



University of Bradford eThesis

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

**An Integrated Intelligent Approach to Enhance the
Security Control of IT Systems**

**A Proactive Approach to Security Control Using Artificial Fuzzy Logic to
Strengthen the Authentication Process and Reduce the Risk of Phishing**

Omran Suleiman Ahmed Salem

**A Thesis Submitted for the Degree of
Doctor of Philosophy**

Faculty of Engineering and Informatics

School of Electrical Engineering and Computer Science

University of Bradford

2012

Abstract

Hacking information systems is continuously on the increase. Social engineering attacks is performed by manipulating the weakest link in the security chain; people. Consequently, this type of attack has gained a higher rate of success than a technical attack.

Based in Expert Systems, this study proposes a proactive and integrated Intelligent Social Engineering Security Model to mitigate the human risk and reduce the impact of social engineering attacks.

Many computer users do not have enough security knowledge to be able to select a strong password for their authentication. The author has attempted to implement a novel quantitative approach to achieve strong passwords. A new fuzzy logic tool is being developed to evaluate password strength and measures the password strength based on dictionary attack, time crack and shoulder surfing attack (social engineering). A comparative study of existing tools used by major companies such as Microsoft, Google, CertainKey, Yahoo and Facebook are used to validate the proposed model and tool.

A comprehensive literature survey and analytical study performed on phishing emails representing social engineering attacks that are directly related to financial fraud are presented and compared with other security threats. This research proposes a novel approach that successfully addresses social engineering attacks. Another intelligent tool is developed to discover phishing messages and provide educational feedback to the

Omran Suleiman Ahmed Salem

An Integrated Intelligent Approach to Enhance the Security Control of IT Systems

user focusing on the visible part of the incoming emails, considering the email's source code and providing an in-line awareness security feedback.

KEYWORDS: Information Security, Authentication, Email Phishing, Security Awareness, Fuzzy Logic.

Acknowledgements

Thank you God for your great help to finish this work

To the Soul of my father

To My beloved Mom

To my Wife, Kids, and all Family members

To my supervisors, friends

I would not have been able to finish my work without your
support

Thank you all for your patience.

Table of Contents

Abstract.....	i
Acknowledgements	iii
Table of Contents	iv
List of Figures.....	ix
List of Tables	xii
Glossary and List of Abbreviations	xiv
1 Introduction	1
1.1 What is information?.....	1
1.2 What is Information Security?	1
1.3 Why do we need information security?	2
1.4 Methods of Attacks	5
1.4.1 Technical Attacks.....	6
1.4.2 Social Engineering	6
1.5 Social Engineering Categories and Methods	7
1.6 Achieving Information Security and Reducing Social Engineering Attacks....	9
1.7 What are Security Controls?	12
1.8 Auditing and monitoring	13
1.9 Reactive vs. Proactive Systems.....	13
1.10 Human Factor in Information Security Process	14
1.11 Motivation.....	15

1.12	Aims and Objectives	16
1.13	Research Hypothesis	19
1.14	Methodology	20
1.15	Contributions to knowledge	23
1.16	Thesis Map	24
1.16.1	Literature Review	24
1.16.2	Case Study.....	25
1.16.3	Intelligent Measuring Tools for Password Strength.....	25
1.16.4	Email Phishing Capture Module	26
1.16.5	Findings and future works.....	27
2	Literature Review	28
2.1	Social Engineering Attacks	28
2.2	Password Strength.....	31
2.3	Email Phishing	37
2.3.1	Anti-phishing Toolbars	37
2.3.2	Browser Plug-ins	37
2.3.3	Email-Filters.....	38
2.4	Introduction to Expert Systems	39
2.5	Fuzzy Logic.....	39
2.6	Security Awareness and Training	40
2.7	Conclusion:	42
3	Case Study.....	44
3.1	Introduction	44
3.2	A case-study about a severe security breach at a major bank in Jordan	45
3.2.1	Objectives.....	45
3.2.2	Methodology and introduction to the problem.....	45
3.2.3	Security status before 2009	45

3.2.4	Identifying the problem.....	47
3.2.5	The solution.....	50
3.2.6	Security status after 2009.....	51
3.3	A Case-Study of a password policy in an educational organisation	52
3.3.1	Objective:	52
3.3.2	Introduction and methodology	52
3.3.3	Organisation’s policy and guidance	52
3.3.4	Assessing the policy	54
3.4	Potential of conducting an internal phishing attack	55
3.4.1	Objective	55
3.4.2	Introduction	55
3.4.3	Elements of conducting an internal phishing attack	56
3.5	Simulation of phishing attack, awareness measurement and educationally based feedback	59
3.5.1	Objectives:.....	59
3.5.2	Elements and Method:.....	60
3.5.3	Survey and feedback of the study:	68
3.6	Findings.....	74
4	Password Strength.....	76
4.1	Introduction.....	76
4.2	Factors affecting password strength.....	78
4.2.1	Shoulder surfing (password length)	78
4.2.2	Dictionary based.....	78
4.2.3	Password entropy (Character sets).....	78
4.3	Existing Tools and Approaches	79
4.3.1	Microsoft.....	79
4.3.2	CertainKey Cryptosystems.....	81

4.3.3	Google:.....	82
4.3.4	Yahoo:.....	83
4.3.5	Facebook:.....	85
4.4	Proposed Methodology	86
4.5	Combined Model.....	90
4.6	Quantitative Approach	91
4.7	Experiments and Results	91
4.7.1	Length:	91
4.7.2	Dictionary based.....	92
4.7.3	Entropy	94
4.8	Proactive Proposed Tool	102
4.9	Conclusion.....	104
5	Phishing Emails Capture Module	106
5.1	Introduction	106
5.2	Phishing techniques.....	109
5.2.1	Impersonation.....	109
5.2.2	Forward attack.....	109
5.2.3	Pop-up attack.....	109
5.2.4	Voice phishing	110
5.2.5	Mobile phishing	111
5.3	Anti-phishing Solutions	111
5.3.1	Anti-phishing toolbars.....	112
5.3.2	Browser plug-ins	112
5.3.3	Email-filters.....	112
5.4	Phishing emails features.....	113
5.4.1	Source code features (back-end)	113
5.4.2	IP-based URLs and bon-matching URLs.....	114

5.4.3	The use of scripts	114
5.4.4	The use of multiple domains	115
5.4.5	Content features (front-end).....	115
5.4.6	Generic salutation.....	115
5.4.7	Security promises, requires a fast response or “Click Here” link	115
5.4.8	Links to https:// domains	116
5.5	Intelligent model for detection and protection	116
5.5.1	Using fuzzy logic approach.....	116
5.5.2	Experiment and results	125
5.6	Conclusion.....	129
6	Conclusion and Future Work	131
	REFERENCES.....	134
	APPENDICES	141
6.1	Published Contributions	142
6.2	Feedback of the survey conducted at section 3.5	143

List of Figures

Figure 1: The three important elements of Information Security (Olzak 2011)	2
Figure 2: CSI/FBI Computer Crime and Security Survey Results (Panko 2003).....	3
Figure 3: Total Number of Vulnerabilities identified, 2006 – 2011	4
Figure 4: A continuous process of the Security Plan	10
Figure 5: Cost-effectiveness diagram of different security control types (Sapronov 2005)	14
Figure 6: Types of information security controls.....	17
Figure 7: Integration of people with policies and logical security controls.....	18
Figure 8: Research Methodology	22
Figure 9: Steps taken to conduct a simulation SE attack	29
Figure 10: Steps to implement a security awareness program (Mark Wilson and Hash 2003)	42
Figure 11: three major types of information security controls.....	46
Figure 12: An illustration of how the Conficker worm works (Microsoft 2009)	49
Figure 13: password change page shows the enforced policy	53
Figure 14: Phishing Attack Scenario.....	57
Figure 15: First example of Facebook phishing email.....	64

Figure 16: First example of phishing Facebook website	65
Figure 17: Second example of Hotmail phishing email.....	66
Figure 18: Second example of phishing Hotmail website	66
Figure 19: Responses to Question 1	69
Figure 20: Responses to Question 2.....	70
Figure 21: Responses to Question 3.....	71
Figure 22: responds to Question 4	72
Figure 23: CertainKey password checker fail to rate strong password.....	82
Figure 24: password checker from Google	83
Figure 25: password checker from Yahoo shows a strong password as weak password	84
Figure 26: Facebook Password checker shows strong password.....	85
Figure 27: Entropy of different character sets.....	89
Figure 28: The Fuzzy Process	90
Figure 29: Membership Function of Password Length in MATLAB	92
Figure 30: Membership Function of Dictionary-based in MATLAB	93
Figure 31: Password checker for password “abcd1234”(PTool).....	103
Figure 32: Password checker for password “fsdf334dsr£\$df” (PTool)	104

Figure 33: Password checker for password "4524556547673"	104
Figure 34 : Scam email shares graphics with legitimate website.....	108
Figure 35 : Scam email using forward attack technique	111
Figure 36 : Non-Matching URLs	114
Figure 37 : Separating front end and back end of incoming email	118
Figure 38 : Using script to extract features of each layer then rate each layer	119
Figure 39: Three-dimensional plots for rule base 2	125
Figure 40: Results of evaluating phishing and healthy emails.....	126
Figure 41: Results of comparison the proposed tool with Microsoft Windows live mail 2009.....	127
Figure 42: Results of comparison the proposed tool with Thunder bird and Avira Anti- virus.....	127
Figure 43 : Front End vs. Back End.....	128
Figure 44 : Phishing emails capture module	129

List of Tables

Table 1: Number of Vulnerabilities and Security Incidents Reported (Berg. 2006)	4
Table 2: Various passwords tested	54
Table 3: Demographics analysis of the case study	68
Table 4: Passwords tested by Microsoft password checker	80
Table 5: Passwords tested by Yahoo password checker	84
Table 6: Length of different character sets	88
Table 7: Membership of password length	92
Table 8: Membership of dictionary based	93
Table 9: Character set and Entropy of 8 character password	94
Table 10: Passwords of keyboard patterns (Ptool represents the proposed tool)	96
Table 11: Results of passwords based on dictionary	98
Table 12: Results of high entropy passwords	99
Table 13: Results of low entropy or sequence passwords	100
Table 14: Quantitative approach	100
Table 15: Table of existing tools weaknesses	101
Table 16: Features extracted from phishing email	120

Table 17: Back end features rules	123
Table 18: Front end features rules.....	124
Table 19: Rule Based 2 for Final Email Evaluation	124

Glossary and List of Abbreviations

Ser.	Abbreviation	Full description
1	SE	Social Engineering
2	IDS	Intrusion Detection Systems
3	ISO	International Organization for Standardization
4	ISO 27001	Information Security Standards
5	APACS	Association for Payment Clearing Services
6	VPN	Virtual Private Network
7	COBIT	Control Objectives for Information and Related Technologies

1 Introduction

Background

1.1 What is information?

Information is an asset like any other important business asset (ISO 2005) which can exist in many forms; it can be a written document, an electronic document (such as a video or voice recording) or data stored on backup media. It is therefore important to be protected, as it is extremely valuable to organisations.

1.2 What is Information Security?

Managing information security was defined by the ISO 17799 standards as *“the protection of all kinds of information including systems from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities”* (ISO 2005). This applies to both private and public sector where the reputation and revenue of the business are concerned.

By implementing an information security plan, three elements can be preserved for any business:

1. Confidentiality, to ensure that important information can be accessed by authorised people.
2. Integrity, to ensure that transmitted information is not altered or updated by unauthorised people.

3. Availability, to ensure that authorised people can access the information whenever they need it.

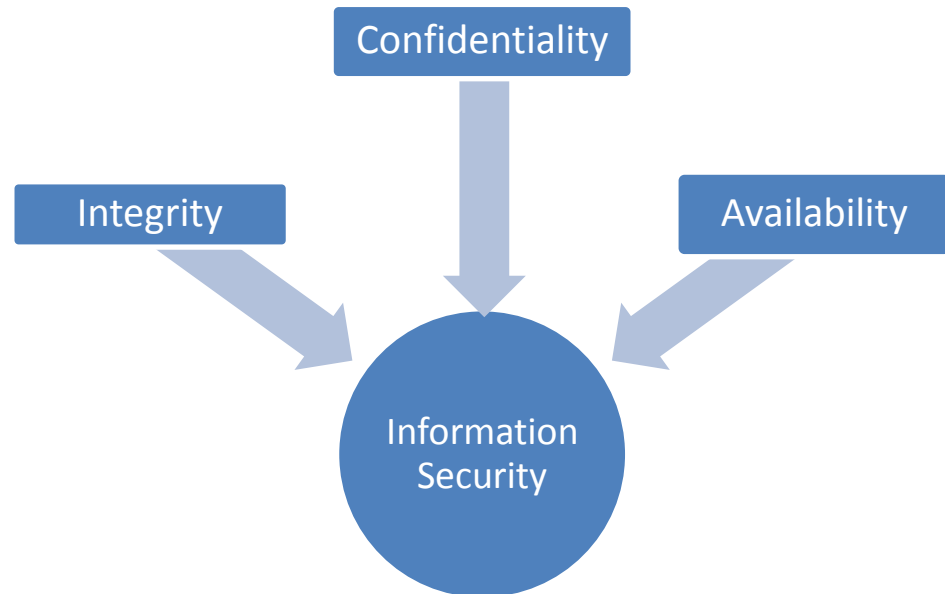


Figure1: The three important elements of Information Security (Olzak 2011)

Information security can be performed in different ways. It can be policies and procedures that guide managers and employees to protect their assets against threats and breaches. It can be software such as antivirus and IDS (Intrusion Detection Systems) or it can be hardware such as firewalls or access cards, it can also be a training awareness programs for administrators, technical and end-users. In other words, we can use the above-mentioned ways as security controls to protect information.

1.3 Why do we need information security?

Threats, breaches and identity thefts are occurs every day (Whitman and Mattord 2012); failure to prevent business hindrances could cause huge losses.

CHAPTER ONE

Companies are striving daily to counter all kinds of IT attacks, thus illustrating the seriousness of the matter.

A CSI/FBI Computer Crime and Security Survey (conducted by the Computer Security Institute) showed that average annual losses increased from US \$320m to \$1.1b for the period between 1997 and 2002 (Panko 2003). In most cases, computer threats are increased by more than 300%, as shown in figure 2. Meanwhile, new figures reported by federal agencies to US-CERT (the United States Computer Emergency Readiness Team) between 2006 and 2010 showed that the number of incidents had increased from 5,503 to 41,776 (Wilshusen 2011).

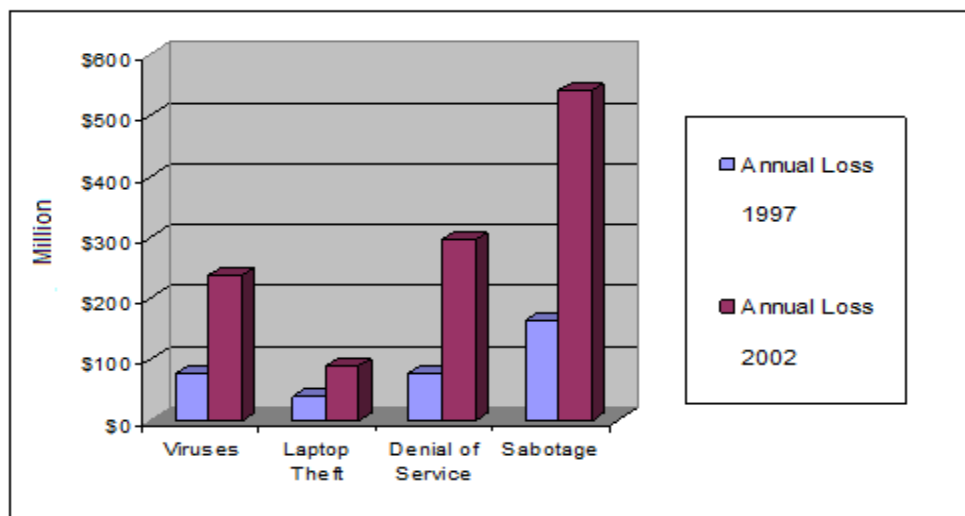


Figure 2: CSI/FBI Computer Crime and Security Survey Results (Panko 2003)

The number of vulnerabilities is on the rise as well. The following table shows the number of vulnerabilities and security incidents in the years 1999, 2000 and 2001 (Berg. 2006)

CHAPTER ONE

Year	Number of Vulnerabilities Reported	Number of Security Incidents
1999	417	10,000
2000	1,090	21,756
2001	2,437	52,658

Table 1: Number of Vulnerabilities and Security Incidents Reported (Berg. 2006)

During the period 2006-2011, Symantec Corporation's analytical study showed the number of vulnerabilities at ~4800 new vulnerabilities in 2011, a decrease of about 20% in new vulnerabilities as reported in 2010. The study concluded that the actual number of new vulnerabilities discovered decreased while the trend is still upwards (Symantec April 2012). Figure 3 shows the new vulnerabilities identified between 2006 and 2011, based on Symantec's internet security threat report published in April 2012.

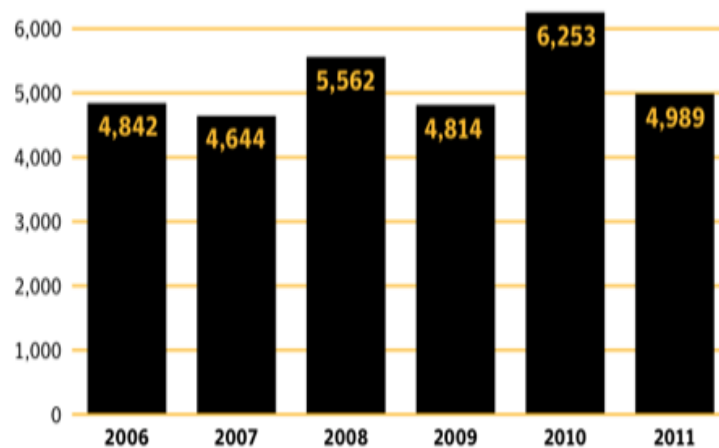


Figure 3: Total Number of Vulnerabilities identified, 2006 – 2011

CHAPTER ONE

More than 300 million security threats (to infect users' computers) were detected by *Kaspersky Security Network (KSN)* in the first quarter of 2010, recording a 26% increase in attempts observed in the fourth quarter of 2009 (Namestnikov 2010).

On the other hand, bank fraud is on the increase as well. Phishing attacks and malware are considered a real threat to bank customers (O'sullivan 2009). Figures (released by the payments group APACS) in 2009 show that online bank threats in England cost customers approximately £52.5m, while card fraud losses total £609.9m.

Information security is important in protecting critical infrastructures in both public and private sector businesses. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks.

Security is not a one-time effort. Reviewing and monitoring the security plan is important to keep the organisation secure and safe.

1.4 Methods of Attacks

Based on the nature of the attack, targeted groups and successful methods of attack, researchers concluded that attacks against information and organisations can take many forms and can be categorised into the following types (Berg. 2006):

1.4.1 Technical Attacks

This type of attack is carried out by software or malicious code to damage systems; it can take the form of a virus, a worm, a Trojan horse or some kind of spyware in order to slow down network traffic, stopping service (Denial of Service) or to gain valuable information. In this case attackers or hackers use tools such as assembly language and the power of the computer and networks to achieve their goals. Usually these tools (which are widely available on the Internet) are sent to users in the form of programmes as attachments to emails or sometimes as scripts embedded in harmful websites.

To provide protection against this type of attack, antivirus, anti-spam, firewalls and IDS can be used. In addition, a VPN and encryption algorithm can be implemented to increase the security level of network environments.

1.4.2 Social Engineering

This type of attack could take the form of malicious actions against people, physical theft of laptops and computer equipment, phishing and shoulder surfing. Lack of knowledge and awareness are the main reasons behind the success of this type of attack knowing that people are the weakest link in the security chain (Barrett 2003; Orgill, Romney et al. 2004; Berg. 2006; Gregg 2006).

Different definitions of Social Engineering (SE) attacks have been demonstrated to describe one of the most serious security threats at the moment.

Kevin Mitnick (the FBI's most-wanted computer hacker) in his famous book "*Art of Deception*" defines social engineering as:

CHAPTER ONE

“Taking advantage of people’s naivety via influence, persuasion and manipulation to obtain vital information.”(Mitnick and Simon 2002).

