



SOCIAL ENGINEERING ATTACKS AND MITIGATION STRATEGIES

James Beard (1901671) BSc Computer Networks and Cybersecurity

Email: jamesadbeard90@gmail.com

1. Introduction

Social Engineering is one of the most common threats in cybersecurity[1]–[3]. This attack focuses on and exploits human vulnerabilities instead of vulnerabilities in the software and infrastructure of a network [3]. This poster discusses the research and experiments conducted showcasing why ignoring social engineering is detrimental to online security.

2. Social Engineering Facts

- **Phishing** – An email that impersonates an entity to persuade the receiver to perform a detrimental action [4].
- **83%** of businesses compromised in 2021-22 were breached by phishing attacks [5].
- **94%** for medium to large businesses [5].
- A rise of **11%** from **72%** in 2017 [5].
- **97%** of malicious codes gained entry through Social engineering [6].
- An organisation can be targeted by over **700** social engineering attacks in a year [7].
- Phishing was responsible for **\$12 billion** in losses and **90%** of data breaches in 2019 [8].

References

- [1] Z. Wang, H. Zhu, and L. Sun, 'Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods', *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
- [2] C. Hadnagy, 'A Look into the New World of Professional Social Engineering', in *Social Engineering: The Science of Human Hacking*, 2nd ed., Indianapolis, Indiana: Wiley Publishing, Inc, 2018, pp. 9–10.
- [3] F. Salahdine and N. Kaabouch, 'Social Engineering Attacks: A Survey', *Future Internet*, vol. 11, no. 4, Art. no. 4, Apr. 2019, doi: 10.3390/fi11040089.
- [4] S.-P. Oriano, 'social Engineering', in *CEHV9 Certified Ethical Hacker version 9, Version 9.*, Sybex, 2016, pp. 616–617.
- [5] 'Cyber Security Breaches Survey 2022', *GOV.UK*, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022> (accessed Apr. 16, 2022).
- [6] H. Aldawood and G. Skinner, 'Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions', *IEEE Access*, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280.
- [7] Barracuda, 'Spear Phishing: Top Threats and Trends', *Barracuda • INSIGHTS INTO ATTACKERS' EVOLVING TACTICS AND WHO THEY'RE TARGETING*, vol. 6, p. 1=17, Jul. 2021.
- [8] Deloitte, 'Understanding phishing techniques'. Cyber101, Dec. 2019.
- [9] 'Mother's Day Gift Guide 2020 | Hollywood Jackets', *Hollywood Jackets Blog*, Apr. 30, 2020. <https://www.hjackets.com/blog/mothers-day-gifts-guide/> (accessed Apr. 17, 2022).

3. Experiment

These experiments were conducted on fifty consenting volunteers to test the hypothesis that urgency would be a better technique than reward. The two experiments were conducted using the Social Engineer-Toolkit with a custom Import to create an experiment that would only harvest email addresses and not passwords.

