

SAFESOCIAL: DETECTOR INTELIGENTE DE RIESGOS EN REDES SOCIALES PARA ADOLESCENTES

RESUMEN DEL PROYECTO

El uso de redes sociales entre adolescentes ha crecido de forma exponencial en los últimos años. Sin embargo, muchos jóvenes comparten información personal sin ser conscientes de los riesgos que esto implica. Este proyecto propone el desarrollo de una herramienta educativa capaz de analizar textos e imágenes de perfiles de redes sociales para detectar posibles riesgos de privacidad y seguridad. El sistema identifica elementos sensibles como números de teléfono, ubicaciones exactas o documentos visibles en imágenes, generando un nivel de riesgo y recomendaciones personalizadas para mejorar la seguridad digital del usuario. El objetivo principal es fomentar una mayor conciencia sobre la privacidad en Internet.

INTRODUCCIÓN

Las redes sociales forman parte fundamental de la vida cotidiana de los adolescentes. Plataformas como Instagram, TikTok o Snapchat se utilizan para compartir experiencias, imágenes y opiniones. Sin embargo, este intercambio constante de información puede suponer riesgos importantes si se comparten datos personales sensibles. Entre estos riesgos se encuentran la exposición de direcciones, números de teléfono o información académica que puede ser utilizada por terceros con fines maliciosos. Este proyecto surge con el objetivo de ayudar a los estudiantes a comprender los riesgos asociados a la exposición de información personal en redes sociales mediante el desarrollo de una herramienta de análisis automatizado.

PROPÓSITO DEL TRABAJO

El propósito de este trabajo es diseñar y desarrollar una herramienta informática que permita analizar perfiles o publicaciones de redes sociales para identificar posibles riesgos de seguridad y privacidad. El sistema generará alertas y recomendaciones adaptadas al usuario, permitiéndole comprender qué tipo de información puede resultar peligrosa si se comparte públicamente. De esta manera, el proyecto pretende contribuir a mejorar la educación en ciberseguridad entre adolescentes y fomentar hábitos digitales más seguros.

ESTADO DEL ARTE

En los últimos años han surgido diferentes herramientas relacionadas con la privacidad digital y el análisis de datos en redes sociales. Algunas plataformas de ciberseguridad ofrecen sistemas de detección de fraudes o de contenido peligroso mediante técnicas de inteligencia artificial. Asimismo, investigaciones recientes en el campo del procesamiento del lenguaje natural (NLP) y visión artificial han permitido detectar información sensible en textos e imágenes de forma automatizada.

No obstante, la mayoría de estas herramientas están orientadas a empresas o profesionales de la seguridad informática. Existen pocas soluciones específicamente diseñadas para el ámbito educativo y para adolescentes. Por ello, este proyecto propone una herramienta sencilla y accesible que permita a los estudiantes analizar su propia actividad en redes sociales y comprender los riesgos asociados a la publicación de determinados datos personales.

HIPÓTESIS

Si se desarrolla una herramienta capaz de analizar automáticamente textos e imágenes publicados en redes sociales y detectar información personal sensible, entonces los adolescentes podrán identificar de forma más clara los riesgos asociados a sus publicaciones y modificar su comportamiento digital para proteger mejor su privacidad.

MATERIAL Y MÉTODOS (DESARROLLO TÉCNICO PASO A PASO)

Paso 1. Definir qué riesgos se quieren detectar

Paso 2. Diseñar la arquitectura del sistema

Paso 3. Crear la interfaz de usuario

Paso 4. Análisis de texto con NLP

Paso 5. Análisis de imágenes

Paso 6. Detección de objetos sensibles en imágenes

Paso 7. Sistema de puntuación de riesgo

Paso 8. Generar recomendaciones

Paso 9. Crear el informe final

Paso 10. Pruebas

RESULTADOS

Tras las pruebas realizadas, el sistema fue capaz de identificar diferentes tipos de información sensible en textos e imágenes compartidas. La herramienta detectó correctamente números de teléfono, direcciones de correo electrónico y referencias a ubicaciones específicas. Además, el análisis de imágenes permitió identificar texto visible en capturas de pantalla mediante técnicas de reconocimiento óptico de caracteres.

CONCLUSIONES

La herramienta permite a los adolescentes comprender de forma práctica qué tipo de información personal puede resultar peligrosa cuando se comparte públicamente. Este tipo de soluciones puede contribuir significativamente a mejorar la educación en ciberseguridad y fomentar un uso más responsable de las redes sociales.