Meanwhile the security+ study guide refers to Social Engineering as:

“The process of using human behaviour to attack a network or gain access to resources that would otherwise be inaccessible”(Hausman, Barrett et al. 2003).

One of the simplest definitions is:

“Breaking an organisation’s security by interactions with people”(http://www.computeruser.com/ 2006).

It is clearly noticeable that this kind of attack is performed wherever and whenever people are present; therefore it cannot be completely eliminated, but only reduced. Social engineers target companies’ information using different methods to gain their valuable information.

1.5 Social Engineering Categories and Methods

Social engineering attacks can be conducted in many diverse ways. Usually the first step in any social engineering attack is the collection of information with a company’s website being one of the main resources to gain such information. The attacker could collect the information from search engines, job sites or dumpster diving (Redmon 2006).

Social engineering attacks have many different forms, the following are some common approaches widely used:

a. **Impersonation:**

Impersonation is imitating another person where the attacker can act as an authority figure or assume the identity of a lay user. People are usually intimidated by authorised persons, and this may lead them to reveal important information to the attacker. Additionally, attackers could use the phone to impersonate another person to collect information, or send a phishing email requesting users to update their accounts on the website (Schneier 2004; Redmon 2006).

b. **Developing Trust**

Attackers could build trust between themselves and the victim to gain or exchange future information; this takes time to achieve and it may require several visits (to the targeted victim) to build such confidence. The main goal (of the attacker) during these visits is not to collect information, but to build trust. Kevin Mitnick considered building trust as a stage of the social engineering cycle (Mitnick and Simon 2002).

c. **Moral Duty**

People are used to helping other people or friends even if it means “breaking the rules”. This could occur among people working in teams, when an individual feels the need to show their helpful abilities to others. An employee could reveal a certain code or important document as a favour to a ‘friend’, who can be in this case the attacker him/herselves (George 2001).

d. **Urgency and Persuasion**

This method of collecting information can be implemented by leading the victims to think that, if they don't give certain information quickly, disastrous consequences will overtake the requester (the attacker). Sometimes the attacker convinces the user that everyone else has given him/her this type of information as it is urgently needed; therefore, the user may easily be persuaded to reveal any requested information to the hacker (Granger 2001).

e. **Spying**

Attackers could spy on the keyboard of the user to memorise passwords or pin codes of the access control lock. These actions are called shoulder surfing. Memorable passwords or short pin numbers can be easily observed by shoulder surfers. Because of this type of attack, people are advised to select long and strong passwords and to shield the key pad while they are typing the password or the pin code (Guyot 2003).

1.6 Achieving Information Security and Reducing Social Engineering Attacks

By building a strong security plan, the organisation can secure its information against various threats and minimise risk.

A security plan is needed because security is not a standard procedure or a one-off task but an overlapping mesh of *technology, people, policies and processes*. A security plan will help co-ordinating the whole system and ensure there are no gaps; it will also give a sense of proportion and priority to different

CHAPTER ONE

tasks. There are four steps in creating a good security plan: *Audit, Plan, Execute then Monitor and Repeat* (Corporation 2003).

It is preferable for any security plan to be based on security standards. ISO 17799 and COBIT are two of the most popular guidelines and recommendations to improve the security of information. Since security is not a product, monitoring and managing it is one of the important success factors (the security process 24/7).

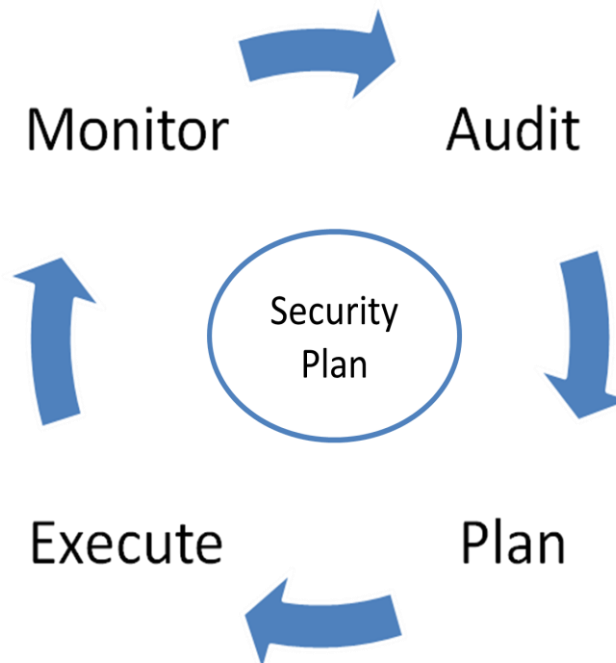


Figure 4: A continuous process of the Security Plan

Social Engineering attacks can be reduced by implementing different security controls. Below are recommended solutions that can help to mitigate the risk of social engineering:

CHAPTER ONE

a. Policies

Policies are one of the most important keys to successfully implementing security controls. Revising policies and procedures are usually the second stage of a security audit process (Kapp 2000) when the first stage is finding the policies. It is important for the enterprise to apply clear and strong policies, procedures and guidance, and enforce them in critical circumstances to reduce human error (Lo and Marchand 2004).

b. Help Desk and Incident Management

By handling security incidents, the level of risk should be reduced, and security policies will be more effective when there are immediate response actions (Symantic 2002). Help desk staff have the ability to reset users' passwords, configure accounts, and allow or revoke permissions. Unfortunately, impersonating help desk staff could enable social engineering attacks (Redmon 2006).

c. Training and Awareness

It is important to communicate the procedure and guidance to the company staff; this can be achieved by training people and conducting regular campaigns such as meetings, posters, leaflets and computer messages (Microsoft 2006). Some companies require employees to review the policy every year and train new employees as soon as they start work (Gulati 2003).

d. Physical Security

Valuable information should be protected against social engineering attacks. Information is stored either in servers or physically in cupboards. Physical security is one of the first lines of defence. The implementation of access control systems (such as fingerprints and ID cards) will make it difficult for social engineering attackers to operate in such a secured environment (Jones 2004; Redmon 2006).

e. Auditing

Auditing and regular assessment of security policies, people's awareness, and access control functionalities could reduce the risk level of technical and social engineering attacks. Addressing the vulnerabilities of computer systems has become a relatively straightforward exercise. The problem nowadays is how to audit and evaluate the security of people (Barrett 2003).

1.7 What are Security Controls?

The contents of a security plan (such as standards, policies, procedures and guidelines) are called Security Controls.

Security controls are divided into three types. The first is management and administrative control, such as personnel security, policies, incident handling, security audits or disaster recovery plans. The second type is physical control, such as selecting secured sites, and securing the equipment or protection of unattended hardware. The last type is called technical control, such as antivirus software, user identification and authentication, access control,

firewalls and Intrusion Detection Systems (NIIT 2004; ISO 2005), the latter is the most commonly used controls.

1.8 Auditing and monitoring

Auditing means to: “Carry out periodic reviews of security risks and implemented controls to take account of changes to business requirements and priorities, consider new threats and vulnerabilities, and confirm that controls remain effective and appropriate” (Milus 2004).

Security auditing is a policy-based assessment of the procedures and practices of a site and assessing the level of risk created by these actions. It is an evaluation process of all security components of an organisation. It can measure and test for vulnerabilities and weaknesses in IT security systems, policies and procedures (Kapp 2000; Lo and Marchand 2004; Research 2004).

Companies that do not have security standards (or any form of implemented policies) are likely to have an unsuccessful audit process.

1.9 Reactive vs. Proactive Systems

The audit process described earlier can be categorised as a corrective process, as it analyses the current status of the security level of the enterprise and gives recommendations at the end of the procedure, though it can't guarantee the implementation of those corrective actions. Nowadays many tools have been developed to monitor security issues in real time. These types of tools are categorised as detective tools, whilst preventive security controls are

CHAPTER ONE

considered the best solution as they can predict the risk and prevent breaches from ever occurring.

The following diagram shows the costs and effectiveness of security control categories mentioned above (Sapronov 2005).

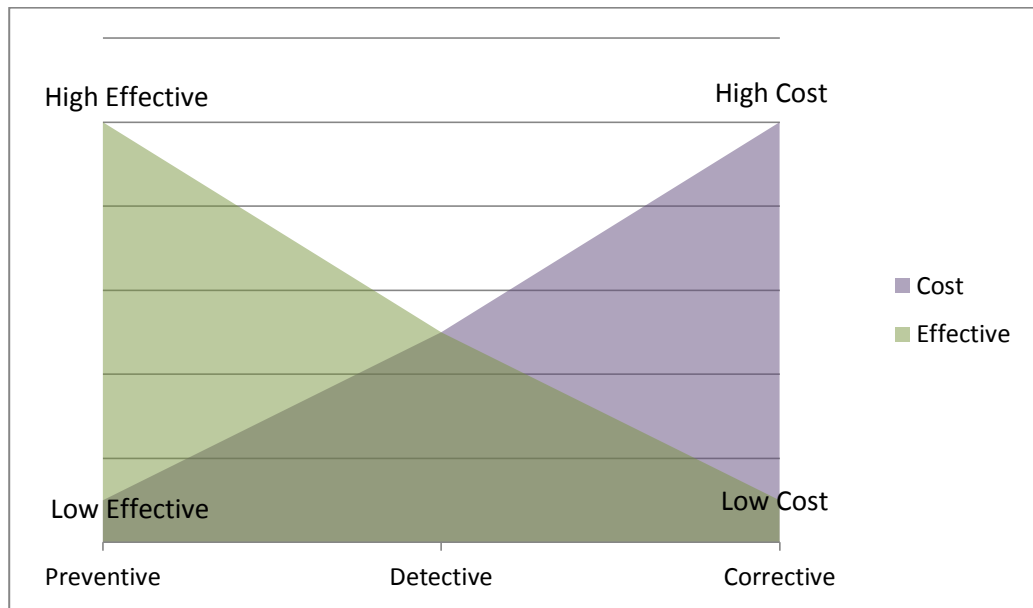


Figure 5: Cost-effectiveness diagram of different security control types (Sapronov 2005)

The above graph demonstrates that preventative controls are less costly and more effective than the detective and corrective controls.

1.10 Human Factor in Information Security Process

Security status cannot be guaranteed just by using security tools. The security process should amalgamate all elements: technology, people and policies. Social engineering attacks usually target weak people who lack knowledge; accordingly, the human factor is the main reason behind the success of many computer attacks. Therefore, interviewing people is an important stage in measuring and assessing their awareness in the security audit process (Lo and

CHAPTER ONE

Marchand 2004) hence monitoring their activities will definitely reduce the risk of such attacks. Social Engineering is a security gap that requires further investigation and should be addressed in future research. Internal end-users (who lack knowledge) could be the vulnerable part of a network infrastructure and cause great harm (Colwill 2010) accordingly, their activities should be monitored and observed in transparent mode.

It becomes clear that people are the weakest link in the security process; thus it is an aim of this research to find a model that can integrate different types of security controls.

1.11 Motivation

Attackers prefer to violate security systems through end-users as they are the weakest link in the security chain. Lack of knowledge and negligence in security policies make them an easy target. Phishing and weak passwords are obvious examples of security vulnerabilities.

The author's experience in the computer section of the Public Works Department of the United Arab Emirates for ten years helped him to realise that all kinds of technologies implemented in that department (including firewalls, antivirus, VPN, restricted policies and procedures) failed to provide the organisation with the required security. As a result, the organisation remained under attack. Based on security audits and security gap analysis, it was concluded that more than 700 employees (computer users of that department) need to have a minimum level of security awareness in order to raise the overall security system level. Additionally, certain policies were enforced, such as selecting 8-character passwords, using a mix of different

CHAPTER ONE

character sets, restricting end-users from installing programs, and making regular checks of personal computers scheduled on a monthly basis. The next security audit showed that security breaches had been reduced following six months of awareness program training and implementation of different security controls.

Despite that, other security breaches increased over the next few months, such as selecting weak passwords, receiving phishing emails and ignoring some security update software that had suddenly stopped its processes. Passwords are widely used nowadays as an authentication method. Many of end-users do not have enough security knowledge to be able to select strong passwords. On the other hand, emails are currently one of the most popular communication methods. Phishing emails are usually look like a legitimate ones in order to deceive people thus, social engineering attacks will only become consistent and successful in areas where people lack awareness and have poor proactive security systems.

Essentially, people are responsible for building, implementing and operating the technology, making them very important players in the security process. The proposed model in this research, therefore, covers and focuses on integrating different security controls into an intelligent and effective control to diminish the risk of social engineering attacks and reduce the security gap caused by people.

1.12 Aims and Objectives

This research aims to integrate different security controls in a module that can avoid, counteract and minimise various security threats of social engineering attacks.

There are three important elements affecting the run of any kind of business; people, product (technology) and process - sometimes partners are added as a fourth

CHAPTER ONE

element (Clinch May 2009). With reference to the ISO 17799, information security controls are categorised into different types: controls related to users, such as awareness programs; controls related to policies, such as the roles and procedures that are applied by organisations' managements; and, finally, physical and technical controls such as antivirus, firewall, user authentication, and logical access controls.

Based on the above, the following diagram (6) shows the three different types of information security control represented as the elements of business:

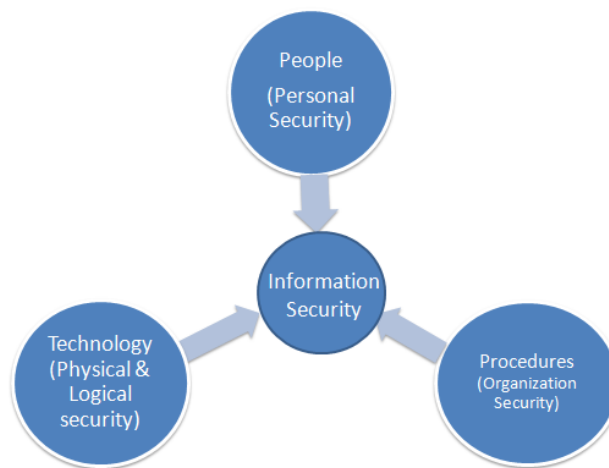


Figure 6: Types of information security controls

- One of the main objectives of this research is to build an integrated model to reduce the risk of social engineering attacks. This model can be applied at different levels at enterprises in order to plug the gap in security chains caused by human neglect.

The suggested model starts as a result of an audit process taking place in the company in order to find the required actions. Stages of “What to do”, “How to do”, and “Why” are implemented in the proposed approach. Administrators

CHAPTER ONE

improve existing policies or write new ones (we call this stage “*What to do*”). The new and improved policies are represented as procedures through development of intelligent tools (such as server side tools or front-end modules). In order to enforce those policies, we need the stage of (“*How to do*”). Finally, the proactive intelligent tools will enforce the policies and recognise security threats before they happen. They then play the role of trainers as they will show the end-users reasons behind the decisions taken, such as why the password is weak or why the email is categorised as a phishing email. This is the stage of (“*Why*”). As security is a process not a product, a security audit should be a continuous process as argued by (Page 2003). Figure 7 represents the suggested model. It shows information security systems surrounded by one control that integrates administrators and end-users with policies and logical information security controls. All are subject to a security audit:



Figure 7: Integration of people with policies and logical security controls

CHAPTER ONE

- The addition of new factors to measure password strength (in order to mitigate shoulder surfing attacks) should be taken into consideration because, as they become widely used, many existing tools are ignoring this factor.
- One other important objective is to measure the strength of passwords effectively and accurately in order to force end-users to select strong passwords through an intelligent module.
- Study the behaviour of phishing emails to prove that phishing emails can be detected by well-trained users. This can be done by separating the incoming emails into front and back ends, analysing each part on the basis of common phishing email features.
- To build an efficient capture-of-phishing-emails tool based on the suggested integrated model. Fewer factors and rules will be used to enhance the module's performance. Ultimately, users will be aware of the module's decision through its awareness feature that this module constructs.
- The literature shows substantial financial losses are taking place across many years due to social engineering attacks.

1.13 Research Hypothesis

- It is possible to improve security and reduce social engineering attacks by combining of different security controls. (ex. Logical/physical, Administration and human factors)
- Password strength can be improved by considering a combination of affecting three factors - length of passphrase, entropy and dictionary-based to avoid social engineering shoulder surf attack.

CHAPTER ONE

- New factors related to password strength are exist and can be used to improve security and its definition.
- More accurate quantitative value of password strength can be measured and used instead of its present qualitative one (“Weak”, “Moderate” and “Strong”).
- Fuzzy logic can be used to improve password security measures.
- Phishing emails capture can be improved by using fuzzy expert approach.
- Improved detective tools are needed to detect visible or invisible phishing emails.
- People can’t easily detect phishing emails.

1.14 Methodology

Methodology is "the strategy or architectural design by which the researcher maps out an approach to problem-finding or problem-solving" (Buckley, Buckley et al. 1976). Meanwhile, (Collis and Hussey 2003) stated that the purpose of research was to review or synthesise existing knowledge in order to generate new knowledge by exploring existing problems to provide solutions. Based on that, the framework of the methodology should address the problem-finding, then the problem-solving, via data collection and analysis, developing tools and procedures. Therefore, the methodological approach of this research (based on a comprehensive literature review, case-studies, tools implementation and interview) to define and address one of the current serious information security threats will be to adopt a quantitative approach based on artificial intelligent fuzzy logic systems. At the end of each experiment, a comparison study is

CHAPTER ONE

applied to validate the proposed models. Additionally, the author's ten years of experience in a technical support section of a department of 1500 employees will add value to this research. This experience caused the author to realise the need for awareness programs and the enforcing of policies in order to reduce the risk of various security threats.

The case-study focuses on real vulnerabilities of implemented security policies. This kind of study helps to address security gaps and serious problems in a short time since it is based on real experience. It is worth mentioning that an unstructured interview with an IT manager of a major bank in Jordan exposed a critical security breach at one of the largest banks in the region.

The experiments conducted in this research require us to collect important data from different sources. A password dictionary (which contains more than 800,000 English words including movies, brands, names and sequences of keyboard patterns added to it) has been used to help manipulate dictionary attacks. We are also required to collect real phishing emails to build the phishing capture intelligent tool. A set of 1200 emails (including healthy and phishing emails) have been used in this research for analysis and comparison studies.

At the end of each experiment a comparison study with various technologies is carried out in order to validate the proposed models. A constructed password checker (Ptool) is compared to Microsoft, Yahoo, Google, Facebook and CertainKey password checkers. Meanwhile, the phishing capture model outcome is implemented in a tool that is compared to *Microsoft Windows live mail 2009*, *Thunderbird email client* and *Avira antivirus*.

