# El Phishing en Colombia: La Pesca Digital de Datos Confidenciales

**Paula Jiménez García**

**Monitora del CIFD**

El phishing es una de las formas más comunes y peligrosas de ciberataque en la era digital. Derivado del término "pescar" en inglés. Según García (2021) el phishing implica engañar a los usuarios para que divulguen información confidencial, como contraseñas, números de tarjetas de crédito o información personal, a menudo haciéndose pasar por entidades de confianza, como bancos, redes sociales o empresas reconocidas.

Según el gremio representativo del sector financiero colombiano Asobancaria (2019), el phishing es una modalidad de fraude que consiste en el envío masivo de mensajes electrónicos en los que aparece una dirección web falsa o clonada de una entidad bancaria, con el fin de captar información sensible de los usuarios, como, por ejemplo, sus claves de acceso, etc. Este método malicioso se ha vuelto cada vez más sofisticado, con los ciberdelincuentes utilizando técnicas de ingeniería social para manipular a las personas y convencerlas de que proporcionen sus datos personales.

A su vez, según Téllez Valdez (1996), el phishing presenta las características de todo delito informático, 1) es de cuello blanco, porque quien puede cometerlo se reduce a un grupo específico de personas o con conocimientos necesarios, 2) son acciones ocupacionales y oportunistas porque se realizan mientras se está laborando, aprovechándose de una necesidad creada dentro del sistema tecnológico, 3) ofrece posibilidades de tiempo y espacio porque no se necesita una presencia física para consumarse y presenta dificultades para ser probado por su carácter técnico.

Para combatir este tipo de prácticas, nace el “Convenio sobre la ciberdelincuencia” (2001) en Budapest, realizado por un congreso compuesto por aproximadamente 66 países, que busca armonizar la tipificación de los ciberdelitos con el fin de que exista un modelo de penalización semejante en el panorama internacional.

Este convenio establece a los Estados parte la obligación de tomar medidas legislativas que resulten necesarias para tipificar el delito en su derecho interno. Sin embargo, al ser aplicable solo a los países signatarios, si un Estado no adopta el convenio, ni regula la ciberdelincuencia por su cuenta, el delito quedará impune.

En el contexto jurídico colombiano, se promulgó la Ley 1298 de 2018 que aprobó el convenio sobre la ciberdelincuencia y la Ley 1273 de 2009, que se encargó de definir y categorizar los delitos informáticos dentro del Código Penal. Esta legislación estableció nueve categorías según la naturaleza de la infracción. Para los propósitos de este análisis, nos enfocaremos en el artículo 269G del Código Penal, que se refiere a la suplantación de sitios web con el fin de obtener información personal de manera fraudulenta.

Este artículo define el phishing como la suplantación de identidad que tiene por finalidad apropiarse de datos confidenciales de los usuarios. Según Zabala (2017), para que la conducta se tipifique como punible, es necesario que el agente actúe con un objeto ilícito, es decir que la

finalidad de la conducta esté en contra de los postulados legales y afecte un interés. Por otra parte, el sujeto activo tampoco debe estar autorizado ni facultado de ninguna forma para llevar a cabo las acciones descritas en el tipo penal.

Por su parte, el sujeto activo de la conducta es indeterminado, pero se asume que se trata de una persona con un alto nivel de competencia en el manejo de sistemas informáticos y tecnologías de la comunicación. Asimismo, los sujetos pasivos, tal como lo menciona Zabala (2017), usualmente son el usuario, quien termina entregando su información personal y financiera, y la entidad bancaria a la cual han suplantado mediante la falsificación de la página web o el envío de mensaje electrónico fraudulento, entre otros. Son ellos, usuario y entidad, quienes hacen uso de los sistemas que utilizan tecnologías de la información y las comunicaciones, adulteradas por la ciberdelincuencia.

Los verbos rectores del delito son: "el que diseñe, desarrolle, trafique, venda, ejecute, programe, o envié páginas electrónicas, enlaces o ventanas emergentes" (Código Penal [C.PEN.], 2000). Estos comparten el mismo objetivo: recopilar información perteneciente a la víctima, información que no solo causa perjuicio a esta última, sino que también vulnera su derecho a la intimidad.

En cuanto al bien jurídico tutelado, señala García Sánchez (2021), es un delito de simple amenaza o peligro abstracto que busca proteger la información contenida en los sistemas informáticos. En consecuencia, el objeto jurídico vendría a estar representado por la integridad del software que soporta esos sistemas informáticos.

Si bien el phishing en sí mismo no implica un incremento patrimonial directo para el perpetrador, puede llevar a la realización de actividades delictivas adicionales que resulten en un beneficio económico. Por ejemplo, una vez que un atacante ha obtenido información confidencial a través del phishing, puede utilizarla para acceder a cuentas bancarias, realizar compras fraudulentas o realizar transferencias de dinero no autorizadas.

En ese sentido, es importante preguntarnos si existe responsabilidad bancaria frente al tipo penal del artículo 269G del código penal. La Corte Suprema de Justicia (2016) ha indicado que las entidades financieras deben asumir la responsabilidad por la defraudación sufrida por sus usuarios a través de transacciones electrónicas y reparar, en consecuencia, los prejuicios sufridos por estos actos, pues ese riesgo es inherente a la actividad bancaria. Además, se aclara que un banco puede exonerarse si prueba que el fraude ocurrió por culpa del cuentahabiente o que su actuar dio lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos.

De esta manera, como lo menciona Zabala (2017) las personas que prestan servicios relacionados con ciberinformación que pueda estar protegida, serán responsables por su participación en infracciones en la medida en que excedan o sean poco diligentes con las funciones propias del servicio que cada uno presta; y en aquellos casos en que reciban algún beneficio económico atribuible a la comisión del delito de phishing, serán responsables por el mismo.

En conclusión, el impacto del phishing puede ser devastador, puesto que puede resultar en robo de identidad, fraude financiero, pérdida de datos empresariales y daños a la reputación de una organización.

En todo caso, aunque en Colombia no existe un número significativo de condenas relacionadas con el ilícito de phishing a la fecha, tal como este se consagra en el artículo 269G del Código Penal, es crucial que exista una legislación clara y actualizada que establezca las responsabilidades de los infractores, así como las consecuencias legales que enfrentarán a través de la cooperación entre jurisdicciones nacionales e internacionales para combatir eficazmente este tipo de delitos dada su naturaleza transfronteriza.

**Referencias**


Asobancaria. (2019). Saber más ser más. *Programa de educación financiera de los bancos en Colombia.* Phishing. Asobancaria.com. http://www.asobancaria.com/sabermassermas/phishing/

Congreso de la República de Colombia. (20 de Julio de 2000). *Código Penal*. [Ley 599 de 2000]

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia*. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Corte Suprema de Justicia, Sala de Casación Civil. (19 de diciembre de 2016). *Sentencia SC18614-2016* [M.P: Salazar, R.].

García, E. (2021) *Delitos contra el patrimonio económico, el phishing en Colombia, aproximación criminológica*. Universidad Nacional de Colombia. Bogotá D.C.

Peirano, J. (2004). Re*sponsabilidad Extracontractual.* 2° Edición. Bogotá D.C. Temis.

Téllez, J. (1996). *Los delitos informáticos. Situación en México. Informática y Derech*o No. 9, 10, 11.

Zabala, J. (2017). *Responsabilidad bancaria frente al delito de phishing en Colombia*. http://hdl.handle.net/10983/14943