<u>Abstract</u>
In recent years, phishing attacks have persisted as a widespread threat in the contemporary digital environment, presenting substantial risks to individuals and organizations. Cybercriminals are devising increasingly sophisticated strategies to deceive users through malicious emails. In response to this challenge, this research focuses on developing a new tool for detecting phishing emails utilizing the BERT algorithm. The tool aims to enhance email security by accurately identifying deceptive emails and protecting users from potential cyber threats. The primary objective of this study is to investigate how leveraging the BERT algorithm can improve the detection of phishing emails compared to traditional methods. The methodology involves fine-tuning the pre-trained BERT model on a dataset comprising both legitimate and phishing emails to learn patterns and characteristics of phishing attempts. The study evaluates the effectiveness of the BERT-based detection tool through various experiments and performance assessments. The results indicate that the BERT algorithm achieves an accuracy of 98% in identifying phishing emails, demonstrating its potential to enhance email security measures significantly. The significant contributions of this research lie in developing an advanced tool for combating phishing attacks, thereby mitigating risks associated with cyber threats. Additionally, this study fills a crucial gap in current email security measures by harnessing the power of state-of-the-art natural language processing techniques for phishing detection. By delivering valuable insights into the effectiveness of the BERT-based approach in safeguarding users against phishing attacks, this research contributes to creating a safer and more secure online environment.

Keywords: Phishing emails, BERT algorithm, Natural language processing, Cybersecurity, Email security