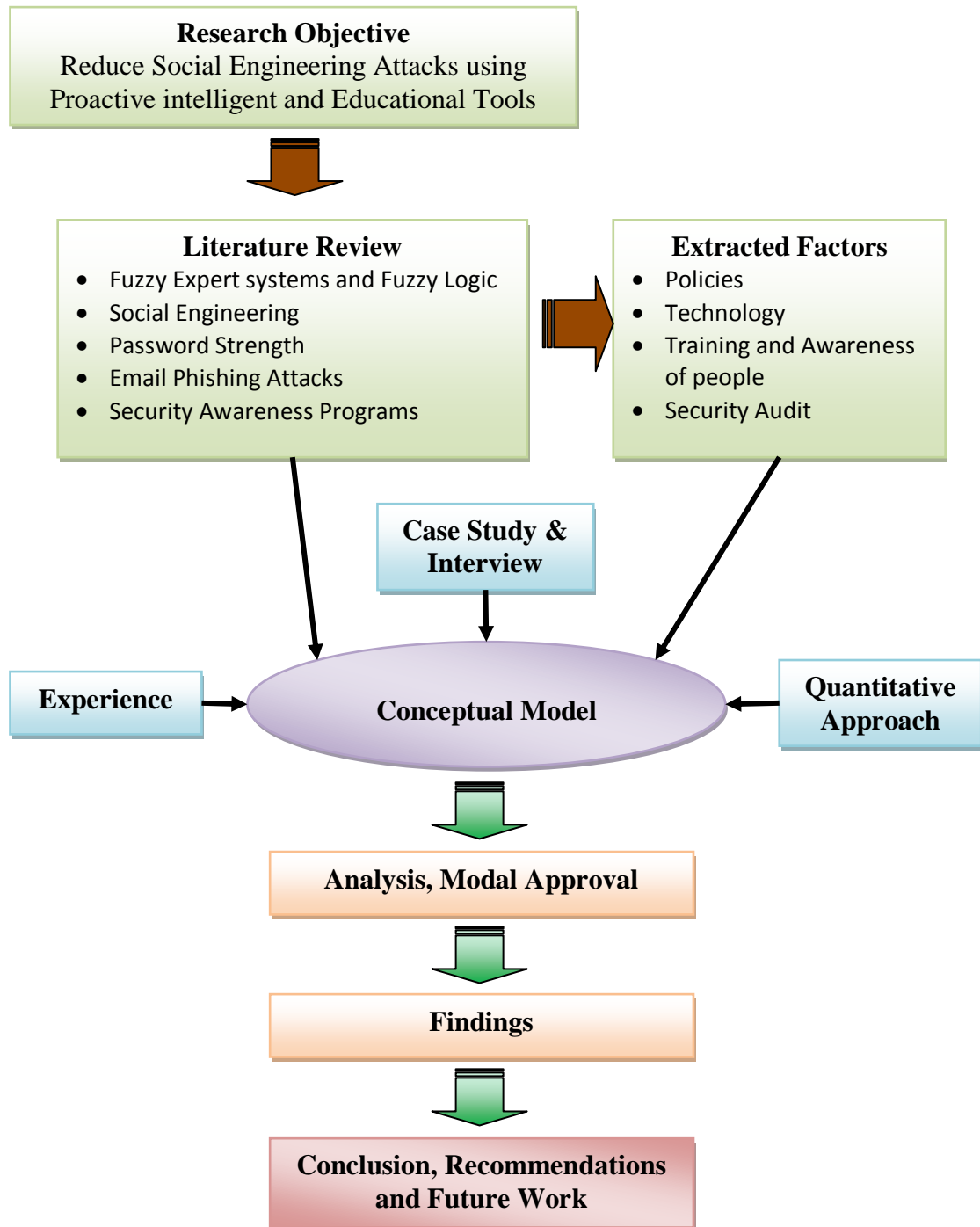


Figure 8: Research Methodology

1.15 Contributions to knowledge

This research has contributed to knowledge in the following areas:

- A security framework is implemented to integrate the three main types of information security controls (people, procedures and physical) into an effective and integrated unit, which helps administrative and security personnel develop required policies that can then be integrated into software modules in order to enforce the said policies. Educational popup messages will help users understand the reasons for the decisions taken by the intelligent tools.
- A new factor is added to measure strength of password, as a shoulder surfing attack is an easy attack with no risk to the attacker (Bidgoli 2008). Shoulder surfing attacks have been ignored by most existing password measuring tools; hence, they are addressed in this research, so that, strong password can be defined as the password that can resist Brute force, dictionary and shoulder surfing attacks
- This study established a quantitative definition of password strength, since this kind of measurement not exists yet.
- An integrated fuzzy model is implemented to measure strength of passwords using three factors - length of passphrase, entropy and dictionary- based; a quantitative measure is represented.
- One of the outcomes of this study is defining password strength, therefore strong password can confront brute force, dictionary and shoulder surfing attacks.
- This research concluded that email phishing attacks are visible attacks with more than 90% of detected phishing emails are easy to detect by human knowledge. In

CHAPTER ONE

other words, they can be avoided by implementing comprehensive awareness security training.

- A new integrated model has been designed using a fuzzy expert system to capture phishing emails in two different layers to reduce the number of rules generated. The first layer is the visible layer (front end of the email) which consists of three main features of phishing emails (generic salutation, Security promises or require fast response and links to https:// domains), then we have the invisible layer (back end of the email or the source code), this layer has three elements as well that are related to phishing emails (IP-Bases, Contain script and number of domains), after that, the output of the two fuzzy processes (front and back end), will be the input of new fuzzy process to get the final rate of the incoming email.
- Finally, incoming emails are categorised into three different types, instead of inbox and junk box folders that are exist in most of the email client software; new folder has been added called *suspicious inbox* to store emails that look like legitimate emails but holding some phishing emails features.

1.16 Thesis Map

This thesis is organised as follows:

1.16.1 Literature Review

In chapter two, a comprehensive review focuses on different technologies and previous work related to this research. This literature review includes expert systems, fuzzy logic in information security, passwords and related measuring tools (existing in the market nowadays); it also addresses

CHAPTER ONE

(through research and discovering different phishing schemas and related researches) this important and serious problem. Finally, information security awareness programs are addressed as this is an important issue that should be taken into consideration during the security process.

1.16.2 Case Study

Chapter three contains case-studies focusing on four different sites. The first was an interview with an IT manager of a renowned bank in Jordan which was exposed to a serious virus attack few years ago. The interview focused on the absence of enforcement of security policies and negligence in implementing security controls such as strong password-measuring tools. The second was a summary study of the implementation of a security policy at an educational establishment, the aim of which was to focus on the importance of the integration of the information security control. Third case study is to find the potential of conducting an internal phishing attacks since there is a lake to implement a restricted security policy. Finally, a simulation of phishing attack has been conducted, including awareness measurement and educational feedback survey, the main objective of this study is to measure the security awareness level of end-users and send an effective concise awareness message to avoid a prospect phishing attacks through a case study.

1.16.3 Intelligent Measuring Tools for Password Strength

This module is a proactive password checker based on Rule-Fuzzy logic to avoid selecting weak passwords. It helps users to gauge their password strength and generate a stronger password to comply with the organisation's policies; it is

based on three factors in measuring password strength such as length, entropy and dictionary-based. The output of this module is categorised into three parts viz. weak, medium and strong. In each category the password is given a strength percentage which gives more accurate results. This module was developed and the results can be found in chapter 4.

1.16.4 Email Phishing Capture Module

In chapter five, the module analyses phishing emails by dividing the incoming email into two parts (back end and front then), then rating the incoming email through fuzzy logic approach. The email phishing model measures the risk of the content of any incoming email by comparing any embedded web addresses with the trusted web addresses in the database. Microsoft and Yahoo (the leaders of the email service providers) still experience problems in distinguishing between safe and phishing emails. Over the last few months the author has received fraudulent emails from Ebay and Paypal websites and various banks. The tool has managed to detect them all.

The proposed solution will estimate the risk of the email through six main features divided into back and front ends. The back end features are invisible to the end-user whereas the front-end features are visible. Accordingly, the incoming email will be ranked as safe, unsafe and partially safe, depending on the content of the email. The user will be able to save the trusted websites on a secured database.

1.16.5 Findings and future works

This chapter provides the final conclusion of this research and sets out the potential for implementing the proposed model in different areas of information security systems.

2 Literature Review

Information security is an important component of the IT management process. It is the way to protect information from a wide range of threats in order to preserve the confidentiality, integrity and availability of any business (Whitman and Mattord 2012).

Social engineering is a serious threat which targets people; it has started to alarm administrators and technicians who believe that tools are the only solution to mitigate security risks (Emirsk 2009). Research and case-studies have addressed the fact that people are the weakest link in the security process, which is why they are usually the preferred target of professionals (Okenyi and Owens 2007). Amanda Andress states that, in order to keep the security infrastructure effective, it is important not to ignore people and processes when spending money on technology (Andress 2003), because products are not enough to build secure IT systems.

In this literature review we will cover the importance of social engineering attacks and the proposed solutions to reduce the risk of this kind of threat; we will then undertake a comprehensive study of shoulder surfing attacks of passwords and email phishing, both of which are two patterns of social engineering threats. After that we discuss the usage of expert systems in information security, focusing on fuzzy logic as that is the technology on which our model is based. Later on, a summary study about the importance of security awareness and training is proposed.

2.1 Social Engineering Attacks

Tim Thornburgh (Thornburgh 2004) argued for the importance of information, especially “who accesses what information”. To access any

CHAPTER TWO

information, the user should be required to pass the IAA steps (Identification, Authentication and Authorisation). The author concentrated on physical security and passwords because of their importance. It can be noted that the social engineering process has a life cycle; it begins with research, rapport and trust, exploiting trust and the utilising of the collected information. Social engineers are usually looking for certain information such as user names, network structure and applications that run on a specific server. By implementing an effective incident response system, subsequent attacks may be prevented. In addition to that, policies, procedures, training and awareness programs may secure the organisation against social engineering attacks.

Gregory L (*et al*) (Orgill, Romney et al. 2004) conducted a case-study by simulating an attack to an organisation using social engineering techniques their methodology based on performing unnoticed a security audit within that organisation. The problem within social engineering auditing is the lack of materials that can be used for this type of auditing. The audit process consists of many phases. Figure 9 shows the steps taken to conduct this case-study.



Figure 9: Steps taken to conduct a simulation SE attack

CHAPTER TWO

Firstly, the attacker obtained a permission from the top management to conduct this audit. Then they started collecting information about the organisation through the website of the organisation and by visiting the offices. After that they used a survey consisting 8 questions to measure the awareness of employees. The trick behind this survey is the questions themselves. The answers to the questions can lead to a real risk to the information system within the organisation. Two of the questions asked for the user names and passwords. After the completion of the audit they discovered that 60% of the employees had submitted their passwords to the auditor and 81% their usernames. This result disturbed the management of the organisation who changed the policies to strengthen their security systems. First, they started educating the employees on the danger of releasing usernames and passwords to unknown people. Then a new multi-factor authentication system was implemented to avoid physical access by unauthorised people.

Barrett (Barrett 2003) discussed how to devise a suitable methodology for evaluating the security of people. The audit process (in his opinion) is not enough to ensure the security level. A focused penetration test is a reliable way of obtaining reassurance. If the results of the penetration testing are successful, that indicates vulnerability in the system. The author's methods of penetration testing were: first, to use tools to attempt to break into and access systems and, second, to use social engineering to gain important information to access those systems. He used two methods to mount social engineering attacks - a simple auditing process, by locating potential targets and identifying the weaknesses in order to exploit them.

CHAPTER TWO

Based on last two case-studies by Gregory L (*et al*) and Barrett, it is noted that people could be the weakest link of security chain; anti-virus and firewalls will not prevent exposing the systems. Awareness and educational programs help organisation to mitigate the risk of social engineering attacks

2.2 Password Strength

Millions of people manage their accounts and protect their documents on a daily basis. The most common method of authentication and protection is to use a username and password (Schneier 2004; Xiaoyuan, Ying et al. 2005) simultaneously. However, the American cryptographer Schneier argues that using passwords is an insecure method to protect offline systems. This is due to that crackers can now break any systems, he stated that using passwords much better on the internet since brute force and dictionary attacks are working best offline (Schneier 2004); hence selecting strong passwords is very important part of to the security process in order to protect privacy. Computer users need to know how to select strong passwords or they should use a measurement tool to gauge the strength of their passwords. A case-study conducted by (Adams and Sasse 1999) showed that many users created their own rules for password selection which may lead to weak passwords.

The term ‘strong password’ is not defined. One of the outcomes of this study is defining password strength. Users and people in general are normally not aware how passwords are cracked (Adams and Sasse 1999). Presently, hackers use many techniques to gain or crack weak passwords. Brute-force attack, which depends on testing all possibilities, is one of the infamous techniques. The new computer processing power helped to perform millions of

CHAPTER TWO

trials in a few minutes (Technology 2006) A dictionary is widely used by password crackers to break into protected documents since most computer users are using common passwords or names for passwords (Kenneth Allendoerfer 2005). The final technique is the shoulder surfing attack which may happen in crowded areas such as internet cafes, airports and computer labs.

The concept of entropy was introduced by Shannon in 1948 as part of the information theory, is defined as “a measure of the uncertainty associated with a random variable” (Ihara 1993)

Password strength can be measured in bits, this measurement concept constructed from the information theory. Therefore Instead of the number of guesses needed to find the password, the base-2 logarithm of that number is used which is the number of "entropy bits" (William E. Burr, Donna F. Dodson et al. 2006).

Therefore, to avoid the aforementioned techniques, security experts agree that strong passwords shouldn't be based on dictionary words, should have sufficient entropy to avoid time crack techniques (Gehring 2002) and should be fully random to evade shoulder surfing attacks.

Many researchers and vendors have developed different methodologies and tools to measure the strength of passwords. Bergadano (et al) (Bergadano, Crispo et al. 1997) used a decision tree to classify passwords as “good” or “bad”. The experiment was performed on passwords of 8 characters and very highly compressed dictionaries. The aim of this research is to find passwords that are partially based on a dictionary or a meaningful word with some

CHAPTER TWO

modification. Meanwhile Duffy and Jagota (Nigel and Arun 2002) presented a connectionist algorithm for testing the quality of passwords by comparing a given password against a large dictionary of words and near-words. They used a compact dictionary stored on the network in distributed form to achieve high performance in testing passwords.

Jeff Yan (Jianxin Jeff 2001) used entropy to measure the strength of passwords. His method depends on exploiting effective patterns to prevent low-entropy passwords. The experiment was conducted on 7-character length passwords.

A machine learning approach to measure a password strength was proposed by (Vijaya MS *et al*, 2009). It was improved by using a combination of different techniques such as Naïve Bayes classifier, Decision tree classifier, Multilayer perception. In addition, a Support Vector Machine (SVM) is applied to train the password strength analysis model. Passwords Features are then extracted from a set of 10,000 passwords based on different categories. In order to simplify the training and implementation, the data set of passwords are generated by a Pc Tools password generator provided by Symantec, a tool that is being used widely to generate strong passwords.

Many websites provide internet users with measurement tools to test their passwords. Other websites (such as Google and Yahoo) apply a password strength meter at the time of creating or updating the password.

Microsoft has developed a web-based tool to measure the strength of passwords (Microsoft 2006). The password rating is divided into four

CHAPTER TWO

categories: “Weak”, “Medium”, “Strong”, and “Best”. By testing many passwords it seems that Microsoft doesn’t consider shoulder sniffing attacks against passwords, e.g., the password “Aaaaaaa1” measured as strong password when was tested in August 2006 and Aug 2010, while “bdztksqfpvwsx” was measured as weak. Basically, the first password complies with the rules of; having small and capital letters and includes number. It is not however sufficiently random hence it can be easily memorised or captured by a shoulder surfing attacker. Miller stated that people can remember 7 ± 2 characters of a given chunk of symbols (Miller 1956); therefore any shoulder attacker can memorise this password at first glance. We can conclude that the first password is easy to remember, but the second one is fully randomised and needs a long time to crack (it needs around 26^{13} probabilities i.e. ~ 64 bits, which makes it stronger than the first one which needs 62^8 probabilities i.e. ~ 48 bits).

CertainKey Cryptosystems is a security company specialising in security and cryptosystems to secure small and medium-sized business networks. The Pass-phrase Strength Analyser is a commercial product for testing the strength of passwords; one can test it online before purchasing (CertainKey 2006). The results of testing a password depend on the number of days needed to crack the password or pass phrases. If the password needs more than approximately 300 days it passes the test. Otherwise the result will be 0 days to crack with a red cross – as conducted on 29thMay, 2011).

By using a dictionary, calculating the entropy of the password “Qwerty123” and using a mixture of character sets (consisting of capitals,

CHAPTER TWO

small characters and a number), this word will take around 4505 days to crack. The reader may notice that this word is an easy one to remember; hence, from a shoulder surfing point of view, this password is not secure enough.

On the other hand, the password “WE3r\$t^4g34&SkY” (which is 16 characters long) has failed the test because it is partially based on the dictionary word “sky” at the end of it. Actually the first 13 characters of this password are fully random with high entropy.

By testing this portion of the password we can get a very strong password that will require millions of days to crack. Adding a small meaningful word to a complicated phrase shouldn’t affect the strength of the password before the addition, while the entropy should be increased.

When one visits the **Google** website to open an email account or to change the password, a strength meter appears beside the password textbox. The passwords on the Google website are rated as “Too short”, “Weak”, “Fair”, “Good”, and “Strong”. When testing many passwords in August 2006 and August 2010, it is noticed that very weak passwords were rated as strong. This can be demonstrated by using the password “zxcv11” in 2006, while the password “159632111” (tested in 2010) was rated as strong, though not too long, memorable and with low entropy – it is a keyboard sequence with a repeated number!

Yahoo is a renowned internet service provider which integrates a measurement tool (comprising four green boxes to indicate the password strength) that appears alongside the password box, when the user attempts to

CHAPTER TWO

create an account or update a password. The final rating is divided into 4 levels; one red box means too short, two yellow boxes means weak, 3 green boxes means strong while a very strong password is indicated by 4 green boxes. A password of 6 characters such as “*Aaaa11*” is rated as a very strong password, while the password “*vjfheijdjueudorsk*” which has 16 characters length is rated as a weak password. We noticed that the second password takes ages to crack (using brute force attack) and it is very hard for any person to glance at or memorise this password using a shoulder surfing attack - this password is unbreakable by normal attack whereas the first password “*Aaaa11*”, is easy, simple and breakable.

Finally, a similar test has been applied to the Facebook password strength meter. On Facebook, one of the most famous social networks in the world with more than 900 million users (Carlson May 2012) hence, privacy is an important matter at their site. The password “*vjfheijdjueudorsk*” which was tested on Yahoo as weak and was rated as weak at Facebook as well, but the password “*Aaaa11*” was rated as weak. However, by adding more characters to it, the password “*Aaaaaa11*” has become a strong one even though it can be easily memorised compared with the first one that was extremely hard to remember.

In conclusion, the author noticed that all available tools related to password strength are actually not based on clear measuring criteria. It is also noticed that no quantitative definition of password strength exists; something that this study has managed to establish.

CHAPTER TWO

2.3 Email Phishing

Phishing attacks target people rather than systems. In order to fraud or breach into other systems and compromise people's privacy, it exploits the weakness of end users and aims to collect user information such as passwords, account numbers, credit card details, social security numbers, date of birth and more (Tyler Moore and Clayton 2007) (Engin Kirda 2005)

Several techniques have been proposed to solve this problem. Unfortunately, this type of problem depends on human awareness. Therefore, the phishing detection algorithm should not be based completely on user interaction (Ian Fette June 2006). Since phishing exploits human vulnerabilities rather than software vulnerabilities, education and awareness are the first step to mitigate the risks of phishing attacks (Larcom and Elbirt 2006; Yue Zhang 2007).

Three types of solutions can be used to reduce the risk of *phishing attacks*:

2.3.1 Anti-phishing Toolbars

Ebay, NetCraft, GeoTrust, EarthLink, CallingID and other vendors offer several toolbars to lessen the risks of phishing attacks. These organisations use different methods to determine the legitimacy of websites such as checking the IP address, combination of heuristics, user ratings, and manual verification (2007; Yue Zhang 2007).

2.3.2 Browser Plug-ins

Microsoft has added a new plug-in to IE7 to help users detect phishing websites. It relies on a blacklist hosted by Microsoft. Another tool from

CHAPTER TWO

SpoofStick is a simple browser extension that helps users to detect fake websites. SpoofStick makes it easier to spot a spoof website by prominently displaying only the most relevant domain information (2005). The Netscape Navigator 8.1 web browser includes a built-in phishing filter. Firefox 2.0 includes a new feature designed to identify fraudulent websites (Yue Zhang 2007).

2.3.3 Email-Filters

Email filters are the most effective solution for detecting spoof websites, since most victims are directed to spoof websites by phishing emails (Liu, Guanglin et al. 2005). By detecting spoofed emails, the user is more secure and the solution, in this case, is categorised as a preventive solution, while the toolbars and browser plug-ins are detective techniques. Ian Fette *et al* proposed a simple technique (to detect spoof emails) called PILFER (Ian Fette June 2006). The filter works by incorporating features specifically designed to highlight the deceptive methods used to fool users. Other researchers classify the email based on structural features such as the number of words in the email, the structure of the subject line, and the presence of 18 keywords that usually exists in phishing emails (M. Chandrasekaran, K. Karayanan et al. 2006). Thunderbird is email client software from Mozilla includes scam and phishing detection capabilities (Mozilla 2010). Other security suits include such filters that integrate with outlook such as Norton internet security suits, Avira and Microsoft Live email.

