Sri Lanka Institute of Information Technology

Information Security Project

Project proposal submission

Submitted by:

Student Registration Number	Student Name
IT20028046	S.B.M.B.S.A Gunathilaka
IT19108100	Herath H.M.C.S.B

CS-Y3S2

Date of submission: 20/08/2022

Topic – social engineering awareness project

Video link -

https://drive.google.com/drive/folders/1GNYvdqCtQgWg49DSlzRWyb_HE6b7RXQ1?usp=sharing

https://mysliit-my.sharepoint.com/:v:/g/personal/it20028046_my_sliit_lk/EQsz5HFYEupAhN-ogPfT7u8BT8CT7NsFpLZfzfsvAQRObw?e=MWc9cW

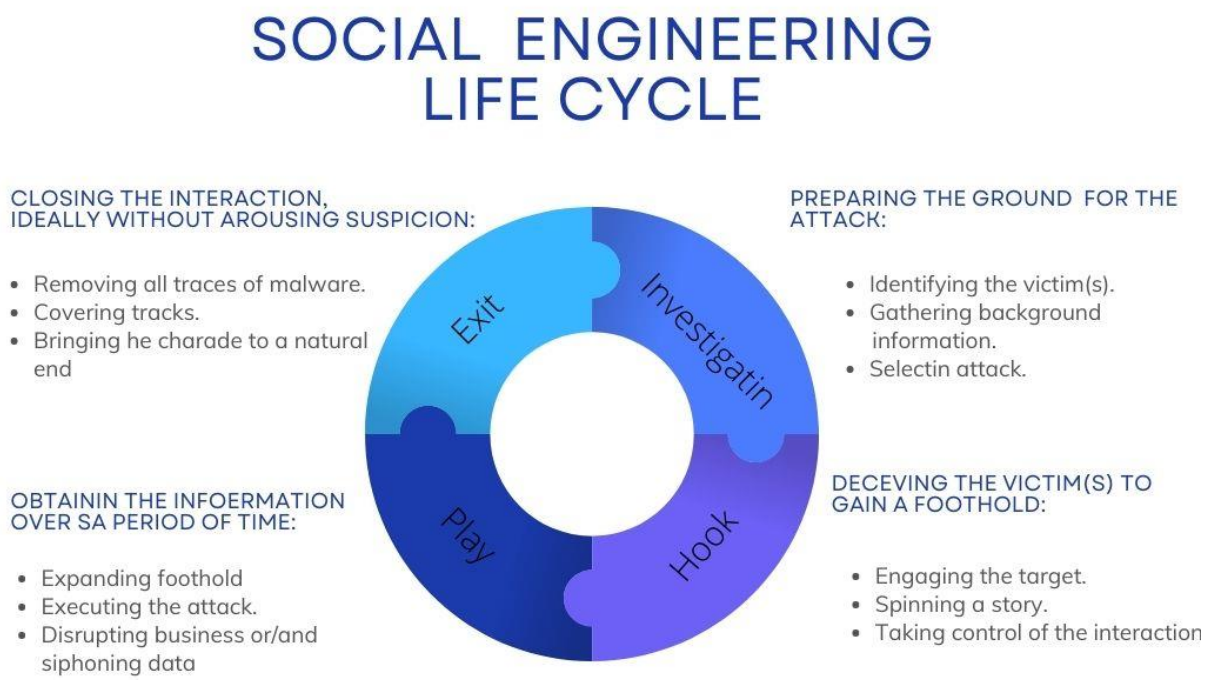
Introduction

In the context of information security, Social engineering is a major threat to businesses with its infrastructure and people working closely with it. In social engineering activity, it does a psychological manipulation to reveal sensitive information about a person or trick a person do some actions which resulting reveal confidential information. We can use too many tools and tutorials for social engineering an attack on the internet. Some tools are already installed when we install some operating systems like kali Linux, parrot os, etc.

There are many ways to carry out a social engineering attack, and it has enough resources on the internet. Still, there is a low effort the internet community has taken to secure people from social engineering attacks and know them about it. By doing this project, we are trying to create a platform to come up with a platform that helps people to understand how a social engineering attack happens, how the attackers trick them, and make them fully aware of this attack.

Literature

As we already know, social engineering is not a single-step process. First, the attacker comprehensively investigates the victim and collects the information he needs, such as financial information, potential points of entry, and weak security controls. Then the attacker tries to get his attention and trust towards him, trick the victim into breaking his own security controls, and do some actions that give the attacker the necessary information or access.



If we look at the past incidents that happen because of these social engineering attacks, it seems like we still have these types of attacks. Because it uses human weaknesses, we can create a system with

the best security controls and eliminate all vulnerabilities, but humans working there are still vulnerable.

