World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:18, No:05, 2024

Enhancing Email Security: A Multi-Layered Defense Strategy Approach and an AI-Powered Model for Identifying and Mitigating Phishing Attacks

Authors : Anastasios Papathanasiou, George Liontos, Athanasios Katsouras, Vasiliki Liagkou, Euripides Glavas

Abstract : Email remains a crucial communication tool due to its efficiency, accessibility and cost-effectiveness, enabling rapid information exchange across global networks. However, the global adoption of email has also made it a prime target for cyber threats, including phishing, malware and Business Email Compromise (BEC) attacks, which exploit its integral role in personal and professional realms in order to perform fraud and data breaches. To combat these threats, this research advocates for a multi-layered defense strategy incorporating advanced technological tools such as anti-spam and anti-malware software, machine learning algorithms and authentication protocols. Moreover, we developed an artificial intelligence model specifically designed to analyze email headers and assess their security status. This AI-driven model examines various components of email headers, such as "From" addresses, 'Received' paths and the integrity of SPF, DKIM and DMARC records. Upon analysis, it generates comprehensive reports that indicate whether an email is likely to be malicious or benign. This capability empowers users to identify potentially dangerous emails promptly, enhancing their ability to avoid phishing attacks, malware infections and other cyber threats.

Keywords : email security, artificial intelligence, header analysis, threat detection, phishing, DMARC, DKIM, SPF, ai model
Conference Title : ICCCC 2024 : International Conference on Cybersecurity, Cybercrime and Cyberthreats
Conference Location : Montreal, Canada
Conference Dates : May 23-24, 2024