CHAPTER TWO

2.4 Introduction to Expert Systems

Expert Systems are defined as: “Computer programs that are derived from a branch of computer science research called *Artificial Intelligence* (AI). AI's scientific goal is to understand intelligence by building computer programs that exhibit intelligent behaviour. It is concerned with the concepts and methods of symbolic inference, or reasoning, by a computer, and how the knowledge is used to make those inferences will be represented inside the machine” (Engelmore and Feigenbaum 1993). Expert systems have been widely used in several scientific fields such as medical, engineering and computer applications. Knowledge Based Systems, Fuzzy Logic, Case-Base Reasoning, Neural Networks and Data Mining are major technologies that make up the field of Artificial Intelligence and Expert Systems

2.5 Fuzzy Logic

Fuzzy Logic was conceived by Lotfi Zadeh (in the 60s) who presented data by allowing partial set membership rather than crisp set membership (Kaehler 1998). This is used widely in network security and security risk assessment to measure the exact value of the security status (Luo, Bridges et al. 2001; Shi, Li et al. 2004; Dong-Mei, Jing-Hong et al. 2005). It is easy to understand, close to human thinking and depends on expert knowledge (Negnevitsky 2005). Fuzzy Logic works as a human language to describe the characteristics of a process with terms such as probably, unlikely, quite near etc (Gordon and Jorgensen 1998).

Xingjian Shi(*et al*)(Shi, Li et al. 2004) estimated the network security state exactly. Shi and his team used a fuzzy set and membership function for the input. They used the latter and the predefined fuzzy rule to arrive at the fuzzy conclusion. The detectors collected the raw data from a network, and then audited them using their own rules. The pre-treatment unit fuzzes those results into a fuzzy set and passes it to an inference unit which is communicating with a rule unit to influence the result. Ultimately, the conclusion base stores the final results. The input of the fuzzy set can be captured from the output of the network detectors which are already running in the organisation to monitor network traffic.

Dong-Mei, Zhao (*et al*) used Fuzzy Logic and Entropy theory to estimate the degree of the Information Security risk by using analytic hierarchy process (AHP) (Dong-Mei, Jing-Hong et al. 2005). Since the risk of information security is mutable and uncertain, they used fuzzy logic to estimate then degree of risk of different security threats such as cheating the password, illegal visits, data leaking, destroying equipment etc.

2.6 Security Awareness and Training

The gap between security awareness programs and technical security tools is large. Companies and financial firms should strike a balance between the different elements of security controls (Andress 2003). End users are the weakest link within the security infrastructure, the lack of knowledge leads non-technical users to harm networks in different ways such as selecting weak password, visiting websites infected with malware, responding to phishing e-mails, or even releasing sensitive information over the phone when exposed to

CHAPTER TWO

social engineering attacks (Brodie 2008). Security awareness training should be conducted at all levels of the enterprise (including employees and executive management) at least annually because situations and policies change (Wold March 2006). A study conducted by (D'Arcy, Hovav et al. 2009) at different companies suggested that user awareness of security policies is vital; security education, training, and awareness are three practices that prevent information system misuse. Designing and implementing a security awareness program is not a straightforward task; it is difficult and frustrating (Herold 2010) since dealing with computer boxes is simpler than dealing with humans. Information security specialists state that, in order to improve information security effectiveness within organisations, their recommendation was to encourage good end-user behaviours and limit bad end-user behaviours (Jeffrey M. Stanton, Kathryn R. Stama et al. 2005). Awareness programs should be performed through four steps as in figure 10 in order to achieve the goals and success of such awareness programs. First of all, the program structure should be constructed by assessing the users' needs; this will help to determine the training goals and the target audience. The next step is to develop or purchase awareness materials in any form such as training sessions, posters, guidance, or policies. The materials should be easy to use, scalable to large audiences, and provide a way to track who is using them. After that, the program should take place with full management support. Finally, it is very important to measure the effectiveness of the implemented program through a regular audit team (Mark Wilson and Hash 2003).

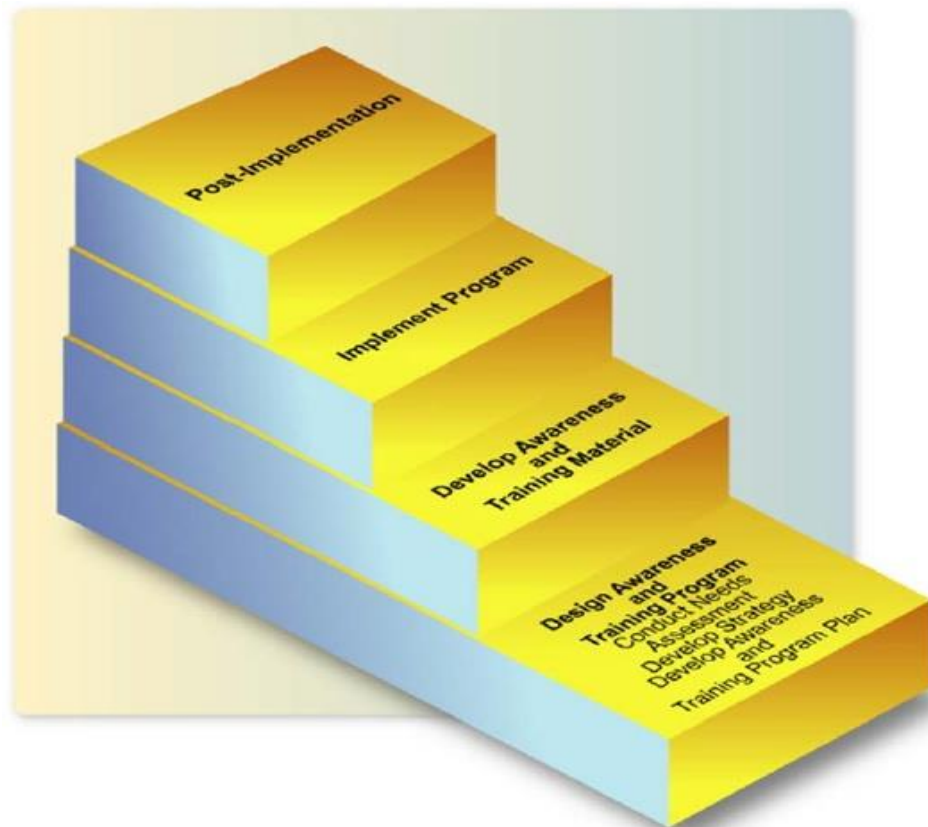


Figure 10: Steps to implement a security awareness program (Mark Wilson and Hash 2003)

Implementing an information security awareness program does not guarantee that all employees will understand their role in ensuring the security and safeguarding of information and information assets. Assessing the awareness program is an important practice in order to address the weaknesses of such programs. A suggested prototype model by (Kruger and Kearney 2006) makes use of a simple data-gathering process and weighting system and combined with certain multi-criteria problem solution techniques to provide a quantitative measurement of security awareness levels.

2.7 Conclusion:

Information security threats are serious problems that can expose enterprises and internet environments as well as individuals to different forms of risks. In

CHAPTER TWO

addition to that, threats are continuously growing yearly. Social engineering attacks are one of the most serious menaces at the moment, since it is targeting the systems through the weakest link in the security chains; the human element. The two forms of social engineering attacks that we discussed in this review are shoulder surfing and phishing emails threats; the first one is a serious problem that has not been taken into considerations seriously by both; security systems solutions providers and researchers. As a result, losing millions of US Dollars is imminent. This matter has caused consumers to fear and losses of confidence in the e-service.

Expert systems used widely in different fields nowadays. Recently, computer solutions including intrusion detection systems, anti-virus, learning systems, decision making algorithms. etc, depends on various expert systems such as knowledge based systems, fuzzy logic, data mining, neural networks and wide range of artificial intelligence techniques.

In this research a security framework is implemented using fuzzy logic expert system to integrate the three main types of information security controls (people, procedures and physical) in order to reduce the risk of two major forms; social engineering attacks including shoulder surfing and phishing emails. The suggested integrated model helps to develop the required policies that can be integrated into software modules in order to enforce security policies in both; public and commercial establishments. Educational popup messages in the form of feedback will help users understand the reasons behind all decisions taken by the intelligent tools.

3 Case Study

3.1 Introduction

Financial organisations are one of the main sectors targeted by hackers nowadays. Additionally, around 60% of information security breaches (in organisations in 2005) were found because of human mistakes. Researchers found that people are the weakest link in the security chain (Peter Hoonakker 2009). In order to address the impact of the absence of a security policy and the failure to implement any part of a security policy, both of which could lead to security breaches. This chapter will discuss three different case-studies. The first one is an interview with an IT manager of one the major banks in Jordan; it highlights a serious security breach that was about to negatively affect the bank's reputation. The second case-study analyses a password policy in an educational organisation. The final case-study is an experiment in conducting an internal phishing attack.

The purpose of this chapter is to show that slackness in implementing basic security policy could leave organisations vulnerable to different kind of attacks, while leniency and neglecting Information Security Policies can cause serious breach of the system. Accordingly, forcing security policy is taken seriously in some organisations. On the other hand, serious attacks such as phishing have succeeded in penetrating systems due to lack of security awareness among employees; in addition to that, security policies need to take into consideration the new and evolving methods of cyber-attacks such as social engineering.

3.2 A case-study about a severe security breach at a major bank in Jordan

3.2.1 Objectives

The case-study aims to address the following objectives:

- a. Study the impact of reluctance to implement security policies.
- b. Importance of security awareness paradigm among employees.

3.2.2 Methodology and introduction to the problem

This case study is based on a direct interview with the IT manager in one of the major banks in Jordan which faced a serious security breach in 2009. For the purpose of this study and to preserve confidentiality, we will be calling this bank “Bank X”, and the manager’s names will be concealed.

This study has shed a light on the bank in discussion in Jordan, which has about 50 branches distributed around Jordan and the region with approximately 1,500 employees and half a million clients. Bank X has led the financial services industry in Jordan and beyond for around 50 years.

3.2.3 Security status before 2009

Most security specialists divide security controls into three main types as in the following diagram (Olzak 2011):

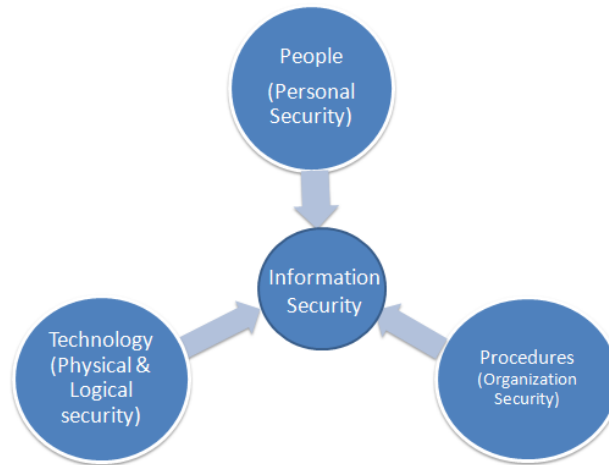


Figure 11: three major types of information security controls

As a financial enterprise, this bank spent hundreds of thousands of dollars building a solid IT infrastructure including hardware and software firewalls, anti-virus VPN to connect their 45 branches, intrusion detection systems, intrusion prevention systems, encryption devices and many other measures. The bank has several security policies but, unfortunately, most of them were not implemented properly and in many cases they were neglected or implemented improperly; according to their IT manager.

The software side was secured by a multi-layer authentications procedure where those end-users who were authorised to use the financial software were forced to access it through four passwords: power-on password, operating system password, core banking system password, and the login to a specific banking module. According to the audit process (conducted in 2009) it was observed that more than 90% of the bank users were using an easy password such as 123 and 1234!

CHAPTER THREE

The bank IT department emphasised on the physical security controls but did not impose the other two controls as expressed in figure 11. The importance of dealing with the human factor and ensuring that the security policies and procedures were properly implemented in order to fully secure the organisation were ignored. As far as we know, people are the weakest link in the security process hence they are likely to be targeted by hackers (Schneier 2000).

The following is a list of security controls which should have been implemented (but were not):

- Regular security awareness program
- Implementing a complex password authentication policy
- Some of the vital policies were not enforced properly such as internet policy and password authentication policy.
- Misconfiguration of some of the procedure implementation
- Lack of antivirus and prevention system monitoring. The audit process, for example, revealed huge carelessness regarding the antivirus definition automatic update
- Access control policies regarding the back-end server room were not implemented and applied

3.2.4 Identifying the problem

The problem started when some users found their user accounts had been locked. The technical support staff mistakenly concluded that an incorrect password had been entered by the user and did not pay any serious attention to the problem. At the end of the day, complaints regarding locked accounts

CHAPTER THREE

increased dramatically to hundreds; the problem at this stage became more serious and precarious.

The network team investigated the locked accounts on the server side to better identify the source of the problem. They checked all back-end servers such as database, web servers and Unix servers in addition to switches, routers and other network components. During that stage it was noticed that the bandwidth traffic was seriously low and sometimes down. Within 24 hours, the network team had declared the problem as a **Conficker** worm attack.

According to the Symantec Corporation, the worm Conficker has different effects on systems, and when computers are compromised by Conficker they are unable to access external sites. As a result, users have to download Conficker removal tools (Symantec 2009). On the other hand, the Conficker worm can also disable important services on infected computers, so systems will not be able to work. This has led to the infection of the bank's applications and additional breaches of the security systems have took place (Microsoft 2009).

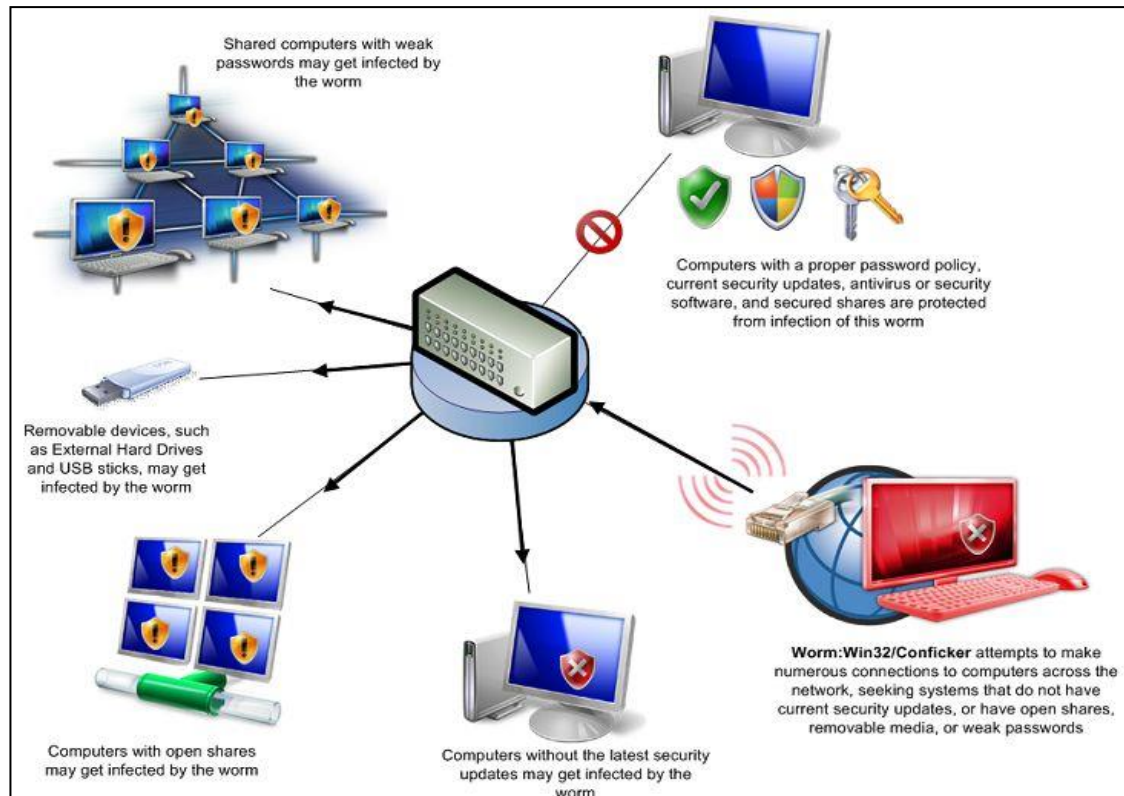


Figure 12: An illustration of how the Conficker worm works (Microsoft 2009)

According to Microsoft, the Conficker worm works using dictionary attacks to access the systems. As explained in the following figure 12, it can be noted that the Conficker worm works properly when there is slackness in the implementation of password and authentication policies. In addition, computers without the latest security updates and with out-of-date antivirus protection are likely to be infected by the worm.

The worm attack took place and succeeded on the basis of two breaches. In the first instance, no password and authentication policy was enforced (the audit process found that more than 90% of users were using weak passwords such as 123). Subsequently, on the server side, the antivirus protection failed to update the client's workstations with the latest security updates. Secondly, no monitoring procedure was applied to observe the update of security applications.

CHAPTER THREE

Consequently, the bank had two main back doors that allowed the attack to succeed:

- 1 – No password and authentication policy was enforced.
- 2 – Lack of security awareness, since more than 90% of users used very weak passwords.

3.2.5 The solution

In order to recover the locked accounts, enable the stopped services, continue the bank services, restore the privacy of thousands of clients and keep the reputational risk low, the network team decided to go through parallel solutions:

First of all, the technical team traced the virus in order to disable its effects. The worm slackens network traffic, so it was important to reduce its effects. This solution (tracing the virus) is considered a corrective one.

Secondly, the team went through proactive solutions by enforcing all policies related to the authentication process such as password length, password life, and multilayer authentication. In addition, a security awareness program was established in order to maintain the confidentiality, integrity and availability of information at both; the technical and end-user levels. A proper and effective security awareness program allows end-users to observe IT security threats and respond within the appropriate time and in the right way (Mark Wilson and Hash 2003).

CHAPTER THREE

Implementing and enforcing new polices were faced by many constraints.

The two major difficulties noticed were:

- The technical team took around 12 weeks to provide training to around 1000 employees in the organisation.
- Furthermore, since most of the users (95% of the bank's customers) were using what could be described as weak passwords such as '123' or 'abc'. The new password policy has managed to force users to have a password of 8 or more characters using a blend of upper and lower case together with numeric characters. Users considered this a challenge exercise that in turn kept the technical helpdesk initially occupied with the re-setting of passwords.

3.2.6 Security status after 2009

This attack forced top management to establish a security department office dedicated to manage and audit all security policies and procedures. The security and compliance personnel established and ensured all information security components are to include people, physical and administrative controls. Nowadays the bank has a regular awareness program conducted by the information security officers. Additionally, a regular biannual security audit is carried out to address any security gaps and other potential threats aiming to improve and sustain the implementation of the security plan.

3.3 A Case-Study of a password policy in an educational organisation

3.3.1 Objective:

The objective of the study is to assess and analysis the email password policy efficiency in educational organisations based on privacy issues and the name of the organisation whether it is a veiled one.

3.3.2 Introduction and methodology

Our case-study examines an academic organisation which has thousands of email accounts of both; staff and students. Protecting such emails is important to that organisation as well as to their staff and students. The organisation has appropriate policies and procedures to reduce security vulnerabilities that could breach the system.

By accessing the webpage of the email portal, users could download the password guidance which includes the security policy and guidance for selecting strong passwords.

The methodology adopted as part of this study is to rigorously test passwords in order to ensure their compliance with the organisation's password policy and guide lines.

3.3.3 Organisation's policy and guidance

The password policy, which can be found on the password change page, states: "*Passwords should contain at least one number, one small and one capital letter and be 8 characters long...e.g Qwerty12*", as shown on figure 13.

CHAPTER THREE



username:

Current password:

Choose password: Verify password:

NB Passwords should contain at least one number, one small and one capital letter and be 8 characters in length...e.g Qwerty!2

Figure 13: password change page shows the enforced policy

The policy guidance states:

- a) A password **MUST** be 8 characters long and **MUST** contain at least one number and one **UPPER** case letter. It **MUST NOT** contain more than 3 repeated characters.
- b) **DO** use a password with non-alphabetic characters, eg digits or punctuation marks.
- c) **DO** use a password that is easy to remember, so that you **DON'T NEED TO WRITE IT DOWN**.
- d) **DO** use a password that you can type in quickly.
- e) **DON'T** use your username in any form (as is, reversed, capitalised, doubled, etc).
- f) **DON'T** use your first name or last name in any form.
- g) **DON'T** use anyone else's name.
- h) **DON'T** use other easily-obtained information about yourself (eg car registration, street name, telephone number).
- i) **DON'T** use a word contained in a dictionary, spelling list, or other list of words.

CHAPTER THREE

3.3.4 Assessing the policy

It was noticed that students were unable to change their passwords when off campus – this facility is only available at the university. Part-time students are not able to change their passwords overseas!

