2017

Can Phishing Education Enable Users To Recognize Phishing Attacks?

Hanaa Alghamdi

Technological University Dublin

Follow this and additional works at: https://arrow.dit.ie/scschcomdis

Part of the Computer Engineering Commons

Recommended Citation

This Dissertation is brought to you for free and open access by the School of Computing at ARROW@TU Dublin. It has been accepted for inclusion in Dissertations by an authorized administrator of ARROW@TU Dublin. For more information, please contact yvonne.desmond@dit.ie, arrow.admin@dit.ie, brian.widdis@dit.ie.

This work is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 License
Can Phishing Education Enable Users To Recognize Phishing Attacks?

Hanaa Alghamdi

D15123687

A dissertation submitted in partial fulfilment of the requirements of Dublin Institute of Technology for the degree of M.Sc. in Computing (Security and Forensics)

2017
I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Security and Forensics), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute’s guidelines for ethics in research.

Signed: _________________________________

Date: 03 January 2017
ABSTRACT

Phishing attacks have increased rapidly and caused many drastic damages and losses for internet users’. The purpose of this research is to investigate on effectiveness of phishing education and training to help users identify different forms of phishing threats. The study has been conducted through developing a phishing quiz mobile application which includes four kinds of phishing threats. It tested the ability of users to recognize spoofed emails, SMS phishing (SMshing), scam phone calls (Vishing), and phishing through social media networks. A comprehensive literature review was discussed to investigate on the research area, understand the research problem, support the proposed research work and identify the research gap to contribute in the body of knowledge. The aim of the study is to measure users’ ability of recognizing phishing threats and evaluate the effectiveness of online anti-phishing educational materials. To achieve this objective, a phishing quiz mobile application has been designed to conduct pre- and post-test experiment to see if there is a significant difference in mean pre- and post-results of participants after phishing education and training materials. The study also addressed the phishing quiz mobile application design and its contents. The research findings revealed that the results of 43 subjects after imparting phishing education to participants, there observed no significant change in the test results. The research discussed factors that may affect the results e.g. difficulty in understanding the phishing educational materials. However, further investigation is needed to tackle these problems and several of avenues for further research are considered.

Keywords: Phishing Attack; Social Engineering; Security training; Spam; Phishing Education.
ACKNOWLEDGEMENT

I am so grateful to ALLAH ALMIGHTY for without his blessing, mercies, and graces I would not be able to accomplish anything.

I would like also to express my deepest gratitude and appreciation to many people for their help, support, and continues encouragement, without which this study would not have been possible.

I would like to thank my parents for their love, unconditional support, having spent all their life taking care of me, and without their faith in me all my success could not have happened.

Special thanks to Dr. John McAuley, my supervisor; for his great suggestions, advices, and very useful comments which have encouraged me and contributed to accomplish this study successfully.

Dr. Luca Longo for the efforts, explanation and suggestions during Research Methods classes.

My brothers Ali and Mohammed, for being such a huge source of support and encouragement that help me to overcome all obstacles I faced during the long journey of my study abroad. Thanks also to my awesome sisters, friends and colleagues.

King Abdullah (may Allah have mercy on him), who established the scholarship program and give me the chance to make my dream true to study abroad.

I would like also to acknowledge DIT academic staff especially my teachers at school of computing for their help, support, and kindness.
# TABLE OF CONTENTS

ABSTRACT .................................................................................................................. II

ACKNOWLEDGEMENT .............................................................................................. III

TABLE OF CONTENTS ............................................................................................... IV

TABLE OF FIGURES ..................................................................................................... VI

TABLE OF TABLES ....................................................................................................... VII

1 INTRODUCTION .................................................................................................... 8

1.1 Overview of the Research Area ................................................................. 8

1.2 Background .................................................................................................. 8

1.3 Research Problem ...................................................................................... 9

1.4 Research Question .................................................................................... 10

1.5 Research Aim and Objective ................................................................. 10

1.6 Research Methodology ............................................................................ 11

1.7 Dissertation Outline .................................................................................. 12

1.8 Summary ................................................................................................... 12

2 LITERATURE REVIEW .................................................................................... 13

2.1 Introduction ............................................................................................... 13

2.2 Understanding Phishing Attacks ............................................................. 14

2.2.1 What is Phishing? .................................................................................. 14

2.2.2 The Reasons behind Why People Fall for Phishing Attacks .......... 15

2.2.3 Forms of Phishing Attack ................................................................... 16

2.3 The Negative Impact of Phishing Attacks ............................................. 22

2.4 Countermeasures for Fighting Phishing Threats ..................................... 22

2.4.1 Technical Efforts to Reduce Phishing Attacks .................................. 23

2.4.2 Educating and Training Users against Phishing Attacks ............... 26

2.5 Summary of Literature .............................................................................. 27

2.5.1 Gaps in Literature .............................................................................. 30

2.5.2 The Research Question Discussion ................................................. 31

2.6 Summary ................................................................................................... 32
**TABLE OF FIGURES**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Framework to identify phishing attacks (mental model).</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>Fake Facebook login page using fake URL (fbstarter.net)</td>
<td>21</td>
</tr>
<tr>
<td>3.1</td>
<td>Some Screens of the Application Initial Prototyping (See Appendix A)</td>
<td>34</td>
</tr>
<tr>
<td>3.2</td>
<td>Flowchart explains how the phishing quiz work</td>
<td>36</td>
</tr>
<tr>
<td>3.3</td>
<td>Application Description on Google Play Store</td>
<td>37</td>
</tr>
<tr>
<td>3.4</td>
<td>Account Login and Sign up Screens</td>
<td>37</td>
</tr>
<tr>
<td>3.5</td>
<td>Survey Screens appears to users who take quiz for first time</td>
<td>38</td>
</tr>
<tr>
<td>3.6</td>
<td>Examples of phishing questions</td>
<td>38</td>
</tr>
<tr>
<td>3.7</td>
<td>Results Feedback to show users the risk level depending on their score</td>
<td>39</td>
</tr>
<tr>
<td>3.8</td>
<td>Result Report Screen.</td>
<td>40</td>
</tr>
<tr>
<td>3.9</td>
<td>Learning Resources Center Screen</td>
<td>40</td>
</tr>
<tr>
<td>3.10</td>
<td>Examples of Educational Materials (Vishing, Email)</td>
<td>41</td>
</tr>
<tr>
<td>3.11</td>
<td>Examples of Educational Materials (Social Media, SMshing)</td>
<td>41</td>
</tr>
<tr>
<td>3.12</td>
<td>Example of Phishing Email which included in the quiz</td>
<td>44</td>
</tr>
<tr>
<td>3.13</td>
<td>SMS which appears from Apple store to hook people</td>
<td>44</td>
</tr>
<tr>
<td>3.14</td>
<td>Example phishing URL using Twitter trying to convince users to click the link</td>
<td>45</td>
</tr>
<tr>
<td>4.1</td>
<td>Responses of subjects of Have you ever heard or know about any of these terms?</td>
<td>52</td>
</tr>
<tr>
<td>4.2</td>
<td>Responses of subject whether they have taken phishing quiz previously or not</td>
<td>52</td>
</tr>
<tr>
<td>4.3</td>
<td>Responses of subjects about educational materials</td>
<td>53</td>
</tr>
<tr>
<td>4.4</td>
<td>Bar chart shows subjects age group</td>
<td>54</td>
</tr>
<tr>
<td>4.5</td>
<td>Subjects Occupation</td>
<td>54</td>
</tr>
<tr>
<td>4.6</td>
<td>Responses about online scams</td>
<td>55</td>
</tr>
<tr>
<td>4.7</td>
<td>Subjects usage of Internet</td>
<td>56</td>
</tr>
<tr>
<td>4.8</td>
<td>Line Chart depicting pre-test and post-test trend</td>
<td>58</td>
</tr>
</tbody>
</table>
TABLE OF TABLES

Table 2-1 Summary of literature ........................................................................................................ 28
Table 3-1 Pre-test questions (Quiz1) ............................................................................................... 45
Table 3-2 Post-test questions (Quiz2) ............................................................................................. 47
Table 4-1 Descriptive Statistics ....................................................................................................... 50
Table 4-2 Mean value .................................................................................................................... 57
Table 4-3 Paired t test differences ................................................................................................. 58
1 INTRODUCTION

1.1 Overview of the Research Area
This research concerns about testing the ability of regular web users to recognize different forms of phishing attacks. The main aim of this research is to determine whether a phishing educational mobile application quiz can help users to identify phishing threats or not. Four forms of phishing attacks were included in this study: Email phishing, Vishing, SMshing, and Social Media scams. The participants recruited for the study were familiar with the web and computers in general but would be considered regular web users and not specific technical experts.

1.2 Background
According to recent research, technology alone is not enough to provide sufficient solutions for IT security issues. So far, little work has been done on training and educating end users on how to cope up with malicious IT threats like phishing attacks (Anderson and Agarwal, 2006; Aytes and Terry, 2004; Liang and Xue, 2009; Susan, Catherine and Ritu, 2006; Woon, Tan and Low, 2005; Workman, Bommer and Straub, 2008; Purkait, 2012).

According to (Gorling, 2006) many researchers have argued that “if we could only remove the user from the system, we would be able to make it secure”. Of course, it is impossible to stop the user, i.e. in home use, training and educating user about security prevention will be the best possible approach (Mitnick and Simon, 2002; Schneier, 2000).

Research has showed that well designed user security education and training can be very useful and effective (Kumaraguru, et al., 2007; Sheng, et al., 2007). For example, contextual or embedded training or web-based educational materials can help users to avoid phishing attacks.

Therefore, this study attempts to find out whether a mobile application quiz is an effective way of educating and training people to identify and avoid different kinds of phishing attacks.

