

Project Proposal

by Connor Wilson

Submission date: 28-Oct-2022 02:41PM (UTC+0100)

Submission ID: 187619484

File name: 24870_Connor_Wilson_Project_Proposal_443262_1951017543.docx (109.53K)

Word count: 1982

Character count: 10706

Social Engineering Attacks and Mitigation Strategies

Research Proposal

Connor Michael Anthony Wilson

Dr Nitheesh Kaliyamurthy

Contents

Page 1 – Introduction

Page 1 – Project Choice

Page 1 - What is social engineering?

Page 2 – Background to the Proposed Research

Page 2 & 3 – Research

Page 4 – Aims and Objectives

Page 5 – Project Design

Page 5 – Outline of Project Process

Page 5 – Data Collection

Page 5 – Data Evaluation

Page 5 – Risks & Limitations

Page 5 – Ethical Issues

Page 6 – Resource & Planning

Page 6 – Resources required

Page 6 – Hardware Resources

Page 6 – Software Resources

Page 6 – Other Resources

Page 7 - References

1. Introduction

Project Choice.

The project choice which is Social Engineering Attacks and Mitigation Strategies was chosen as after hearing about this in lectures this year with Niteesh I thought this was an engaging concept as it is out of a lot of content of learned about thus far.

As no matter how secure a system is in terms of their technological solution individuals can always be exploited for a success attack, information, etc.

For this reason, it is important that individual's tech literate or otherwise should be more aware of how to stay protected from these intrusions.

What is social engineering?

Social engineering is the act of using psychological manipulation of other humans into providing sensitive or otherwise unknown information to an attacker. This differs from other forms of these manipulations as it usually part of complex plan or procedure as an attempt does not work then it may not be possible to go back to gather more information.

a common way for private investigators to acquire information is pretexting — phoning an individual for information providing them with false information like masking their identity, as they will be likely to provide information to a trustworthy source. Such attacks of this nature are known as social engineering. [1]

2. Background to the Proposed Research

To have a better understanding of the subject area of this project there will be brief research with this proposal which will then be expanded on within the full project. Using a variety of accredited academic works in the way of government statistics, academic articles/case studies as well as books. This will allow for a more well-rounded project hopefully and make it more credible.

For this initial research in the proposal, an investigation into the historical progression of social engineering to get a better idea of how it has evolved over time and its applications. Looking at noteworthy academic writing to have more Nuanced understanding of the modern interpretations of this technique and allowing for me to develop methodology for me to test ideas for the project.

Research

The act of social engineering can encompass a variety of things such as acquiring information from a staff member of a building however the virtual world has to be considered as well as one of the most popular forms of social engineering attacks today online is known as “phishing”.

In 1996 hackers were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The popularized first mention on the Internet of phishing was made in the alt.2600 hacker newsgroup in January 1996. [2]

From 1996 to the present-day phishing has become one of the most common forms of fraud-related crimes committed internationally with the crime on the rise year by year

In Q2 of 2022 alone the Anti-Phishing Working Group reported that 1,097,811 total phishing attacks were recorded by their organisation. APWG reported that this was the worst to date recording that the organisation had ever seen and that the amount had quadrupled since 2020 [3].

The number of phishing attacks reported to APWG has quadrupled since early 2020, when APWG was observing between 68,000 and 94,000 attacks per month [4].

The amount of this uptick could be down to a variety of different factors. This could be due to the quarantine over the two years bringing financial hardship to people and/or slowing the economy into the current recession which can be linked to a variety of reasons.

Looking at statistics, contrasting and comparing these during the research phase of the project will likely be beneficial as it will give me more of an idea of what areas which should be focusing on when creating a solution for the project say if there is more of a specific type of attack that is occurring it may make more sense to develop a solution around that.

The only issue with finding these statistics that just during completing the research for this project there have already been some roadblocks in acquiring these statistics as some organisations that provide information like “The office for national statistics” will not provide this information as they feel like this could be unethical to provide that information as it could allow criminals to exploit people further.