Knowing how the attacker is carrying out this attack is essential to prevent being a victim is necessary. Therefore, we have planned to give critical awareness about how the attacker carries out this attack from our platform. There are several ways a social engineering attack can happen, but we are trying to focus on the most common types.

Product functionalities

We plan to develop a website as our awareness platform while contributing to some of the other GitHub projects. Our web page will look like this when we finish our project.

Desktop view

Mobile view

Via this awareness platform, we are going to implement one section to introduce the social engineering attack and how it works using some videos, diagrams, and questionnaires. We decide to put a questionnaire on this platform because it gives a proper way to measure how the user is vulnerable to social engineering. Furthermore, it inspires the user to follow our program.

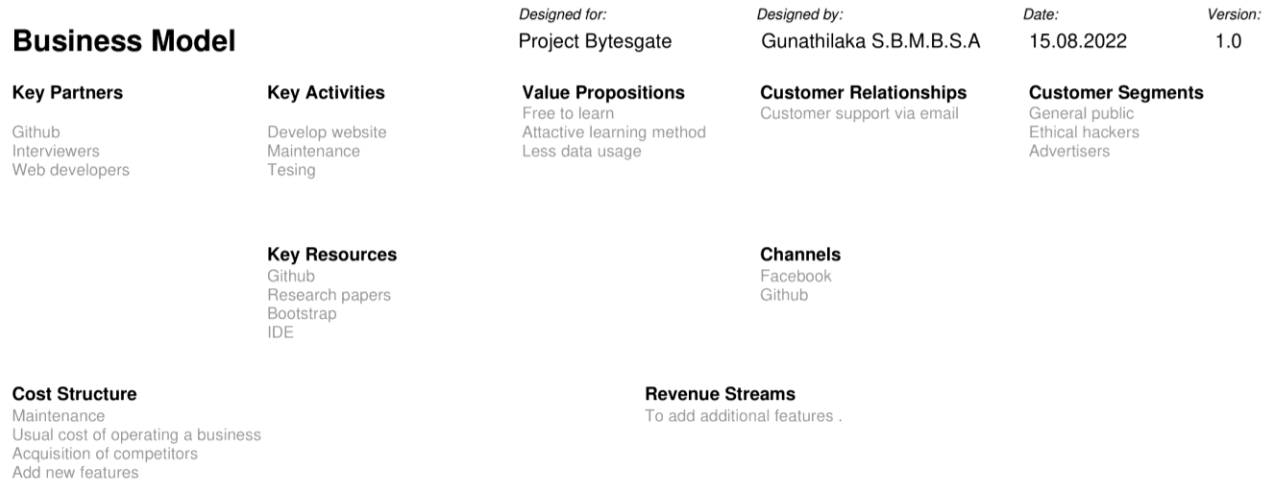
Then the next section consists of attack types and what are the techniques they use to trick the users and earn their trust. After the users go through this section, they will be able to identify an attacker and give some sort of prevention knowledge to users.

In the third section, we have planned a program to teach users how to protect themselves from an attack. Again, we are getting these materials from reliable sources, and we will mention in that section; that these are the sources which give them a chance to learn more.

The final section is not for the general public, but it is a separate section for ethical hackers and red teaming-related people .this section consists of pretexts (made-up stories that social engineers use to convince a victim to reveal secret information or take malicious action.)

Methodology and Business Model

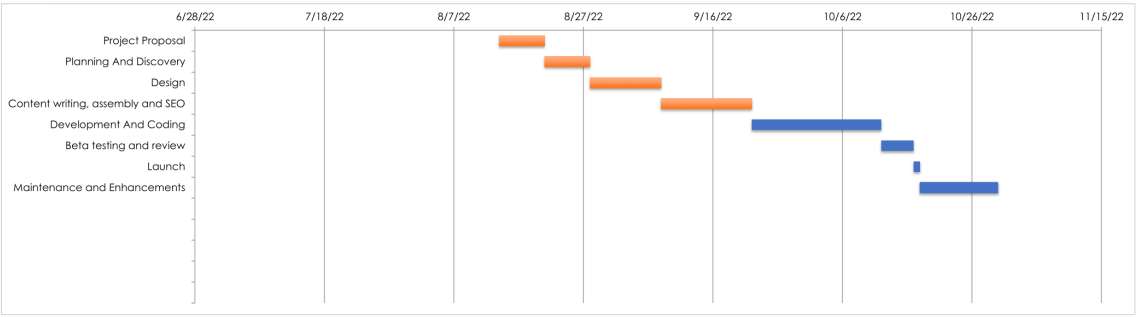
Basically, we are trying to make a website, so we will have to use programming languages such as HTML, CSS, and javascript.to create the appearance of the website and some of the functionalities like tables and buttons, we have to use frameworks like Bootstrap because we need a responsive site that should be rendered properly on mobile devices. So we decided to use Bootstrap, a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains HTML, CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components. We will host our website using Github pages. It reduces the hosting cost and is easy to edit anytime.