To address the issue, the study focuses on conducting pre- and post-test experiment through developing a phishing quiz mobile app to measure users’ ability of identifying phishing attacks.
1.3 Research Problem
Phishing attack is a dangerous cyber-threat that target computer users and leverage the human vulnerability rather than exploring and exploiting technical errors and weaknesses (Arachchilage, Love, & Maple, 2015). According to (Mann, 2012) the counter measures concentrated on technical aspects although the information security is about a user’s weakness. Many researchers repeatedly mentioned that the most important factor in computer security systems is human-focused (Ciampa, 2013; Howard & Prince, 2010; Whitman & Mattord, 2011; Mitnick & Simon, 2009). That means the users must be trained and educated to ensure that they are well protected and safe when using online services.

Many efforts have been made by information security researchers to develop automated anti-phishing tools to protect and alert users of potentially scams emails or phishing websites. One example of these technical efforts is anti-phishing toolbars, i.e. Anti-Fraud Toolbar, EarthLink Toolbar, Firefox 2, eBay Toolbar and Netcraft Toolbar. However, (Sheng et al., 2010) mentioned that, such toolbars are not sufficient in combating phishing scams. Zhang, et al. has also reported that most of the best anti-phishing tools failed to recognize about 20 percent of phishing websites.

In relation to this, some researchers have also mentioned that well designed end-users training and education can be effective to mitigate such threats (Kumaraguru, 2009). This can be web-based educational materials or embedded training system to protect users against phishing attacks.

One of few examples that enhanced this idea is Anti-Phishing Work Group (APWG). Another example is a mobile game introduced by (Sheng et al., 2007) aims to help users to detect URLs and thwart websites phishing attacks, details about these studies will be discussed in chapter 2.

Nevertheless, it appears that there is a gap in literature where most of the approaches that have been discussed are preventive in nature when it comes to technical efforts. On the other side, the efforts made in the domain of security and training users concentrated on web-based education about email phishing attacks while other forms of such threats should be included. This research focuses on studying how a mobile application phishing quiz can be helpful to educate and measure the ability of users to recognize phishing attacks and training them to stay safe online.
In addition, the research will conclude the findings and provide recommendations for future work to improve the security training and educational methods to be more effective and helpful for regular users. Thus, it is expected that this study will contribute to the subject area of the information security specifically training and education users against online threats.

1.4 Research Question
The research aims to answer and investigate the following research question:

Can Phishing Education Enable Users To Recognize Phishing Attacks?

Specifically, the aim of this research is to evaluate whether a phishing quiz mobile application which also include phishing educational materials can help users to identify different forms of phishing attacks. For example, Email phishing, SMsihng, Vishing, and Social Media phishing threats. All these types of phishing threats will be discussed in chapter 2. In this study, web regular users are targeted that have a normal knowledge about computer science and not expert in IT security.

1.5 Research Aim and Objective
This research aims to investigate the effectiveness and usefulness of creating a mobile application quiz for users to training them about phishing attack. The research also examines whether online phishing educational materials make a positive difference on training users or it just raise their fear of such threats. This will be done by designing a phishing quiz mobile application to create a simple training and educational environment which suits web regular users. This app contains a demographic survey. It also includes the pre-test which examines the ability of subjects before they get any information about identifying phishing scams. The app displays different educational materials resources to train users then let them test their progress by taking a post-test. Lastly, the study aims to analyze the results and test the hypotheses which predict that there is a significant difference in mean pre- and post-results of participants after phishing education and training materials (see chapter 3). It will also provide the findings and conclusion for further research and studies in the future. It is expected that this study will contribute to the information security area specially the field of security awareness and user protection against social engineering. The research objectives are:
• To examine and review related studies which contributed on the field of training users to avoid security threats and help them to stay safe online. Different past studies will be gathered and examined carefully.
• To evaluate the previous knowledge of participants about phishing attack, phishing quizzes, phishing educational materials and how it would be effective for them.
• To test the usefulness of using mobile application environment to conduct such training quiz.
• To test whether this phishing quiz measures the ability of users to identify phishing scams or it just raises fear of falling for such threats.
• To recommend further features and recommendations that could improve the phishing training quizzes, games or systems which was created to educate and learn users to avoid such attacks.

1.6 Research Methodology
The main aim of this research is to determine whether phishing quiz application will be helpful to educate and measure the ability of users to identify different forms of phishing attacks. To attain this aim, pre- and post-test experimental design will be used to conduct the research. According to Dimitrov&Rumrill:

‘Pretest-posttest designs are widely used in behavioral research, primarily for the purpose of comparing groups and/or measuring change resulting from experimental treatments’ (Dimitrov&Rumrill, 2003)

This method used as a measurement of the learning received by participants during the experiment. It will measure their knowledge in phishing attacks before in a pre-test and after the training or learning from educational sources in a post-test.

To achieve this, mobile application will be developed to create a simple educational environment for users. Many reasons were behind choosing mobile application. The most significant reason is the estimation of the number of mobile phone users in the world today is 1.5 billions, which is three times more than the number of personal computers (PCs) (Naismith, Lonsdale, Vavoula, & Sharples, 2004).
A demographic survey will be conducted before subjects embarking on pre- and post-test experiment to collect specific information that will help to get valid results and finding (see chapter 3).

1.7 Dissertation Outline

- **Chapter 2:** This chapter will show the definition of phishing attacks. It will also discuss why people fall for phishing attacks. Moreover, it will give an overview of the forms of phishing and the countermeasures to avoid it. It will review the literatures that discussed both technical and educational efforts to reduce such threats. Lastly, it will discuss the gap the literature and summaries it.

- **Chapter 3:** This chapter will display the design of the experiment and the methodology used to conduct this study. It will also discuss the justification of this design.

- **Chapter 4:** This chapter will illustrate the findings and analysis of the experiment. It will also present the discussion and evaluation of these results and findings.

- **Chapter 5:** This chapter will summaries the research and concludes it by showing an overview of all the work that has been done during this study. Moreover, it will discuss the research findings, future work and recommendations.

1.8 Summary
This Chapter has provided a brief overview of the research topic, and discussed the relevance of phishing attacks, specially educating users how to recognize phishing scams through mobile application quiz. This research aims to contribute to the field of user training to avoid online threats by providing a detailed evaluation of how can a mobile app quiz help users to stay safe online and update their information about phishing threats to avoid it in the future. To achieve these objectives, the next chapter will discuss past studies on phishing attacks, forms of phishing attacks, the technical efforts has been made to avoid such threats and lastly the training and educating users methods.
2 LITERATURE REVIEW

In this chapter, current approaches to the education of phishing will be addressed. First, an overview about phishing attack, what is it, why people fall for phishing, forms of phishing threats, and negative impact of security scams will be addressed. Next, countermeasures to reduce phishing threat both technical efforts and training approaches will be discussed. Finally, summary, gap in literature and research question discussion will conclude this chapter.

2.1 Introduction

The world today is developing very rapidly, particularly when we talk about technology. Almost every person depends on the Internet and numerous other organizations and corporations, in order to make use of them. Due to the convenience, ease, and portability brought forth by the Internet, people can shop, attain countless services and buy goods. They also can get educated online and the list of the advantages of the Internet goes on. Today, from a child to grown-ups to elderly people all of them rely on and benefit from online services. The facilitative ease that has been brought forth by online commerce is embraced not only by consumers but by criminals as well.

Phishing is a method used by cybercriminals to steal personal credentials and information through the Internet in order to use that for financial fraud. Over the years phishing has become a very drastic criminal act on the Internet. However, a great amount of work has been carried out when it comes to identifying phishing threats. To identify the hazards that can be caused by phishing, people involved in businesses, customers and consumers ought to be educated. On the other hand, an increase in the diversity of phishing attacks and the sophistication in technical knowledge attained by individuals who conduct online crimes, for instance, financial frauds via phishing have been witnessed. Phishing negatively influences the economy via financial damages; that are faced not only by businesses but by consumers as well. Phishing scams can reduce people’s confidence in commerce when the Internet is involved. There has been a large increase in the variety of phishing attacks. The technical equipment that is needed to implement the phishing attacks can be easily attained as they are available via private and public sources.
The automation and streamlining of some of the technical equipment have allowed them to be used even by non-technical cybercriminals. Due to the fact that these technological resources are readily available increases the number of phishing attacks. This activity of making individuals believe that they are giving their credentials to a trusted party while they are really giving their details to thieves is not new. Since the Internet has been introduced social engineering scams have been occurring. Before the Internet was accessible to the common man, what criminals did was that they misused the telephone in order to disguise like trusted agents and attain sensitive information. The word “Phishing” has been originated from the mid-1990s, back then it was used to illustrate the attainment of the account information of the ISP or the Internet Service Provider. But today, the word has completely changed to include various scams and attacks which are used to aim at personal information.

In the literature of this paper numerous technical capabilities which can be made use of to implement phishing attacks have been identified. Moreover, the ways that can be adopted in order to get protected from such scams have also been discussed in detail. The literature extends to concentrate on the training methods and techniques that are presently used to educate users in order to protect them from phishing scams and consequently from financial and reputational loss.

2.2 Understanding Phishing Attacks

Despite the fact that a substantial interest in phishing as a potential security issue, there is a need to examine the human factors of such attacks. Particularly the experimental or empirical grounds and support for how effective and influential phishing is, and hence exploring ways of developing defense mechanisms against it.

2.2.1 What is Phishing?

A phishing attack can be termed as a kind of social engineering and online spoofing mechanism. In this kind of attack the offenders or attackers trick the users and make them disclose their sensitive or private information. One other major threat that can be caused by these attacks is that attackers make users install malware on their computers (Hong & Hong, 2012). Phishing attacks are directed to reveal and access confidential information for instance credentials, credit card regarding information, in order to make use of these data maliciously. What phishers do is that
they always make their victims believe that they provide trustworthy services in electronic communications.