Phishing emails are not recorded by either the Crime Survey for England and Wales (CSEW) or police-recorded crime figures. Phishing is an enabler of committing fraud, and no separate crime is recorded concerning phishing. [5]

This may provide some issues during the research but there should be some quality statistics which will allow for good analysis.

It is somewhat of an outdated stereotype to have phishing only being through scam emails and texts though this does happen people's awareness of this specific form of phishing through the cliché of emails from far-off royalty that have asked for financial support to a random text from someone attempting to disguise themselves under a guise of a company and any of these messages being filled with poor grammar or spelling.

Often there are templates available for Linux command line programs such as Zphisher and other similar tools which allow users to send templates that replicate that of a variety of companies and make a fake webpage to capture users' login details and such.

It became very popular nowadays that is used to do phishing attacks on Targets. Zphisher is easier than Social Engineering Toolkit. [6]

These tools and their ease of access are making the entry level for these types of phishing attempts more accessible to those with little advance to no advanced knowledge of malicious types of hacking/social engineering attacks.

The awareness of the type of tools that are popular for social engineering attacks will help to make a better mitigation strategy and will help to have a more comprehensive solution at the end of the project furthermore looking into this in the main body of said research.

With consideration for these kinds of tools being used also need to be considered the longevity of the final solution as due to the nature of defending you are always going to be at a disadvantage to attackers as they are going to Innovate, and you will not necessarily be aware of these innovations till an attack is occurring and the unpredictability of technological advancement through software and hardware.

Therefore, looking into future technology and current defence strategies will be important to allow for more longevity to the solution though staying relevant for long periods is not viable due to the progressive nature of technology.

Social engineers use strategies to gain people's trust. it is easier to convince someone to reveal his or her password hacking, this field is associated with sociology with cyber security. The social behaviour of humans affects online activities and influences the issue to a great extent. [7]

With this consideration looking into rudimental sociology and some basic psychology is in order due to the nature of the attacks and their level of human interaction which will be evaluated for the defence strategy.

3. Aims & Objectives

- To create a comprehensive and effective mitigation strategy against social engineering attacks
- Consider in person and virtual forms of social engineering when creating a strategy
- Use research to develop knowledge to facilitate in the creation of the final product.

4. Project Design

Project will contain a main body of comprehensive research at the beginning of the project to help enhance the knowledge in the study area and assist with the making a product at the end of the project with looking at current practices, technologies, and strategies.

The next step starts the development of a solution and at this stage I will be documenting the creation process, any testing and modifications as the production process changes.

The Final part of the project will reflect the project. How the process could be adapted if completed again and how effective the solution is.

4.1 Outline of Project Process

Detailed above

4.2 Data Collection

Data will be collected via Microsoft forms using mediums such as survey and/or questionnaires.

4.3 Data Evaluation

Data evaluation will be completed using excel to evaluation the data set provided from the questionnaire/surveys and then can be presented in readable formats such as

4.4 Risks & Limitations

A limitation might be that due to the ethical issues that companies or organizations find with sharing data regarding phishing or fraudulent time it might create difficulties during the research phase and make troubling to find specific areas that are being exploited by cyber fraudsters.

4.5 Ethical Issues

Protection of user's data during surveys/questionnaires during research but there is a configuration in Microsoft forms which allows for all data entries to be kept anonymous which would resolve the issue.

The collection of data for this project may facilitate in aiding fraudsters in identifying weak areas for exploitation but as this data is only being shared with the university and will not be published externally then this will be a note issue.

5. Resources & Planning

5.1 Resources Required

A midrange computer that is already in my own possession. Software such as a word processor, an form maker and data analysis tool and software for the creation of the solution that has not been decided currently.