Agile project plan

PROJECT NAME	PROJECT MANAGER	START DATE	END DATE		OVERALL PROGRESS
Bytesgate	Buddhika / Chiran	14-Aug	30-Oct		5%

AT RISK	TASK NAME	FEATURE TYPE	RESPONSIBLE	STORY POINTS	START	FINISH	DURATION (DAYS)	STATUS	COMMENTS
☐	Project Proposal		Chiran		8/14/22	8/21/22	7	Complete	
☐	Planning And Discovery		Buddhika		8/21/22	8/28/22	7	In Progress	
☐	Design		Chiran		8/28/22	9/8/22	11	Not Started	
☐	Content writing, assembly and SEO		Buddhika		9/8/22	9/22/22	14	Not Started	
☐	Development And Coding		Chiran		9/22/22	10/12/22	20	Not Started	
☐	Beta testing and review		Buddhika		10/12/22	10/17/22	5	Not Started	
☐	Launch		Chiran		10/17/22	10/18/22	1	Not Started	
☐	Maintenance and Enhancements		Buddhika		10/18/22	10/30/22	12	Not Started	
☐									
☐									
☐									
☐									
☐									



Technology and architecture

Since we are trying to create a website, it requires a front end and maybe a back end according to the upcoming requirements. Therefore we have to use some frameworks like Bootstrap and some languages to develop the front end. In addition, we have planned to use browser optimization technology to speed up the loading and keep the rendering accuracy. Then we have to separate the static and dynamic parts of the website and use technologies specific to that areas .in the static part, we have to implement the website logo, button icons, tables and text areas. For the development of those things, we have to use JS and CSS. Also, the pictures are important to our websites because we put a lot of diagrams .there will be many customizations in that section. Other than that, we need to keep the URL simple and user-friendly .and to keep the ease of use, and we have to create a simple but user-friendly navigation menu.

References

https://www.researchgate.net/publication/355585293_Counteracting_social_engineering_attacks

https://journals.sagepub.com/doi/full/10.1177/0162243921992844

https://www.sciencedirect.com/science/article/pii/S2451958821000749

https://www.mdpi.com/2076-3417/12/12/6042/htm

https://www.sciencedirect.com/science/article/pii/S2214212614001343

https://books.google.com/books?hl=en&lr=&id=9LpawpklYogC&oi=fnd&pg=PT7&dq=social+engineering+research+paper&ots=vcksLYd3SR&sig=jzwB81KZWC7KKyvvIFe-yE7zFuQ

https://search.proquest.com/openview/6535856a33b27389b0f070f8a841c1bd/1?pq-origsite=gscholar&cbl=52433

https://dl.acm.org/doi/abs/10.1145/1059524.1059554?casa_token=izHMiJ3mAOcAAAAA:k7wHC54trT1fXhSVoS2sHmR_V19ZAjZoEK65V5moGu8yGVqjdpX4oT-5mQR-twHySFFJyammFTommVQ

http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf

https://ieeexplore.ieee.org/abstract/document/6950510/?casa_token=bJJfrBabXxEAAAAA:W3pWtYF4SkYkiJufLUGlZa_Om1SnLGmKCzkNWuclO9wNfuPTuFJqX_A0luKcx4mEdSxZhoLRnNvHMvc

https://www.researchgate.net/profile/Nabie-Conteh-2/publication/294421084_Cybersecurityrisks_vulnerabilities_and_countermeasures_to_prevent_social_engineering_attacks/links/56e2733408aebc9edb19eebc/Cybersecurityrisks-vulnerabilities-and-countermeasures-to-prevent-social-engineering-attacks.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail

https://github.com/PreTeXtBook/pretext

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi12Kv229T5AhVmg84BHYuxD8AQFnoECBUQAQ&url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F332151597_Social_Engineering_Attacks_A_Survey&usg=AOvVaw2XtV1vqRXRBlj0qq66BlNr

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi12Kv229T5AhVmg84BHYuxD8AQFnoECAgQAQ&url=https%3A%2F%2Fwww.cmu.edu%2Fiso%2Fnews%2F2020%2Fpretexting.html&usg=AOvVaw3WT5Cfw-byRLvrpnZ7mHHY

https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi12Kv229T5AhVmg84BHYuxD8AQFnoECCUQAQ&url=https%3A%2F%2Fwww.ijstr.org%2Ffinal-print%2Foct2020%2FSocial-Engineering-New-Era-Of-Stealth-And-Fraud-Common-Attack-Techniques-And-How-To-Prevent-Against.pdf&usg=AOvVaw3F4KQ0-gv5W54vJARP610s

https://www.imperva.com/learn/application-security/pretexting/