HONORABLE CONGRESO DEL ESTADO DE CHIHUAHUA

P R E S E N T E.-

El suscrito **Omar Bazán Flores**, Diputado de la LXVII Legislatura del Honorable Congreso del Estado, **integrante al grupo parlamentario del Partido Revolucionario Institucional,** con fundamento en el artículo 68 Fracción I de la Constitución Política del Estado y 167 fracción I y 168 de la Ley Orgánica del Poder Legislativo para el Estado de Chihuahua, comparezco ante esta Honorable Representación Popular para someter a su consideración **Iniciativa con carácter de Decreto con el propósito de reformar el Código Penal del Estado de Chihuahua, a fin de que se adicione una fracción XI en el Artículo 224, con la finalidad de sancionar el Smishing,** por lo que me permito someter ante Ustedes la siguiente:

EXPOSICIÓN DE MOTIVOS

"Smishing" es un término que se utiliza para describir una forma de estafa en la que los delincuentes intentan engañar a las personas a través de mensajes de texto o SMS (Short Message Service). Es una combinación de las palabras "SMS" y "phishing".

En una estafa de smishing, los estafadores envían mensajes de texto falsos que parecen provenir de una fuente legítima, como un banco, una empresa o una entidad gubernamental. Estos mensajes a menudo incluyen enlaces o números de

teléfono que los destinatarios se les pide que llamen. Los estafadores utilizan diversas tácticas para engañar a las personas y persuadirlas a proporcionar información personal o financiera, como números de tarjetas de crédito, contraseñas, números de seguridad social u otros datos confidenciales.

El smishing es una forma cada vez más popular de delincuencia cibernética. Según el informe State of the Phish del 2023 de Proofpoint, el 76 % de las organizaciones experimentaron ataques de smishing en 2022.

El smishing es alarmante porque las personas tienden a confiar más en los mensajes de texto que en los mensajes de correo electrónico. La mayoría de las personas son conscientes del riesgo para la seguridad que conlleva hacer clic en vínculos incluidos en mensajes de correo electrónico. Sin embargo, no puede decirse lo mismo cuando se trata de mensajes de texto.

El smishing usa elementos de ingeniería social para que comparta información personal. Esta táctica se aprovecha de su confianza para obtener información. Los atacantes buscan todo tipo de información: desde contraseñas en línea hasta el número de la seguridad social o información de su tarjeta de crédito. Una vez que los obtienen, pueden comenzar a realizar compras a su nombre. En ese momento es cuando comienzan los problemas.

Otra táctica que usan los atacantes es informarle que, si no hace clic en un vínculo y especifica su información personal, se le comenzará a cobrar el uso de un servicio de forma diaria. Si no se inscribió para el servicio, ignore el mensaje. Si ve cargos no autorizados en el resumen de su tarjeta de débito o crédito, eleve el reclamo a su banco.

En general, no debe responder mensajes de texto de personas que no conoce. Esa es la mejor forma de permanecer protegido. Esto se aplica particularmente cuando el SMS proviene de un número de teléfono que no lo parece, por ejemplo, el número de teléfono 5000. Esta es una señal de que, en realidad, el mensaje de texto se trata de un correo electrónico enviado a un teléfono.

La lucha contra el smishing (SMS phishing) y otras formas de estafas electrónicas es un tema de preocupación para muchas organizaciones y gobiernos. Las iniciativas para abordar el smishing y proteger a las personas de este tipo de estafas suelen incluir varios componentes:

Educación y concienciación: Las organizaciones, gobiernos y agencias de seguridad cibernética llevan a cabo campañas de educación y concienciación para informar a las personas sobre los riesgos del smishing y cómo reconocer los intentos de estafa. Esto puede incluir consejos sobre cómo verificar la autenticidad de los mensajes de texto y qué hacer si se sospecha de un smishing.

Colaboración entre partes interesadas: Las empresas de telecomunicaciones, las instituciones financieras, las fuerzas del orden y otras partes interesadas a menudo trabajan juntas para abordar el smishing. Esto puede incluir compartir información sobre amenazas y mejores prácticas para combatir estas estafas.

Desarrollo de tecnología de seguridad: Las empresas de tecnología y seguridad cibernética trabajan en el desarrollo de soluciones técnicas para detectar y prevenir el smishing. Esto puede incluir el desarrollo de aplicaciones de seguridad móvil y sistemas de filtrado de mensajes de texto.

Protección de datos personales: La protección de datos personales y la regulación de cómo se almacenan y utilizan los datos pueden ayudar a reducir la cantidad de información sensible disponible para los estafadores.

Herramientas de denuncia: Se fomenta el uso de líneas directas o sitios web donde las personas puedan denunciar intentos de smishing y otras estafas. Esto permite a las autoridades rastrear y responder a estas amenazas.

Para protegerse del smishing, es importante ser cauteloso al recibir mensajes de texto de fuentes desconocidas o sospechosas. No haga clic en enlaces ni comparta información confidencial a través de mensajes de texto sin verificar la autenticidad de la fuente. Si recibe un mensaje de texto sospechoso, es aconsejable ponerse en contacto directamente con la entidad o empresa involucrada utilizando la información de contacto oficial proporcionada en su sitio web o en documentos legítimos, en lugar de utilizar la información proporcionada en el mensaje de texto. También puede informar los intentos de smishing a su proveedor de servicios móviles y a las autoridades locales.

Por lo anterior es que me permito someter a consideración de este **H. Congreso del Estado de Chihuahua**, el siguiente proyecto de decreto:

DECRETO:

ARTICULO PRIMERO. - Se reformar **el Código Penal del Estado de Chihuahua, a fin de que se adicione una fracción en el Artículo 224, con la finalidad de sancionar el Smishing,** para quedar redactados de la siguiente manera:

Artículo 224.

I.- al X.- ….

XI. Utilice diversas tácticas para engañar a las personas y persuadirlas a proporcionar información personal o financiera, como números de tarjetas de crédito, contraseñas, números de seguridad social u otros datos confidenciales, a través de mensajes de texto o SMS falsos que parecen provenir de una fuente legítima, como un banco, una empresa o una entidad gubernamental.

TRANSITORIOS

ARTICULOS PRIMERO. - El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Estado.

ECONÓMICO. - Aprobado que sea, túrnese a la Secretaría para que elabore la minuta en los términos en correspondientes, así como remita copia del mismo a las autoridades competentes, para los efectos que haya lugar.

Dado en el Palacio Legislativo del Estado de Chihuahua, a los 6 días del mes de mayo del año dos mil veinticuatro.

ATENTAMENTE

DIPUTADO OMAR BAZÁN FLORES