

Social Engineering Attacks and Mitigation Methods

Author(s):

School of Applied Computing, Faculty of Architecture, Computing and Engineering, University of Wales Trinity St

Jamie Gau, IQ, Swansea, SA1 8EW, Email: 1910799@student.uwtsd.ac.uk

INTRODUCTION

Hackers are constantly finding new ways to breach networks. With the constant evolution of these attacks comes new mitigation methods that have to be used in order to prevent these attacks. There is, however, one type of attack that remains very prevalent in today's society, as it is known for being extremely difficult to protect a network against. This attack is called a "social engineering attack".

AIM OF THE PROJECT

The main aim of this project was to outline the many social engineering attacks that are utilised against unsuspecting users and companies on a daily basis, and what mitigation strategies can be taken in order to prevent them from happening, or just mitigate the damage they can do.

PRIMARY RESEARCH EXPERIMENT

In order to find out just how aware users are of these attacks; a primary research experiment was conducted in the form of a survey. The responses (pictured below) comes from a pool of over 70 people, questioning them on their knowledge of these attacks, and how prepared they are to deal with them.

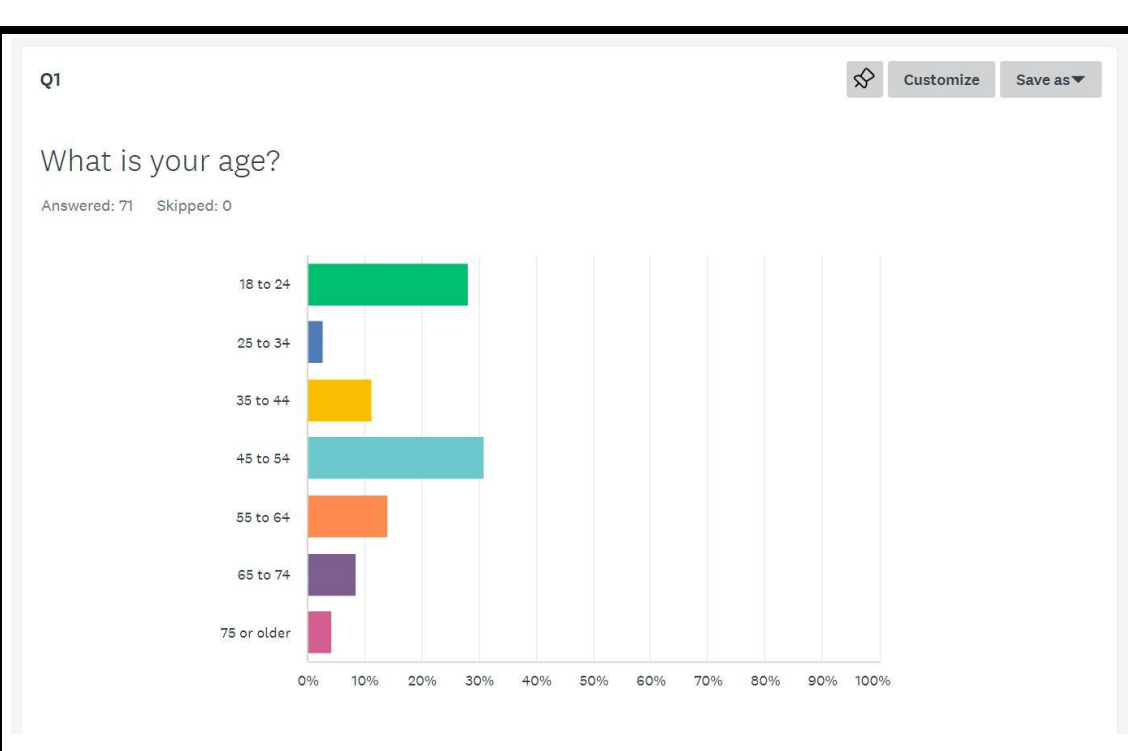


Figure 2 – Question 1

