COMBAT PHISHING ATTACKS WITH MACHINE LEARNING

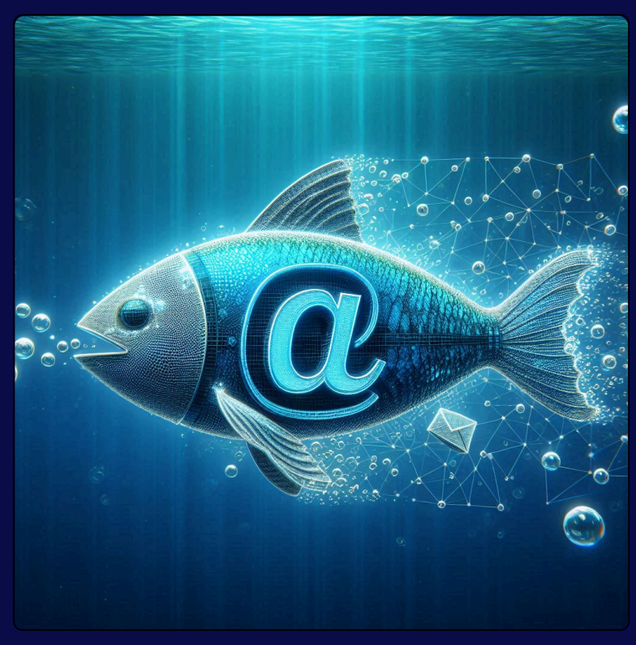
PHISHING ATTACKS: THE DIGITAL THREAT

Phishing attacks trick individuals into revealing sensitive information by masquerading as trustworthy entities. They are a significant threat to cybersecurity, targeting both individuals and organizations.

Approximately 3.4 billion phishing emails are sent each day. Phishing attacks are a major cause of data breaches and cyberattacks, growing in number every day. Automated tools using AI and machine learning are essential to analyze and prevent these threats. Our project focuses on using these advanced techniques to detect phishing emails, aiming to improve security and raise awareness about the dangers of phishing attacks.

90%
OF DATA BREACHES BEGIN WITH PHISHING

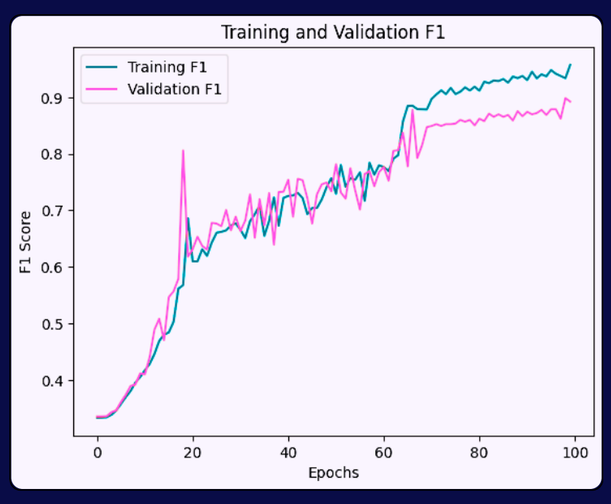
$27.6 BILLION LOSS
(OVER LAST 5 YEARS)



"Specifically, CNN reached an overall accuracy of 99.98% and an F1 score of 97.86% on the training set, with validation accuracy peaking at 99.00% and validation F1 scores reaching 89.85%."

"CNN model showcased competitive performance."

"In comparing our CNN model with traditional machine learning algorithms, we observe that the CNN model outperforms them in both accuracy and F1-score."



PROTECT YOURSELF WITH 99.06% ACCURACY

The main problem we're trying to solve in this project is accurately identifying phishing emails from legitimate ones using the textual data of the emails. Traditional rule-based detection systems often can't keep up with the constantly changing tactics of phishers. Phishing emails can look very different from one another, making them difficult to catch with static rules. This is why we need advanced machine learning (ML) as well as deep learning methods that can adapt to new phishing strategies and provide reliable detection.

We believe that using CNNs along with traditional machine learning methods (e.g SVM, KNN, MNB, RF, LR), will make phishing email detection systems more accurate and reliable. CNNs can recognize patterns in text, which will help traditional models catch more advanced phishing emails. By combining different models, we may be able to balance out their weaknesses, making a better detection system.

This project has the potential to really change email security by providing a reliable, automated way to detect phishing attempts. With further development and real-world testing, these models could become a crucial tool in protecting email users and cutting down on phishing attacks.

LEARN MORE AT
odd509.github.io/phishing-detection-website/

Mr. Fresh Bro, 2024