


Senado de la Nación

SENADO DE LA NACION DIRECCION DE MESA DE ENTRADAS	
	21 JUN 2022
EXP. 5	Nº 1423/22 Hora 15

PROYECTO DE RESOLUCIÓN

El Senado de la Nación

RESUELVE

Solicitar al Presidente del Ente Nacional de Comunicaciones (ENACOM) que:

- a) En el término de 120 días, implemente las normas, disposiciones y/o acciones necesarias que permitan, dentro del ámbito de su competencia, compeler a la incorporación de más medidas de verificación por parte de las empresas de telefonía móvil a los usuarios que adquieran tarjetas SIM;
- b) Informe a este honorable cuerpo legislativo los avances en torno a lo solicitado en el inciso anterior.



DR. EDUARDO A. VISCHI
SENADOR NACIONAL



FUNDAMENTOS

Sra. Presidenta:

El fraude de suplantación de identidad digital, un implica un proceso de ingeniería social mediante el cual es posible contratar una línea de teléfono en nombre de otra persona. Es una actividad que viene en crecimiento durante los últimos años en Argentina.

Según un estudio del laboratorio de investigación de ESET, desde el año 2017 los delitos de suplantación de identidad vienen en aumento.

El intercambio de SIM o SIM swapping incluye duplicar la tarjeta SIM de un teléfono inteligente. La tarjeta SIM o Módulo de identidad del suscriptor en un teléfono móvil almacena el código de acceso de cliente y el número de teléfono de la compañía telefónica.

El peligro del intercambio de SIM es que no necesita acceso físico al dispositivo móvil para clonar la tarjeta SIM. Para ello, los ciberdelincuentes se ponen en contacto con el servicio de atención al cliente de los operadores de telefonía y se hacen pasar por usuarios legítimos.

Si tiene éxito, obtendrá una nueva tarjeta SIM y podrá acceder a la información confidencial almacenada en ella (contactos, contraseñas, datos bancarios, etc.). De esta manera, secuestrarán la línea telefónica de la víctima y usarán toda su información, como solicitar una nueva contraseña y obtener un código de verificación para acceder a su banca en línea.

Para comenzar este proceso de estafa se busca recolectar información personal de la víctima, para ello se utilizan técnicas como el phishing y el smishing (vía SMS), además es posible acceder a información personal en sistemas de bases de datos públicas de fácil acceso.



Senado de la Nación

Luego, con esta información se comunicaban con la compañía telefónica haciéndose pasar por usuarios legítimos y de esta manera obtener una nueva tarjeta SIM con el mismo número de teléfono.

La tarjeta SIM, dependiendo de la empresa telefónica y la zona geográfica, puede ser obtenida presencialmente en una oficina o enviada a un domicilio. Para esta situación basta acreditar identidad, en algunos casos mencionando datos personales, en otros presentando el DNI físico. Según investigaciones del programa Buenos Días América del 30 de marzo del 2022, las personas que cometen este delito han llegado a falsificar documentos en miras a obtener la tarjeta SIM de la víctima.

En América Latina esta problemática también existe. En Argentina, el delito ha presentado un crecimiento constante desde el 2017, y se reportan cada vez más casos de víctimas que dicen haber sufrido el robo de dinero como consecuencia de la clonación del chip.

Para evitar esta situación resulta necesario aumentar la cantidad de requisitos que se solicitan a los usuarios de telefonía móvil para acreditar su identidad al momento de adquirir una tarjeta SIM.

Por todo lo antes expuesto solicito a mis pares que me acompañen con su voto.

DR. EDUARDO A. VISCHI
SENADOR NACIONAL