Secondly, the following passwords have been tested and they comply with the organisation's policy:

Ser.	Password	Description
1	Qwerty11	Keyboard sequence
2	Aaaaaa1	Repeated key
3	Abcdefg1	Alphabet
4	AA1salem	Last 5 characters included from the username
5	Zxcv1234	Sequences of keyboard keys and numbers
6	English1	Famous known word with number
7	Qq123456	Ends with sequence of numbers

Table 2: Various passwords tested

Noticeably, all passwords in table 2 can be easily memorised and vulnerable to shoulder surfing attacks. The above passwords comply with the organisation's policy in that they are all 8 characters long and contain capital and small letters and numbers!

CHAPTER THREE

3.4 Potential of conducting an internal phishing attack

3.4.1 Objective

The main goal of conducting this case-study is to find out the potential of conducting an internal phishing attack at the same educational organisation where we carried out the previous case-study.

3.4.2 Introduction

Phishing attacks are web-based tricks that lead victims (end-users, students, buyers) to reveal passwords or other important credentials such as credit card numbers or any other sensitive information (Basnet, Mukkamala *et al.* 2008). They are conducted by using misleading (fake) web pages and emails that look legitimate. One of the most unusual and dangerous phishing attack methods is when the attack is conducted internally using the same domain as the targeted website. For instance, if the intruder uses what appears to be an authorised domain together with a fake email to give a false impression to the user, who logs on to the phishing web page resulting the user inadvertently provides their bona fide details.

A personal file space is allocated for each student where they can store their personal files, assignments, research papers, and other works. Students are able to build a personal website to present their work using a default password given to any registered student based on their date of birth and consist of 6 digits in “*ddmmyy*” format (eg. 210578 to represent 21/05/1978).

According to our investigation, the organisation's policy does not force students to change their passwords when they first log in. An attacker could exploit this with a social engineering attack since finding people's dates of birth is a common, simple method using social engineering techniques such as Pretexting (FTC February 2006). People are encouraged not to reveal their sensitive information including date of birth, national security number or other financial information under any circumstances (US-CERT 2011; Association July 2008).

3.4.3 Elements of conducting an internal phishing attack

The environment of the organisation under consideration has the main elements needed to establish a successful phishing attack. The following diagram shows the main steps of planning, designing, establishing and applying the phishing attack in this educational organisation.

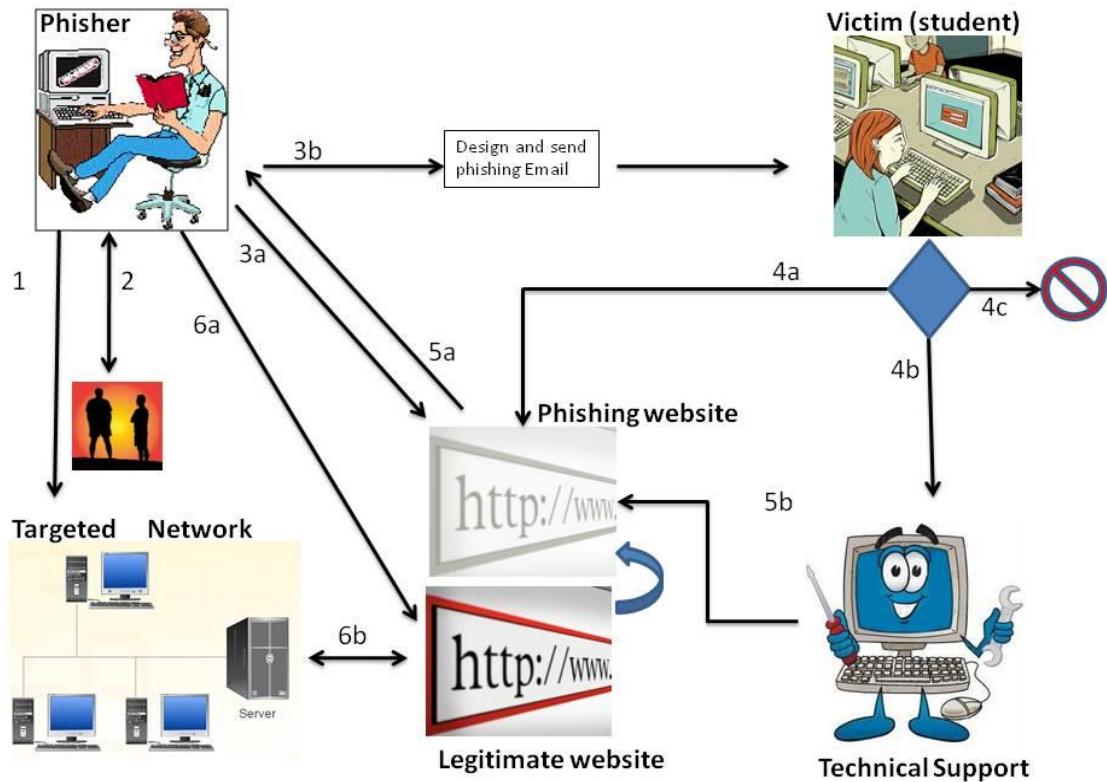


Figure 14: Phishing Attack Scenario

- 1) The attacker usually starts by studying the targeted network and the potential for conducting the phishing attack, finding a web page that will be the potential counterfeit page - in this case studying the target page which is the webmail server page.
- 2) Secondly, the attacker needs to discover the novel network password in order to access the personal web space of the student to build the counterfeit email page. As mentioned above, students are given 6-digit date-of-birth default passwords at the time of registration. According to interviews with some students, they admit to their intention of not to change these passwords and never did in their three years of study. Actually, they have no idea how to do it.

CHAPTER THREE

A simple and smart social engineering dialogue is needed to obtain the date of birth of any person. The following discussion led the victim (student) to reveal the date of birth:

Attacker: Hello, how are you?

Victim: Good, thanks.

Attacker: Happy Birthday, I hope you have a great day!

Victim: But, today is not my birthday, I was born on (21st Sep).

Attacker: Oops, I was confused between your date of birth and another friend's.

Victim: It is ok, no problem.

Attacker: So, on 21st Sep you will be 31 years old.

Victim: No, I will be 33.

According to this dialogue, the victim's date of birth can be easily calculated. Other methods could be used to obtain it, such as using a Facebook account or conducting a phishing call (Mitnick and Simon 2002).

- 3) Once the intruder captures the password, the phishing attack becomes easier; the next step is to design the fake website (step 3a) and then send the phishing email (step 3b).
- 4) The users respond to the phishing emails in different ways (Downs, Holbrook et al. 2007); they either respond to the phishing email by clicking on the fake website (step 4a) or report the phishing email to technical support (step 4b). They may also ignore the email (step 4c).
- 5) If the email is reported to the technical support team or to the help desk, the suspicious website will be blocked immediately (step 5b). It's recommended

that such emails be reported to APWG (reportphishing@apwg.org) (APWG 2012).

But, should the user respond to the email by clicking on the link that leads to the fake website, it is most likely that the attacker will collect the credentials of the user if they try to login (step 5a).

6) Finally, the hacker will be able to use the username and the password of the victim to access the legitimate website using valid credentials (step 6a and 6b).

According to this case-study, we can conclude the following facts:

1. Users are allocated web-space for research and backup purposes.
2. The password policy does not force the users to change their passwords at first login, so users will continue to use their date of birth as a default password to their web-space.
3. Based on the previously-mentioned points and the required elements to successfully conduct a phishing attack in section 3.4.3, we conclude that some members of the educational organisation were exposed to internal phishing attacks using internal servers.

3.5 Simulation of phishing attack, awareness measurement and educationally based feedback

3.5.1 Objectives:

1. Assess the security awareness level of end-users.
2. Send an effective concise awareness message to avoid prospective phishing attacks through a case-study

3.5.2 Elements and Method:

Based on the fact that sending spoof and phishing emails and collecting people's credentials is considered an offence or crime according to most countries' laws (RCMP 2012) (2001). This case-study has been conducted using a safe method to achieve the mentioned objectives while protecting the privacy of participants. The case-study involves sending people examples of phishing emails from known service providers that are familiar to everybody. They are then requested to click on a spoof link to direct them to the phishing website. Phishing websites are normally designed as a perfect match to the genuine ones to deceive users. In order to avoid any errors and omissions by the participants, all the "input box" objects are built as dummy objects. In addition, a warning message is attached to each page to clarify that this page is a "fake website" to show users the similarity between the legitimate and fraudulent websites. At the end of the study a survey is conducted to obtain users' feedback about their experience aiming to measure their security awareness.

The following are the elements of the study:

a) **Selecting the target group**

Since internet users nowadays include various categories, the selected groups are to include students, employees and home users of different ages. They will also include females and males with various educational levels such as undergraduate, postgraduate and high school studies. It is important to point out that students aged between 15 and 20, who are usually unaware of these kinds of attacks, have been included in this study since social networks allow this age group to setup accounts. Furthermore, most of the famous social networks have

become preferred targets of hackers and phishers who use different methods to deceive people. Snap Sniper, the website dedicated to making people aware of Facebook scams, hoaxes and other internet pitfalls, gives useful information about the proper use of Facebook settings. It recently gave a phishing warning about a new type of phishing attack where friends posting links to victim's wall urge them to watch a video. In actual fact, it leads them to fake websites.(Sniper 2012)

b) Selecting the phishing websites

We include in this study two famous phishing schemes. Since most of the 15-20 age group categories are school students, so that most of them don't have bank accounts to suffer from such phishing problems. Accordingly we prefer not to use bank phishing email examples as it will not effectively contribute to the research.

A studied of several common social networks and email service providers has taken place. It was important to find high-demand websites that are concerned about the privacy of their members. Based on this inspection, a decision of selecting Facebook and Microsoft Hotmail is concluded. The first one has more than 990 million users (Carlson May 2012) where privacy is considered extremely important on social networks. The latter (Microsoft Hotmail) is the world's largest web-based email service having more than 324 million members as per comScore figures available in June 2012 (Rigby July 2012). Both of the selected websites are subject to daily phishing attacks.

c) Invitation to participate in the case study:

Approximately 240 invitation emails were sent out to different groups of friends, employees, colleagues and family members in seven different countries asking them to participate in this study. Good responses of 112 were received representing 46.6% of invitations.

d) Defining the problem for the users

The first page is the welcome statement and encouragement to support this study. The following message presenting phishing attacks problem is then presented:

One day, you might receive an email from a company you are familiar with, such as (Facebook, Twitter, your bank or hotmail .etc). They invite you to visit their website to sort out a certain problem.

Alternatively, you could receive an email inviting you to make a donation for a current disaster appeal.

The email will most likely be prepared perfectly. It will look like a legitimate email. In fact, the email could be sent by hackers in order to hijack your credentials or steal your money. The email will encourage you to click on a spoofed link to re-direct you to a fake website.

This kind of scam is called phishing (not fishing). It is one of the most serious problems currently facing internet security.

Briefly, Phishing is *“attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by*

CHAPTER THREE

masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details on a fake website which looks and feels identical to the legitimate one”.

In this study, you will see fake emails and fake websites, then ask you kindly to answer some related questions at the end.

Important note: your credentials will not be saved, only demographic information will be collected for study purposes. } End of the message.

e) **The phishing emails and the spoofed websites**

The first example of a phishing email purports to come from Facebook; the email urges Facebook users to change their password due to an unusual number of invalid login attempts on their account, a common feature of phishing emails. This example warns users to take action within 24 hours - otherwise their Facebook accounts will be suspended.

In addition to that, it contains a reassuring statement such as “*traffic is securely encrypted with a 2048 bits encryption system ensuring that your information remains safe*”

Finally, the spoofed link is included. The visible part is (<https://www.facebook.com>) while the actual link is

CHAPTER THREE

<ahref="http://www.laps.ac.uk/~osasalem/index_eng3.htm"><https://www.facebook.com>).

Figure 15 shows the fake Facebook email as an example of a phishing email.

It is noticeable that this page contains a warning message.

Example 1: Fake Email from Facebook:

Note: if you click at (<https://www.facebook.com>) it will direct you to a spoofed website

.... click at the link below (at the email example) to continuo the study ...

facebook

Dear Facebook user :

Due to unusual number of invalid log in attempts on you account, we had to issue this warning message and put some extra verification process to ensure your identity and your account are secured.

To ensure your protection, we've now blocked access to your accounts. You now need to verify your access online.

Please fill in the form on our secured website below to verify your Facebook account:

<https://www.facebook.com>

If your information will not be confirmed with us within 24 hours your account will be permanently suspended and your funds will be on hold until further notice.

Please note:

1. Your information needs to be exactly as the one we have on file.
2. All the traffic is securely encrypted with a 2048 bits encryption system ensuring that your information remains safe.
3. This is a compulsory measure. Failure to update your information will lead to service suspension.

We are sorry for any inconvenience that this might have caused.

Thanks,
The Facebook Team

You can also use Facebook to plan a [special birthday event](#).

This message was sent to you. If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

Figure 15: First example of Facebook phishing email

When the user clicks on the Facebook link, he/she will be directed to the phishing website, showing in figure 16:



Figure 16: First example of phishing Facebook website

The phishing Facebook page has a high percentage of similarity with the legitimate one. In order to avoid any privacy violation as a result of publishing this page, a warning message has been expressed in red to warn visitors about it. In addition, the text box for the email and password doesn't save any credentials.

The second example is related to Microsoft Hotmail, and the same features have been included on the fake Hotmail page. Figures 17 and 18 show the phishing email and the fake Hotmail page.

CHAPTER THREE

Example 2: Fake Email from Hotmail:

Note: if you click at (<https://www.hotmail.com>) below, it will direct you to a spoofed website
.... click at the link below to continuo the study please...

Windows Live

Welcome to Hotmail

Our system detected someone trying to access your email account several times

To make sure you are the original owner of the account Follow these steps:

- Click on the confirm link below.
- Login to your email account using this email and update your password

<https://www.hotmail.com>

- For more information, visit: <http://login.live.com/help>

For more information or for general questions regarding your e-mail account, please visit [Windows Live Hotmail Help](#).
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA. © 2012 Microsoft Corporation. All rights reserved

Figure 17: Second example of Hotmail phishing email

Microsoft Hotmail

click to complete the study

This is a fake hotmail page !!!! all links are valid !! compare it to original hotmail page ! :)

Schedule an inbox cleanup

Set up Hotmail to clear out old messages so you can focus on the important ones.

[See how it works](#)

Don't have a windows live ID? [Sign up](#)

One Windows Live ID gets you into Hotmail, Messenger, Xbox LIVE - and other Microsoft services.

sign in

Windows Live ID:

Password:

keep me signed in

[Sign in](#)

Not your computer?
[Get single use code to sign in with](#)

2012 [Microsoft](#) | [Terms](#) | [Privacy](#) [Help Center](#) | [Feedback](#)

Figure 18: Second example of phishing Hotmail website

It is worth mentioning that 83% of respondents agreed that the fake websites in this study are very similar to the legitimate Facebook login page and

CHAPTER THREE

the hotmail page, some people having filled in both username and password before we clearly showing the warning message.

f) The awareness part of the case-study:

The second objective of this study is to send an effective, concise awareness message to users to attempt implementing the educational part of the experiment and to avoid the prospect of phishing attacks. Therefore, the following message is used:

Title: How to protect yourself from phishing

Based on our studies, we found that phishing attacks are visible problems. It is also found that awareness training programme is effective in helping people to avoid falling in such traps. Below is some advice that will help you to be better safe:

- Usually, official emails don't include general salutations such as “dear user” or “dear customer”. It should contain your name. General salutations mean suspicious email.
- Use the keypad, not the mouse. Type in URLs instead of clicking on links for online shopping and banking sites that are typically asking for credit card and account numbers. Feeling lazy and clicking on links may take you to an unwanted sites resulting unprecedented experiences.
- Financial organisations or service providers will never ask you for a password or private data. It is also important not to email your information since emails are not secured.
- Don't use public computers to login to your private accounts, as they could be unprotected and risky i.e. having programmes that can register your information.

CHAPTER THREE

3.5.3 Survey and feedback of the study:

Following table 3 shows the Demographics analysis:

Serial	Category	Sub	Number	Total
1	Age Group	15 – 20	20	112
		21 – 25	13	
		26 – 30	18	
		31 – 35	18	
		36 – 40	20	
		41 – 45	12	
		46 – 50	8	
		>50	3	
2	Gender	Female	26	112
		Male	86	
3	Job	Businessmen	5	112
		Employees	54	
		Not Working	4	
		Students	49	
4	Education Level	Diploma	6	112
		School	22	
		High Studies	47	
		University Graduate	37	
5	Country	Canada	2	112
		Jordan	57	
		Kuwait	1	
		Saudi Arabia	8	
		UAE	11	
		USA	2	
		UK	28	
		Other	3	

Table 3: Demographics analysis of the case study

All participants were asked four questions in order to measure their awareness level and assess their knowledge of phishing attacks. The questions and feedback collected are as follows:

1. Have you heard about phishing problems before?

Available answers:

- It is the first time I hear about it
- I'm not sure about it
- Yes I know it very well

Figure 19 shows the responses to Question 1:

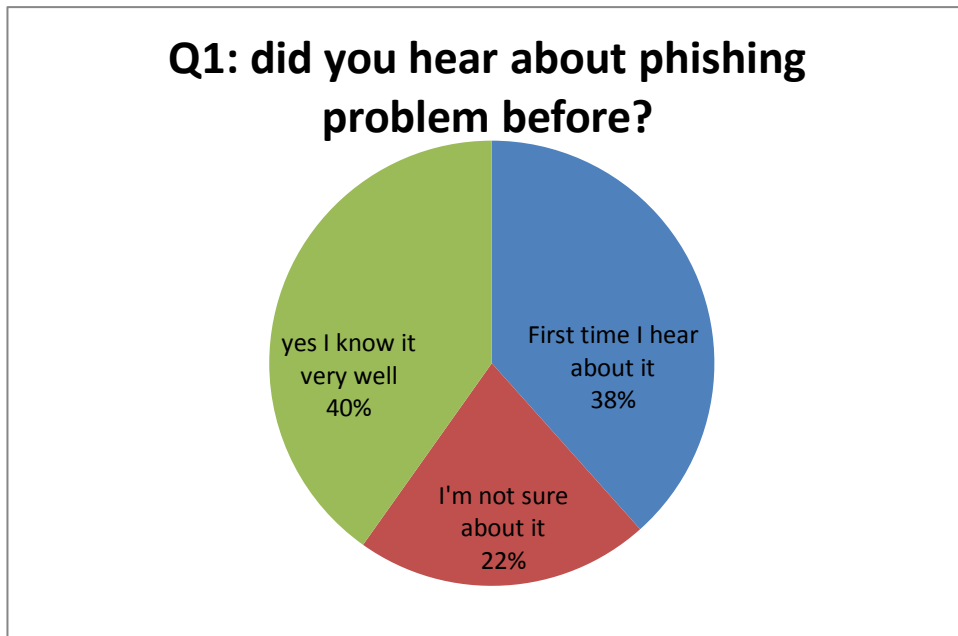


Figure 19: Responses to Question 1

It is noticeable that this problem is quite well-known nowadays, since 62% of the people who answered this question are either knew the problem very well or were not sure about it. However, this does not mean that this sample of end-users is aware of how to protect themselves against attacks.

