

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

Kevin Julian neisa Gonzalez – 20222020224

En Colombia, el phishing se ha convertido en una de las principales amenazas de ciberseguridad. Este ataque busca engañar a las personas, a través de correos, llamadas o mensajes falsos, para obtener información privada como contraseñas, números de documentos o datos bancarios.

Uno de los grupos más afectados son los adultos mayores, quienes, por la falta de experiencia con la tecnología, tienen más dificultad para reconocer cuándo se trata de un fraude. Esto ha generado un aumento de casos de robo de identidad, lo que trae consecuencias como pérdidas económicas, suplantaciones y desconfianza hacia los medios digitales.

Aunque existen campañas de educación y medidas de seguridad, el phishing sigue creciendo y adaptándose. Por eso, es necesario pensar en nuevas estrategias. Aquí surge la Inteligencia Artificial (IA) como una opción viable, ya que con técnicas como el procesamiento de lenguaje natural y el aprendizaje automático se pueden crear sistemas que analicen mensajes en tiempo real, detecten fraudes y alerten al usuario de manera clara.

De esta forma, se busca investigar cómo aplicar la IA en herramientas de prevención de phishing para adultos mayores en Colombia, con el fin de protegerlos en sus hogares y darles mayor confianza en el uso de la tecnología.

Pregunta Problema

¿Cómo prevenir el robo de identidad por phishing en adultos mayores en Colombia mediante el uso de inteligencia artificial en los hogares?

Objetivo General

- Analizar cómo el phishing provoca el robo de identidad en adultos mayores en Colombia y desarrollar una propuesta de solución preventiva basada en inteligencia artificial que pueda implementarse en los hogares.

Objetivos Específicos

1. Identificar los patrones más comunes en ataques de phishing dirigidos a adultos mayores en Colombia.
2. Entrenar un modelo de inteligencia artificial capaz de detectar intentos de phishing en correos, mensajes de texto o enlaces web.
3. Implementar un prototipo de sistema basado en IA que alerte en tiempo real a los adultos mayores sobre posibles intentos de phishing.
4. Evaluar la efectividad del prototipo mediante pruebas en escenarios simulados de uso en el hogar.
5. Proponer un diseño de interfaz amigable que permita a los adultos mayores interactuar fácilmente con la herramienta de IA.

Resultados Esperados

1. Identificar claramente cómo funciona el phishing en Colombia y qué tanto afecta a los adultos mayores, mostrando ejemplos reales de los engaños más comunes (correos falsos, mensajes de texto, llamadas, etc.).
2. Recolectar y analizar datos que permitan entrenar un modelo de inteligencia artificial capaz de detectar señales típicas de phishing, como lenguaje sospechoso o enlaces maliciosos.
3. Diseñar un prototipo básico de IA que pueda funcionar como filtro o asistente digital, alertando al usuario cuando detecte un posible intento de robo de identidad.
4. Probar el prototipo en un entorno controlado, midiendo qué tan bien identifica los intentos de phishing y qué tan fácil resulta para un adulto mayor usarlo.
5. Proponer una interfaz sencilla y accesible, pensada especialmente para adultos mayores, que muestre advertencias claras sin necesidad de conocimientos técnicos avanzados.
6. Plantear recomendaciones finales sobre cómo se podría aplicar esta solución en los hogares, integrándola a correos electrónicos, navegadores o aplicaciones de mensajería.