

Morgan Harries - Project Proposal

by Morgan Dean Harries

Submission date: 21-Oct-2022 11:56AM (UTC+0100)

Submission ID: 187189238

File name: 40801_Morgan_Dean_Harries_Morgan_Harries_-_Project_Proposal_443262_490519052.docx
(978.88K)

Word count: 1744

Character count: 10402

Social Engineering Attacks and Mitigation Strategies

Research Proposal

Morgan Harries

Desired Project adviser - Dr Nitheesh Kaliyamurthy

Table of Contents

Table of Contents	2
Figures	3
Project Brief	4
Introduction	4
Current Literature	5
Social Engineering: Methodology	6
<i>Tools and Uses</i>	7
<i>Physical approach</i>	7
<i>Social Approach</i>	8
<i>Technical Approach</i>	9
Data Collection	9
Project Timeline	10
Bibliography	11

Figures

<i>Figure 1, Desired information, and Targeting Techniques</i>	<i>6</i>
<i>Figure 2, Attack Methods, Uses and Predicted Outcomes</i>	<i>7</i>
<i>Figure 3, Information Gathering Spreadsheet Example</i>	<i>9</i>
<i>Figure 4, Risks/Limitations and how to overcome them</i>	<i>9</i>
<i>Figure 5, Project Timeline.....</i>	<i>10</i>

Project Brief

In this project, Social Engineering Attacks are investigated, and countermeasures to mitigate attacks are recommended to minimise the severity of the attacks. This paper will address the following proposed questions:

- 1) What is Social Engineering?
- 2) What are the different social engineering attacks?
- 3) What are the threats to anyone who may encounter an attack?
- 4) How can these threats be identified, and which counteractions are best chosen to mitigate the risks of an attack?

An experiment will be conducted to carry out this research. The investigation will consist of preparation, engagement, manipulation, and execution. This process will be carried out over the academic year, only targeting those who agree to be involved in this project. The outcome of this project will be educating and protecting those unaware of social engineering attacks and mitigation strategies through the medium of a report and conceptual models.

Surprisingly, humans are frequently overlooked in the security of information. Many security practices further ignore human manipulation to compromise information security. This research project focuses on making the risks of social engineering attacks transparent. Social engineering mitigation methods can be roughly divided into human and technology-based detection. The forms need to be used together to enhance and increase detection accuracy so that social engineering attacks can be stopped and prevented.

As more organisations and individuals digitise processes and boost internet access, Social Engineering poses a severe challenge to their security. This project demonstrates Social Engineering attack methods and analyses the current protection measures, tools, and policies for organisations and individuals to prevent attacks after identifying the behaviour and the issues it raises.

Introduction

Social Engineering remains an increasing attack vector for the proliferation of malicious programs. The phrase "Social Engineering" describes various computer exploits that leverage several different attack vectors and techniques to manipulate a user psychologically. [1] Even though the effectiveness of security procedures to protect sensitive information is advancing, humans remain vulnerable to manipulation. Social Engineering preys on humans' psychological and emotional aspects to access a restricted area or obtain sensitive information for various purposes. Various methods, such as Trojan and phishing emails, impersonation, persuasion, bribery, shoulder surfing, and dumpster diving, are frequently employed in Social Engineering attacks [2].

Current Literature

Whilst researching previous studies, I discovered there was a lack of real-life examples and conceptual models to demonstrate their findings. To help with futureproofing against social engineering attacks, I believe implementing educational posters/models for work environments would significantly improve information protection, according to a pilot survey to identify '*What impact do posters have on academic knowledge transfer?*' - "94% agreeing that poster imagery is most likely to draw viewer's attention" [3]; this means if someone is ever in doubt about the validity of potential attacks, they would be drawn to the example for immediate advice.

As this project is based on a real-life example, the results will be 100% accurate, allowing a more in-depth analysis of the methods used to mitigate threats. The results of this analysis will enable me to rank the mitigation strategies in order of most effective and how they can be related to specific attacks.

