Recibido: 13/09/2022
Aprobado: 18/10/2022

Campañas sociales, una alternativa para combatir el *smishing* en Colombia[1]

Palabras clave: *Smishing*, ciberdelito, suplantación, información y campañas sociales.

A medida que el mundo avanza tecnológicamente y existe cada vez mucha más interacción entre las personas y los diferentes dispositivos electrónicos que se manejan cotidianamente, se establece una relación más estrecha con el mundo digital y los productos que este promociona. Esto permite que, en general, de una forma más segura se pueda acceder a diferentes servicios que se ofrecen por parte de diversas entidades, por lo que gran parte de la información personal se maneja en estos equipos. Sin embargo, con este avance informático, a la par nacen también nuevas formas de ciberdelito, que a través de distintos medios buscan acceder ilegalmente a los datos sensibles de los usuarios para realizar diferentes tipos de robos o estafas, con el fin de generar un lucro en detrimento de los ciudadanos afectados.

Entre los distintos tipos de ciberdelito que existen hoy en día, se puede destacar a la técnica *phishing* como una de las más recurrentes al momento de querer apropiarse de la información de las personas. Esta técnica consiste en enviar un correo electrónico en el que se suplanta la identidad de una empresa o institución reconocida y así, intenta disuadir a las personas para que ingresen a ciertos enlaces enviados de páginas web, que fueron diseñadas como imitaciones de plataformas oficiales, para que estas potenciales víctimas ingresen sus usuarios y contraseñas allí, y permitan de esta manera a los delincuentes lograr apoderarse de la información de forma más rápida y directa (Swarnalatha K.S. et al., 2021). Según un análisis del informe de la policía en relación con las tendencias del cibercrimen en Colombia para los años 2019-2020, se encontró que "los incidentes más reportados en Colombia siguen siendo los casos de *phishing* con un 42%, la suplantación de identidad 28%, el envío de *malware* 14% y los fraudes en medios de pago en línea con 16%" (Ceballos et al., 2019). Son muy preocupantes tales estadísticas, pues dan

[1] Documento elaborado en el curso Competencias Idiomáticas Básicas a cargo de la Facultad de Filosofía y Ciencias Humanas de la Universidad de la Sabana, Chía-Cundinamarca, Colombia. Orientado por Lic. Liliana Triana Perdomo.

cuenta de la vulnerabilidad de los ciudadanos y su fragilidad para caer en este tipo de engaños.

Con el masivo uso de los *smartphones*, el *phishing* ha pasado por varias transformaciones a lo largo de los años. Una de sus variantes más conocidas es el *smishing*, sobre la cual se enfocará el tema de este ensayo. Esta forma de ciberdelito está encaminada al envío de mensajes de texto (SMS) a través de los distintos dispositivos móviles (Mishra & Soni, 2020), y al igual que el *phishing*, hace uso de la ingeniería social, entendida como la forma en cómo los cibercriminales interactúan con los usuarios, con el fin de engañarlos y apoderarse de sus datos personales (Alghenaim et al., 2022), e incluso fingir ser personas allegadas a la víctima y así cumplir su objetivo.

Desde una perspectiva financiera, el gerente de producto del Banco Falabella, César Serrato, indicó en su momento que "el *smishing*, a diferencia de formas de robo que se soportan en el uso de armas, acciones violentas y amenazas, busca confundir al consumidor haciéndole pensar que está accediendo a los canales del banco del cual es cliente" (Colombia.com, 2019). Adicionalmente, el gerente agregó que "esta falsa sensación de seguridad hace que el riesgo sea mayor al de otras modalidades pues el usuario no tiende a desconfiar al momento de ingresar sus datos más sensibles, quedando altamente vulnerable ante los delincuentes que capturen su información financiera" (Colombia.com, 2019).