Phishing has the potential of not only ruining a company’s reputation but its financial position in the market as well; it can have a severe negative impact on banks, organizations, and marketing and customer relations. Phishing attacks can be carried out through e-mails, social networks, phones and instant messages. In all cases, phishers imitate a trusted medium (for instance a bank’s helpdesk, a retailer’s automated support response etc.) and hence the victim believe that it is their trusted source they are sharing their sensitive information with (Ollmann, 2007).

2.2.2 The Reasons behind Why People Fall for Phishing Attacks

Many users fall for phishing attacks simply because they lack knowledge on how to make online trust decisions. Psychological studies have illustrated that people who are under stress do not take the options in their consideration when they make decisions. They also tend to make irrational decisions and ignore all possible solutions (i.e. accessing e-mail when they are busy at work)(Keinan, 1987). Dhamija et al. conducted a laboratory study where he found that 90% of 22 participants became victims of sophisticated phishing websites. He found that the reason behind that is 23% of the participants ignored the browser cues like status and address bar or the other security indexes. Dhamija et al. also classified the reasons why do people fall for phishing scams into three groups: lack of knowledge (about computer systems and security indicators), visual deception (Visually deceptive text, deceptive look and feel of images and logo), and bounded attention to absence and presence of security indicators (Dhamija, Tygar, & Hearst, 2006).

Milletary mentioned that cybercriminals take advantage of the increase in online services and every day or routine activities which include: online banking, shopping and leisure services, to collect user’s sensitive information. Along with that increase, they rely on three main factors: users’ unawareness of phishing threats, victim’s unawareness of organizational policies, and criminals’ leveraging from the technical sophistication (Milletary, 2005).

Cyber criminals target users’ information in order to benefit from this amplified acceptance and adoption of services that are made possible by the Internet. These services are day-to-day activities, for instance, shopping, banking, and other leisure acts. Phishers are enticed by users
who want to avail these services because they provide phisher with an opportunity since they have valuable information. Beside a severe escalation in the quantity of potential victims, the following three key factors can be termed beneficial for the phishers.

**Users with no awareness about the scam:** When the users are not aware of the fact that their personal information may actively be targeted by cyber criminals, they will not be able to recognize phishing hazards. Such users may also ignore the precautions that are mandatory while involving in online activities.

**Users having no policy awareness:** Phishers find it extremely enticing when their targets have no policy awareness about their organization. Sometimes customers do not even know what procedures to follow when they contact customers specifically regarding problems of fraud investigation and account maintenance. Those customers who are not aware of an organization’s procedures are more possibly to be targeted by phishers no matter they possess technical knowledge.

**The technical sophistication of criminals:** Activities for instance: DDoS or Distributed Denial of Service attack, spamming, and electronic surveillance are technically difficult but have been proven to be performed by technically sophisticated criminals. Today, customers have realized that these scams are extremely dangerous. However, phishers have developed more technical deceptions in order to make the phishing scams more effective and deceptive (Milletary, 2005).

### 2.2.3 Forms of Phishing Attack

Lately phishers have been making use of various channels, these channels range from instant messages to e-mails, the facility of phone (with text messages and calls), and Social Networks. These channels are exploited to trap more and more victims. Subsequently, the modern day has become a multi-faceted or tiered and more prevalent threat and according to studies the modern day phishing is extremely difficult to analyze (Maggi, Sisto, & Zanero, 2011).

1. **Emails Phishing Attack**

Today, the importance of making use of e-mail is extremely significant, and almost all the people throughout the world need to use it for either personal or business use. The fact is that anyone who has used e-mails could be potential target for the cybercriminals. To distinguish between a
clean e-mail and a phishing e-mail according to (Ledford, 2013; Wang et al., 2012), the following important signs have been identified which can help anyone to identify a phishing e-mail. These signs are:

- Using urgent words in messages: Attackers usually use words that show urgency and make the victims get results very quickly.
- It includes a request of sensitive and personal information: This is the aim of most attackers to deceive their targeted victims into trusting them to gain their personal details.
- Unknown Sender: However, there is a type of phishing attack called spear phishing, this kind of phishing attack is more concentrated and what the attacker does is that within the same corporate domain they impersonate a co-worker.
- Has a fake Hyperlink: Phishing mails usually have a fake hyperlink that takes the victim to a spoofed phishing website.
- The contents of the mail are structured using poor language and it usually contains spelling and grammatical errors.
- Contains images and logos to visually represent impersonation.
- The attachments in the mail are designated to make the victim install malware on their computers.

A framework developed by (Lötter & Futcher, 2015) has been presented in this manuscript which would help us identify spoofed e-mails. The framework as shown in figure (2.1) is entirely based on the common signs that are contained by phishing attacks and it demonstrates the danger of phishing attacks to the users of e-mail. It includes nine steps that email users should ask themselves so they can determine whether an email should be trusted or not. Despite the fact that this framework was initially created to be benefited from as a mental model by e-mail users, small alterations can be made to it in order to implement it for e-mail clients. Users should be enabled to visually see the security status the whole time. Increasing awareness in users is one of the most important ways of successfully mitigating phishing attacks.
Figure 2.1 Framework to identify phishing attacks (mental model).

Source: (Lötter & Futcher, 2015)
2. Vishing

Vishing is the term used to illustrate the practice of using voice messages based on IP (i.e. VoIP or Voice over Internet Protocol) in order to socially plot a targeted user and make them reveal their financial, personal or any other kind of confidential details to gain some financial benefit from it. The stated term has been derived from two different words i.e. voice and phishing. Since the invention of the telephone landline, telephone systems have been used to persuade individuals to do something. The current enormous upsurge in the Internet Protocol telephony destines that most of the telephone services may be started or ended from PCs that can be located anywhere in the world. Moreover, the expense at which these telephone calls are made has decreased down to be very little. This grouping of aspects and factors has turned it into a practice that is financially implementable and enticing for phishers, and they can leverage VoIP in the attacks they plot. The fact that Vishing is likely to have an even greater success rate than those of other phishing methodologies is supported by the following points:

- The trust record of telephone systems is way longer than the new messaging techniques which rely on the internet.
- The number of people that can be accessed via the phone is greater than that via e-mail.
- The automated systems used to validate phone have attained a widespread adoption and generic recognition and approval.
- The users of telephone can be classified into a particular population groups for instance the elderly, who can be termed as more accessible.
- Message timing can be made use of in order to increase the chances of success.
- Telephones are a great way of personalizing the message of social engineering.
- The most interesting fact is the rapid increase in the number of call centers which points to the fact that people can actually trust strangers who might appear to have accents. Once they start believing in you they can share their confidential information as well.

Despite the fact that numerous ways are available to phishers with which they can conduct their scams, however, understating the types of information which can be attained by the attackers
with ease when IP telephony is leveraged. Naturally, information that involves numbers is more likely to be handed over by the victim when they are replying to vishing attacker while using a mobile phone (Ollmann, 2007).

3. SMishing

This phenomena which is termed as Smishing, the word has been derived from the combination of two words i.e. SMS and phishing, is an indicator that mobile phones have become another way of exploitation for criminals.

The amount of damage that has been caused by Smishing has increased abruptly over the last few years. Thievery of personal information and causing direct financial injury in association with graphics sewing machine hacking is occurring. Studies have been done to analyze laboratory examples of actual breach to the security systems. For instance, one study is used to analyze the breach in vinegar sewing machine hacking system has been analyzed which is a foremost measure of security that intends to prevent the damage that has been done to the system of payment. The study analyzes and conducts a thorough research in order to discover whether smart phones can be used to implement a safer and convenient way of enforcing online payment or not (In-Woo &Dea-Woo, 2013).

4. Social Media Phishing

As the name suggests, it means kind of phishing that has been carried out via the social media. Provided the fact that phishing attacks have been conducted to take benefit from not only technical but also social vulnerabilities, there are numerously different attacks.

Phishing attackers can refine and improve their tactics through the use of readily and publicly available information from the greatest source i.e. the social media. The essence is to make use of people’s social contacts in order to surge the magnitude of such attacks and it is analogous to the technique where the “ILOVEYOU” virus utilized email address books in order to virally propagate itself. One study carried out extensive research to find out that how easy and effective it is for a phisher to abuse the data that are available on social networks. The study concludes that it is extremely easy and indeed very effective. Studies also found that users of the internet are four times likely to become the victims of phishers particularly if they have asked by people
who appear to be their known acquaintance (Jagatic, Johnson, Jackobson&Menczer, 2007). For example, users of Facebook receive a message from someone on their friends-list where they are urged to “check it out” and which include a link to some webpage. The webpage appears to be a Facebook login page; however it is a forged website and is used to steal users’ information as they type in their credentials. Once the user clicks on the worm it propagates itself to the friends-list of the user as well. It is reported that one of the web addresses used for such purposes was “fbstarter.net” as it can be seen in figure (2.2).

![Fake Facebook login page using fake URL (fbstarter.net)](image)

**Figure 2.2 Fake Facebook login page using fake URL (fbstarter.net)**

Facebook finds out about the phishing attack either through its users who notify Facebook or its employees who notice that some different URL has been propagated to users. What Facebook does is that it deletes the URL, does not allow such postings, and also eliminates the redirect to the URL (Mills, 2009).
2.3 The Negative Impact of Phishing Attacks
Studies reveal that phishing attacks have caused some drastic damages and losses. APWG or the Anti Phishing Working Group began tracking data in 2014 and it revealed that as compared the rest of the years or their quarter in the first quarter (Q1) of 2016 there have been more phishing attacks. APWG reported that there has been an increase of 250 percent in the number of phishing websites from October 2015 to March 2016. In Q1 of 2016, the APWG has detected a splendid 289,371 different phishing websites, among which 123,555 websites have been reported in March 2016 only. On the contrary only 44,575 distinct phishing websites have been reported in November 2015.