2. How much did the spoofed websites that I showed you look like legitimate ones?

Available answers:

- Slightly different
- They are not similar
- They are very similar

Figure 20, shows the responses to Question 2:

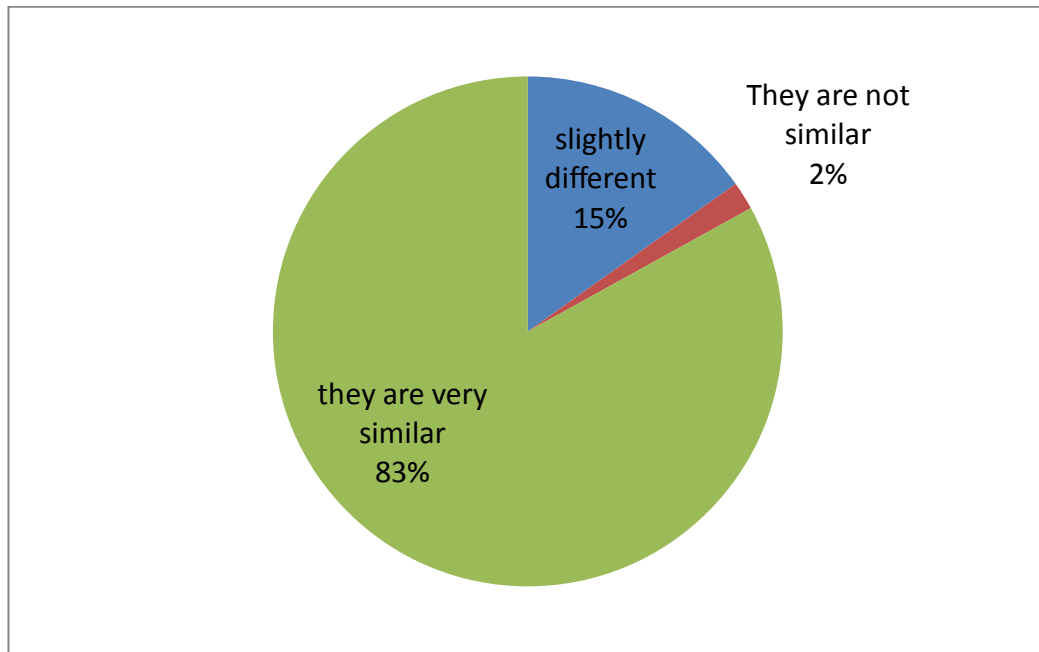


Figure 20: Responses to Question 2

In this figure, the majority of the participating users believed that the fake websites included in this study are similar to the official pages of Facebook and Hotmail. It is worth mentioning that one of the users sent us an email showing that the Site Safety Centre software from Trend Micro Security systems has detected our fake page as a suspicious phishing page. Meanwhile, Norton

CHAPTER THREE

Internet Security 2012 prevented some users from completing the study as the visited page is a phishing page.

3. One of the study objectives is to make you aware about this problem. Do you think it was a useful study?

Available answers

- No, it wasn't
- Yes, very useful
- Yes, it was ok

Figure 21 shows the responses to Question 3:

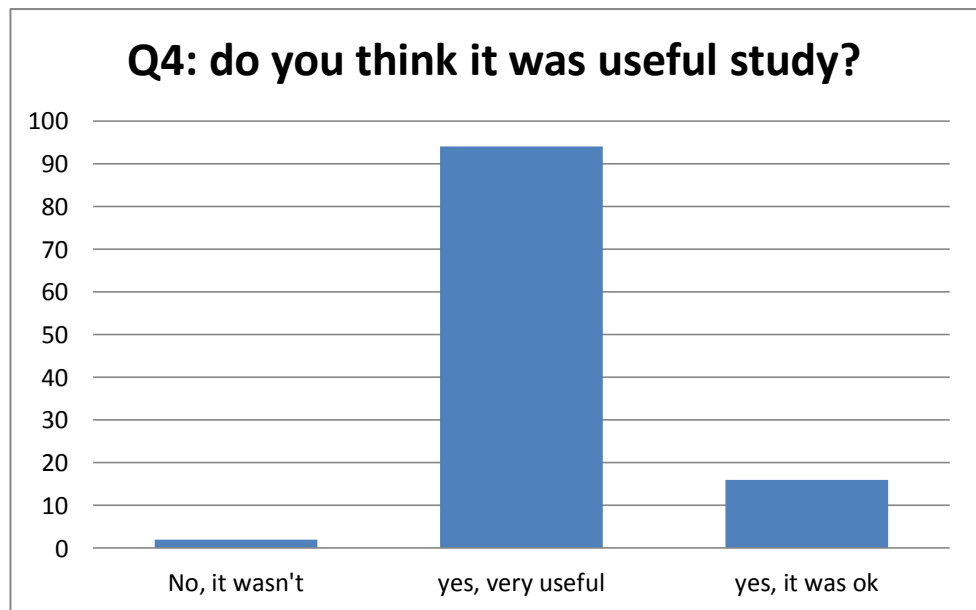


Figure 21: Responses to Question 3

It can be concluded that this study objective has successfully attained as, in this question, around 94 of the 112 participants (84%) believed that the experiment was very useful while 16 said it was acceptable. Only 2 users have found it not useful where they can be security educated ones.

4. How do you think the risk of this problem (phishing) can be reduced?

Available answers

- Anti-phishing tools and security software
- By training and awareness programs
- Both of them

Figure 22 shows the responses to Question 4:

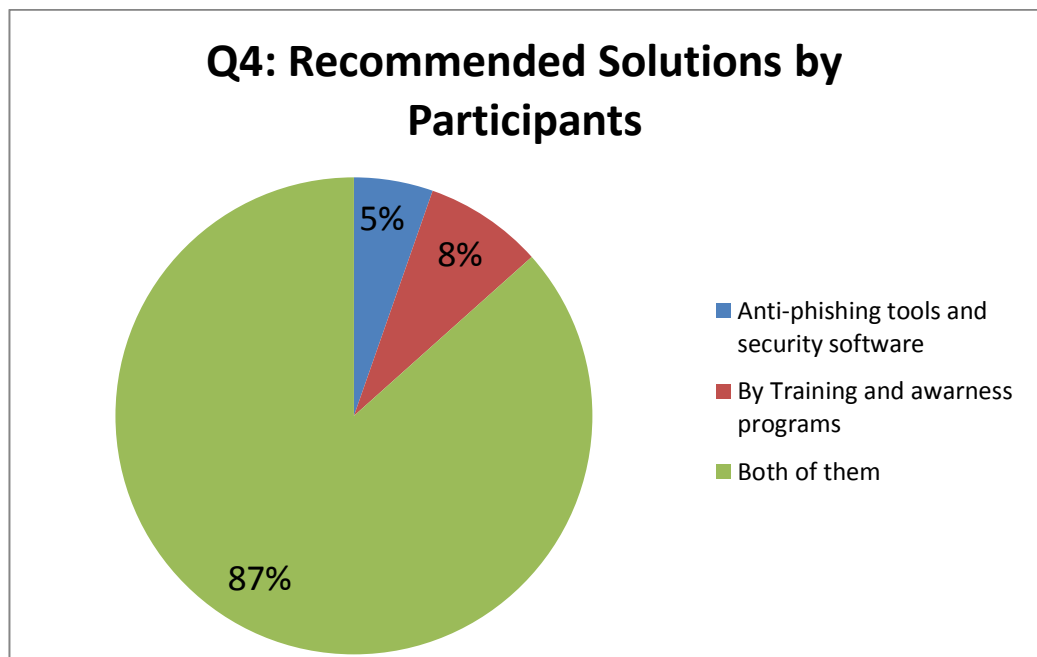


Figure 22: responds to Question 4

The majority of the respondents (87%) believed that this problem can be reduced by installing anti-phishing tools which are already built into most security software and awareness programs.

The final section of this study asked the participants to send their feedback about the study and their experience related to phishing problems. The following are some of pinions expressed at the end of the survey.

CHAPTER THREE

- “I know this problem from some messages which I received from my bank highlighting this problem; there was some software distributed by this bank to help avoid phishing websites. The software is called Trusteer”.
 - “Many forums and websites help people to create phishing websites; you don't have to be a hacker in order to defraud people.”
 - “My Facebook account has been stolen, then I managed to recover it through my email; it's better to use different passwords for different accounts.”
 - “I heard about this problem before, but I didn't know that hackers could create the same pages of the social networks that make people trust it. Usually I don't open any suspicious emails except in some cases like sending email for specific destinations.”
- “Phishing could be accurately described as unauthorised activity during which an intruder and unscrupulous computer user tricks individuals into divulging privilege information and bank and credit card numbers”
- “I had friends who received spoofed PayPal emails from people who wanted to buy their items. So the person receives fake email from "PayPal" telling them that money has been put into their account and the person who is uneducated about this topic does not log into the real PayPal to check - he sends out the item and is scammed”.
 - “I have read about this problem in different media and newsletters, but I never expected that they could build fake pages with high similarity.”

- In addition to that, many of the contributors expressed their gratitude and compliments to the organisers as it was a useful study since it made them aware of this serious problem. It's important to indicate that, for more than 38% of the participants, this was the first time they had realised this problem existed.

3.6 Findings

The first case-study shows that neglecting security policies implementation has exposed the bank to a severe problem. The investigations revealed that 94% of the users were selecting easy passwords such as “123” this allowed the virus to infect the systems in few hours and halted the bank's services. On the other hand, in the second case-study we found that the organisation forces users to select a password with a certain length and a mixture of small and capital characters with numbers. However, it is found that people could select repeated characters such as “Aaaaaaa1” that can be easily captured by shoulder surfing attack. Therefore, the password policy should take into consideration all kinds of password attacks such as brute-forcing, dictionary-based and shoulder surfing attacks. In the third case-study we found that slackness in implementing a basic security policy could leave the organisation vulnerable to an internal phishing attack, since the users were given a default “Date of Birth” password which they were not forced to change at first login. In addition to that, granting people web-spaces in the organisation's servers under (considering weak policies are in place) subjected the organisation to internal phishing attacks that have managed used the official domain of the enterprise.

CHAPTER THREE

The final survey indicates that phishing emails are still a serious threat for internet users. Anti-phishing tools are not enough to reduce the risk of this problem. Training and awareness programs are playing a role in protecting the privacy of the internet environment.

In order to increase the performance of security systems to reduce the impact of social engineering attacks such as shoulder surfing and phishing, it is important to integrate security policies, anti-phishing solutions and awareness programs into a homogeneous security scheme augmented by a continuous security audit process on a regular basis to address and ensure the smooth flow of the working systems.

Based on the above studies, it is obvious that policies should be written, implemented and observed through a regular audit process. The mere existence of a security policy doesn't mean that the risk of attacks is reduced.

4 Password Strength

4.1 Introduction

Many computer users are managing their accounts and stock portfolios, accessing e-services and taking measures to protect their systems and documents every day. Authentication is the most common method used in these measures, where the user is using system passwords or document protection (Schneier 2004; Xiaoyuan, Ying et al. 2005).

A report from Cambridge University Computer Laboratory states that one the most famous vulnerabilities nowadays is using weak and insecure passwords (Bonneau 2012), hence selecting strong passwords is very important factor of protecting our privacy. Many computer users do not have enough security knowledge to be able to select strong passwords; hence they should use a measurement tool to gauge the strength of their passwords. Many users create their own rules for password selection which may lead to the selection of weak passwords (Adams and Sasse 1999).

The term ‘strong password’ is vague. Users and people in general are normally not aware how passwords are cracked (Adams and Sasse 1999), since some long passwords can be cracked in seconds (Dieterle 2010). Hackers use many techniques to gain access to or crack weak passwords; one of the most famous techniques is a brute-force attack which depends on testing all the possibilities. The new computer processing power helps to perform millions of trials in a few minutes (Technology 2006). A dictionary attack is widely used by password crackers to break into protected documents since most computer users are using common passwords or names for password protection

CHAPTER FOUR

(Kenneth Allendoerfer 2005). The shoulder surfing attack is a third technique being used. It often takes place in crowded areas such as internet cafes, airports and computer labs, users are responsible to defend against this kind of attacks (Wiedenbeck, Waters et al. 2006). Therefore, to prevent the three aforementioned techniques (brute-force, dictionary and shoulder surfing attacks) security experts agree that strong passwords should not be based on dictionary words, should have sufficient entropy (Gehring 2002), and should be fully random.

Many researchers and vendors have developed different methodologies and tools to measure the strength of passwords. These include Microsoft, Google, Yahoo, etc. Bergadano and co-authors (Bergadano, Crispo et al. 1997) used a decision tree to classify a password as “good” or “bad”. The experiment was performed on passwords of 8 characters in length and very highly compressed dictionaries. The aim of the research was to find passwords that are partially based on the dictionary or meaningful words with some modification. Meanwhile Duffy and Jagota (Nigel and Arun 2002) presented a connectionist algorithm to test the quality of passwords by examining a given password against a large dictionary of words and near-words. They used a compact dictionary stored in the network in distributed form to achieve a high performance in testing passwords.

Jeff Yan used entropy to measure the strength of passwords; his method conducted on 7 characters length of passwords and depended on exploiting effective patterns to prevent low-entropy passwords (Jianxin Jeff 2001). Length and complexity are important factors in strengthening passwords (Scarfone and Souppaya 2009).

CHAPTER FOUR

4.2 Factors affecting password strength

Literature shows that there are three Critical Factors affecting password strength.

These are:

4.2.1 Shoulder surfing (password length)

Length of a password is an important factor, people should aware about it, since it is their responsibly to protect themselves against such attacks (Wiedenbeck, Waters et al. 2006). Human ability is capable to memorise words consisting of (7 ± 2) characters (Miller 1956), length is not enough to secure passwords in some circumstances as a 14 characters password could be cracked in seconds (Dieterle 2010).

4.2.2 Dictionary based

This kind of attacks is based on using huge dictionaries, it is success at offline systems usually (Schneier 2004) and with easy to remember passwords that people are used to choose (Lin Chun-Li, Sun Hung-Min et al. 2001). So it is important to select strong password that is not based on dictionary.

4.2.3 Password entropy (Character sets)

Password entropy is related to complexity of the password length and character sets used, so in order to double the number of guesses required cracking the password, adding one bit of entropy to the password will make the attacker's task twice as difficult. (William E. Burr, Donna F. Dodson et al. 2006)

CHAPTER FOUR

Since the entropy estimates the time required of crack, passwords with low entropy are considered weak (Jianxin Jeff 2001). The entropy of a given password can be increased by increasing the size of the password and the variety of different character sets used.

4.3 Existing Tools and Approaches

Several online measurement tools are provided for internet users to test their passwords. Google, Yahoo and Facebook for example have a password strength meter integrated with the registration form which can be utilised when creating a new account or changing a password.

Microsoft, (the global software leader) CertainKey Cryptosystems, Google, Yahoo, and Facebook have qualitative online measurement tools. The following are the main characteristics of these tools:

4.3.1 Microsoft

Microsoft has developed a free web-based tool to measure the strength of passwords (Microsoft 2006) with an update in 2011 (Microsoft 2011). Passwords are divided into four categories: “Weak”, “Medium”, “Strong”, and “Best”. Following the testing of many passwords, it appears that Microsoft does not consider shoulder surfing attacks in their assessment of passwords. Table 4 shows two different passwords that were tested on a Microsoft platform in May 2006 and June 2011.

CHAPTER FOUR

Password	Length	Entropy	Memorable	Rate 2006	Rate 2011
Bbbbbbb1	8	~48 bits	Easy	Strong	Weak
eoqpwsjfhvdlfkep	16	~75 bits	Hard	Weak	Strong
aaaaaa1234567	13	~67 bits	Easy	-	Strong
aaaaaaaaaaaaa	14	~66 bits	So Easy	Weak	Strong

Table 4: Passwords tested by Microsoft password checker

Basically, the first password complies with the rules of having small and capital letters and one numerical digit, but it does not have sufficient randomness and just two keys of the keyboard are used, one of them used twice as small and capital letters.

According to Miller's findings, this type of password can easily be memorised and captured by any shoulder surfing attacker at first glance. We agree that this password is easy to remember, however, the second one is not because it is fully randomised and needs a long time to crack. Additionally, the second password is hard to capture by a shoulder surfing attacker (it needs around 26^{16} probabilities ~ 75bits, making it much stronger than the first one which needs 62^8 probabilities ~ 48 bits). The third and fourth passwords are long but they are easy to memorise and can be captured easily by shoulder surfing attacks.

It is worth mentioning that Microsoft has updated its password strength measurement technique. We noticed that the ratings for the first two passwords in table 4 have been changed from weak to strong, and from strong to weak, respectively i.e. moving in the right direction. meanwhile the last two passwords in the previous table show that shoulder surfing attacks have not been considered, as these passwords “aaaaaa1234567” and “aaaaaaaaaaaaaaaa” can be captured easily by curious people in spite of the fact that they have high entropy rates.

4.3.2 CertainKey Cryptosystems

This is a security company specialising in security and cryptosystems to secure small and medium-sized business networks. The ‘Pass-phrase Strength Analyser’ is a commercial product for testing the strength of passwords; one can test it online before purchasing (CertainKey 2006). The result of testing a password is based on the number of days needed to crack the password or pass-phrase. The password will pass the test if it takes more than approximately 300 days to crack. Otherwise, the result will be 0 days to crack, showing a red cross (conducted on 21st Jun 2010).

By using a dictionary, calculating the entropy of the password “zxcvbnm111” and using a mixture of character sets (consisting of small characters and numbers); it will take around 27888 days to crack this password. The reader may notice that this word is easy to remember as it consists of the last line on the keyboard with a repeated number, so from a shoulder surfing point of view this word is not secure enough.

CHAPTER FOUR

On the other hand the password “*EDkfeux\$£dkwo12boy*” (which is 18 characters long) failed the test because it is partially based on the dictionary word “boy” as shown in figure 23. Actually the first 15 characters of that password are fully random with high entropy. By testing this portion of this password we get a very strong password that will require millions of days to crack, i.e. adding a small meaningful word to a complicated phrase shouldn’t affect the strength of the password.

Passphrase cannot be based on an English word		
Based on: 'boy'		
Lower-case Letters	12	✓
Upper-case Letters	2	✓
Decimal Digits	2	✓
Other Characters	2	
Total Characters	18	✓
Entropy (in bits)	3.94	✓
Days to Crack Passphrase	0	✗
Passphrase	EDkfeux\$£dkwo12boy	

Figure 23: CertainKey password checker fail to rate strong password

4.3.3 Google:

By visiting the Google website to open an email account or change the password, a strength meter, integrated with the registration form, appears beside the password textbox. Passwords on the Google website are rated as “Weak”, “Fair”, “Good”, and “Strong”. By testing many passwords on the 22nd Jun 2009, it was noticed that, according to our definition, very weak passwords were rated

CHAPTER FOUR

as strong. This can be demonstrated by using the password “zxcv1111”. This is rated as a strong password as in figure 24, though it is memorable and has a keyboard sequence with a repeated number!

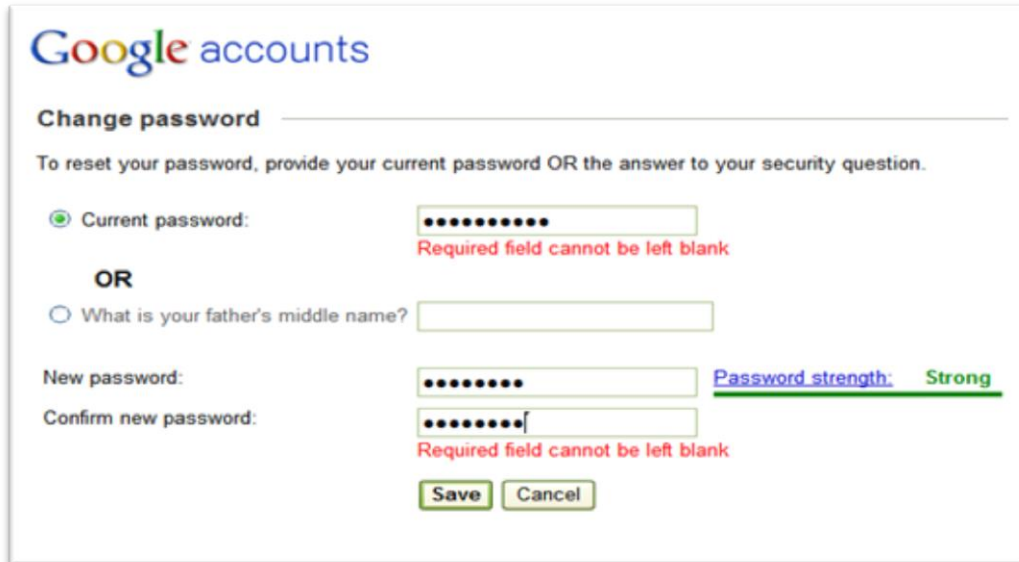


Figure 24: password checker from Google

By performing the same test on the Google website in June 2011, we noticed that passwords of 8 characters, such as “zxcv1111”, were rated as “Good” while adding one digit at the end makes it a strong password such as “zxcv11111” which was considered “Strong”.

4.3.4 Yahoo:

This is one of the largest internet service providers in the world and has a similar technique for rating a given password. When the user attempts to create an account, an integrated password checker helps to gauge the strength of the new password.