Se logra evidenciar con lo anterior una falta de conocimiento por parte de la población colombiana acerca de cómo deben actuar para evitar caer en este tipo de trampas. El difícil acceso a datos sobre esta modalidad de ciber-robo y la baja periodicidad en la entrega de información serían causas directas de su aumento. Urge la necesidad de fomentar y reforzar estos temas de forma masiva a través de diversos medios de comunicación, mediante el uso de campañas de *marketing social* elaboradas de forma didáctica, que proporcione educación o capacitación al respecto. Este tipo de campañas son consideradas como una buena herramienta que logrará repercutir en el actuar de la gran mayoría de los ciudadanos, las cuales podrían estar patrocinadas por instituciones gubernamentales e incluso por las mismas entidades financieras, ya que son sus usuarios los que generalmente más sufren este tipo de robos, para garantizar de esta manera una alta recepción.

En primer lugar, el *marketing social* puede entenderse como la implementación de técnicas o metodologías de mercadotecnia que ayudan a promulgar ideas que estén a favor de la comunidad (Martínez Escareño et al., 2018), para así lograr influenciar de manera positiva en ciertos comportamientos de las personas. Con el uso de estas campañas sociales, se intenta que la población en general se eduque, concientice y reflexione sobre sus actitudes y conductas, de tal manera que sean capaces de percibir el perjuicio que les puede acarrear el no tener la suficiente prudencia y seguridad al momento de aceptar las invitaciones que les llegan directamente por mensajes de texto, de parte de diferentes personas o grupos de ciberdelincuentes que usan como fachadas los sitios aparentemente oficiales de las empresas reales.

En cuanto a su difusión, el mensaje puede propagarse de una forma bastante atractiva a través de muchos medios audiovisuales y eventos, ya que este tipo de campañas permiten gran flexibilidad e ingenio en su ejecución, en el cual el anuncio se puede transmitir de diferentes maneras. Incluso, se hace partícipe al receptor de este para generar mayor conciencia del problema al cual se encuentra expuesto, donde no necesariamente todo esto supondrá una gran inversión, pero sí una gran organización y creatividad. En Colombia, estos esfuerzos podrían aprovecharse de mejor manera si estuvieran amparadas por el gobierno, ojalá con una participación de las entidades privadas, logrando llegar más fácilmente a todos los rincones del país para generar un impacto positivo en el público, quienes podrían experimentar mayor confianza en estas instituciones, al sentir su constante protección y respaldo.

En segundo lugar, profundizando en el contexto colombiano, se han llevado a cabo campañas sociales con diversas temáticas, las cuales han tenido diferentes repercusiones en la población, debido a la forma en cómo se han realizado y, sobre todo, por el tiempo de exposición que han tenido, pues en algunos casos limitado por el corto tiempo que se han mantenido en los medios tradicionales de comunicación, como lo son la televisión, la radio y la prensa. A pesar de ser los medios más masificados entre la población, la mayoría de las campañas solo llegaron a concebir algunos cambios transitorios; sin embargo, todas intentaron mostrar un contenido concreto y directo sobre la problemática que desearon abordar (Sierra, 2017).

Entre algunos ejemplos de campañas cuya duración no fue la adecuada, y, por tanto, no generaron el impacto esperado, se pueden resaltar las campañas sociales

lideradas por las empresas de Green Peace Colombia y Centrales Energéticas de Norte de Santander (CENS), las cuales estuvieron centradas en la sostenibilidad, enfocadas a crear conciencia sobre las problemáticas relacionadas al medio ambiente. Dichas campañas incluyeron la difusión de videos, artículos y noticias para transmitir su mensaje, pero por el poco tiempo que estuvieron expuestas, quedaron en el olvido (Sierra, 2017). Por tal motivo, es imprescindible recalcar que estos esfuerzos para producir cambios en las conductas e impulsar hábitos seguros requiere tiempo, por lo cual es fundamental que este mensaje se mantenga por periodos largos para que generen recordación y el efecto deseado.

A partir de lo anterior, para atacar esta problemática del *smishing*, la campaña social debe enviar un mensaje lo suficientemente contundente y reiterativo para lograr impactar en la población que lo reciba, donde el objetivo sin duda será disminuir las tasas de ciberdelincuencia que abarcan esta modalidad. Esto favorece indirectamente a las empresas que se utilizan como fachadas para realizar estos engaños, debido a que se verán beneficiados muchos de sus usuarios.