Phishing attack is one of the most popular cybercrimes and forms of a serious threat to all the facets of any country’s economic activity and this threat is more pronounced in financial institutions (Mugari, Gona, Maunga, & Chiyambiro, 2016). Phishing influences an organization’s economy negatively by bringing financial losses for both businesses and costumers. It also damages the customer confidence or loyalty in commerce when the internet is involved. These drastic scams have increased in number as they have been successful in recent years because conditions for them have been favorable in terms of both economics and technology. Technical resources that are required to make phishing attacks possible can be attained without any difficulty via private and public sources. Criminals who are not so good with technology can also execute phishing attacks as some technical means have been automated and streamlined. Because of this phishing execution has been made not only economically but technically practical for people who are not technically expert (Milletary, 2005).

2.4 Countermeasures for Fighting Phishing Threats
Researchers have been proposing and implanting different kinds of strategies to protect regular web users from phishing attacks. There are two main categories of methods: the implementation of technical procedure, and educating users so that they do not fall for phishing attacks (Kirlappos&Sasse, 2012). Numerous solutions have been proposed and developed to minimize the damage that has been caused by phishing scams. Both technical and non-technical areas of problems have been targeted via these solutions (Milletary, 2005). This section will discuss both technical and non-technical aspects, identifying current trends and areas that have been neglected.
2.4.1 Technical Efforts to Reduce Phishing Attacks

There are number of different technical solutions available, all require some level of technical implementation and more importantly awareness of the issue of phishing in the first place. In this section, different technical solutions are reviewed, most importantly web browser toolbars, strong authentication and authorization, and spyware prevention.

2.4.1.1 Web Browser Toolbars

The warnings that are displayed on the security toolbar or the security related information in the interface of the web browser is what many proposals rely on to stop phishing scams. Two studies were conducted by Wu et al. on three different toolbars of security, address bar of the browsers, status bar to test whether they protect the web regular users from phishing attacks or not. Keeping the severity of damage that has been caused by phishing scams in mind, what they disclosed was not surprising. They found that these in placed security measures are ineffective when it comes to preventing users from becoming victims of phishing scams. They also discovered that many of the people who took the test did not pay any attention to the security warnings prompted by the toolbars. Some subjects ignored it because they thought the contents of the webpage seemed legitimate (Wu, Miller, & Garfinkel, 2006).

Cranor et al. conducted a study where they tested the efficiency of about 10 toolbars of security. They discovered that 3 out of those 10 toolbars successfully identified more than 75% of the phishing sites that were tested on them. Furthermore, 4 out of those 10 security toolbars could not identify about 50% of the sites that were tested on them. They concluded that there was an issue in the plan and design of these resolutions, moreover, further work should be done in order to improve the efficiency and quality of their results (Cranor, Egelman, Hong, & Zhang, 2007).

Despite the fact that toolbars of security have many advantages, however, they are still suffering from numerous disadvantages that let loose of the users and gradually those users become victims of phishing scams (Abu-Nimeh & Nair, 2008).

2.4.1.2 Strong Authentication and Authorization

The inability of users to differentiate among the right and spoofed websites is what entices the phisher and that is what they take advantage of. Recent work has shown that users should be educated about this distinction but the hard part is that on every occasion users ought to make the right decision. However, with humans come some limitations one of which is that they are not
best suited to perform security checks. These security checks are significantly needed to identify secure sites, to avoid compromising users’ account not even one mistake can be made. Essentially, users ought to be authenticated with the help of information that may not be revealed readily by them to parties which may use it for hazardous use. This can be achieved if security is not relied on users and at the same time the process of authentication is enhanced to ensure maximum security and frauds are eliminated.

Studies propose a device which is said to be trusted and which performs a kind of authentication that is mutual i.e. eliminating the reliability on the perfect and aware behavior of users and the Man in the Middle kind of attacks are prevented, and despite the fact that threats may be present the users’ privacy is protected. Studies have demonstrated the usability, reliability, feasibility and practicality of this system by means of a prototype implementation (Parno, Kuo, & Perrig, 2006).

However, more studies reveal that when phishing threats are involved the web browser is particularly targeted by criminals in order to interrupt information that is sensitive while it has not left the computer of the customer. Moreover, realizing the significance of transactions’ authorization is extremely necessary. Majority of the phishing threats and attacks aim at the information of authorization due to the fact that it is comparatively easier, simpler and cheaper and it pays of really well for them. But with the implementation of the two-factor authentication these scams can change their strategy and aim at the shortcomings residing in the authorization.

Businesses are trying to increase their customers’ awareness about the danger of phishing and also regarding their business practices and policies of how they contact their customers. The need of enabling customers to verify the validity of communications that are carried out electronically is still felt.

A specialized kind of malware has also been observed which is used to target sensitive information and which possesses higher potential threats. The means of creating hazardous phishing scams is provided by malware to the criminals, and with that help of that they can victimize numerous businesses simultaneously. Malware is developing to attain specific information that is sensitive and which has particularly been created to authorize online transactions of commerce.
Another kind of authentication that can be utilized to increase security is the Two Factor Authentication, which requires multiple authenticators. This can have information like password or PIN or something that can be possessed for instance hardware token or a credit card. When online commerce and transactions are involved, the two-factor authentication can be made use of in a way that the customer is given a hardware token to generate a frequently altering component to authenticate their credentials. The objective is to provide the user with a secure medium and protect them from loss even if their credentials were stolen by criminals. The correctness of the altering component is what reduces the ability of the attackers of using the customers’ credentials. However, there are some loopholes which can initiate funds transfer from authenticated sessions; these theoretical possibilities need to be tackled.

One other robust solution that has been made use of by banks for authenticating their customers is TANs or transaction numbers. Customers receive a collection of TANs along with monthly statements from their banks, and what they do is that they provide an unused TAN when they have to make an online transaction. Users can be tricked here as well; they receive requests asking them to reveal their TANs. These requests are sent to them via an out of band procedure for instance a text message on mobile, as studies suggest some kind of phisher is always there to trick the customers in order to divulge their TANs. In case the criminal succeeds in acquiring the TAN they have a limited but definite time to benefit from the user’s bank account (Wu et al., 2006).

### 2.4.1.3 Virus, Spyware, and Spam Prevention

A common definition for spam does not exist, but majority of the sources approve the core idea of the phenomenon that such messages are not solicited. Spam may lead to numerous issues not only unethical but can uneconomical as well, resulting in particularly in the efforts of prohibiting spam. The most famous and well developed technique to anti-spamming is a filter that is based on learning. Currently, filters use machine learning, and artificial intelligence’s algorithms and classification techniques, Naïve Bayes is said to be the best one (Blanzieri&Bryl, 2008).

Some phishing scams are technically very strong and use known shortcomings that reside in famous web browsers for instance the Internet Explorer in order to install malicious software (that is malware) for collecting sensitive information about the target. Key logger is one example
used to make a log of all keys that are pressed when users visit a particular website like a bank’s website (Kirda & Kruegel, 2005).

Solutions that aim at protecting users from Trojans, viruses, spam and spyware play a significant role when it comes to phishing threats. With the noticeable surge in malware, products that are used to detect and avert the installation and implementation of code that is malicious are extremely necessary portion of environments for securing home computing (Wu et al., 2006).

2.4.2 Educating and Training Users against Phishing Attacks

Anti-phishing researchers have developed different methods to help internet users recognize and avoid phishing attacks. Much of their work focused on developing techniques to warn users about phishing websites. However, less effort has been concentrated on training users and educate them how to identify such threats. The most important dos and don’ts of getting protected from phishing scams are listed below which should be known by every user.

Dos:

- Security browsers and software should be kept updated all the time.
- Links should be hovered over in order to tell obvious fakes, and it should be made sure that the embedded link is actually taking us to the very link it appears to be.
- E-mails should be inspected for obvious red flags.
- Rather than clicking on some link that has been sent in an e-mail visit the website.

Don’ts:

- Blindly trust unknown senders and click on links sent by them.
- Send suspicious e-mails to friends and family.
- Download material that is identified by your browser or software of security to be malicious.
- Provide information like credit card or social security card numbers, or home address to sites which you think may be suspicious (Mary & Molly, 2015).

A study used a game to train users so that they can identify phishing scams, it also conducted a user study where the efficiency and effectiveness of the game. The stated made use of online
training materials and a video tutorial was made that was founded on the game. The study discovered that those participants who played the game actually performed did better than recognizing the phishing sites than those who received two different kinds of trainings. The results of the study reveal that interactive games might turn out to be an auspicious way of training users to dodge phishing threats (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007).

Users should be trained so that they do not blindly follow links to websites, particularly, where they are used to provide their credentials is the most effective remedy of phishing threats. But, thinking that the entire group of users will perceive and understand the threats of phishing and browse accordingly is not realistic. If it is stated that there will always be some users who would be made to believe that some fake websites are real. Hence, it is significant that researchers and practitioners to deliver viable solutions for tackling phishing hazards (Kirda & Kruegel, 2006).

