# Inteligencia Artificial para la detección de phishing y prevención del robo de identidad en adultos mayores en Colombia

Kevin Julian Neisa González - 20222020224
Facultad de Ingeniería, Universidad Distrital
Email: kjneisag@udistrital.edu.co

**Resumen**

El phishing se ha consolidado como una de las principales amenazas de ciberseguridad en Colombia, afectando de manera significativa a los adultos mayores debido a su limitada experiencia en el uso de tecnologías digitales. Esta vulnerabilidad ha provocado un aumento de casos de robo de identidad, con consecuencias que incluyen pérdidas económicas, suplantaciones legales y desconfianza hacia los medios digitales. Frente a esta problemática, se propone una investigación orientada al diseño de una solución preventiva basada en inteligencia artificial (IA), enfocada en la protección de adultos mayores en el entorno del hogar. La metodología contempla la identificación de los patrones más frecuentes en ataques de phishing, el diseño y entrenamiento de un modelo de IA capaz de detectar mensajes fraudulentos en correos electrónicos, mensajes de texto y enlaces web, y el desarrollo de un prototipo que genere alertas en tiempo real. Asimismo, se plantea el diseño de una interfaz accesible y amigable, adaptada a las necesidades cognitivas de los adultos mayores, que facilite la interacción con la herramienta. Se espera que esta propuesta contribuya a reducir los riesgos de robo de identidad, fortalecer la confianza digital de los adultos mayores y aportar un enfoque innovador a la ciberseguridad en el ámbito doméstico.

**Palabras Clave -** Phishing, robo de identidad, adultos mayores, ciberseguridad, inteligencia artificial, hogares digitales.

**Abstract**

Phishing has established itself as one of the main cybersecurity threats in Colombia, significantly affecting older adults due to their limited experience using digital technologies. This vulnerability has led to an increase in identity theft cases, with consequences that include financial losses, impersonation, and distrust of digital media. In response to this problem, we propose a research project aimed at designing a preventive solution based on artificial intelligence (AI), focused on protecting older adults in the home environment. The methodology includes identifying the most common patterns in phishing attacks, designing and training an AI model capable of detecting fraudulent messages in emails, text messages, and web links, and developing a prototype that generates real-time alerts. We also propose designing an accessible and user-friendly interface, adapted to the cognitive needs of older adults, to facilitate interaction with the tool. This proposal is expected to contribute to reducing the risks of identity theft, strengthen older adults' digital trust, and provide an innovative approach to cybersecurity in the home environment.

**Keywords -** Phishing, identity theft, older adults, cybersecurity, artificial intelligence, digital homes.

## Introducción

En Colombia, el phishing se ha consolidado como una de las amenazas más relevantes en ciberseguridad, porque los atacantes usan correos, SMS, llamadas y enlaces fraudulentos para suplantar identidades y obtener datos sensibles (contraseñas, números de documento, datos bancarios). Los estudios sobre fraude muestran que este tipo de estafa ha crecido y diversificado sus vectores en los últimos años, afectando con especial gravedad a poblaciones con menor alfabetización digital. [3],[1]

En el ámbito doméstico, los hogares se convierten en el escenario principal donde se produce el robo de identidad por phishing: los atacantes apuntan a cuentas de correo, servicios bancarios en línea y llamadas de "soporte técnico" que inducen a transferencias o a revelar información personal. Estas tácticas explotan la urgencia y la confianza del usuario, y se manifiestan por canales múltiples (email, SMS, robocalls, redes sociales), lo cual evidencia la necesidad de soluciones que operen en tiempo real y de forma integrada. [3],[1]

Los adultos mayores constituyen un grupo especialmente vulnerable en los hogares colombianos por varias razones: brechas en habilidades digitales, impactos del ageismo en el diseño de tecnologías, dependencia de "expertos cálidos" (familiares) para resolver problemas técnicos, y dificultades para interpretar señales lingüísticas o formales de un mensaje fraudulento. Estudios sobre envejecimiento y tecnología muestran la heterogeneidad de este grupo y cómo la falta de interfaces inclusivas y de apoyo accesible incrementa su exposición al fraude. Además, investigaciones centradas en la autenticidad del contenido han identificado indicadores lingüísticos (gramática, sintaxis, tono) que los atacantes descuidan y que, si se enseñan o se automatizan, pueden ayudar a detectar phishing dirigido a personas mayores. [2],[5]

Las consecuencias en los hogares son múltiples: pérdidas económicas directas, suplantación de identidad en trámites familiares, impacto emocional y pérdida de confianza en servicios digitales. Aunque existen medidas tradicionales de higiene digital (contraseñas fuertes, MFA, antivirus), el dinamismo del phishing exige soluciones adaptativas. En este contexto, la Inteligencia Artificial (IA) presenta una alternativa prometedora: modelos de procesamiento de lenguaje natural y clasificación que identifiquen patrones de phishing en mensajes y enlaces, y que, al mismo tiempo, requieran un diseño inclusivo para no dejar fuera a poblaciones vulnerables. Sin embargo, el desarrollo de sistemas basados en IA debe atender riesgos de sesgo en los datos y a la necesidad de interfaces accesibles para adultos mayores. [1],[4],[5]

