Respetados señores,
Comisión de Regulación de Comunicaciones - CRC

El proyecto de agenda regulatoria 2021 – 2022, dispone, en el numeral 4.4.6, que la "CRC tiene previsto recolectar información de mercado asociada a la neutralidad de red, para así, elaborar un documento de consulta que permita conocer de primera mano el estado de la neutralidad de red en el país en comparación con las nuevas tendencias y desafíos de mercado".

En ejercicio de esta función, proponemos que la CRC diseñe una estrategia que permita combatir delitos como el phishing y el smishing que por la normatividad y marco legal actual no cuentan con un "plan de ataque" o método para reducir su impacto. De igual manera, proponemos que la CRC reglamente un procedimiento expedito para atacar esta forma de ilegalidad, en la que se utilizan marcas registradas de entidades financieras con el fin de capturar información financiera de las personas.

Dentro de las facultades legales previstas en la Ley 1369 de 2009 (artículo 20 numeral 3) y en la Ley 1341 de 2009, le corresponde a la Comisión de Regulación de Comunicaciones -CRC-, la función de expedir toda la regulación de carácter general y particular en las materias relacionadas con la protección al usuario y las materias relacionadas con principios y obligaciones del acceso e interconexión de las redes de los proveedores de redes y servicios de telecomunicaciones.

Así mismo, la Resolución 5111 de 2017 en su artículo 2.1.10.10 establece que: "el usuario tiene el derecho a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, por lo que los proveedores de servicios de acceso a Internet no podrán limitar el acceso a contenidos, aplicaciones o servicios de terceros proveedores, **salvo en aquellos casos que por disposición legal o reglamentaria estén prohibidos**". De igual manera, la resolución 3101 de 2011 en su numeral 4.9 establece que: "los proveedores de redes y servicios de telecomunicaciones se abstendrán de imponer restricciones al acceso a cualquier servicio, aplicación o contenido de otros proveedores, **salvo en aquellos casos que, por disposición legal, reglamentaria, o regulatoria éstos estén prohibidos o restringidos**". En este sentido, ambas resoluciones abren la posibilidad para que la CRC regule esta materia sin necesidad de tramitar una nueva Ley.

El Phishing y el Smishing son dos modalidades de fraude por medio de las cuales los ciberdelincuentes engañan a los usuarios del sistema financiero mediante un correo electrónico (Phishing) o un mensaje de texto (Smishig), que supuestamente llega de parte de una entidad oficial, como una entidad bancaria, para que el usuario haga clic en el enlace que viene en el cuerpo del correo.

De acuerdo con el informe "Threat Intelligence Insider Latin America" de Fortinet, a nivel mundial en el segundo trimestre de este año, hubo un aumento en los intentos de engañar a los usuarios a ir a sitios maliciosos o de proporcionar información bajo mensajes relacionados con la pandemia actual, identificando campañas de phishing relacionadas con COVID 19 por correo electrónico. Según el mismo informe, México es el país donde más se detectaron amenazas de este tipo en la región, seguido de Perú, Brasil y Colombia.

De acuerdo con las cifras de la superintendencia financiera de Colombia, entre el 6 de abril y el 31 de agosto de 2020 (periodo de duración de la cuarentena en Colombia), el uso de canales digitales como internet y banca móvil aumentó un 34% y un 23,2% respectivamente.

Teniendo en cuenta el valor de las reclamaciones por fraude y la transaccionalidad del sector, se pudo evidenciar un incremento del 10,47% del fraude en canales digitales, pasando de $0,26 pesos por cada $10 mil pesos transados en el período enero a agosto de 2019 a $0,29 pesos en el mismo periodo de 2020. En este sentido, el phishing y el smishing (robo de datos) representa el 74,24% de las reclamaciones por posible fraude y son las principales amenazas de seguridad para los usuarios sistemas financiero que realizan sus transacciones.

Con respecto al smishing, en Colombia se ha evidenciado que los proveedores de contenidos y aplicaciones - PCA, venden paquetes de códigos cortos a diferentes empresas para el envío masivo de mensajes de texto - SMS con el fin de promocionar sus productos y servicios. Sin embargo, se ha identificado que algunas "empresas" (legalmente constituidas) adquieren estos servicios para desplegar sus ataques de smishing y cometer fraudes.

Si bien la Comisión de Regulación de Comunicaciones – CRC, cuenta con algunos sitios web que pueden servir de apoyo en las investigaciones que realizan las autoridades para identificar los proveedores o asignatarios de los códigos cortos de los mensajes de texto (http://www.pnn.gov.co/mapa/) y otro sitio web para obtener la información detallada de los proveedores de contenido y aplicaciones (PCA) (http://www.siust.gov.co/siust/), el problema no se ha resuelto y aún existen grandes dificultades para identificar a quienes envían estos mensajes de texto masivos con contenido engañoso, así como en la identificación de los propietarios de los números telefónicos desde los cuales se envían.

Han pasado más de 20 años desde que se identificó el primer caso de phishing. Sin embargo, la problemática sigue vigente y se usa para robar información personal, credenciales en línea y detalles de tarjetas de crédito. La defensa contra los ataques de phishing es uno de los desafíos más difíciles que enfrenta la seguridad de la red actualmente.

En Asobancaria y sus entidades agremiadas proponemos la implementación de un mecanismo mediante el cual sea posible, de forma expedita, suspender los medios electrónicos que se utilizan de manera evidente para la comisión de un delito, como lo es la suplantación de páginas web de entidades financieras o el hurto de información confidencial o personal.

Consideramos necesario establecer unos protocolos claros para que los proveedores de Internet (ISP) logren bloquear aquellos contenidos que sean considerados ilegales por el uso fraudulento de marcas registradas o porque su propósito es estafar a las personas con mensajes engañosos para obtener sus datos, este proceso podría realizarse a través de un canal seguro y ágil para que las entidades financieras y las autoridades reporten el hallazgo de una página web o un SMS fraudulento a los ISP, de forma tal que puedan gestionar rápidamente su bloqueo.

Cordialmente,

Jaime Andrés Rincón
Director de Gestión Operativa y Seguridad
Carrera 9 No. 74 - 08 Piso 9 Ed. Profinanzas - Bogotá
Teléfonos: 326 6600 ext:1382
jrincon@asobancaria.com
www.asobancaria.com