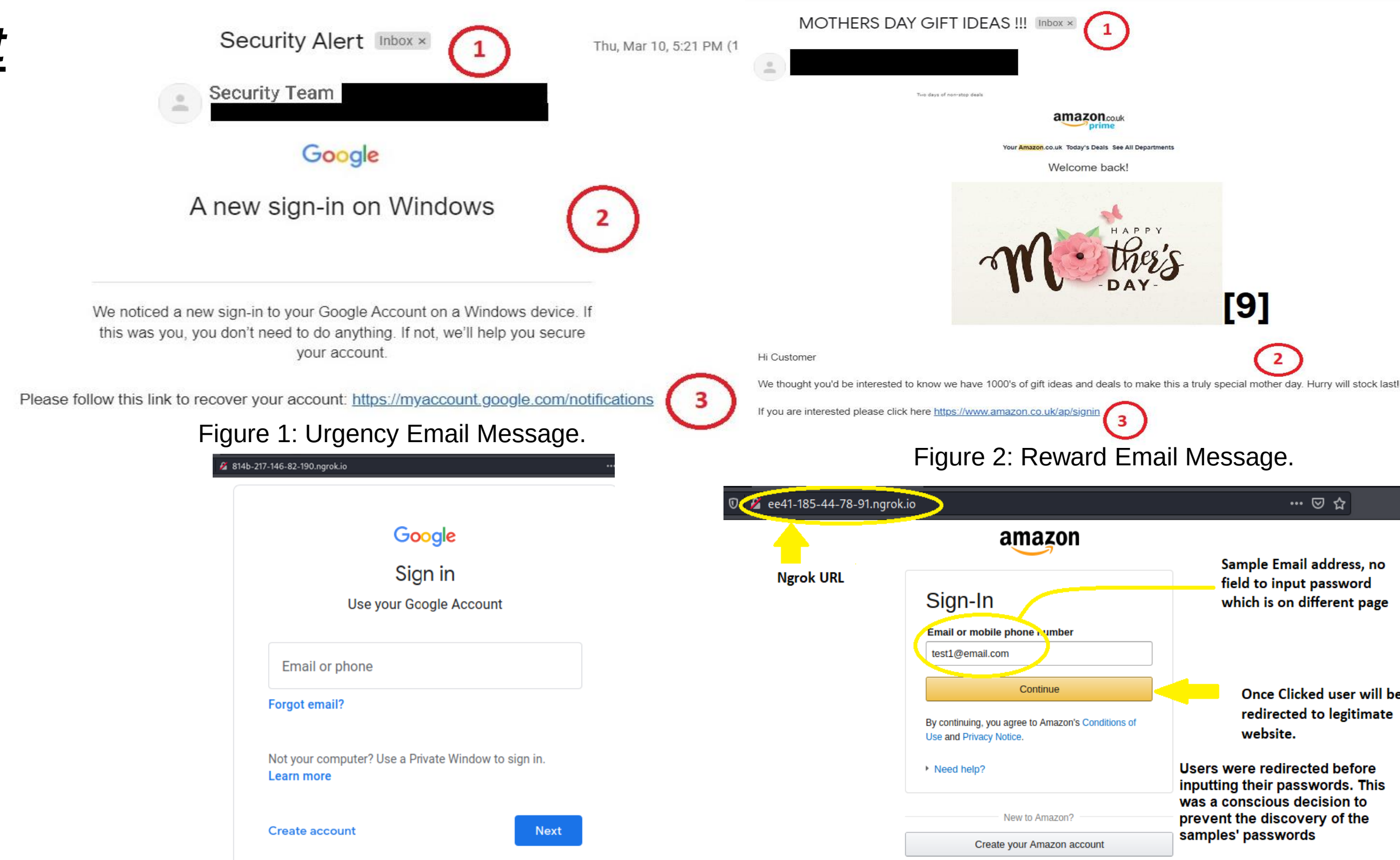


Figure 3: Cloned Website Template (Urgency Experiment).

Figure 4: Cloned Website Template (Reward Experiment).

4. Results

The results show the majority ignoring or not clicking on the link. However, a criminal would see these results as successful as this is five accounts that could be breached and used to send attacks to contacts from a more trusted source. The criminal would also add the compromised users' email contacts to their list of targeted email accounts.

