Abstract

In recent years, we have witnessed a dramatic raise in the use of web and thus email becomes an inevitable mode of communication. This is the scenario where the attackers take advantage by the mode of spam mails to the email users and misguide them to some phished sites or the users unwittingly install some malwares to their machine. This shows the importance of research activities being carried out in the field of spam mail detection. In this paper we tend to project a replacement methodology to segregate spam emails from non-spam (legitimate) emails using the distinct structural features available in them. The experiments with 8000 emails show that that our methodology preserves an accuracy of the spam detection up to 99.4% with at the most 0.6% false positives.

References

- S. Abu-Nimeh, D. Nappa, X Wang, S. Nair, &quot;A comparison of machine learning techniques for phishing detection.&quot; In Proceedings of the anti-phishing working groups
Spam Email Detection using Structural Features

- X. Carreras, L. Marquez and J. G Salgado, "Boosting trees for anti spam filtering.," In International conference on Recent Advances in Natural Language Processing, 2001, pp. 58-64.

Index Terms

Computer Science

Security
Keywords
Spam Detection; Structural Feature Selection; spam classification; Machine learning application.