5.1.1 Hardware Resources

Midrange Desktop PC (Personal)

Specs:

Intel i5 8600k at 4.9ghz

16gb of Corsair Vengeance 3200mhz DDR4 ram (2 Channel memory kit)

Nvidia RTX 2060 Gigabyte OC 6gb model

Corsair 750w gold certified power supply

3 x BeQuite 120mm case fans

2 x BeQuite 140mm case fans

Westend Digital Blue 1TB Nvme drive

4tb generic HDD

5.1.2 Software Resources

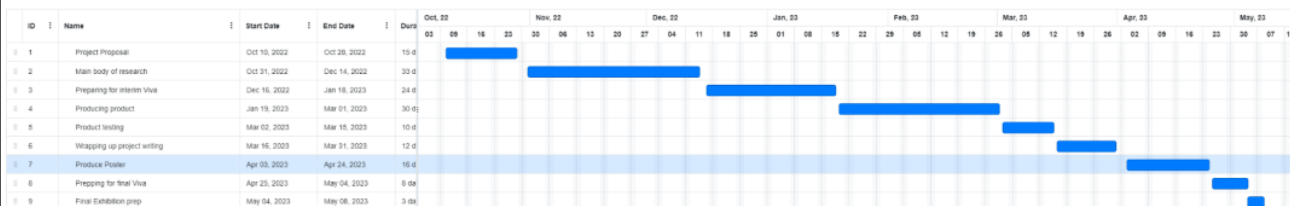
Microsoft Office Suite (Excel, Word and Forms)

5.1.3 Other Resources

N/A

5.2 Planning Chart

I have created a ganatt chart outlining a rough outline of the progression with dates for the duration of the project.



6. Reference List

- [1] Anderson, R. J. (n.d.). Security Engineering A Guide to Building Dependable Distributed Systems Second Edition. *Security Engineering Edition 2*. Retrieved October 20, 2022, from https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf.
- [2] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), 3629–3654. <https://doi.org/10.1007/S00521-016-2275-Y/TABLES/9>.
- [3] *Phishing E-mail Reports and Phishing Site Trends 4 Brand-Domain Pairs Measurement 5 Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks 6 Use of Domain Names for Phishing 7-9 Phishing and Identity Theft in Brazil 10-11 Most Targeted Industry Sectors 12 APWG Phishing Trends Report Contributors 13 2 nd Quarter 2022 PHISHING ACTIVITY TRENDS REPORT*. (2022). <http://www.apwg.org>,
- [4] *Phishing E-mail Reports and Phishing Site Trends 4 Brand-Domain Pairs Measurement 5 Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks 6 Use of Domain Names for Phishing 7-9 Phishing and Identity Theft in Brazil 10-11 Most Targeted Industry Sectors 12 APWG Phishing Trends Report Contributors 13 2 nd Quarter 2022 PHISHING ACTIVITY TRENDS REPORT*. (2022). <http://www.apwg.org>,
- [5] Office for National Statistics. (2019, March 15). *Damage caused by phishing - Office for National Statistics*. Office for National Statistics. <https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/damagecausedbyphishing>
- [6] mohdshariq. (2022, August 5). *Zphisher - Automated Phishing Tool in Kali Linux - GeeksforGeeks*. Geeks for Geeks. <https://www.geeksforgeeks.org/zphisher-automated-phishing-tool-in-kali-linux/>.
- [7] Thakur, K., Shan, J., & Pathan, A.-S. K. (2018). View of Innovations of Phishing Defense: The Mechanism, Measurement and Defense Strategies. *International Journal of Communication Networks and Information Security (IJCNIS)*, 10(1), 20–21. <https://ijcnis.org/index.php/ijcnis/article/view/2991/746>

Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

56 / 100

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 What is the aim of the project? Objectives will need to be refined and expanded, . You were supposed to explain why the project is worth doing and provide a discussion of what the project needs to do to be a success. Its still not clear on deliverables that will be produced at the end of the project.	20	10
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	13

It is a good thing you have looked at some initial literature in area of research, but description of how work to be done in the project relates to the work identified in literature is not explicitly given. You need to discuss any ethical issues raised by the project and select relevant models and concepts.		
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 Development methods to be used and why they are appropriate is not clearly outlined. I was expecting to see Visual representations of your Design. There is no mention of tools to be used, and you are not clear on how collected data will be analysed	30	17
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices	15	8

I did not see a list of deliverables, your tasks in Planning Chart need to be reviewed. I did not see any completed ethics form, and you should start building on your appendices		
Document Presentation		
Correct spelling, grammar, and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit The document is lacking a professional look , as table of contents is manually done, and the formatting can be improved.	15	8
TOTAL	100	56

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7

