# The Psychological Factors Behind Phishing Attacks

Mark Doyle
C00257481@setu.ie

## Introduction

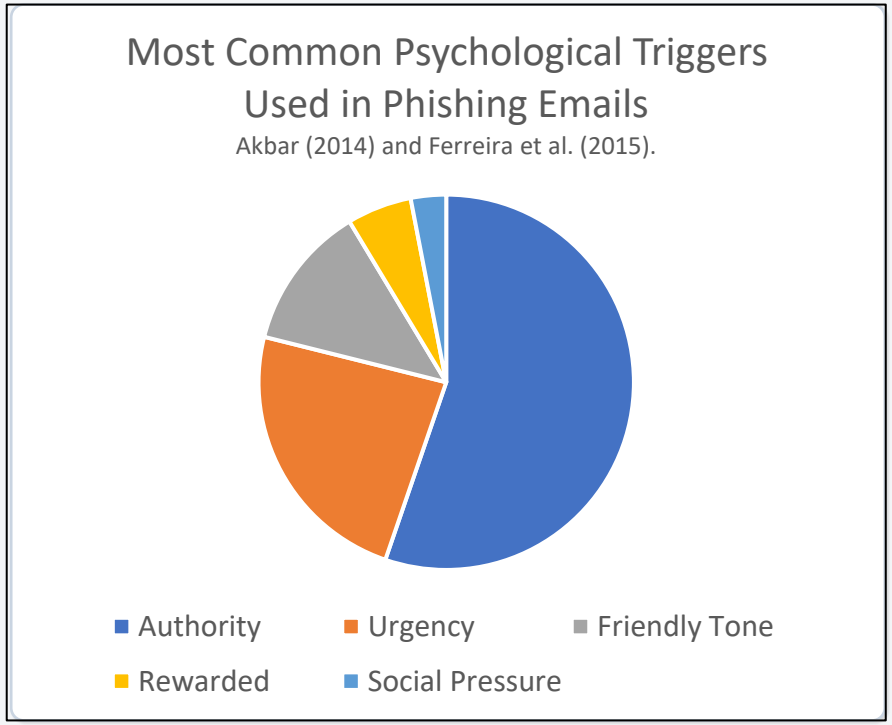
- Phishing continues to be a major threat to cybersecurity
- Attackers manipulate their targets into believing that their message can be trusted
- Generative AI makes phishing messages more tailored and convincing to the target

## Research Questions

- What factors influence a phishing interaction?
- Does the use of AI increase the rate of phishing interactions
- Do users detect AI generated phishing less often than non-AI generated phishing?

## Research Gap

- Limited research on how users respond to realistic AI-generated phishing messages
- Fewer studies examine a user's confidence and decision making and their detection accuracy
- More human centered research is needed to understand why phishing succeeds




## Methodology

- Interview a mixed demographic group of participants
- Present them with legitimate, traditional, and AI generated phishing emails
- Measure detection accuracy, confidence and reasons for each decision
- Compare responses across different phishing scenarios

## Background

- Phishing messages often use the same factors to influence users
- These factors are designed to encourage quick decisions without careful thinking
- Generative AI makes phishing messages look more convincing and tailored to its target

## Literature Review

- Previous research shows that phishing relies on persuasion and social engineering
- Studies have highlighted the increased use of AI generated of phishing
- Recent papers focus more on detection systems rather that user behavior

## Expected Results

- The most common psychological triggers linked to a successful phishing attack
- Explore if AI generated phishing changes how users judge a phishing attempt