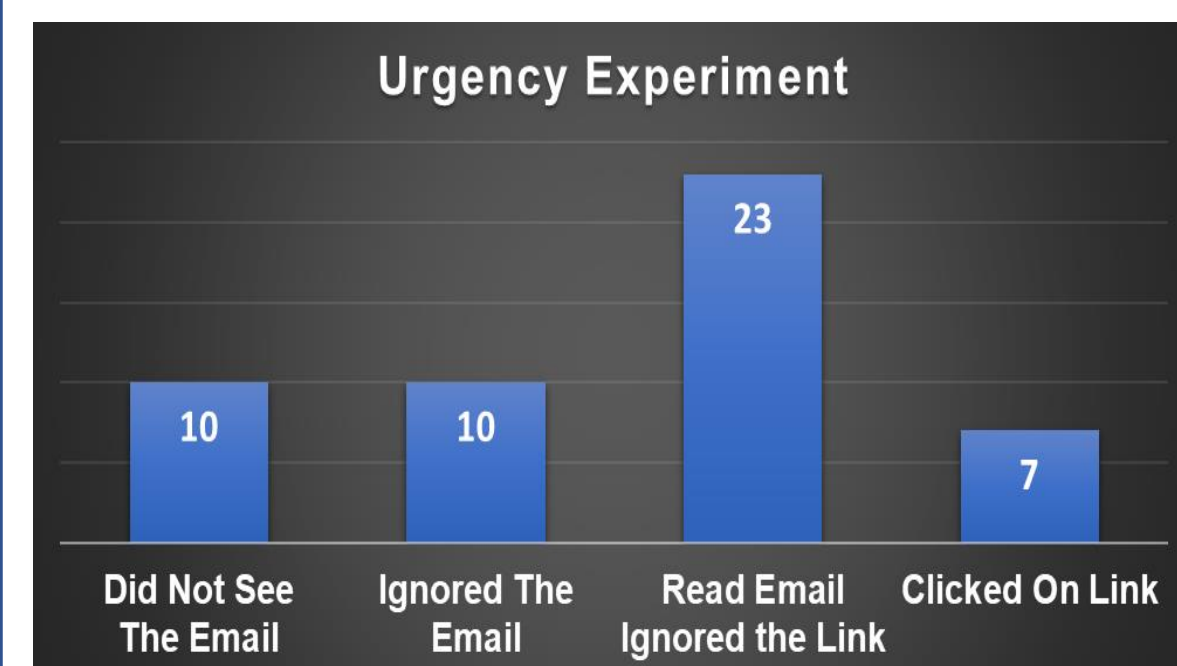


Figure 7: Urgency Results Bar Chart.



Figure 5: Reward Results Bar Chart.

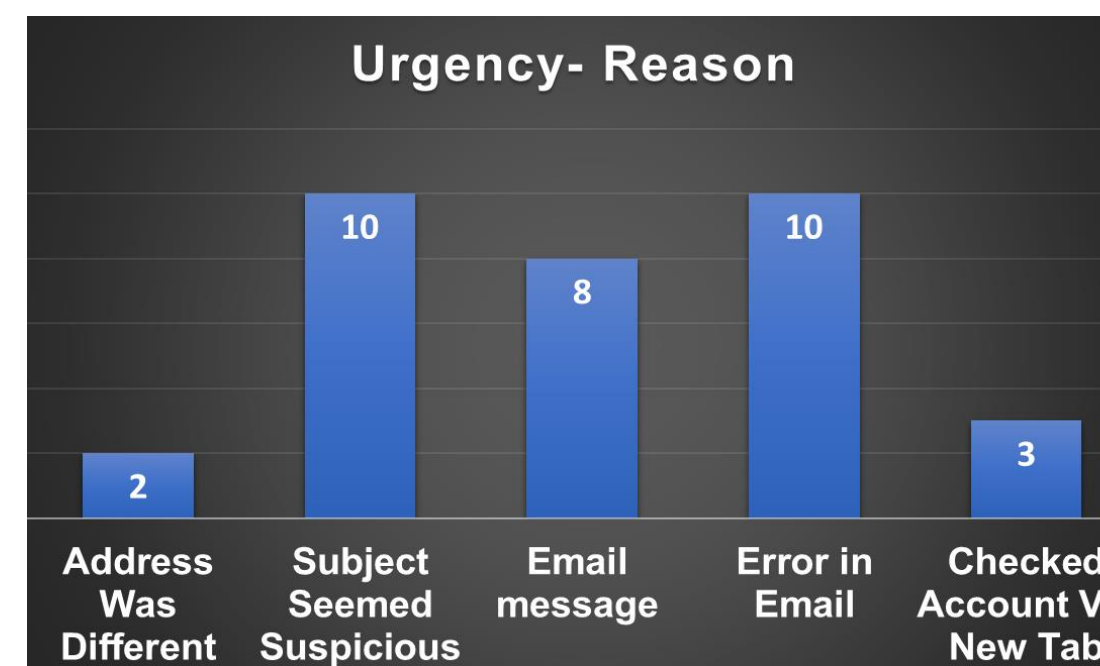


Figure 8: Reason For not Clicking Link (Urgency) Bar Chart.



Figure 6: Reason For not Clicking Link (Reward) Bar Chart.