Numerous studies describe the effects of social engineering attacks in various contexts. In prior studies, social networking has been one of the most popular attack vectors. [4] The academic journal "*Social Engineering Attack Strategies and Defence Approaches*" defines attack methods and defence strategies. This paper does an excellent job of explaining both attack and defensive techniques. However, the defensive methods are not applied to real-life situations. No models are used to support the evidence they have found.

Social Engineering: Methodology

For this Project to be successful, objectives need to be set. An attack will be committed on fellow students. Their current knowledge is what encouraged this decision. Although my peers are aware of cyber security, the project will outline how social engineering attack strategies can persuade even those who are intellectually aware.

Social engineering attacks exist to access information/systems by exploiting vulnerabilities. Attack methods are varied; this includes physical, social, and technical aspects. This section explains some attack methods and how each attack will be approached. The attacks do follow a similar cycle despite the various forms. [5]

1. Information Gathering - Planning
2. Development of Relationships
3. Exploitation
4. Execution aimed at achieving the objective

There are several ways to go about information-gathering, such as through social media, open sources, relationship building, etc. I have produced a diagram that shows the attack's information-gathering phases:

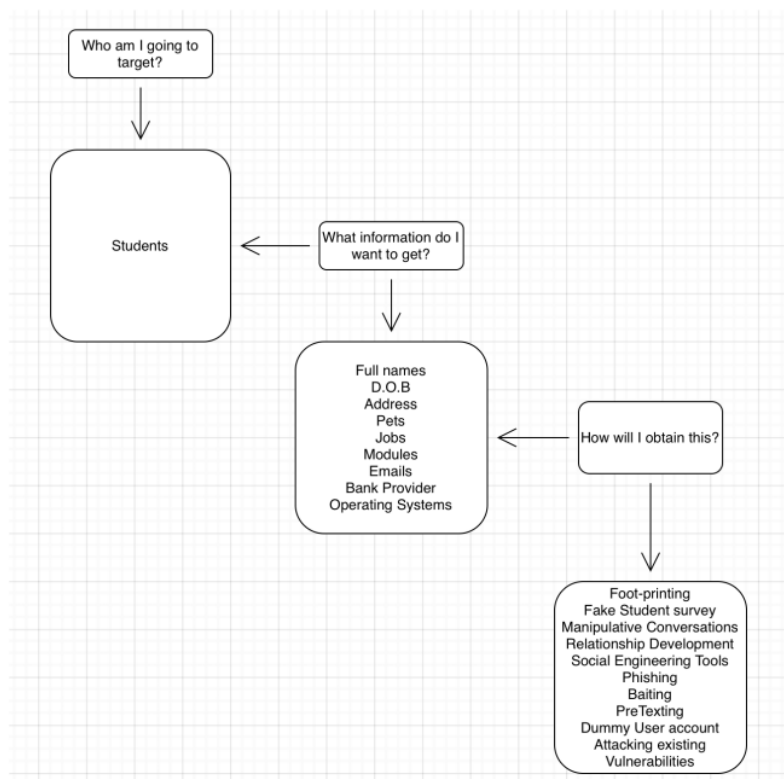


Figure 1, Desired information, and Targeting Techniques, adapted from: Author's own

To successfully gather information, specific objectives need to be set; the figure above states the initial targeted information desired and how that information can be obtained. The information-gathering phase will consist of weeks of continued studying of the targeted individuals. [6]