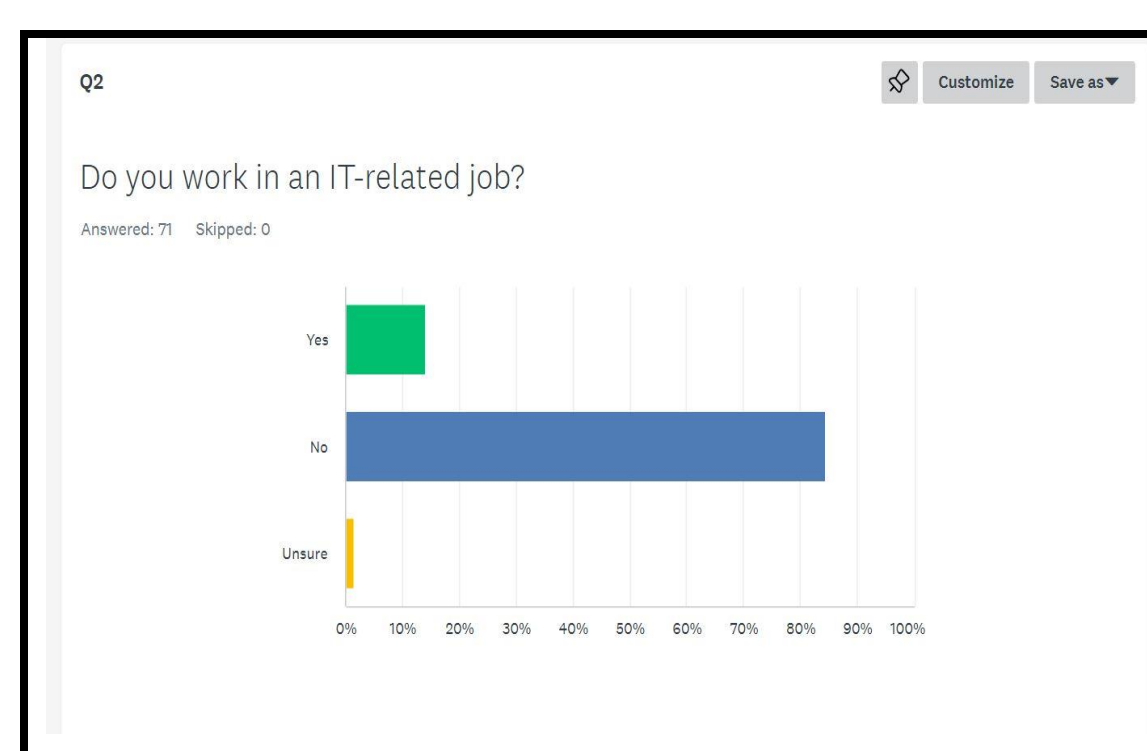


Figure 3 – Question 2

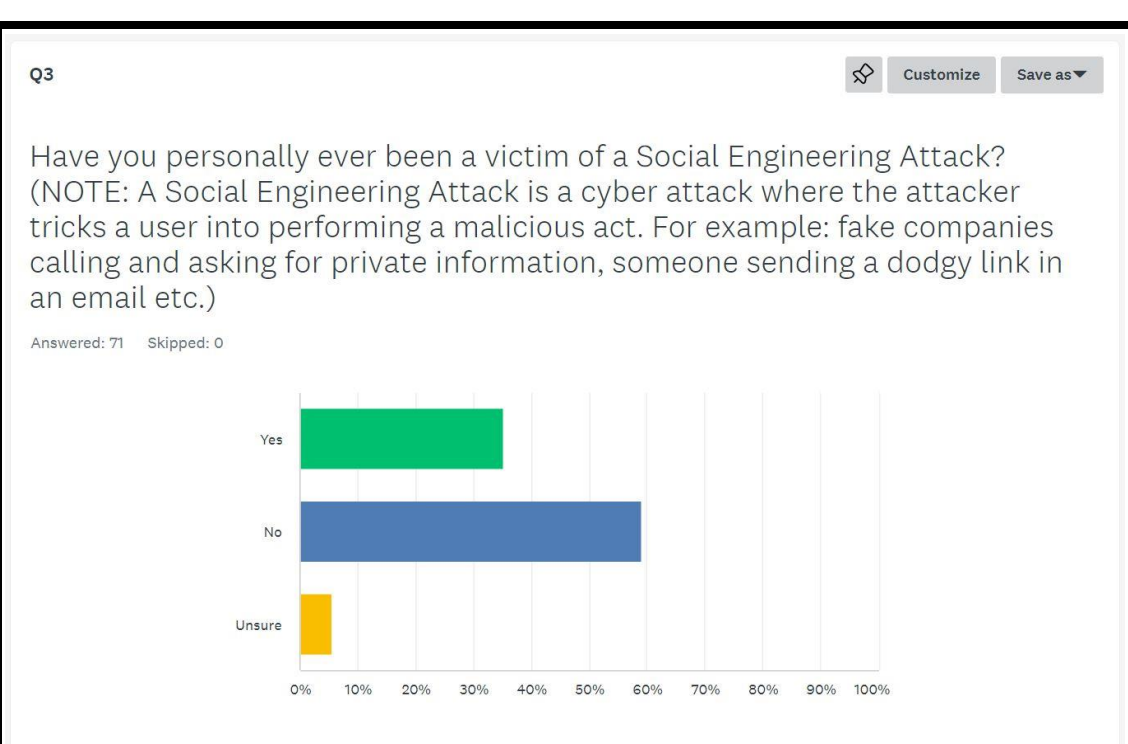


Figure 4 – Question 3

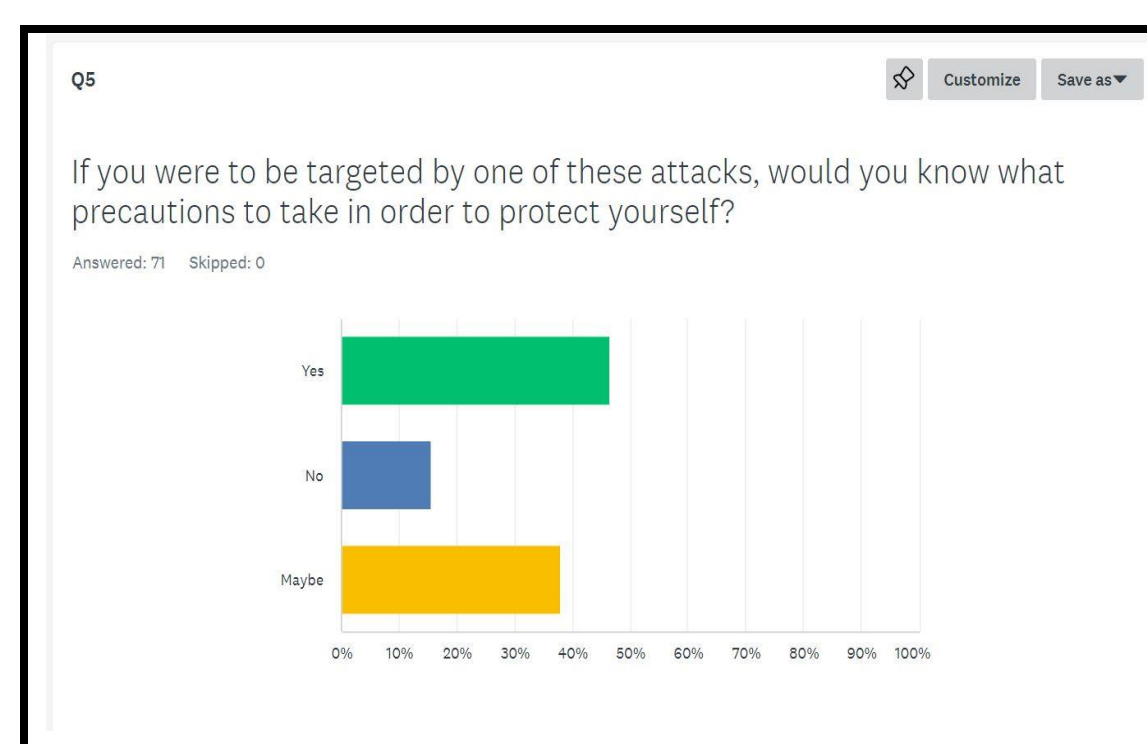


Figure 5 – Question 4

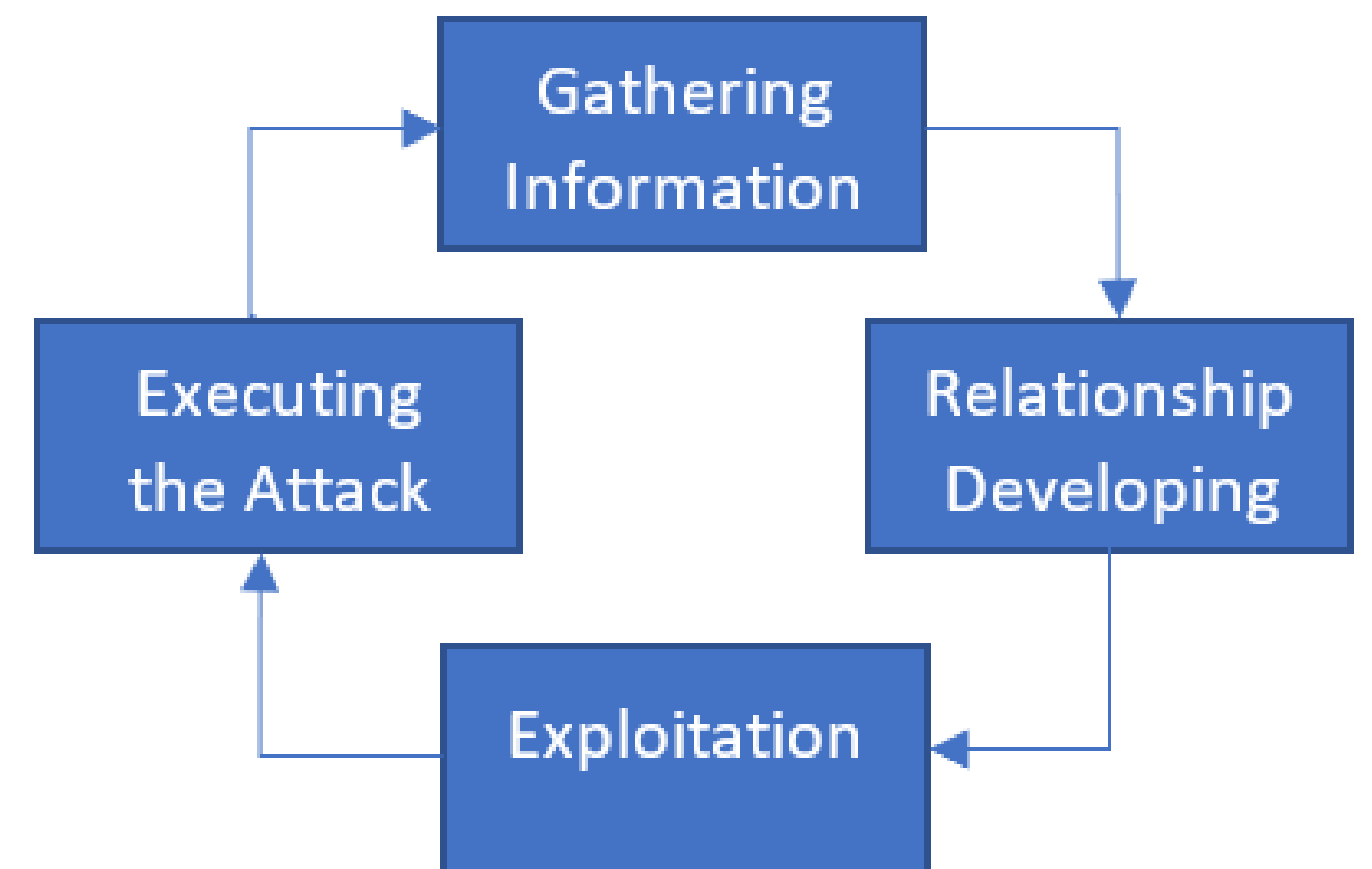


Figure 1 – Social Engineering Attack Process

RESEARCH/REVIEW OF LITERATURE

A social engineering attack is an attack that involves manipulating a person into performing a malicious act, usually without their knowledge or consent. This includes attacks such as phishing, a very popular attacking method where an attacker sends an email or text to a target, containing a link. When the user clicks on this link, malware is uploaded to the target computer, allowing the hacker to potentially have access to the user's files. These attacks are hard to mitigate, as human psychology is not often a controllable factor. The most important mitigation method for these attacks are to make people aware of their existence and how they can guard themselves from them.

FINDINGS/CONCLUSION

From the survey, results show that users are generally aware of what these attacks are, and the damage that they can do. An open question, proposing an attack scenario, at the end of the survey concluded that, if people were to be put in a phishing attack scenario, they would generally know how to protect themselves, as all of the participants answered it correctly.