CHAPTER FOUR

Four green boxes appear beside the password's textbox to indicate the strength of the given password. The final rate is divided into 4 levels; one red box means too short (as in figure 25), two yellow boxes means weak, three green boxes means strong while a very strong password is indicated by four green boxes.



Figure 25: password checker from Yahoo shows a strong password as weak password

By testing many passwords, it can be noticed that the password strength measuring tool doesn't work properly. Following are some passwords tested in June 2009

Password	Length	Entropy	Memorable	Rate
aaa111	6	~31 bits	Easy	Strong (3 green boxes)
eRxq1pwQsjfNhvd\$ffff	20	~112 bits	Hard	Too short (1 red box)

Table 5: Passwords tested by Yahoo password checker

We noticed that the first password can be easily cracked, since it is 6 characters long, has low entropy and is easy to memorise. This password was rated as strong in June 2009 by Yahoo's password checker. On the other hand, the second one is more complicated; it is 20 characters long, has high entropy and is hard to catch via shoulder surfing attacks. The last 4 digits of the password are repeated, but that should not affect the whole password, since the first 16

CHAPTER FOUR

characters are strong. According to the new rating system supplied by Yahoo, the second password was rated as Very Strong.

4.3.5 Facebook:

Finally, we tested Facebook's password checker. Facebook is one of the largest e-society websites worldwide, where privacy is important. A password meter as shown in figures 26 helps the user to measure the strength of the selected password.



Old password: [password masked]

New password: [password masked] ?
(required) Password strength: **Strong**

Confirm password: [password masked]
(required) **Passwords match**

[Change Password](#)

Figure 26: Facebook Password checker shows strong password

A password such as “A1111111” was rated as strong, although it can be easily captured by a shoulder surfing attack. Meanwhile, a password such as “e0qpwasjfhbvdclfkex” was rated as weak, although it consists of 20 characters, is fully random (~94 bits Entropy) and is hard to capture by a shoulder surfing attack. Clearly, this checker failed to measure the strength against shoulder surfing attacks.

In this chapter we present an investigation into the evaluation of password strength by using a new tool to measure the strength of passwords using Fuzzy rules. The new tool is designed using artificial intelligence to measure password strength against any dictionary, brute-force and shoulder

surfing attacks. Finally, comparative performances of the proposed tool and existing tools are presented and discussed to demonstrate its merits and capabilities.

4.4 Proposed Methodology

The proposed methodology was built using the fuzzy logic rule base. Fuzzy logic is used widely in network security and risk assessment to measure the exact value of security status. It was conceived as a better method for handling data since it mimics human control logic. It uses an imprecise but very descriptive (more like a human operator) language to deal with input data. It is very robust and forgiving of operator and data input and often works when first implemented with little or no tuning.(Luo, Bridges et al. 2001; Shi, Li et al. 2004; Dong-Mei, Jing-Hong et al. 2005).

To build a strong measurement algorithm using Fuzzy sets to prevent dictionary, brute-force and shoulder surfing (social engineering) attacks, three factors are considered:

Password length is the first factor taken into consideration; the password is supposed to be long enough to avoid brute-force attacks and confound human memory. Recent experiments performed by Lockdown Security Centre (Center 2006) show that a password of 6 characters can be instantly cracked regardless of the entropy of that password, while cracking those of 7 or 8 characters in length is dependent on the entropy of the passwords and the machine used to crack it.

CHAPTER FOUR

Back to Miller's research (Miller 1956) on human mind capability, who stated that a person can remember 7 ± 2 symbols from a given string of random characters. Therefore, to prevent single-glance shoulder surfing we might consider a 10-character-length password as the start of a strong password, depending on the other factors.

The second factor is dictionary-based passwords. Many researchers agree that passwords should not be based on a dictionary (Gehring 2002; Xiaoyuan, Ying et al. 2005), simply because the hackers are using huge dictionaries that consist of thousands of words, names, brands, movie names and common passwords to crack protected documents and websites. In some cases the password could be partially based on a dictionary (as in the 16 characters password "Edkfeux\$dkwo1boy" which CertainKey tool regarded as weak because it contains the word "boy" that represents no more than 20% of the total word length while the other 80% is very complicated phrase and so hard to be glanced or hacked). In this case we may accept the password to be partially based on dictionary as long as the other portion is enjoying adequate strength. Accordingly, the keyboard patterns are to be considered in the measurement.

A Visual Basic algorithm is deployed to consider all the sequences and patterns of keyboard keys, alphabetic and numerals, to avoid creating easy passwords that are vulnerable to shoulder surfing attacks.

Entropy of the password is the third factor and a very important one. The entropy estimates the time required to crack the password. Passwords with low entropy are considered weak (Jianxin Jeff 2001). The entropy of a given

CHAPTER FOUR

password can be increased by increasing the size of the password and the variety of different character sets used.

To calculate the Rate (R) of a language containing L characters, we use the Log base 2 algorithm (Schneier 1996):

$$R = \text{Log}_2 L \quad (1)$$

On the other hand, the Entropy of a character set can be calculated by using Shannon's estimation (Shannon 1951):

$$H = -\sum P(x) \log_2(P(x)^{-1}) \quad (2)$$

Where $x \in$ Character set

The two formulae (1) and (2) will produce the same result, The following table shows the character set's components, and the size of each character set:

Character Set used	Character Set Size
Numbers	10
Capital or Small Letters	26
Special Characters	33
Numbers & Small Letters	36
Small Letters & Special Characters	59
Small Letters, Capital Letters & Special Characters	85
Using all Character Sets	95

Table 6: Length of different character sets

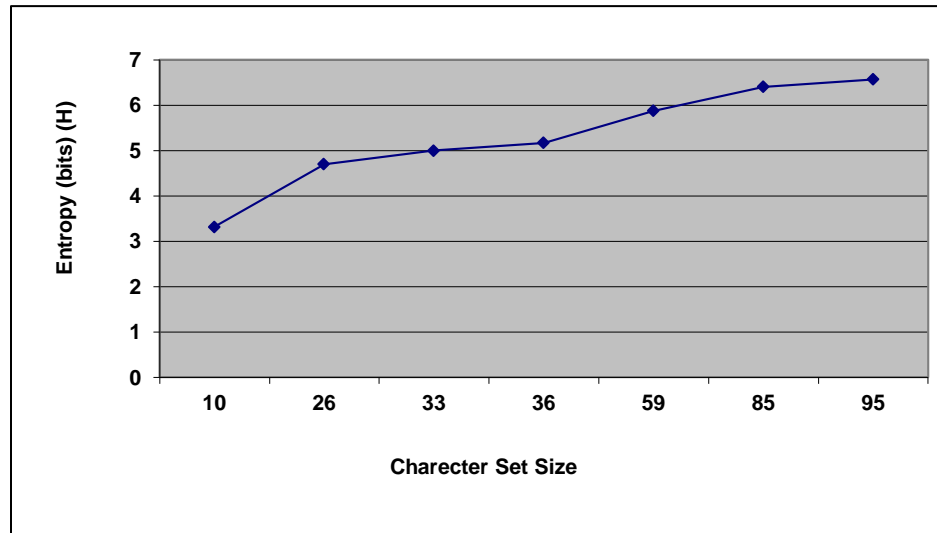


Figure 27: Entropy of different character sets

It is noticed that the entropy can be increased by using a mixture of different character sets.

The Entropy PW_E of a fully random password of length L can be calculated as follows:

$$PW_E = H * L \quad (3)$$

For a given password of 10 characters and mix of numbers and small letters, the key space of the password (according to table 6) will be 36 characters. Therefore, the maximum entropy will be $\log(36) / \log(2) \sim 5.16$ bits per symbol and the entropy of the password according to equation (3) will be $5.16 * 10 = 51.6$ bits.

For English words, Shannon estimated the rate of entropy (R) as 2.3 bits per symbol, while Bruce Schneier in (Schneier 1996) estimated it as 1.3 bits per symbol based on Thomas Cover's studies. Thus we are using the latest

CHAPTER FOUR

estimation technique of Schneier to calculate the Entropy of meaningful passwords which is 1.3 bits per symbol.

In case of passwords that have English words and random text, according to equation (2) (which shows that the entropy is a summation of the probabilities of each character) we consider the total entropy to be equivalent to the summation of the entropy of each part.

$$PW_E = H * L_{(Random\ part)} + R * L_{(English\ word\ part)} \quad (4)$$

4.5 Combined Model

The three factors (Length, Dictionary-based and Entropy) are combined into one model through a fuzzy process in order to obtain the rating of the password with each given factor represented as a membership function on three different levels. As a rule, fuzzy systems have been built to provide the rating of a given password; detailed membership function is shown in section 4.7. The following figure demonstrates the fuzzy process

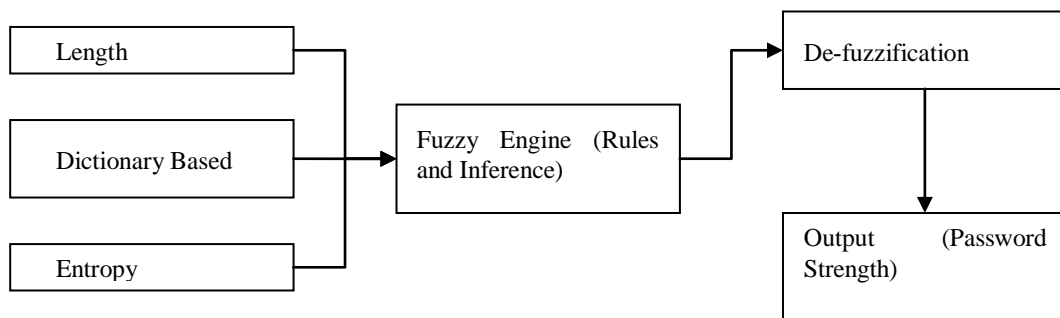


Figure 28: The Fuzzy Process

4.6 Quantitative Approach

Based on the quantitative values given to the password strength factors, it is possible to quantify the measurement and make it easy for the interested users to measure the strength of their passwords to help them make a decision.

The reader may have noticed that all addressed tools are indicating the strength as Weak, Medium, Passed and Strong. The proposed tool is designed to show the results as a percentage of a strong password using the three known measures simultaneously. Knowing that 50% of password strength does not reflect a weak password, organisations may choose the present at which a password is accepted to them.

4.7 Experiments and Results

The three factors mentioned above are weighted carefully to produce a strong password that can resist dictionary, brute-force and shoulder surfing attacks. Each input has three-membership functions of a Fuzzy scheme.

4.7.1 Length:

Length of a password is an important factor, due to the human ability to memorise words consisting of (7 ± 2) characters (Miller 1956). Any given password is considered *short* when it's 7 characters or less, while a complicated 10 characters password is considered *Long* since it will take a long time to be cracked using a brute force attack. Finally, password length of 7 to 12 characters are considered *medium* based on other factors.

CHAPTER FOUR

Three membership functions (Short-Medium-Long) of length factor are shown in table 7:

<i>Length of password</i>	<i>Membership</i>
0 - 7	Short
7 - 12	Medium
10 - 14	Long

Table 7: Membership of password length

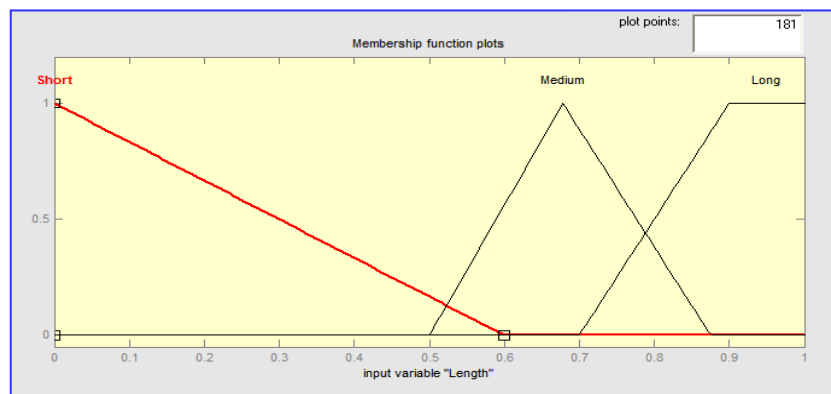


Figure 29: Membership Function of Password Length in MATLAB

4.7.2 Dictionary based

The importance of this factor is to avoid dictionary attack; if a dictionary word forms more than 60% of the length of a password, the password is considered “*fully based*”, while those with more than 30% and less than 80% are considered “*partially based*”. If more than 70% of the password is not based on

CHAPTER FOUR

a dictionary word it is considered “*not based*”. The following password table 8 shows the three memberships of the dictionary-based factor.

<i>Dictionary Based</i>	<i>Membership</i>
More than 60% based on dictionary	Fully Based
30% to 80% consists in dictionary	Partially
More than 70% not based on dictionary	Not Based

Table 8: Membership of dictionary based

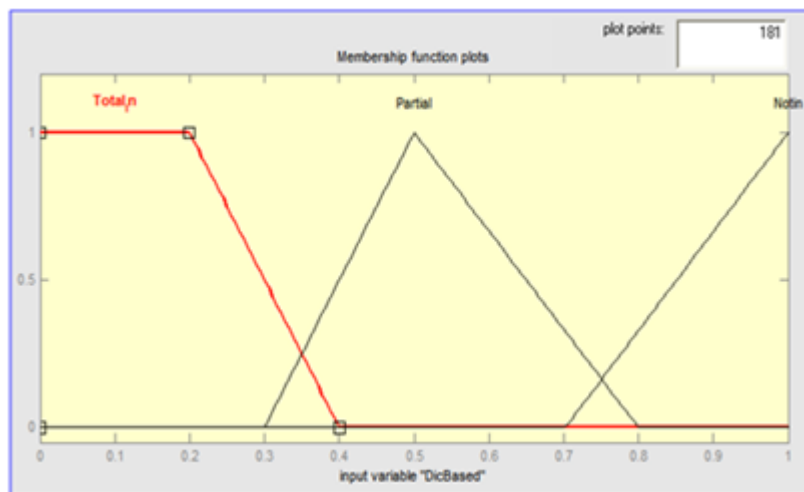


Figure 30: Membership Function of Dictionary-based in MATLAB

Additionally, a combination of a developed algorithm and a huge English dictionary can be used to find any hidden word in a password within milliseconds.

CHAPTER FOUR

4.7.3 Entropy

Based on the time needed to crack a given password, the entropy membership is categorised as Low, Medium and High.

The following table 9 shows the entropy per symbol for all character sets (Schneier 1996).

Character Set used	Character Set Size	Entropy per symbol	Total Entropy of 8 characters password
Numbers	10	3.3 bits	26.4 bits
Capital or Small Letters	26	4.7 bits	37.6 bits
Special characters	33	5 bits	40 bits
Numbers & Small Letters	36	5.17 bits	41.36
Small letters & Special Characters	59	5.88 bits	47.04 bits
Small letters, Capital Letters & Special Characters	85	6.4 bits	51.2 bits
Using all character sets	95	6.57 bits	52.56 bits

Table 9: Character set and Entropy of 8 character password

CHAPTER FOUR

Since the entropy of a given password is based on the character set used (Table 9) and length of the password,

MS Access with Visual Basic was used to analyse the password before using these parameters as the input to fuzzy sets. The dictionary¹ used consists of more than 800,000 words, in addition a Visual Basic algorithm was used to generate all the horizontal and vertical sequences of the keyboard, alphabetic characters and numbers to avoid using easy patterns that can be memorised by a shoulder surfing attacker. Finally the entropy was calculated according to equation (3).

The output of the tool is shown below:

For the password “AdSrGhcgFTrzdG”:

- Length = 14 characters
- Dictionary Based = 1 (means doesn't base on dictionary at all)

¹ The dictionary can be downloaded from

<http://sunsite.mff.cuni.cz/MIRRORS/ftp.funet.fi/pub/unix/security/passwd/crack/dictionaries/american/dic-0294.tar.gz>

CHAPTER FOUR

- Entropy = $L * H$ (based on equation 3)

$$= 14 * 5.7$$

$$\text{Total entropy} = 79.81$$

So, the input of this password will be 14,1,79.81

The following table shows the results of keyboard and alphabet pattern passwords.

<i>Ser</i>	<i>Password</i>	<i>Microsoft^a</i>	<i>CertainKey^a</i>	<i>Google^a</i>	<i>Yahoo</i>	<i>Facebook</i>	<i>PTool^a</i>
1	Abcdefghij	Medium	Passed	Strong	Strong	Medium	Weak
2	Asdfghjkl	Medium	Passed	Strong	Strong	Medium	Weak
3	Poiuytrew	Medium	Passed	Strong	Strong	Medium	Weak
4	098765432	Weak	Failed	Strong	Weak	Medium	Weak
5	Qwertasdfgh	Medium	Passed	Strong	Strong	Medium	Weak
6	Asdfghj123456	Strong	Passed	Strong	V. Strong	Strong	Weak
7	Zxcvbnm111	Strong	Passed	Strong	V. Strong	Strong	Weak

(a) The tests were conducted in June 2010.

Table 10: Passwords of keyboard patterns (Ptool represents the proposed tool)

The keyboard-pattern passwords are usually easy to memorise by the shoulder surfing attacker because they are dependent on the hand motion and the

CHAPTER FOUR

locations of the keys on the keyboard. The first password in table 6 is an alphabetic sequence that makes it easy to track even if the first character is a capital letter. The second one is a sequence of the second line of the keyboard, while the third one is the first line from right to left. Noticeably, the fourth password is a numeric sequence which was failed in Microsoft and CertainKey and passed in a Google test. The next one is a sequence from the first and second lines on the keyboard. The last two passwords are two concatenated keyboard sequences.

A set of passwords that are based on a dictionary are tested and compared to PTool with the following table showing the results of passwords based completely and partially on a dictionary:

Ser	Password	Microsoft ^a	CertainKey ^a	Google ^a	Yahoo ^a	Facebook ^a	PTool ^a
1	Simulation	Medium	Failed	Strong	Strong	Medium	Weak
2	Communication 1	Best	Failed	Strong	Very strong	Strong	Weak
3	Kids2000	Strong	Failed	Strong	Very strong	Strong	Weak
4	Dell1234	Strong	Failed	Strong	Very strong	Strong	Weak
5	smile1%r&y*7	Strong	Failed	Strong	Very strong	Strong	Medium
6	Ab\$z2y3%u3Dr 5boy	Best	Failed	Strong	Very strong	Strong	Strong

CHAPTER FOUR

7	K\$es&kpw\$312 bye	Best	Failed	Strong	Very strong	Strong	Strong
---	-----------------------	------	--------	--------	-------------	--------	--------

(a) The tests were conducted in June 2009.

Table 11: Results of passwords based on dictionary

The first word in table 11 is based fully on a dictionary; it failed in CertainKey, was rated as medium on Microsoft's website and was strong on Google. Since hackers use huge dictionaries to crack protected documents and websites, this password should be rated as weak. 93% of the second password is an English word and thus makes it easy for a shoulder surfer to predict or spy; this password should also be rated as weak. The third, fourth and fifth passwords are based partially on a dictionary, but the rest of the third one does not include sufficient randomness when compared to the fifth one which is rated medium while the third one is weak. The last two are 16 characters long with less than 20% of them based on a dictionary. The first portions of these passwords are very strong with high entropy so they are not easy to crack. At the same time, they are not memorable so adding a small English word would not affect their strength substantially.

