malicioso o fraudulento.

Ante este escenario, el INAI emite las siguientes recomendaciones de seguridad a los usuarios de Internet para proteger su privacidad y evitar ser víctimas 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.

**-o0o-**