### 2.5 Summary of Literature

A rapid development can be witnessed in technological world, almost all people now depend on technology and particularly the internet has turned out to be very essential. Not only people, but organizations and corporations use the internet because of the ease, facility, portability and time saving that has been provided by it. The normal users use it to shop and acquire a vast range of other facilities from it, and people aging from 2 years old to elderly people are fond of the internet. However, the facilitative ease that has been brought forth by online commerce is embraced not only consumers but criminals as well. One such thing that has been a vital source for cybercriminals is phishing, which is a method used by them to steal personal credentials and information through the world of the Internet in order to use it for financial fraud. Over the years phishing has become a very drastic criminal, particularly act on the Internet. A great amount of research has been carried out when it comes to identifying phishing threats. To identify the hazards that can be caused by phishing, people involved in businesses, customers and consumers ought to be educated. On the contrary, a surge in the diversity of phishing attacks and the sophistication regarding technical knowledge is attained by individuals who conduct online
crimes such as financial frauds via phishing has been witnessed. What phishing does is that it negatively influences the economy by financially damaging not only the businesses but the consumers as well. Phishing damages have decreased the amount of faith and confidence they had in online commerce. Phishing attacks have been increasing because of the favoring technological and economic conditions. The technical equipment that is needed to implement the phishing attacks can be easily attained as they are available via sources that both private and public. There are numerous kinds of phishing i.e. emails phishing attack, vishing, smishing and social media phishing. A vast amount of research has been conducted in order to tackle this problem but there still is some research gap and further work needs to be done. Table 2.1 discusses the summary of literature.

Table 2.1 Summary of literature

<table>
<thead>
<tr>
<th>Summary</th>
<th>Method used to train user</th>
<th>Results</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>A game was used to train users so that they can identify phishing scams, it also conducted a user study where the efficiency and effectiveness of the game.</td>
<td>A game was used to train users, and afterwards a test was taken from the participants. There were two kinds of participants: the ones who played the game and others who were given eBay’s and Microsoft’s tutorials.</td>
<td>The results of the study reveal that the gamers’ performance (87% accuracy) was better than those who studied the tutorials (74% accuracy). The pre-test results of the gamers were 69% accurate while those of the non-gamers were 66% accurate.</td>
<td>Games can assist in teaching and educating users about phishing scams identification (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong &amp; Nunge, 2007).</td>
</tr>
<tr>
<td>Intel Security released the findings of their</td>
<td>No Training provided.</td>
<td>Out of the approximately Nineteen and a half</td>
<td>97% Of People Globally Unable to Correctly Identify</td>
</tr>
<tr>
<td>Study</td>
<td>Method</td>
<td>Results</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>A phishing quiz which tested consumer knowledge of, and ability to detect, phishing emails. It included 10 questions that were accumulated by McAfee Laboratories.</td>
<td>thousand respondents merely 3% could recognize each e-mail correctly,</td>
<td>Phishing Emails. Games and apps do need to be developed in order to train users (Mary &amp; Molly, 2015).</td>
<td></td>
</tr>
<tr>
<td>A study of phishing attacks and browser anti-phishing defenses, 27 users each classified 12 web sites as fraudulent or legitimate.</td>
<td>Trained in the use of green address bars (indicating extended validation certificates that appear only at legitimate sites).</td>
<td>Training caused more real and fraudulent sites to be classified as legitimate (Jackson, Simon, Tan &amp; Barth, 2007)</td>
<td></td>
</tr>
<tr>
<td>A study was conducted where 40 subjects were asked to answer a set of questions from residing phishing IQ tests.</td>
<td>Trained participants were more likely to classify the real, confusing site as legitimate as compared to the untrained users.</td>
<td>The results of the two tests implicate that the participants did not get better after educated about phishing; they became more suspicious to all stimuli that were shown to them in the post and ended up falsely labeling many legitimate stimuli as phish.</td>
<td></td>
</tr>
<tr>
<td>The participants were asked to take a phishing IQ test pre and post to being educated on phishing.</td>
<td>Merely educating users about phishing increases the level of suspiciousness of the user. It does not make them better at recognizing what is a phish and what is legit (Anandpara, Dingman, Jakobsson, Liu &amp; Roinestad, 2007).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.5.1 Gaps in Literature

Techniques that are used for anti-spamming purposes for instance filtering might not be very useful when issue of phishing detection is involved. Filters are mostly made use of for classifying the contents of e-mails founded upon the incidence of specific kind of keywords. These filters might evaluate words incorrectly which seem to have appeared in other e-mails which had not been labeled as spam previously. Furthermore, as time passes and technology finds out more efficient and better ways of recognizing spam and fraudulent e-mails and not letting it bother anyone, phishers are also going to find new ways to deceive technology and hiding their purpose. What else can happen is that the user might not opt for using the spam filters, or may not remember to update the filters every time it needs to done, the result will not be different and the user may become a victim of phishing. Users’ permanent and persistent trust can only be gained if the filter is reliable and consistent with its results. The most derailing drawback of these filters is that they can term a normal and useful e-mail as a false positive and that makes a user lose faith in the filter. Filters have caused trouble and inconvenience to users by numerous labeling a legit e-mail as a spam one. If such kind of events occurs the users might not be willing to use the spam filter (Olivo, Santin & Oliveira, 2013).

Furthermore, if the attackers equip themselves with the ability of targeting a class of with great effect for instance, spear phishing most of the phishing and spamming filters will not be able to screen out the hazardous e-mails (Brody, Mulig & Kimball, 2007).

In order to win the battle against phishing revising the standards of e-mail could be significantly effective. However, some studies suggest that the way e-mails work should be altered. But amending and making changes to the way e-mails are sent and received may consume years. This idea of changing the whole process of e-mailing is neither very wise nor feasible and entirely relying on it for tackling the issues caused by phishing (Liao & Luo, 2004).

The most significant aspect of filters is that their nature is reactive and as a consequence only some of the spam e-mails could be prevented from reaching the users, while some of them can still reach the users. These techniques cannot stop phishers from sending spam e-mails to the users. Some studies suggest the use of digital signature, but that for entire community of Internet
users becomes a very expensive proposition. Not only that but these signatures may also result in a bottleneck for people who use multiple computers to make use of their e-mail (Garfinkel, Margrave, Schiller, Nordlander & Miller, 2005).

Most of the approaches that have been discussed in this literature review are preventive in nature. What a phisher does is that he principally goes after the naïve users. These naïve users can at times be termed as the most fragile link in the chain of security. Multiple usability studies reckon and conclude that neither client side warnings and toolbars nor server side security pointers can be completely successful when it comes to preventing susceptible from deception (Purkait, 2012).

2.5.2 The Research Question Discussion

Can Phishing Education Enable Users To Recognize Phishing Attacks?

One study describes the strategy and evaluation of Anti-Phishing Phil, which is an online game which aims to teach users good ways in order to assist them in avoiding phishing threats. They used the principles of designing and iteratively refining the game. The game has been evaluated via a users’ study: participants took a test based on their ability to recognize fake and deceitful web sites both pre and post to spending about 15 minutes of engagement in one of the three anti phishing activities of training (which were reading a tutorial on anti-phishing which was created on the base of the game, and/or reading residing online materials of training, and playing the game). The study discovered that those who participated and played the game were significantly better in identifying those websites were fake in comparison to those who did not play it. The study attributed this impact to both the material of the training messages offered in the game and also to the presentation of the contents in a good and interactive format of game. The results of the study can be used as an efficient and influencing way of making the people aware regarding phishing and other such security threats (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007).
A study survey that was conducted by Intel Security disclosed the results of their survey; the survey took a quiz from its participants. The quiz was conducted from December 2014 till February 2015. It included 10 questions that were accumulated by McAfee Laboratories. The total number of participants who responded to the quiz was 19,458 who belonged to 144 different countries. As stated earlier the quiz had 10 emails which were compiled by Intel Security and respondents were inquired to recognize attempts being made for phishing purposes like stealing information and others which were in fact real and legit. Out of the approximately Nineteen and a half thousand respondents merely 3% could recognize each e-mail correctly, around 80% of the whole lot of respondents could not correctly identify at least one of the phishing examples, and that is what is required to turn a user into a victim.

If we talk about global facts and figures regarding phishing, the age group between 35-44 years was the best to answer and they secured a mean of 68% of all the questions correctly. Women on the other hand, under 18 and over 55 seemed to be having a difficult time when it came to distinguishing between phony and legit e-mails. The stated group of women on average could only identify 6/10 messages correctly. While talking about men, they seem to have done slightly better on average with 67% of accurate results (Mary & Molly, 2015).

While keeping the difference that is present between the two results of these papers, we can conclude that identifying phishing scams and threats can only be done via proper user training. The users especially the normal users should be trained and educated about the phishing scams, and in order to make them aware the extent to which phishing scams can be severe and hazardous should be told to them. For that purpose a mobile application can be developed, which would be used to train users, moreover, the results of (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong &Nunge, 2007) reveal that making it fun or turning it into a game might actually help. The same app can then be used to test their ability of whether they can successfully differentiate between real and fraudulent scams or not.

### 2.6 Summary

This chapter reviewed literature in phishing attacks and the countermeasures to avoid it, specifically phishing education and training approach. It provided a summary of literature and a discussion of research question to fulfill the gap in literature.
3 RESEARCH METHODOLOGY

3.1 Introduction
In the last chapter the current approaches of education of phishing have been addressed. The following chapter will discuss research methodology. First, it will give an overview of application design. Second, it will explain the design of experiment by providing demographic survey and pre- and post-test method. Finally, the analytical procedure applied to collected data will be presented.

3.2 Application Design
Mobile application environment has the “mobility” which is a significant feature such as mobility of user, device and services. This feature enables users keep contact everywhere and all time whenever they want. For example, users can play a game on their mobile devices while waiting in a queue or traveling on a train (Parsons & Cranshaw, 2006). Moreover, there are estimation of the number of mobile phone users in the world today is 1.5 billions, which is three times more than the number of personal computers (PCs). Today’s sophisticated phones and their processing power which compete most of PCs one, lead some observers to say that many users will start to see mobile devices as an alternative to a personal computers (Naismith, Lonsdale, Vavoula, & Sharples, 2004). A previous study conducted by Anandpara et al. claims that phishing IQ tests like Sonic Wall do not measure the ability of users to identify phishing attacks. They claim that phishing education makes people more paranoid about such threats, and that phishing IQ tests measure their fear and not the ability of recognizing phishing attacks (Anandpara, Dingman, Jakobsson, Liu, & Roinestad, 2007). In this research and to accomplish the study, a phishing quiz mobile application was developed to answer the question: Can Phishing Education Enable Users to Recognize Phishing Attacks? Next section will give an overview of the phishing quiz app prototyping.