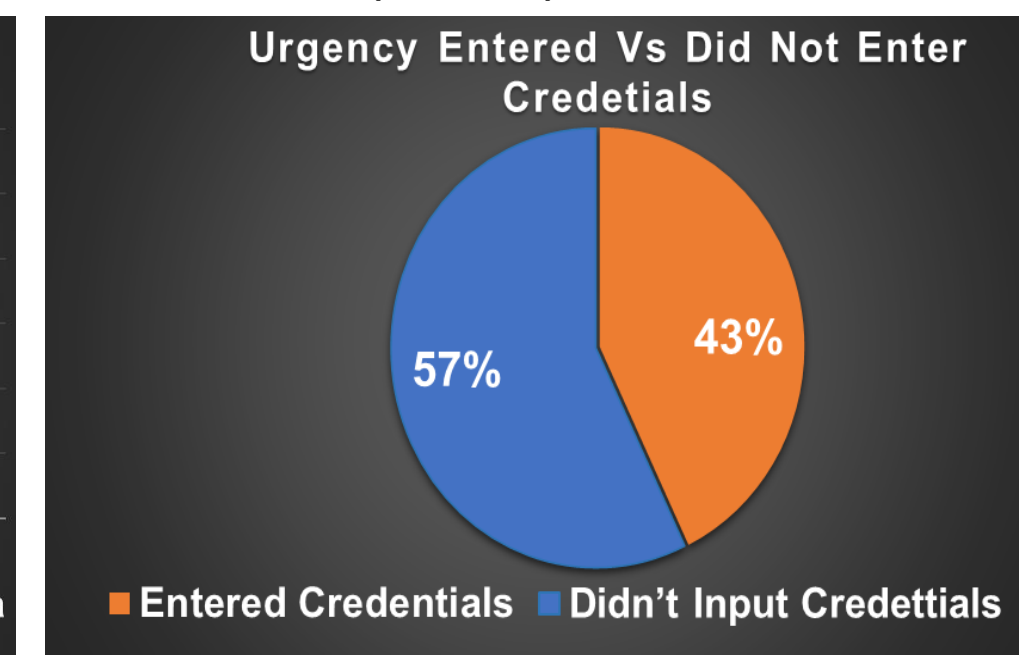


Figure 9: Entered VS Did Not Enter Email Address Pie Chart.

5. Comparison

As seen the hypothesis was correct, urgency performed better than reward with twice the clicks on the link and nearly twice the number of individuals who opened the email. However, there was only a difference of one in terms of email addresses entered.



Figure 10: Urgency Vs Reward Clicks Bar Chart.

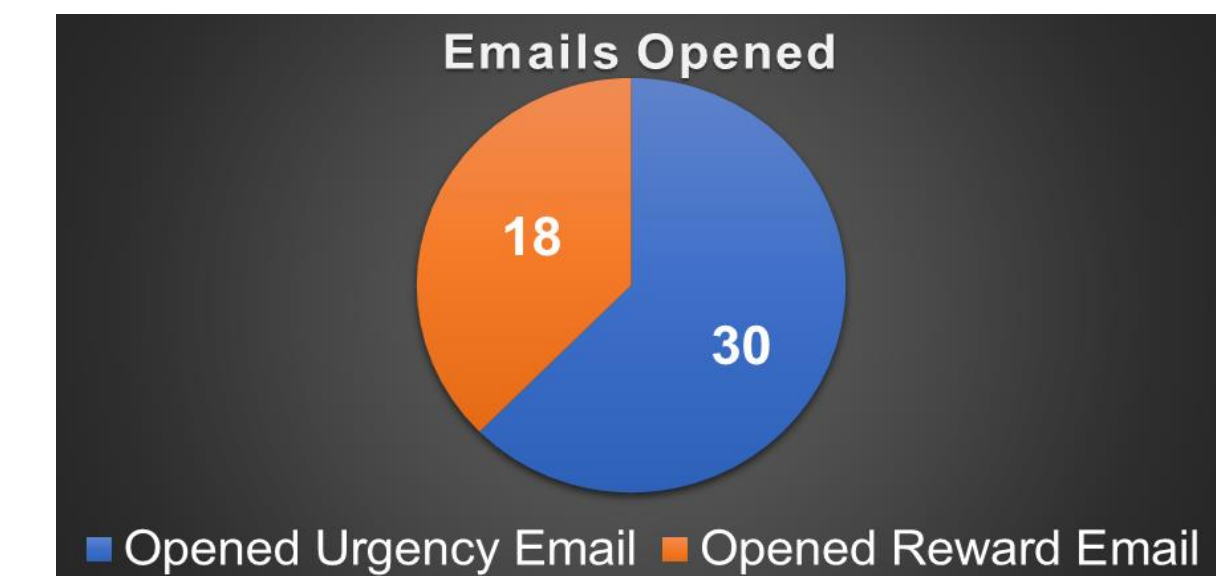


Figure 11: Urgency Vs Reward Emails Opened Pie Chart.

6. Conclusion

In conclusion, this poster shows that it can still be difficult to differentiate between legitimate and malicious emails/ websites. The hypothesis that urgency was a better technique than reward was accurate in the case of this experiment. Finally, Social engineering is a prevalent threat that is only getting worse.

Future Work

- Experiment using more techniques.
- Use an email domain.
- Conduct a spear phishing experiment.
- Perform other forms of social engineering attacks.