Tools and Uses

Attack Method	Reason for use	Predicted Outcome
Physical		
Relationship Building	Building relationships with peers will allow trust to be gained, this way possible personal information can be obtained freely. Using the Cialdini's techniques, relationship building can become an access point to personal information	Developing a relationship will allow me to note any personal information the victim allows me to access. I can further analyse this information and identify how I may benefit from it
Dumpster Diving	The attacker will be searching throughout the classroom for disregarded information.	Any unsupervised information left can be used to make notes to assist with future analysis
Shoulder Surfing	The attacker will look over nearby victims shoulders to gain usernames, passwords, emails etc.	Analysing keyboards and monitors could potentially allow access to user credentials
Eaves Dropping	Listening out for any personal information released in conversations with others	Find out any personal information that could benefit me in the future.
Social		
Cialdini's "Principles of persuasion"	Reciprocity, Authority and liking are three of the most beneficial techniques I will be using to help persuade victims to give me answers to the questions I ask.	
Relationship Building	Building relationships with peers will allow trust to be gained, this way possible personal information can be obtained freely. Using the Cialdini's techniques, relationship building can become an access point to personal information	Developing a relationship will allow me to note any personal information the victim allows me to access. I can further analyse this information and identify how I may benefit from it
Social Media	Becoming "Friends" or "Following" peers on social media platforms creates further opportunities to access personal information. Individuals tend to post more personal information to their social media audience. This will allow me to analyse personal information within an online presence	Social Media relations will allow me to spend extra time analysing the victim outside on university, reducing my limitation on information gathering
Technical		
Phishing	The online phishing attack method is established on multiple platforms, including Emails and social media. The Phishing attack involves the attacker influencing the victim to carry out an online questionnaire or signing into a compromised website tricking them into submitting personal information. The emails would imitate a legitimate university email form and impersonated email addresses.	Using Kali Linux, I can create a phishing email, imitating from the university directing them to log in to an imitation website. Storing their credentials.
Impersonation	I will contact the IT department (Lee and Ray) asking for permission to create a dummy user on the UWSTD system. I will use the dummy user to send out emails with links to compromising questionnaires.	Students will complete the questionnaire and submit personal information for me to analyse

Figure 2, Attack Methods, Uses and Predicted Outcomes

Physical approach

When an attacker attempts to compromise information from their victim, they can use a physical approach; Tailgating, Dumpster Diving, Eavesdropping, Piggybacking, Shoulder Surfing, Impersonation, and Dumpster Diving are all methods of Physical attacks. [1]

Whilst in the classroom, there are specific physical methods that will be carried out:

Dumpster Diving

Dumpster diving is a common tactic that will be used in future attack strategies throughout this project. According to PrivacySense, "Dumpster diving refers to retrieving information from discarded items to perpetrate a cyber-attack". [7] According to PrivacySense, Dumpster diving traditionally means searching through trash to find information about a target; however, dumpster diving will have a different approach for this project. In this instance, the attacker will be searching throughout the classroom for disregarded information, i.e., old registers and student ID cards left unattended. Images of this information will be captured and left in place as if uncompromised.

Shoulder Surfing

"Shoulder surfing uses direct observation techniques, such as looking over someone's shoulder, to get information." [8]

Peeking over the target's shoulders is a simple way to obtain information. This method will allow me to acquire User IDs, Passwords, and any other confidential data in plain text. The benefit of this method is its flexibility. It can be done anywhere at any time.

Social Approach

A practical social approach is one of the most effective methods of Social Engineering information gathering. Whilst performing an attack, some of Cialdini's "Principles of persuasion" (Reciprocity, Authority, and Liking) will be adhered to. [9]

Reciprocity

The most fundamental rule of influence is reciprocity, giving what you desire in return. For example, giving a target personal information and engaging with them could potentially lead to exchanging the same information. [9]

Authority

To convince the victims of the validity of the attack method, the use of my lecturers could be utilised to influence participation by the victims. [9]

Liking

The ability to persuade people with common interests. We can communicate more effectively and sway their decisions if we appear to share common interests with them. Whilst in the classroom, the correct choice of wording can manipulate the targets to give information without being aware of a planned attack. As the students aren't very familiar with one another, a team-building exercise would be a perfect opportunity to execute this method, getting to know who is in your group and obtaining personal information about them. [9]

Technical Approach

Technical information gathering will consist of using different online Social Engineering techniques to source information. Spam, Phishing, Chats, and Pop-up Window Attacks are some other strategies I will use on the computer to attempt to manipulate the students.