3.2.1 Prototype Development
This section shows the initial prototype of phishing quiz application. The principle focus of designing the phishing quiz app is to create a better educational environment for users to learn how to identify phishing attacks. Also, to see whether such quiz measure their ability of recognizing online security threats or not. Figure (3.1) below shows some screens of the
application initial prototyping using Justinmind prototyping tool which has the functionality to create mobile wireframes within the platform itself.

Figure 3.1 Some Screens of the Application Initial Prototyping (See Appendix A)
3.2.2 Quiz Flowchart and App Contents

This app is a simple educational environment which designed to suit all users. It has been designed using Unity3D\(^1\) which is a game engine that enables developers to create games and deploy them to a number of different devices including web, PCs, iOS, and Android (Creighton, 2010). The flowchart below figure (3.2) represents the phishing quiz app process and how it works.

Figure 3.2 Flowchart Explains How the Phishing Quiz Work
How it works:

The application is published on Google Play Store for all users as it can be seen in figure (3.3).

![Application Description on Google Play Store](image)

**Figure 3.3** Application Description on Google Play Store

![Account Login and Sign up Screens](image)

**Figure 3.4** Account Login and Sign up Screens

When a user installs the app, he/she can register a new account or login into an existing one as figure (3.4) illustrates. Each user has a user name and password so he/she can login anytime to take the quiz and learn from the phishing educational materials which are included in the app.
The following steps provide how the app has prepared for conducting the experiment:

- When a user login into the account for the first time, a demographic survey screen appears as it can be seen in (figure 3.5). The demographic survey will be discussed in the next section of this chapter.
- After the survey, user can progress to take the first quiz which consists of 12 questions; this is the pre-test questions before a user has got any knowledge about phishing attacks. Figure (3.6) shows two examples of pre-test questions one about phishing on social media and the other about Vishing.

![Image showing risk levels for quiz results](image)

**Figure 3.7 Results Feedback to show users the risk level depending on their score.**

- In this step, the result appears and explains the level of risk to users depending on their score, as figure (3.7) shows.
Subsequently, results report appears to give a general idea to users about which area of phishing attacks they must learn more about. As it can be seen in figure (3.8) the user failed to answer any question about email phishing.
- Depending on the result report, users can read and learn from the learning resources center which includes instructions on how to avoid each type of online scams figure (3.9). Educational material examples are shown in figure (3.10) and (3.11). These educational materials are publicly available online\(^2\).

In this stage, user takes quiz 2 which is posttest. It also consists of 12 questions which are different from pretest one; this will be discussed in next section experimental method. The survey and quiz (pre and post) results all will be stored a database using Amazon Web Services (AWS) and MySql Workbench to be extracted and analyzed later.

3.3 Experimental Method

This section will discuss the experimental method which will be used to conduct the study. Based on an analysis of the review of literature, and following the design of the application and educational material, the following two hypotheses were formulated:

The 'null hypothesis' is: H0: There is no significant difference in mean pre- and post-results of participants after phishing education and training materials.

And an 'alternative hypothesis' is: H1: There is a significant difference in mean pre- and post-results of participants after phishing education and training materials.

We implemented a pre and posttest with a demographic survey (see section 3.3.1) using an app with a sample of participants recruited online. All participants should have usual knowledge of computer science which enables them to use online shopping, banking or bill paying. In this study, people who are experts in security or computer science are excluded.

3.3.1 Demographic Survey

One of the methods to collect appropriate data about participants and their knowledge is through demographic survey. In this research, an online survey conducted to get respondents from participants to determine their age, their previous knowledge about phishing attacks. Also, to count how many of them have fallen for online scams or taken a phishing quiz before. The survey also shows whether participants employed or students and in which field. Moreover, it will give an insight about how many of them have trained themselves through online materials.
The aim of designing this survey is to choose the appropriate subjects to conduct this experiment. For example, all subjects they answered as an employed in the field of information security or as computer science experts are excluded. Moreover, it gives a general idea about the knowledge of subjects about phishing attacks. For instance, it shows how many of them have ever taken any type of phishing quiz, or experienced any security issue like credit card fraud or any kind of online scams. The survey also illustrates whether the information security educational materials have a wide reputation among internet users. It also determines which is more favorable: mobile device or personal computer when it comes to browsing internet, online banking or even shopping. Survey questions must be answered by subjects before embarking on the experiment see (Appendix B).

3.3.2 Pre-test

In the pre-test users take the quiz for the first time so they should not have a strong knowledge about information security or phishing attacks. The quiz will begin after user takes a survey so that will determine the kind of users who took the quiz. The participant answers 12 questions some of them were taken from existing phishing IQ test like SonicWall\(^3\) see figure (3.12) illustrates phishing email from Paypal. The questions contain screenshots for emails, SMSs, Social Media, and some recorded voice calls. Figure (3.13) and (3.14) show some examples.

\(^3\)SonicWall Phishing IQ Test\url{https://www.sonicwall.com/phishing/}
Figure 3.12 Example of Phishing Email which included in the quiz

Figure 3.13 SMS which appears from Apple store to hook people
The subject should choose whether it is legitimate, phishing or no answer. The questions divided into four groups (three questions about email phishing, three about SMshing, three about Vishing, and three about social media) as it can be shown in table (3.1). The test score appears to show users risk level depending on their scores (Critical, High, Medium, or Low). It also shows a simple report to explain percentage of correct answers in each type. Hence, users know where their vulnerability is, and then they must read over some educational materials to learn how to detect such attacks. Table 2 illustrates pre-test questions subject, the correct answer, and type of questions.

Table 3.1 Pre-test questions (Quiz1)

<table>
<thead>
<tr>
<th>Questions /Quiz1</th>
<th>Correct Answer</th>
<th>Type</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Phishing</td>
<td>Email</td>
<td>From PayPal</td>
</tr>
<tr>
<td>2</td>
<td>Legitimate</td>
<td>Email</td>
<td>From Wells Fargo</td>
</tr>
<tr>
<td>3</td>
<td>Phishing</td>
<td>Email</td>
<td>From Internal Revenue Service (IRS)</td>
</tr>
<tr>
<td>4</td>
<td>Phishing</td>
<td>SMshing</td>
<td>Apple Store Account</td>
</tr>
<tr>
<td>5</td>
<td>Phishing</td>
<td>SMshing</td>
<td>Google Verification Code</td>
</tr>
<tr>
<td>6</td>
<td>Phishing</td>
<td>SMshing</td>
<td>Tesco Gift Card</td>
</tr>
<tr>
<td>7</td>
<td>Phishing</td>
<td>Vishing</td>
<td>Phone Call Survey Questionnaire Collecting Sensitive Information</td>
</tr>
<tr>
<td>8</td>
<td>Phishing</td>
<td>Vishing</td>
<td>Recorded Voice from BOA</td>
</tr>
</tbody>
</table>

Figure 3.14 Example phishing URL using Twitter trying to convince users to click the link.


<table>
<thead>
<tr>
<th></th>
<th>Phishing</th>
<th>Vishing</th>
<th>Recorded Voice from BOA</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Social</td>
<td>Facebook Login Page</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Social</td>
<td>Message from Facebook Support Team</td>
</tr>
<tr>
<td>12</td>
<td>Legitimate</td>
<td>Social</td>
<td>Android Account on Twitter</td>
</tr>
</tbody>
</table>

### 3.3.3 Learning Resources Center

After the pre-test step, user can go through educational materials screen which presents four groups (Email, SMshing, Vishing, and Social Media). So, depending on the result report, subjects can choose which area they should learn more about. The materials are simple to understand and easy for self learning. It gives instructions on how to avoid each type of phishing attacks. An infographic from Digital Gurdinian designed by Loard has been included (Lord, 2016).

Learning Resources Center shows different training materials as figure (3.10) and (3.11) showed previously. For example, in email phishing part, instructions are given to users on how to recognize spoofed emails. It warns about replying or clicking suspicious links. It also notes them to hover over links to see where it really points out. The Vishing as well as SMshing parts advice users to not click on links which sent through SMS by unknown number, or providing sensitive information through phone calls e.g. Credit Card Number. The last part is for social media scams which describe the most popular phishing techniques used by hackers such as Facebook and Twitter.

### 3.3.4 Post-test

After the educational and training step, user should take quiz 2 by pressing quiz 2 button, see figure (3.9). In this stage, the test questions will be different as shown in table (3.2) below. This
time the questions of legitimate screenshots are more than the pre-test, so that will help to analyze whether the quiz can test the ability of recognizing phishing threats.

