**Abstract**

Presently phishing, spoofing and fraudulent emails attacks have become too common at such level that it stands difficult to differentiate an attack from a legitimate or genuine mail. 96% of these attacks are done using emails. The individuals and organizations face an average of global losses to cybercrime total $1.5 trillion per year. These attacks can be done internally within an organization or specifically targeting an individual across the globe. The attackers have a tendency to attack the weakest link of all, among potential victims. In this paper we propose a mechanism to find relevancy between two email users based on exchange of emails between them.

**Introduction**

The individuals or organizations face an average of [1] global losses to cybercrime total $1.5 trillion per year, which amounts to $2.9 million per minute, a new report by RiskIQ shows. Some of the largest companies are losing $25 each minute due to security breaches. Phishing campaigns accounts for losses of $17,700 per minute and ransomware attacks are expected to cost the world $22,184 per minute this year.

**Links**

[1] <https://blog.knowbe4.com/this-year-phishing-causes-losses-of-17700-per-minute-and-ransomware-attacks-will-cost-22184-per-minute>