The online phishing attack method is established on multiple platforms, including Emails and social media. The Phishing attack involves the attacker influencing the victim to carry out an online questionnaire, tricking them into submitting personal information. The emails would imitate a legitimate university email form and impersonated email addresses.

Social Media profiles can almost be used as an online information database; However, this information might not be legitimate; it can be used to relate to the target and assist with the social approach methods.

Data Collection

The data collected will be stored in a spreadsheet; this way, any information discovered can be updated on the spreadsheet at any given time on a phone or computer. The spreadsheet will have titles with the related information stored underneath each column. Keeping the collected information on a spreadsheet allows online storage; this way, data cannot be lost, stolen, or misplaced.

Victims Name	Age	D.O.B	Email	Information Gathered
Joe Bloggs	22	19.02.2000	joebloggs@example.com	works at homebargains, lives in Ilanelli, drives a renault, iphone 13, phone password 1234

Figure 3, Information Gathering Spreadsheet example

Figure 3 displays how the data will be contained. Storing on a spreadsheet prevents any risk of data loss or exposure; this is due to the access being restricted to only one person (attacker).

Risks/Limitations	How to overcome
Liability of Information Gathered	Information needs to stored securely, no information to be gathered physically, only digital infromation stored on a local device.
Intrution of Personal Information	When asking for consent, ensure the participant is fully aware of every intention. This will allow the participant to refuse consent if they no longer want to be part of the projecet
No consent from anyone	Lack of consent from peers will slow the project, resulting in a new target to be identified and new research carried out on how to attack them.
Not enough information gathered	Lack of information will not mean the project has failed it will have to be re-evaluated. If this is the case I will research which mitigation strategies they have used to prevent the attacks being successful
Data Loss/Exposure	If infromation was lost or exposed in anyway, it would be mv responsibility to contact the victims and