<table>
<thead>
<tr>
<th>Questions /Quiz2</th>
<th>Correct Answer</th>
<th>Type</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Phishing</td>
<td>Email</td>
<td>From Bank of America (Alert Massage)</td>
</tr>
<tr>
<td>14</td>
<td>Legitimate</td>
<td>Email</td>
<td>From Bank of Choice (Online Statement Massage)</td>
</tr>
<tr>
<td>15</td>
<td>Legitimate</td>
<td>Email</td>
<td>From Chase (Confirmation of Recent Transaction)</td>
</tr>
<tr>
<td>16</td>
<td>Legitimate</td>
<td>SMshing</td>
<td>News from Gulfnews.com</td>
</tr>
<tr>
<td>17</td>
<td>Phishing</td>
<td>SMshing</td>
<td>Unknown number (Win a prize)</td>
</tr>
<tr>
<td>18</td>
<td>Phishing</td>
<td>SMshing</td>
<td>Apple Account has been frozen</td>
</tr>
<tr>
<td>19</td>
<td>Legitimate</td>
<td>Vishing</td>
<td>Phone call from Medical Center</td>
</tr>
<tr>
<td>20</td>
<td>Phishing</td>
<td>Vishing</td>
<td>Phone call from Microsoft employee</td>
</tr>
<tr>
<td>21</td>
<td>Legitimate</td>
<td>Vishing</td>
<td>Phone call from a company to remind for a job interview</td>
</tr>
<tr>
<td>22</td>
<td>Phishing</td>
<td>Social</td>
<td>Unknown Account trying to convince people to click a malicious link on Twitter</td>
</tr>
<tr>
<td>23</td>
<td>Phishing</td>
<td>Social</td>
<td>Fake Instagram Account for British Airline providing Fake URL in bio description.</td>
</tr>
<tr>
<td>24</td>
<td>Phishing</td>
<td>Social</td>
<td>Facebook Massage from Support team</td>
</tr>
</tbody>
</table>
3.4 Analysis of Results

This section provides the method that will be used to analyze the experiment results. Paired Samples t test technique will be used in this study. It is a statistical technique that is used in ‘before-after’ studies, case-control study, or matched pairs(Sigma, 2009). It compares two means that are from the same individual, object, or related units. Two different times are represented by those two means (e.g., pre-test and post-test with an intervention between the two time points). The aim of such kind of test is to determine whether the mean difference between paired observations on a specific outcome is significantly different from zero.

Data requirements:

- Dependent variable that is continuous. The paired measurements must be recorded in two separate variables.
- Related samples/groups: The subjects in each sample, or group, are the same. This means that the subjects in the first group are also in the second group.(Kent State University, 2016)

In this study, the data contains two variables represented in columns to be used in the analysis. The two variables are quiz marks for participants before (pre) and after (post) learning from educational materials. By using the paired sample t-test, it can be statistically concluded whether or this training app has tested the ability of users to identify different forms of phishing attacks or not.
3.5 Summary

This chapter has given an overview of the research methodology used to conduct this study. As mentioned above, mobile phishing quiz application has been designed to create a small training environment to test the participants online. Hence, data can be easily gathered and statically analyzed to get valid results. Also, the technique used to analyze data has been discussed in this chapter.
4 EXPERIMENT RESULTS AND ANALYSIS

4.1 Introduction
The previous chapter discussed the research methodology which applied in this study and also illustrated an overview of the quiz app used to conduct the experiment. This chapter is a continuation of the previous chapter and it discussed the findings and results of the research experiments. The results from both the survey and (pre and post) test will be discussed here in more details. We conclude with a summary of the chapter.

4.2 Survey Results and Discussion
The survey results below show the answers of 68 participants. After analyzing survey results, 24 participants were excluded from this study, 6 of them were employed either in information security or information technology sectors, the other 18 subjects answered only the first quiz.

<table>
<thead>
<tr>
<th>Table 4.1 Descriptive Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
</tr>
<tr>
<td>&lt;18</td>
</tr>
<tr>
<td>18-25</td>
</tr>
<tr>
<td>26-35</td>
</tr>
<tr>
<td>36+</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Have you ever fall for online scams like PayPal or Online Credit Card/Banking Scam?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>59</td>
<td>85.3</td>
</tr>
<tr>
<td>Yes</td>
<td>9</td>
<td>13.2</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>100.0</td>
</tr>
</tbody>
</table>

What do you usually use the internet for:

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Banking</td>
<td>41</td>
<td>57.4</td>
</tr>
<tr>
<td>Checking Emails</td>
<td>7</td>
<td>10.3</td>
</tr>
</tbody>
</table>
### Table 4.1

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media</td>
<td>10</td>
<td>14.7%</td>
</tr>
<tr>
<td>Shopping</td>
<td>9</td>
<td>13.2%</td>
</tr>
<tr>
<td>Education Purpose</td>
<td>1</td>
<td>1.5%</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>100%</td>
</tr>
</tbody>
</table>

Which one you use more to browse the Internet: smartphone or Personal Computer?

<table>
<thead>
<tr>
<th>Device</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Phone</td>
<td>48</td>
<td>70.2%</td>
</tr>
<tr>
<td>Personal Computer</td>
<td>20</td>
<td>29.4%</td>
</tr>
<tr>
<td>Total</td>
<td>68</td>
<td>100%</td>
</tr>
</tbody>
</table>

Have you ever trained yourself on how to avoid phishing scams through using online educational materials?

<table>
<thead>
<tr>
<th>Response</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>55</td>
<td>80.9%</td>
</tr>
<tr>
<td>Yes</td>
<td>12</td>
<td>17.6%</td>
</tr>
<tr>
<td>Total</td>
<td>67</td>
<td>98.5%</td>
</tr>
</tbody>
</table>

Table (4.1) shows that, out of 68 respondents who participate in the study, 34 (50.0%) were in the age group 26-35 years, 18 (26.5%) were in the age group 18-25 years, 13 (19.1%) were in the age 36+ years and 3 (4.4%) were less than 18 years of age. When asked about ever fall for online scams like PayPal or Online Credit Card/Banking Scam, 58 (85.3%) were not fall in any of the scams while 9 (13.2%) fell in online scams. Respondents were asked about the purpose they use the internet for, 41 (57.4%) were replied they use the internet for online banking, 10 (14.7%) were replied they use the internet for using social media applications, 9 (13.2%) respondents use the internet for Shopping purpose, 7 (10.3%) respondents use the internet for checking emails and 1 (1.5%) respondent use internet for educational purpose. 48 (70.2%) of respondents use smartphones to browse internet and 20 (29.4%) respondents use personal computers for browsing the internet. 55 (80.9%) respondents told that they have not trained them on how to avoid phishing scams through using online educational material while 12 (17.6%) trained them on how to avoid phishing scams through using the online educational material.
As seen on Figure (4.1), participants were also asked if they have heard about phishing, vishing, smishing, spoofed email or social engineering terms. The results show that the most heard terms were phishing and social engineering. However, 38.8% respondents show they have not heard about any of these terms.

Figure 4.2 Responses of subjects whether they have taken phishing quiz previously or not
They were also asked if they have taken a phishing quiz before, as it shown in figure (4.2), 87% of the participants answered that they haven’t taken a quiz before. The rest of them answered the opposite.

Figure 4.3 Responses of subjects about educational materials

Figure (4.3) shows the results of subjects’ replies when they were asked about if they have ever trained themselves on how to avoid phishing scams through online educational material, 18% respondents replied they were trained and 82% replied they were not trained to avoid phishing scams through the online educational material.
As it is shown on the Figure (4.5), the occupations of the study group was studied, and results reveal that subjects are constituted of 31(46.3%) students, 21(31.3%) employed participants and 15(22.4%) unemployed participants. The majority of participants were students in the study.
When respondents were asked about whether they ever fall victim of online scams, 58 (86.6%) replied they have not fallen victim whereas 9 (13.4%) replied they fall victim of online scams, as shown on figure (4.6).

Figure 4.6 Responses about online scams

When respondents were asked about whether they ever fall victim of online scams, 58 (86.6%) replied they have not fallen victim whereas 9 (13.4%) replied they fall victim of online scams, as shown on figure (4.6).
Bar chart of figure (4.7) shows that when respondents were asked for which purpose they were used the internet for. Majority of the respondents replied they were used for online banking purpose 40(59.7%), 7(10.4%) were used for checking emails, 10(14.9%) use for using social media applications, and 9(13.4%) respondents use for online shopping purpose.

4.3 Pre and Post Test Results and Discussion

Phishing quiz is tested on participants and observations are recorded at two different time points. The purpose is to measure if there is any gain in knowledge of participants about Phishing and test whether such training through educational material help participants to gain knowledge about phishing, for this purpose Paired sample t-Test is used.
Paired Sample t-Test:

To test whether the mean differences between paired observation is statistically significantly different from zero paired sample t-Test is used. In the case of paired observations, observations on same participants are tested at two-time points under two different conditions on the same response variable these are the matched observations. The paired-samples t-test is also referred to as the dependent t-test, repeated measures t-test, or simply abbreviated to the paired t-test.

Hypothesis:

The 'null hypothesis' is:

H0: There is no significant difference in mean pre- and post-results of participants after phishing education and training materials.

And an 'alternative hypothesis' is:

H1: There is a significant difference in mean pre- and post-results of participants after phishing education and training materials.

<table>
<thead>
<tr>
<th>Table 4.2 Mean value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>Pre Test</td>
</tr>
<tr>
<td>Post Test</td>
</tr>
</tbody>
</table>

Table (4.2) explains mean value of pre-test is 6.8140 with a standard deviation of 2.08 and mean of post-test is 7.23 with a standard deviation of 1.99 when look at the standard error it is found that least variability observed within the sample in post-test as compared to pre-test.
Table 4.3 Paired t test differences

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>SD</th>
<th>SE</th>
<th>95% Confidence Interval</th>
<th>T</th>
<th>Df</th>
<th>Sig</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lower</td>
<td>Upper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-test*Post-test</td>
<td>0.41860</td>
<td>2.19559</td>
<td>0.33482</td>
<td>1.09431</td>
<td>0.25710</td>
<td>-1.250</td>
<td>42</td>
</tr>
</tbody>
</table>

Table (4.3) shows that paired sample t-test was employed to test the significance of the difference between pre-test score and post-test score. It is seen that t-value is -1.250 with 42 degrees of freedom with associated probability level of P=0.218. In this case, we fail to reject the null hypothesis and conclude that there is no significant difference in mean pre- and post-results of participants after phishing education and training materials. After imparting phishing education to participants there observed no significant change in the test result.