Por último, la importancia de combatir esta modalidad de robo se da no solo porque puede atacar a los ciudadanos del común, sino también debido a que lo pueden hacer con las pequeñas y medianas empresas del país (PYMES). Dichas empresas muchas veces no cuentan con sistemas robustos de seguridad informática o la suficiente capacitación hacia sus empleados, quienes en medio de su desconocimiento pueden ingresar a estos sitios indebidos (Cesce, 2022). Estas acciones permitirán el robo de información confidencial de sus organizaciones e incluso, en casos extremos, el acceso a las claves bancarias, lo que traerá consecuencias nefastas para estas y ocasionará muchas pérdidas económicas (Asobancaria, 2020). Adicionalmente, las empresas que son suplantadas corren el riesgo de verse afectadas en su reputación, principalmente aquellas que manejan sus transacciones de tipo online, ya que, por culpa de estos ciberdelincuentes, la confianza de sus usuarios se ve mermada.

Para finalizar, es indispensable que las campañas encaminadas a educar o capacitar a una población objetivo, lleven consigo un mensaje concreto, claro y directo sobre la problemática a trabajar, es decir, que sea pedagógico, y que, en lo posible, se ejecuten de manera creativa. En este caso, estas campañas sociales deben enfocarse en cómo las personas deben enfrentar los delitos cibernéticos,

especialmente el que tiene que ver con la modalidad del *smishing*, para crear conciencia en las personas y desconfianza frente a los mensajes de texto que se puedan recibir, mejorando su ciberseguridad, y logrando así a largo plazo, la disminución de los altos porcentajes de casos presentados en el país.

Ana Lucía Quintero Vargas
Ingeniería Informática
Correo: anaquiva@unisabana.edu.co

Referencias

Alghenaim, M. F., Bakar, N. A. A., & Rahim, F. A. (2022). Exploring the Factors Influencing Employee Awareness of Social Engineering Threats: A Review. *Applied Mathematics and Information Sciences*, *16*(4), 491–500. https://bit.ly/3TXmsK3

Asobancaria. (2020). Impacto económico y social del phishing y el smishing en Colombia y el mundo. *Banca & Economía*, *1256*, 1–13. https://bit.ly/3UgWCjI

Ceballos, A., Bautista, F., Mesa, L., Argáez, C., Durán, A., Miranda, F., Acevedo, R., Prada, W., Ruiz, J., Santos, H., & Bautista, L. (2019). *Tendencias Cibercrimen Colombia 2019 - 2020*. https://bit.ly/3TWYpuB

Cesce. (2022, julio 14). El smishing, una amenaza virtual para las pymes. *Cesce Perú Blog*. https://bit.ly/3U2tP2Y

Colombia.com. (2019, octubre 29). *Smishing, la nueva forma de robo virtual que aqueja a Colombia*. https://bit.ly/3UcpJ7U

Martínez Escareño, I. M., Casillas Rancurello, M. F., Núñez Alfaro, C. M., González Galindo, A. D., Aguilera Valdez, A. E., & Portales, L. (2018). Influencia del marketing social y prácticas de RSE en la intención de compra de los millennials. *Universidad & Empresa*, *20*(35). https://bit.ly/3h0tsXX

Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, 803–815. https://doi.org/10.1016/j.future.2020.03.021

Sierra, S. (2017). Implementación del marketing social en Colombia. En *Trabajo de grado* (Issue Facultad de Ciencias Empresariales). Editorial Bonaventuriana. https://bit.ly/3Wkjhxx

Swarnalatha K.S., Ramchandra K.C., Ansari, K., Ojha, L., & Sharma, S. S. (2021, diciembre 16). Real-Time Threat Intelligence-Block Phising Attacks. *CSITSS 2021 - 2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solutions, Proceedings*. https://bit.ly/3SYzENg