Figure 4, Risks/Limitations and how to overcome them

Project Timeline

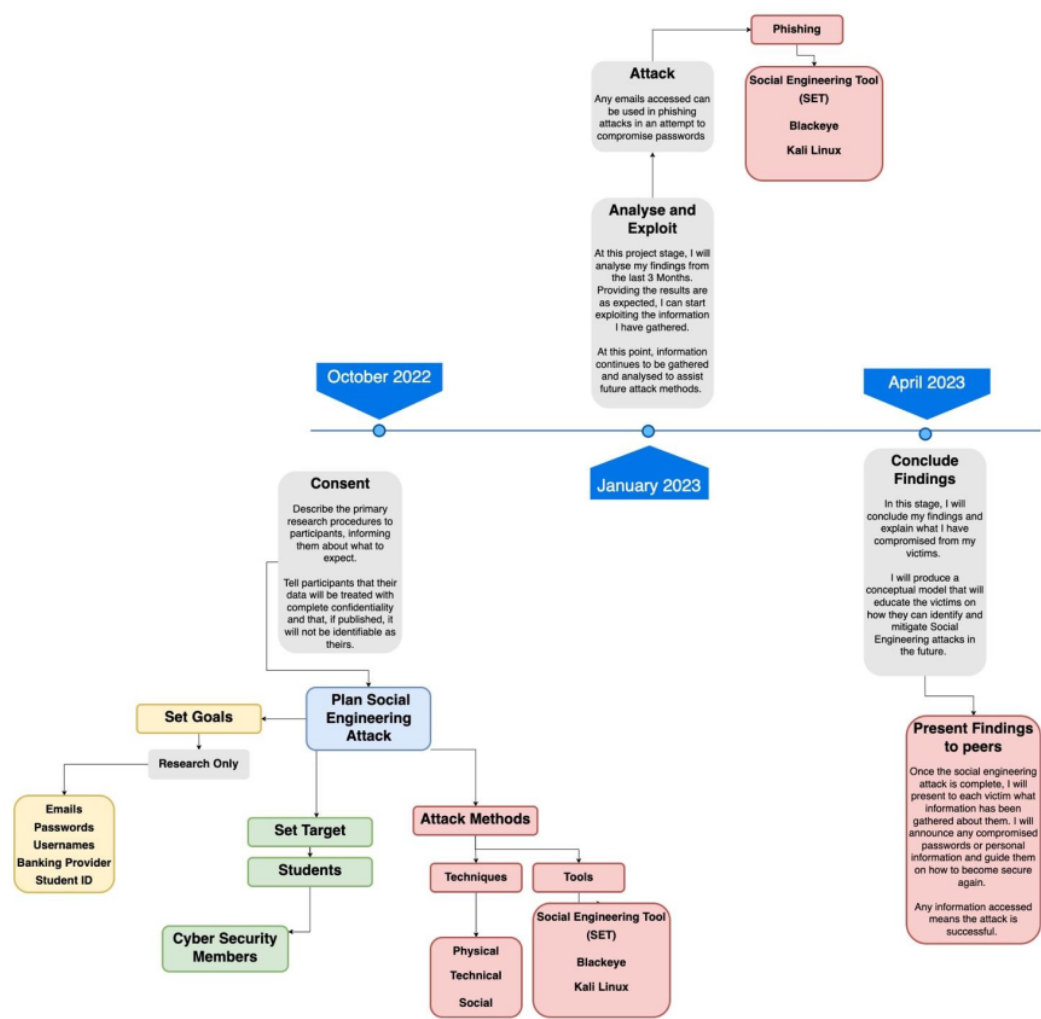


Figure 5, Project Timeline

Figure 5 presents a timeline for how the project plans to be conducted. The project will be broken into three sections. Consent/Plan, Analyse/Exploit, and Conclusion. Information about each phase of the project is shown in the figure above.

Bibliography

- [1] Abraham, S. and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Social* 32.3, vol. 32, no. 3, pp. 183-196, 2010.
- [2] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches," *IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 145-149, 2016.
- [3] N. I. D. Rowe, "What impact do posters have on academic knowledge transfer? A pilot survey on author attitudes and experiences.," vol. 9, no. 71, 2009.
- [4] A. Algarni, "Measuring Source Credibility of Social Engineering Attackers on Facebook,," *IEEE*, p. pp. 3686–3695, 2016.
- [5] A. Algarni, Y. Xu, T. Chan and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," *IEEEExplore*, 2013.
- [6] S. T. Education, "Security Through Education," [Online]. Available: <https://www.social-engineer.org/framework/information-gathering/>. [Accessed 2022].
- [7] PRIVACYSENSE.NET, "PRIVACYSENSE.NET," October 2021. [Online]. Available: <https://www.privacysense.net/terms/dumpster-diving-attack/>. [Accessed 2022].
- [8] whatis. [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/shoulder-surfing>. [Accessed 2022].
- [9] H. Blogs, "Harappa Education," 27 March 2021. [Online]. Available: <https://harappa.education/harappa-diaries/robert-cialdinis-principles-of-persuasion/>. [Accessed October 2022].
- [10] H. H. M. H. E. W. Katharina Krombholz, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113-122, 2015.

Morgan Harries - Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

63 / 100

Instructor

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	65
Generally a reasonable proposal, however the actual content on how it is going to be executed really needs discussion urgently before commencing, as there are a number of ethical and practical issues that need clarification!		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts	20	62

Background info fair, however title says “....and mitigation strategies” This doesn't really seem to have been covered ??		
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed	30	65
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Project plan needs more detail in terms of actual dates to be of much use. Should there be an ethics form attached? Can't see one, and this project, really, REALLY needs to have some ethical issues discussed before starting as some things (such as spying on your fellow students) needs review/clarification!	15	60

Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit Generally well presented. Try not to use the 'I' 1st person style though. Some of the text didn't flow as well as it could have – re-writing would have made it easier to read.	15	62
TOTAL	100	63%

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9
PAGE 10