**Figure 4.8 Line Chart depicting pre-test and post-test trend**

It can be seen clearly in figure (4.8) that there is no significance different in pre- and post-test scores after training users about phishing attacks.
4.4 Summary

In this chapter, both demographic survey and pre- and post-test experiment results were discussed. Paired sample t-test was employed to test the significance of the difference between pre-test score and post-test score. Also, data were collected from 68 participants. Half of the subjects in the study group were between 26 and 35 years of age. On the other hand, 30.9% of the subjects were younger than 26 years of age and the rest of them were older than 35 years of age. Most of the participants (87%) have never taken a phishing quiz previously. They have no prior experience of phishing quiz. The majority of the participants have never fallen victim of online scams such as Paypal, Online Credit Card, and Banking. Almost three-quarter of the participants (70.2%) browse the internet over the smartphone. Study subject comprises of nearly half of students, about 31% are employed and rest is unemployed. Most of the participants when asked about for what purpose they are using the internet, responses reveal that more that the half are using it for Online Banking applications, about 15% are using for Social Media applications, the other 13.2%, and 10.3% are shopping and checking emails, respectively. Very least (1.5%) responded they are using it for Education Purpose. Paired sample t-test was employed to test the mean difference between pretest and posttest of 43 subject’s results and it is found that there is no difference in mean pre- and post-results of participants after phishing education and training materials. After imparting phishing education to participants there observed no significant change in the test result.
5 CONCLUSIONS AND FUTURE WORK

5.1 Introduction

This chapter of this research displays and discusses the research findings. Hence, recommendations are provided relying on these findings. Also, this chapter concludes the study by giving suggestions for future works to the subject area, and focusing on the limitations were faced during conducting the study.

5.2 Research Overview

As previously mentioned, phishing attack is a kind of social engineering which becoming increasingly sophisticated. Phishing has spread to not only include emails but also SMSs, VIOP and social media. Despite of the number of mechanisms an organization use to avoid phishing attacks such as firewalls, encryption software, certificates, and two factor authentications, it will not be useful if the person behind the computer falls for phish. Hence, training users is essential part of computer security and the least popular approach, but some researchers argued that educating users doesn’t guarantee complete protection (Hong & Hong, 2012). Considering this, the current research attempted to answer the research question:

**Can Phishing Education Enable Users To Recognize Phishing Attacks?**

Quantitative research methods were employed in this study to ensure the validity of the research’s findings. The primary data gathered from demographic survey and pre post test experiment and analyzed using statistical tools. To conduct the experiment, mobile application phishing quiz were developed and designed to be reached and used by participants.

5.3 Contribution of the Body Knowledge

There are studies in the literature in chapter 2, focused the efforts on technical capabilities which implemented to protect users against phishing attacks. However, there is a need to examine the human factors of such attacks. Few researches contributed on phishing training and education to study the effectiveness of aware people about such threats. Currently, most of these studies
concentrate on testing users’ ability on how to avoid email phishing attacks and malicious URLs. Moreover, they targeted computer student as a sample to conduct the study as it was infeasible to collect a random sample from the entire population of computer users (Arachchilage, 2016).

Therefore, the findings of this study are significantly relevant to phishing education and training filed, as they provide an in-depth investigation on the ability of users to identify different types of phishing attacks such as Vishing, SMshing, and Social Media. This study also distinguishes from the literature work discussed in chapter 2, by developing quiz app in mobile environment which is more favorable among users. It also tests the effectiveness of phishing quiz and educational materials that already have been published online to aware users against these threats.

It is expected that the findings, conclusions, and recommendations of this study will contribute to the field of information security, specifically using phishing education and training approach to avoid the human factor as a serious vulnerability. It will also be valuable to future researchers or studies in this field.

5.4 Results, Discussion and Recommendation
This section will discuss the effective results of developing phishing quiz training app, and give a summary of the findings of this study.

5.4.1 The Effectiveness of Developing a Mobile Application as a Phishing Training Tool

The research work reported in chapter 4 has illustrated that almost 70% of subjects use smartphones for browsing the internet and only 29% said they use personal computers. Moreover, 87% responded that they have never taken a training phishing quiz to test their ability to identify phishing threats and only 13% have knowledge about such quizzes. The results also illustrate the low percentage (18%) of users who have read online anti-phishing educational materials before. Hence, it can be said that using mobile application as an anti-phishing educational tool is useful and would be more effective than using web-based one.
5.4.2 Summary of the Study’s Results
The current study main objective is to determine whether phishing education quiz will help users to identify different forms of phishing attacks or not rather than just reading anti-phishing articles which might be boring. As it has been discussed in the literature chapter 2, previous studies showed that phishing training games and apps need to be developed in order to train and assist users to recognize phishing threats (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong &Nunge, 2007; Mary & Molly, 2015). However, another study argued that educating users about phishing increases the level of suspiciousness of the user. It does not make them better at recognizing what is a phish and what is legitimate website (Anandpara, Dingman, Jakobsson, Liu &Roinestad, 2007).

This study used Paired sample t-test to conduct phishing quiz experiment and test the significance of the difference between pre-test score and post-test score of subjects. The results show that there is no significance difference in mean pre- and post-results of participants after phishing education and training materials. However, it cannot be said that these results have proved phishing education is not useful. There are some factors that could be affected on the results (e.g. language of the learning material contents and the difficult terminology used); this will be discussed in details in the next section.

5.5 Research Limitations

The research was conducted using mobile application which works on Android platform only, which makes several limitations. First, subjects were recruited online and most of users were not using Android mobile devices that limit the number of participants, while it was expected to get a larger sample size. Second, the app contents are in English language and few of participants their first language was not English which makes some parts of the anti-phishing educational materials hard to be understood. Also, the learning materials used to conduct this study could be difficult to learned from for regular user who has not have enough knowledge about computer terminologies. More research required in developing effective material that is both localized and
personalized to the user. Therefore, this should be a cautious when it comes to generalising these findings. Also, the phishing quiz app lack of simulating real life phishing attacks to observe people reaction in such environment. Moreover, restriction of time was a big challenge to carry out a lot of work within a short period of time. However, by prioritizing the activities and, starting with developing the app until finishing the experiment, the challenge was resolved.

5.6 Future Work

While this study has been focused on measuring user’s ability of identifying different forms of phishing attacks, there are other relevant subjects can be addressed in future studies. First, phishing attacks are not the only source of malicious IT threats; they could be e.g. denial of service. Therefore, future research can be conducted with different IT threat sources and observe how users can avoid such threats. Secondly, the aim of developing phishing quiz app is to create a better educational environment that suites regular web users and provide feedbacks which enhance them to learn from anti-phishing materials and get progress on their scores. Therefore, future research can be focused on developing a highly sophisticated anti-phishing mobile application that can simulate a real life phishing threats with attractive visual objects and graphics. It also can be conducted to study the effectiveness of online educational materials and training systems and how to better design them to be easier and useful for all kind of computer users.

5.7 Summary

This Chapter has provided a detailed discussion about the main findings of the research work. Furthermore, an overview of the research and contribution of the study has been presented. Finally, the research challenges, limitations and future work were discussed to give more opportunities for forthcoming studies.
REFERENCES


APPENDIX A

Initial Prototyping

First prototyping using Pop app for mobile application:
Second prototyping using Justinmind:
# APPENDIX B

## Demographic Survey Questions:

<table>
<thead>
<tr>
<th>Question</th>
<th>Choices</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is your first language?</td>
<td>English, Arabic, Other:</td>
</tr>
<tr>
<td>What is your age?</td>
<td>Under 18 years old, 18-25 years old, 26-35 years old, 36 or older</td>
</tr>
<tr>
<td>Have you ever heard or know about any of these terms?</td>
<td>Phishing, SMshing, Vishing, Spoofed Emails, Social Engineering, None of them</td>
</tr>
<tr>
<td>Have you ever taken a quiz about phishing attacks to test your ability in how to recognize online scams?</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Have you ever been the victim of an Internet scam like: PayPal, Online Credit Card/Banking Scam, or a Virus-infected website? If YES, please write a brief description about it.</td>
<td>Yes, No</td>
</tr>
<tr>
<td>Which one you use more to browse the Internet: Smart phone or Personal Computer?</td>
<td>Smart Phone, Computer</td>
</tr>
<tr>
<td>What do you usually use the internet for?</td>
<td>Online banking, Online Shopping, Checking emails for work purposes, Social media, Online business, Other:</td>
</tr>
<tr>
<td>Occupation. If you are a student or an employed, please specify your field of studying or work:</td>
<td>Student, Employed, Unemployed, Other:</td>
</tr>
<tr>
<td>Have you ever trained yourself on how to avoid phishing scams through using online educational materials?</td>
<td>Yes, No</td>
</tr>
</tbody>
</table>
APPENDIX C

Results of the Demographic Survey

Participant age group

- Under 18 years old: 20%
- 18-25 years old: 53%
- 26-35 years old: 27%
- 36 or older: 0%

Have you ever fell for online scams like PayPal or Online Credit Card/Banking Scam

- Yes: 13.4%
- No: 86.6%

Participinace who use smart phone to brows internt are more than Personal computer

- Smart phone: 71%
- Personal Computer: 29%
Have you ever trained yourself on how to avoid phishing scams through using online educational materials?

- Yes: 81.5%
- No: 18.5%

Occupation, if you are a student or an employed please specify your field of studying or work:

- Student: 31.3%
- Employed: 46.9%
- Unemployed: 22.4%

What do you usually use the internet for?

- Online banking: 38 (66.7%)
- Online shopping: 38 (66.7%)
- Checking email: 12 (20.8%)
- Social media: 21 (78.1%)
- Online business: 2 (7.7%)
- Other: 1 (7.8%)