

## Task 1 Report

### GAMK

Our phishing detection program works to protect users from malicious emails by providing a score on the likelihood that an email is a phishing attack. While no tool can perfectly protect against phishing, the score produced by our system will help users be aware of some of the attempts to make them fall victim to these attacks.

The phishing detection system evaluates both the subject of an email and the body for signs of phishing. Using our knowledge of typical phishing attacks we determined keywords that are often used to try to trick users. Our system detects words such as “urgent”, “soon”, “expire”, and “immediately” as keywords that are often used to trick users into feeling the need to act quickly and cause them to not carefully consider the phishing message. We next look at keywords such as “offer” and “redeem” to detect against phishing scams of claims that the user had won a fake prize. We also increase our likelihood score for emails containing the keywords “unusual” and “activity” as these words can help protect against phishing attacks that attempt to steal information by making you fear your account has already been compromised. Additionally, we increase our phishing score for the keyword “bank” as bank related emails should have closer examination by users as bank related phishing attacks can have among the most devastating attacks. The more instances of these keywords the higher our phishing score increases. Our system also detects phishing URLs, such as those that replace letters with numbers to try and trick users to visiting their phishing website.

Our system is a prototype with the goal of showing investors that we have the capability to build such a system. If we were to obtain SEED money to continue to build this system there are many improvements and features we could add. One improvement would be to identify phishing phrases rather than single words. We could automatically check URLs through a service such as Google's phishing detection service or build our own website phishing detection system. We could use machine learning algorithms to detect phishing emails by training a neural network or other machine learning algorithm with examples of phishing emails using a supervised learning technique.