Literacy Reviews

Survey Papers

A Systematic Review on Deep-Learning-Based Phishing Email Detection

This review covers dozens of papers from 2017 to 2023 and compares their methods' advantages and limitations.

However, since their performances are all very high, and they used different datasets, it's impossible to say one method is better than another.

So, we may only use this paper as a reference, an index of methods we might look at later on.

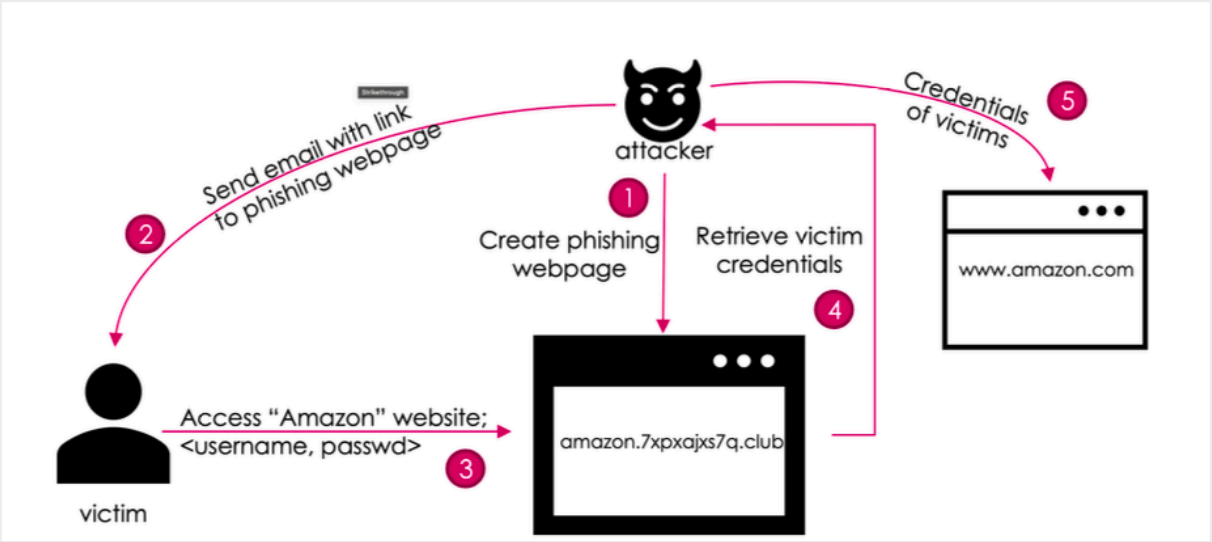
Limitations

One of the significant limitations is the lack of focus on privacy preservation in the proposed models. While the models aim to detect phishing emails, they may also reveal sensitive user information. Therefore, future research should focus on preserving user privacy in phishing detection models.

Another limitation is the misclassification of phishing emails, which indicates that the models are not yet accurate enough. The models may incorrectly classify legitimate emails as phishing emails, or vice versa. This can lead to false positives and negatives, which can harm user trust in the models. Therefore, researchers need to address this limitation by improving the accuracy of the models.

Moreover, the studies focus only on analyzing the email structure and do not consider other factors, such as the sender's reputation and behavior. Therefore, researchers need to explore how to incorporate additional email features.

Phishing Detection Leveraging Machine Learning and Deep Learning: A Review



This paper focused on phishing URLs and webpages instead of email body text.

Table 1: Taxonomy of phishing detection solutions based on learning models

#	Data	Model	Advantage	Disadvantage
1	URL strings	ML-based model with features engineered from URL strings	Fast, no network latency involved.	Limited information in URLs. Manual engineering of features.
2	URL strings	DL-based, with URL strings provided as input to the neural network	Fast, no network latency involved. No feature engineering required.	Limited information in URLs.
3	Webpage contents	ML-based, with features engineered from HTML body (in addition to the URL) of the webpage	Contents provide rich information for models to learn and differentiate between benign and phishing webpages.	Network latency in obtaining the page contents, and expensive feature extraction for real-time detection. Susceptible to evasion techniques.
4	Webpage screenshot	DL models to compare webpage screenshots and visual invariants such as logos	Not dependent on large labeled (benign and phishing) datasets. Instead, only a small reference list of top targeted websites needs to be maintained.	Cost of network latency to fully load a webpage and take a screenshot. Prone to adversarial ML attacks.

Research Papers

Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features

A new dataset of 500 phishing and 500 legitimate websites was created, featuring URL, HTML, and HTTP attributes. These features were fed into various classifiers including k-NN, SVM, Naive Bayes, decision tree, multi-layer perceptron, and stochastic gradient descent. Performance was measured using accuracy,

precision, recall, F1-score, and classification time.

The choice of the meta information-driven URL, HTML, and HTTP features instead of the actual content of a website was mainly influenced by practical, technical, and ethical considerations. Scalability and speed, the adversarial nature of phishing attacks, privacy concerns, generalization across languages and cultures, and interpretability of features were among the main reasons behind this choice.

Analyzing the content of websites can be computationally expensive and time-consuming, especially when considering language complexity and typos. Phishing detection systems need to operate in real-time to effectively prevent users from accessing malicious sites. Therefore, utilizing meta information allows for faster processing and scalability.

URL and HTTP-based features performed best.