CIRCULAR EXTERNA

RESTRINGIDA

CONSECUTIVO	247	**FECHA**	9	MAR	2023	**ANEXOS: SI** ☐ **NO** ☒	
TEMA: **RECOMENDACIONES DE SEGURIDAD**							
COMPLEMENTA CIRCULAR(ES): NINGUNA		**MODIFICA CIRCULAR(ES):** NINGUNA			**DEROGA CIRCULAR(ES):** NINGUNA		

Desde Visionamos SPBV y su área de Seguridad de la Información queremos dar a conocer una nueva modalidad de fraude que se viene presentando en algunas entidades de la Red.

Informamos los pasos que son ejecutados por los delincuentes y su modo de operar, desde el área de Seguridad de la información de Visionamos pedimos la mayor atención a esta información:

1. Se ha identificado que los ciberdelincuentes están aplicando ingeniería social a los asociados de las entidades participantes, esto con el fin de captar la mayor cantidad de información personal y así cometer acciones ilícitas como: suplantación o robo de identidad, llegando al punto de lograr engañar al personal encargado de realizar el proceso de actualización de datos dentro de la entidad cooperativa.

En que consiste la ingeniería social:

- Consiste en utilizar técnicas especializadas de engaño o manipulación para obtener y captar la mayor cantidad de información de una persona o una entidad y así pretender sacar provecho económico de forma ilegal

- La seguridad hoy en día no es sólo una tema que se solucione con tecnología como detectores de intrusos, sistemas contra pérdida de información, robo de información, sistemas de seguridad Web o con el último antivirus, la seguridad es una cuestión que tiene que ver también con las personas.

- El reto aquí es que la ingeniería social es REAL y altamente EFECTIVA porque se concentra en explotar la mayor vulnerabilidad: las personas.

- Este vector de ataque social puede anular los sistemas técnicos más efectivos mediante la manipulación de las personas con técnicas de engaño.

Situación actual:

2. Un supuesto asociado realiza llamada o envía correos electrónicos a la entidad Cooperativa para realizar el proceso de actualización de datos (el delincuente cuenta con la información del suplantado) suministrando número de documento de identidad, fecha de expedición del documento, numero de línea celular y correo electrónico.

3. El proceso de actualización de datos es ejecutado por el encargado en la entidad cooperativa sin percatarse de que fue engañado por el delincuente o tramador y que realizó un procedimiento con datos fraudulentos. **(Consideramos desde Seguridad de la información que este es un punto de control por parte de las entidades)**

4. En este punto el delincuente ya cuenta con nuevo número de celular y nueva cuenta de correo actualizados en el sistema de la entidad. Esta nueva información es notificada a Visionamos a través de las diferentes conexiones que se tiene establecidas.

5. Con estos nuevos datos el delincuente recibe SMS u OTP (según el caso) en el nuevo dispositivo registrado en la entidad participante, lo cual le permite realizar el fraude.

   Nota: Es importante anotar que los datos relacionados para el proceso de actualización no pueden ser modificados o alterados por parte de Visionamos como prestador de servicio transaccional, los datos o insumo para este proceso son proporcionados por cada entidad y actualizados al interior de sus bases de datos.

6. El delincuente o estafador realiza Compras en línea, Retiros en Cajeros, transacciones Web y Transacciones sin Tarjeta.

Visionamos ratifica su compromiso con la seguridad de las transacciones que se realizan a través de los diferentes canales de la Red Coopcentral y recomienda:

- Definir políticas y procedimientos alineados a las normativas correspondientes para la actualización de datos.
- Contar con una clasificación adecuada de la información que pueda evitar una fuga de esta.
- Contar con los controles necesarios para la validación de identidad de los asociados.
- Brindar capacitación y reinducción de seguridad y manejo de datos al personal encargado de los procesos de manejo de información.
- Implementar o adoptar buenas prácticas de Seguridad de la Información y Ciberseguridad, tomando como estándar la norma ISO27001 y 27032.
- Realizar campañas de concientización y sensibilización constante con los asociados, empleados y directivos de la entidad, enfatizando en no compartir datos personales o sensibles a través de llamadas telefónicas; además de no compartir sus accesos ya que estos son personales e intransferibles
- Realizar inspecciones de manera aleatoria con el ánimo de probar las medidas de control definidas para los temas transaccionales.
- El OTP (One Time Password), es un segundo factor fuerte de autenticación en el proceso, para lo cual se requiere dar un buen uso a la contraseña que es el primer factor de autenticación.
- Es importante implementar una labor de educación con recomendaciones de seguridad, dado que estas ayudan a que los usuarios no revelen ni dejen expuesta su información en manos ajenas.

Tener presente que Visionamos constantemente está trabajando en pro de la mejora de los productos y servicios que ofrece a todas las Entidades Participantes, y esto se realiza

a través de medidas como:

- Cumplimiento y certificación en el estándar PCI-DSS.
- Gestión de Vulnerabilidades.
- Gestión Pruebas de Intrusión.
- Cumplimiento y adaptación de la ley 1581 de 2012.
- Ciframiento de las bases de datos.
- Desarrollo seguro de aplicaciones basado en las mejores prácticas.

El área de seguridad de Visionamos estará siempre atenta para recibir sus inquietudes.

Cordialmente,

(Original firmado)
LUIS SANTIAGO GALLEGO VANEGAS
Gerente General