Resumen

Este estudio tuvo como objetivo diseñar e implementar un modelo de precisión para detectar y mitigar ataques Phishing en correos electrónicos, utilizando técnicas de minería de datos. Como primer paso, se realizó una investigación bibliográfica sobre las técnicas, métodos y herramientas actuales de minería de datos empleados en la detección de Phishing. Luego se identificaron las características de correos infectados que hacen que el ataque de Phishing sea exitoso. Para ello, se realizó un análisis de diferentes correos con Phishing de tres importantes fuentes tales como: www.monkey.org, www.enron.org y www.PhishTank.com , los mismos que permitieron la generación de un dataset. Para el diseño e implementación del modelo, se empleó la metodología CRISP-DM. Con ello se generó el modelo de detección, en base a las características que reconocen a un correo como Phishing. Dentro del proceso de minería de datos se desarrolló un análisis predictivo de datos que consistió en la extracción de información existente y su utilización para predecir tendencias y patrones de comportamiento. Así mismo, se desarrolló un análisis descriptivo utilizando algoritmos de minería de datos siendo Random Forest la de mayor precisión. Por último, instalando la librería Twilio en Python, se implementó el despliegue de un mensaje a WhatsApp al detectar un correo con Phishing, motivo por el que se otorga mayor validez a la investigación realizada. En último lugar, se evaluó el modelo, mediante pruebas de concepto en un ambiente controlado, cuyos resultados muestran la funcionalidad del modelo, puesto que alcanzó un grado de precisión superior al 97% en la detección de correos infectados con Phishing.

KEYWORDS:

- **MINERÍA DE DATOS**
- **PHISHING**
- **ATAQUES DE INGENIERÍA SOCIAL**
- **CIBERSEGURIDAD**

Abstract

This study aimed to design and implement a precision model to detect and mitigate phishing attacks in emails, using data mining techniques. A literature review was conducted on current data mining techniques, methods, and tools used in Phishing detection as a first step. Then, the characteristics of infected emails that make a phishing attack successful were identified. To do this, an analysis was carried out of various phishing emails from three important sources: www.monkey.org, www.enron.org, and www.PhishTank.com, which allowed the generation of a dataset. The CRISP-DM methodology was used to design and implement the model. This generated the detection model, based on the characteristics that recognize an email as Phishing. A predictive data analysis was developed within the data mining process, which consisted of the extraction of existing information and its use to predict trends and behavior patterns. Likewise, a descriptive analysis using data mining algorithms was developed, being Random Forest the most accurate. Finally, by installing the Twilio library in Python, a message was displayed to WhatsApp when a phishing mail was detected, which is why the research was given more validity. Finally, the model was evaluated through proofs of concept in a controlled environment, the results of which show the functionality of the model, as it achieved a degree of accuracy greater than 97% in detecting phishing emails.

KEYWORDS:

- **DATA MAINING**
- **PHISHING**
- **SOCIAL ENGINEERING ATTACKS**
- **CYBER SECURITY**