Por todo lo anterior, surge la necesidad de investigar y diseñar herramientas basadas en IA que estén orientadas al entorno doméstico y pensadas específicamente para adultos mayores en Colombia, con el objetivo de prevenir el robo de identidad por phishing y mejorar la confianza de este grupo en el uso de servicios digitales desde sus hogares. Esta investigación debe integrar hallazgos sobre diseño inclusivo, rasgos lingüísticos de mensajes fraudulentos y buenas prácticas de implementación de IA para poblaciones vulnerables. [1],[2],[3],[4],[5]

**Metodología**

La investigación se centra en analizar cómo la inteligencia artificial puede emplearse para la detección de phishing y la prevención del robo de identidad en adultos mayores en Colombia. La pregunta de investigación fue: *"¿Cómo se aplican las técnicas de inteligencia artificial para identificar ataques de phishing y proteger a los adultos mayores en entornos domésticos?"*.

Para responderla, se realizó un estudio comparativo de cinco artículos recientes y relevantes en el área [6],[7],[1],[4],[3]. Esta comparación permitió identificar las metodologías, técnicas, datos y herramientas utilizadas en cada investigación, con el fin de sintetizar buenas prácticas aplicables al contexto colombiano y a la población de adultos mayores.

Se recopilaron datos secundarios, provenientes de revisiones sistemáticas, análisis estadísticos, desarrollos de plataformas de IA y revisiones documentales descriptivas. El proceso de recolección consistió en:

1. Identificación de objetivos y enfoques de cada estudio, destacando si eran técnicos, socioeducativos o aplicados [6],[7],[1],[4],[3].
2. Extracción de metodologías y técnicas de IA, incluyendo machine learning (ML), deep learning (DL), procesamiento de lenguaje natural (NLP), agentes inteligentes y frameworks de chatbots IA [6], [4], [7].
3. Clasificación de los tipos de datos utilizados, como datasets de phishing, reportes institucionales, literatura académica y datos de interacción con usuarios [1][4][3].
4. Evaluación de métricas de desempeño, incluyendo accuracy, F1-score, recall y precisión, para comparar la efectividad de los modelos de IA en la detección de phishing [6], [4].
5. Síntesis de resultados y observaciones clave, para extraer buenas prácticas y limitaciones de cada enfoque, y definir recomendaciones adaptadas al diseño de soluciones inclusivas para adultos mayores [1], [3].

Los instrumentos y herramientas considerados incluyeron: datasets públicos de phishing, entornos de desarrollo y despliegue de IA como LLaMA, Docker y Ollama, así como software estadístico para análisis comparativo de desempeño. El análisis se realizó mediante síntesis cualitativa para categorizar enfoques, objetivos y técnicas, y análisis cuantitativo basado en métricas reportadas para comparar la efectividad de los modelos de IA.

Esta metodología permite que otros investigadores repliquen el estudio, evaluando la eficacia de distintas técnicas de IA en la detección de phishing y la prevención de robo de identidad, y adaptando estrategias inclusivas para adultos mayores en entornos domésticos en Colombia.

**Referencias**


[1] P. Tummala, H. Choi, A. Gupta, T. A. Lapnas, Y. S. Chung, M. Peterson, G. Walther y H. Purohit, “Design Challenges for Scam Prevention Tools to Protect Neurodiverse and Older Adult Populations,” en *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 2024. DOI: 10.1109/TPS-ISA62245.2024.00058.

[2] K. T. Nguyen, “Ageism and Its Impact on Information and Communications Technology Usage and Design,” en *2022 IEEE Global Humanitarian Technology Conference (GHTC)*, 2022. DOI: 10.1109/GHTC55712.2022.9911051.

[3] N. Sugunaraj, A. R. Ramchandra y P. Ranganathan, “Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review,” en *2022 IEEE International Conference on Electro Information Technology (eIT)*, 2022. DOI: 10.1109/eIT53891.2022.9813960.

[4] M. S. Sayeed, H. Tamut e I. K. Dutta, “ElderConnect: An AI-Powered Platform to Empower Seniors Against Cyberthreats,” en *2025 IEEE World AI IoT Congress (AIIoT)*, 2025. DOI: 10.1109/AIIoT65859.2025.11105307.

[5] P. Sannd y D. M. Cook, “Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks,” en *2018 Fourteenth International Conference on Information Processing (ICINPRO)*, déc. 2018. DOI: 10.1109/ICINPRO43533.2018.9096878.

[6] Murugun S, Sheikh Haniah, Shambhavi M Koti, et al., “A Review on Phishing Threats and Data Security in Online Trading Systems using Artificial Intelligence Techniques,” *2024 Second International Conference on Advances in Information Technology (ICAIT-2024)*, IEEE, 2024. DOI: 10.1109/ICAIT61638.2024.10690690.

[7]Statistical Prospects of AI in Tackling Cyber Crimes, Revisión bibliográfica + análisis estadístico, 2022.