**Literature Survey**

Phishing attacks target vulnerabilities that

exist in systems due to the human factor. Many cyber attacks

are spread via mechanisms that exploit weaknesses found in end-

users, which makes users the weakest element in the security

chain. The phishing problem is broad and no single silver-bullet

solution exists to mitigate all the vulnerabilities effectively, thus

multiple techniques are often implemented to mitigate speciﬁc

attacks. This paper aims at surveying many of the recently

proposed phishing mitigation techniques. A high-level overview

of various categories of phishing mitigation techniques is also

presented, such as: detection, offensive defense, correction, and

prevention, which we belief is critical to present where the

phishing detection techniques ﬁt in the overall mitigation process.

Index Terms—phishing; social engineering; phishing detection;

security; email classiﬁcation

Phishing attacks target vulnerabilities that

exist in systems due to the human factor. Many cyber attacks

are spread via mechanisms that exploit weaknesses found in end-

users, which makes users the weakest element in the security

chain. The phishing problem is broad and no single silver-bullet

solution exists to mitigate all the vulnerabilities effectively, thus

multiple techniques are often implemented to mitigate speciﬁc

attacks. This paper aims at surveying many of the recently

proposed phishing mitigation techniques. A high-level overview

of various categories of phishing mitigation techniques is also

presented, such as: detection, offensive defense, correction, and

prevention, which we belief is critical to present where the

phishing detection techniques ﬁt in the overall mitigation process.

Index Terms—phishing; social engineering; phishing detection;

security; email classiﬁcation

Phishing attacks target vulnerabilities that

exist in systems due to the human factor. Many cyber attacks

are spread via mechanisms that exploit weaknesses found in end-

users, which makes users the weakest element in the security

chain. The phishing problem is broad and no single silver-bullet

solution exists to mitigate all the vulnerabilities effectively, thus

multiple techniques are often implemented to mitigate speciﬁc

attacks. This paper aims at surveying many of the recently

proposed phishing mitigation techniques. A high-level overview

of various categories of phishing mitigation techniques is also

presented, such as: detection, offensive defense, correction, and

prevention, which we belief is critical to present where the

phishing detection techniques ﬁt in the overall mitigation process.

|  |  |  |
| --- | --- | --- |
| **Title** | **Author Name** | **Objective** |
| classification Decision Tree, Random Forest and Support Vector Machine | Rishikesh Mahajan  And  Irfan Siddavatam | Their dataset contained 17,058 benign URLs and 19,653 phishing URLs collected from Alexa website and PhishTank respectively, with 16 features each. |
| Machine- learning based phishing detection system by using 8 different algorithms on three different datasets | Mehmet Korkmaz | Artificial Neural Network (ANN). It was observed that the models using LR, SVM and NB have low accuracy rate. In terms of training time, NB, DT, LR and ANN algorithms gave better results. |
| Intelligent phishing detection system using UCI dataset | Abdulhamit Subasi | Different machine learning tools namely, Artificial Neural Networks (ANN), K-Nearest Neighbor (K-NN), Support Vector Machine (SVM), C4.5 Decision Tree, Random Forest (RF), and Rotation Forest (RoF) were used as classifiers for detection of phishing websites. The performance of proposed RF classifier was higher than others. |

Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

phishing attacks aim at exploiting weaknesses found

in humans (i.e. system end-users), it is difﬁcult to mitigate

them. For example, as evaluated in [1], end-users failed

to detect 29% of phishing attacks even when trained with

the best performing user awareness program. On the other

hand, software phishing detection techniques are evaluated

against bulk phishing attacks, which makes their performance

practically unknown with regards to targeted forms of phishing

attacks. These limitations in phishing mitigation techniques

have practically resulted in security breaches against several

organizations including leading information security providers

Phishing attacks aim at exploiting weaknesses found in humans (i.e. system end-users), it is difficult to mitigate them. For example, as evaluated in [1], end-users failed to detect 29% of phishing attacks even when trained with the best performing user awareness program. On the other hand, software phishing detection techniques are evaluated against bulk phishing attacks, which makes their performance practically unknown with regards to targeted forms of phishing attacks.