Table 12 shows passwords with high entropy but which were failed by Microsoft's password checker

<i>Ser</i>	<i>Password</i>	<i>Entropy (Bits)</i>	<i>Microsoft</i>	<i>PTool</i>
1	pwfmnaozryqmd	61.11	Weak	Strong
2	*\$"!£%(+&^)&%\	70.62	Weak	Strong
3	owiehjt5814709	72.38	Medium	Strong

CHAPTER FOUR

4	SKDITRNELWERFTGX	75.21	Weak	Strong
5	AdSrGhcgFTrzdY	79.81	Medium	Strong
6	K1G4T6Y7I5O4P3X3V	87.89	Medium	Strong
7	p*(g)rz^q#a~rx-ufve\$	117.65	Medium	Strong

Table 12: Results of high entropy passwords

All the passwords in table 12 are fully random with high entropy, not based on a dictionary and long enough to resist shoulder surfing attacks. The first password - which has the lowest entropy of the group - needs 26^{13} (~ 2.48 quintillion probabilities) to crack it. This means that if we are using a dual processor computer that can perform 10^6 trials per/second, we need 7867 years to crack the password. Such a password should not be considered weak. The last one consists of 20 characters with 117.65 bits/symbol of entropy. It needs 59^{20} (~ 2.61^{35} probabilities) to crack it resulting in the need for millions of years of processing time. Accordingly, this password should be rated ‘Best’ not ‘Medium’ as stated by Microsoft’s ranking system

Table 13 shows passwords with low entropy or sequences but nevertheless passed by the Google password checker:

Ser	Password	Entropy Or Seq.	Google	PTool
1	maryblige	13.00	Strong	Weak
2	56128911	26.58	Strong	Weak
3	zxcvbasd	Sequence	Strong	Weak
4	oiuytrewq	Sequence	Good	Weak
5	asdf1111	Sequence	Strong	Weak

CHAPTER FOUR

6	zxczxczxczxc	Repeated Sequence	Good	Weak
7	aaasssdddfff	Repeated Sequence	Strong	Weak

Table 13: Results of low entropy or sequence passwords

Noticeably, the first password is a name and is rated as strong by Google. Bruce Schneier estimates the entropy of this password as $1.3 * 11$ (~ 13 bits/symbol). The second password is a number with low entropy and is easy to memorise. The third is a simple password and is also easy to memorise, while the next is a keyboard pattern – part of the first line of the keyboard. The fifth one is a sequence with repeated numbers; the last two passwords are repeated and keyboard patterns; hence, from a shoulder surfing point of view, they can be captured easily. All are rated as Fair, Good and Strong by Google even though they are clearly weak.

The last table shows different passwords with a little difference to presents how quantitative approach is applied

Ser	Password	Strength	Rate
1	1234567890	17.47	Weak
2	8463129507	21.64	Weak

Table 14: Quantitative approach

The two passwords are weak indeed since both are numeric, short and easy to memorise. We noted that the second password a bit complicated comparing to the first one, which is sequence of numbers; therefore it is approximately stronger by 4%.

CHAPTER FOUR

It worth mention that selecting above passwords based on the weakness of the existing tools, following table shows the weakness point of each mentioned tool:

Company	Weakness point	Example
Microsoft	Not consider repeated character as weak password	Aaaaaaaaa1 is strong password
CertainKey	Adding a dictionary word to sufficient strong password weakens the strength of the password.	D4#d3ss35fsw5Boy considered as weak password.
Google	Keyboard sequence passwords can be rated as strong	zxcv1111 is strong password.
Yahoo	Short password consist of 6 repeated letters can be rated as strong.	aaa11 is strong password.
Facebook	Use long variant and complicated letters from same character set with high entropy considered as weak	orfnmdjetirdldkswmeodi considered as weak password.

Table 15: Table of existing tools weaknesses

It is worth mentioning that comparing the proposed Ptool to the existing password tools is a challenging task since it was done while considering many fronts that are not open to users or available for analysis such as algorithms, models and business rules. In addition, the venders of these tools do not release the mechanism used to rate a password. What was available is no more than guidance that is found at their websites. Accordingly, several password patterns were assessed to find out any weakness of the used tools.

4.8 Proactive Proposed Tool

The password policy settings in a group policy may not guarantee good passwords because they are not very flexible (Johansson 2004). As far as we know, policies are implemented to protect the information against strangers, the curious and attackers (Charles Cresson Wood and Lineman 2009). Other researchers suggested that policies should be enforced (Michael E. Whitman 2010) since it is easy to write and improve an effective information security policy but it is extremely difficult to assure the implementation thereof. The PTool can be used as a proactive measuring tool to prevent users selecting weak passwords as it forces them to select strong passwords. In addition to that (and to achieve a maximum level of security during the process of changing the password) an API function such as “SecureZeroMemory” and “NetUserChangePassword” should be deployed at the outset to assess password security and to limit the effect of spyware and hacking scripts.

Following figure 31, shows the complete simulation form and testing the password “*abcd1234*”, it is shows the final WEAK password message in red box, the module has instructions for the user to select strong password, in addition a warning message beside each feature of the password, at the end of windows the rate of the password in quantity form is appear, which is 20.23 in this case:

The screenshot shows a window titled "password checker ver2" with a yellow header "Simulation : Password Strength Measurement". A red banner at the top reads "WEAK password, Not Acceptable". The form contains the following fields and values:

Server Name :	-	Password should be: 1. 10 character length at least. 2. Doesn't include known word or name 3. Doesn't include sequences or repeated characters
User Name :	admin	
Old Password :	dell2000	
New Password :	*****	
Confirm Password :	*****	

Below the form, there are several metrics and a button:

Length weight :	0.57	Med Length password
Based on Dictionary :	0.00	your password NOT based on Dictionary
Entropy :	10.40	your password easy to memorise
Password Strength :	20.23	

A "Change Password" button is located at the bottom right. A tooltip over the Confirm Password field says "your password should be 10 characters length".

Figure 31: Password checker for password “abcd1234”(PTool)

Following figure 32, shows the complete simulation form and testing the password “fsdf334dsrf\$df”, it is shows the final strong password message in green box, the awareness messages are clear, the long is sufficient, the password not based on dictionary and not easy to memorise due to the long and variety of character set uses the password has a re of 78.74 of strength, figure 33 shows a medium rate password.

CHAPTER FOUR

The screenshot shows a window titled "password checker ver2" with a yellow header "Simulation : Password Strength Measurement". Below the header is a green bar with the text "Strong Password, Excellent". The form contains the following fields and values:

Server Name :	
User Name :	admin
Old Password :	dell2000
New Password :	*****
Confirm Password :	*****

Length weight :	1.00	Long passwrd
Based on Dictionary :	0.79	your password NOT based on Dictionary
Entropy :	85.52	your password NOT easy to memorise
Password Strength :	78.74	

A "Change Password" button is located at the bottom right.

Figure 32: Password checker for password “fsdf334dsr£\$df” (PTool)

The screenshot shows a window titled "password checker ver2" with a yellow header "Simulation : Password Strength Measurement". Below the header is a yellow bar with the text "Meduime, try to strength your password". The form contains the following fields and values:

Server Name :	
User Name :	admin
Old Password :	dell2000
New Password :	*****
Confirm Password :	*****

Length weight :	0.93	Med Length passwrd
Based on Dictionary :	1.00	your password NOT based on Dictionary
Entropy :	43.19	your password NOT easy to memorise
Password Strength :	48.74	

A "Change Password" button is located at the bottom right.

Figure 33: Password checker for password "4524556547673"

4.9 Conclusion

Password strength is important in protecting personal and important information. It is found that password strength can be gaged based on three factors; length, dictionary based words and entropy. It is also noticed that no one has used the approach

CHAPTER FOUR

of combining the three factors together in order to accurately assess the password strength.

In this chapter, an intelligent tool (PTool) has been proposed to measure the strength of passwords using Fuzzy rule sets that may help to prevent dictionary, brute-force and shoulder surfing attacks simultaneously. Large dictionaries (consisting of 800,000 English words, common passwords and keyboard patterns) are used to demonstrate the impact of the proposed and existing tools. Lists of passwords were analysed to explore the words that are partially based on a dictionary. Entropy is considered as the tool providing the main factor of password strength to resist brute-force attacks. The devolved tool (PTool) demonstrated through a set of experiments that the length of a password should be longer than 8 characters to resist shoulder surfing attacks. The performance of the proposed tool has been compared with major providers around the world in order to demonstrate its merits and capabilities.

In addition, the password strength can offer quantitative values rather than qualitative description as used by all vendors. This approach quantifies the measurement and makes it easy for the interested parties to measure the strength of their passwords helping to make better informed decision.

Finally, the awareness messages can provide guidance and explains the reasons behind password rate value helping the user to better appreciate password strength.

5 Phishing Emails Capture Module

5.1 Introduction

Millions of electronic financial transactions are executed globally every day through the Internet. Banks, shops and governments offer online account access and online payments (Larcom and Elbirt 2006). Personal information such as usernames, passwords, credit card numbers and account numbers are the core of online transactions.

Hackers and curious people are always seeking new methods to breach privacy through vulnerabilities that exist in the World Wide Web's backbone systems. Securing millions of online transactions is becoming more sophisticated as numerous methods are invented daily to breach privacy. Phishing is one of the methods that deceive people into revealing their personal information (i.e. username, password, bank account and credit card number) by using social engineering and technical tools in place of the traditional methods such as sniffing, Trojan horses or viruses.

What is phishing?

The anti-phishing work group (APWG)² defined phishing as “an attack that uses both social engineering and technical subterfuge to steal consumers' personal identity

²The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.

<http://www.antiphishing.org/>

CHAPTER FIVE

data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick them into divulging financial data”.

Phishing attacks cost companies and consumers thousands to millions of dollars every year. In addition, the e-business sector loses clients' confidence, which is worth millions. According to APWG's phishing report in February 2007, the number of email phishing attacks increased by around 37% in the period between Feb. '06 and Feb. '07. Meanwhile, the unique phishing websites detected by APWG increased by 80% in the same period (Wenyin, Xiaotie *et al.* 2006; APWG 2007). Phishing has become a criminal act, categorised as one of the most effective online scams (Brooks 2006).

How does phishing work?

The phishing process usually starts with a spoofed email influencing people to login to their accounts by using forged web pages that look like the official web page of the legitimate service provider, such as a bank or an e-shop (Engin and Christopher 2005). The spoofed emails often look like valid emails because the phishers use the same logos and graphic pictures as the original website (Microsoft 2006). In addition, the scam emails contain deceptive URL addresses linking to a scam website.

Figure 34 shows a scam email that shares the graphics of eBay website and a deceptive URL linking to a fake website (Microsoft 2006).



Figure 34 : Scam email shares graphics with legitimate website

By clicking on the link, the user will be directed to a false website that looks like the legitimate one. The information is captured as soon as the victim enters the username, password or credit card number. Therefore, users should not forward unauthenticated emails, click on unusual links in an email or use search engines to look for online donations and charitable organisations (Tzer-Shyong, Fuh-Gwo et al. 2006).

Phishing may be conducted directly and telephonically to obtain a victim's personal information. Some phishers pose as employers and call people who have listed themselves on job search websites asking them about their social security number or sensitive information. Another scenario is when someone calls the victim asking him/her to reconfirm the financial information such as the credit card number because of an overdue bill (Charles E. Frank and Werner 2007).

5.2 Phishing techniques

The following are five major techniques used to accomplish phishing attacks:

5.2.1 Impersonation

This is a common technique. Simply, the phishing email falsely claims to be from a legitimate business where the victims might have an account. The phisher uses the same logos and graphics as the original website so that the scam email appears to be an official email asking the user to log in to solve certain problems (Yue Zhang 2007). This type of attack weakens consumer confidence as it makes it difficult for the average user to distinguish between legitimate and fraudulent emails.

5.2.2 Forward attack

This is a sophisticated technique where the phisher collects personal information through a scam email that includes harmful code or script. By using an effective anti-virus, this phishing technique becomes ineffective since the anti-virus picks up the code that collects the victim's information (James 2006). Figure 35 shows an email containing two text boxes to allow the victim to enter their SSN and the PIN code. After typing the information, the code behind the email transfers the user to the legitimate website after collecting the credentials.

5.2.3 Pop-up attack

This technique launches a hostile pop-up in front of the legitimate website asking the victim to login through a secured pop-up window. Once the

user logs in to the pop-up, the phisher captures the victim's credentials and forwards him/her to the official website (James 2006). In this case, the pop-up window works as a 'middleman' to collect the information.

5.2.4 Voice phishing

This is a new technique, improved nowadays by phishers. It is believed to be one of the newest breakthroughs in telecommunications (FBI 2007); it uses VOIP – Voice Over Internet Protocol.

This technique is called vishing as it uses both voice and phishing to conduct the attack. This kind of attack can be conducted in a variety of ways with only a few minor differences as illustrated in the following two types of vishing attacks:

- a) In this first scenario, the victim receives a typical e-mail, like any other traditional phishing scam. They are then asked to provide information over the phone instead of being directed to an internet site. The victim calls the fraud "customer service" number (a VOIP account, not a real financial institution) providing account numbers, passwords, and other critical information through a series of voice-prompted menus (FBI 2007).
- b) In another scenario, the victim is contacted over the phone instead of by e-mail. When the receiver answers the fraudulent call, an automated recorded message plays, warning the victim about account breaches. The recorded message directs the victim to take action in order to protect the account. The trick behind this scenario is that the victim receives the call from a spoofed ID number of the financial company (FBI 2007).

CHAPTER FIVE

5.2.5 Mobile phishing

New technology is on the rise; 2006 was evidence of this when phishing attacks shifted from PCs to mobile devices. This attack manipulates mobile phone operators/carriers' SMS by sending text messages to mobile users trying to trick them into following a malicious mobile internet link (Shah April 2007). These types of phishing traps are commonly known as Smishing.

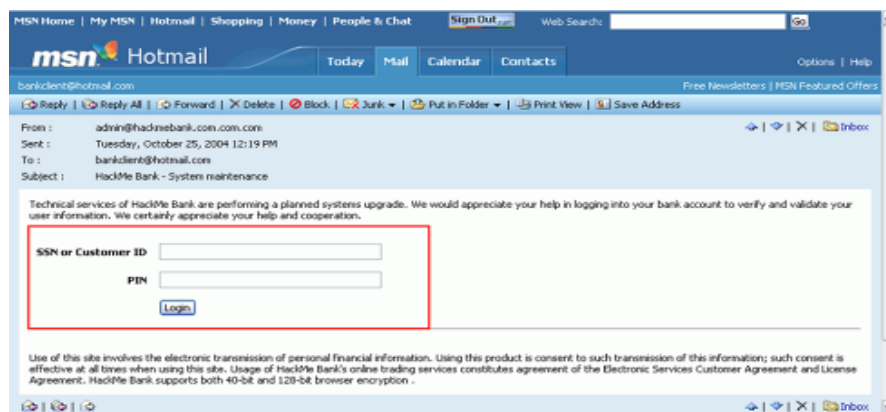


Figure 35 : Scam email using forward attack technique

Several techniques have been proposed to solve this problem. Unfortunately, this type of problem depends on human awareness. Therefore, the phishing detection algorithm should not be based completely upon user interaction (Ian Fette June 2006). Since phishing exploits human vulnerabilities rather than software vulnerabilities, education and awareness are the first steps to mitigating the risk of phishing attacks (Larcom and Elbirt 2006; Yue Zhang 2007).

5.3 Anti-phishing Solutions

Three types of solutions can be used to reduce the risk of *phishing attacks*:

5.3.1 Anti-phishing toolbars

Ebay, NetCraft, GeoTrust, EarthLink, CallingID and other vendors offer several toolbars to reduce the risks of phishing attacks. These organisations use different methods to determine the legitimacy of websites such as checking the IP address, combination of heuristics, user ratings, and manual verification (2007; Yue Zhang 2007).

5.3.2 Browser plug-ins

Microsoft has added a new plug-in to IE7 to help users detect phishing websites. It relies on a blacklist hosted by Microsoft. Another tool from SpoofStick is a simple browser extension that helps users to detect fake websites. SpoofStick makes it easier to spot a spoofed website by prominently displaying only the most relevant domain information (2005). The Netscape Navigator 8.1 web browser includes a built-in phishing filter. Firefox 2.0 includes a new feature designed to identify fraudulent websites (Yue Zhang 2007).

5.3.3 Email-filters

Email filters are the most effective solution to detect spoofed websites, since most victims are directed to spoofed websites from phishing emails (Liu, Guanglin et al. 2005). By detecting spoofed emails, the user is more secure and the solution, in this case is categorised as a preventive solution, while the toolbars and browser plug-ins are detective techniques. (Ian Fette June 2006) proposed a simple technique to detect spoofed email called PILFER. The filter works by incorporating features specifically designed to highlight the deceptive

methods used to fool users.

5.4 Phishing emails features

By reading and investigating a large number of phishing emails, it was noticed that there are many features and tricks that can distinguish legitimate emails from phishing ones; part of these features are hidden from the user and hard to detect, while others are clearly visible.

The data set used in this study consists of 1008 phishing emails (Nazario Oct 2008) found with source code dedicated for academic research, 600 emails to analysis and extract phishing rules while around 408 used for testing the developed tool.

Based on our literature review, the outcome of the survey study at section 3.5, “*Simulation of phishing attack*” and the analysis of over 600 phishing emails (selected from a different pool of emails), it is found that 6 features are exist in more than 96% of this set. All six features are used to develop our technique.

The features have been categorised into two main categories; the hidden features that are invisible to the end-user and normally embedded into the source code and the visible features to the recipient normally embedded into the email’s body.

5.4.1 Source code features (back-end)

These tricks and features are hidden to users and can’t be detected easily, apart from by experts or software tools. The following are some of these features:

CHAPTER FIVE

5.4.2 IP-based URLs and bon-matching URLs

Phishers attempt to obscure the destination Web site by hiding the URL. This trick is conducted by using the IP address instead of the hostname. An example of an IP address used in a fraudulent website is as follows:
<http://210.16.234.67>

In phishing email messages, the link text seen in the email is usually different from the actual link destination. As shown in Figure 36, the email appears to be aiming to be linking the user to:

“<https://vault.woodgrove.com/default.asp>”

But, as a matter of fact, it links it to

<http://203.144.234.138/us/index.html>.

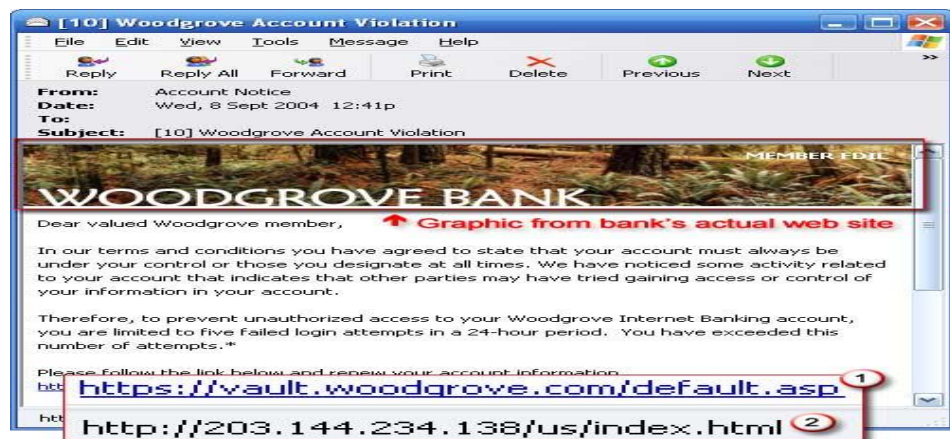


Figure 36 : Non-Matching URLs

5.4.3 The use of scripts

Using scripts could help the phishers to hide the destination URL, the JavaScript event “onMouseOver” is used widely by fraudsters to show the

victim a false URL in the status bar when the mouse moves over the apparent link (Christine E. Drake 2004).

5.4.4 The use of multiple domains

Since the phishers share images and links with the legitimate website, and forward the victim to the phishing website, it is noticed that phishing emails contain multiple domains.

5.4.5 Content features (front-end)

These tricks and features are not hidden to the user, and can be easily detected if the user acquires sufficient training. Following are then main features that can be noticed in phishing emails:

5.4.6 Generic salutation

Personalisation of salutation increases the trustworthiness of people who are official subscribers and they should receive a personal salutation rather than a generic one. Examples of generic salutations are as follows: Dear valued customer, Dear client, etc. Some hackers use the email at the welcome salutation or extract part of the name from the email.

5.4.7 Security promises, requires a fast response or “Click Here” link

To gain the trust of the victim, phishers regularly emphasize security issues. They convince users to visit their website, claiming that it is secure and safe.

Phishing emails may claim that the client's account information is out of date, their credit card has expired, or the account must be verified as a regular security procedure. The phishers try to collect information as soon as possible before the phishing website is shut down, so they ask the victim for a fast response.

In addition to that, phishers try to trick the victims by using a clear hypertext link such as "Click here to login". The phisher wants the user to click this link since it is the most important link in the email. Other links are maintained in the email to keep the genuine "feel", such as the link to the privacy policy, and the link to the user agreement, images and logos.

5.4.8 Links to https:// domains

In order to deceive the victims, phishers used to post links to https:// domains in the front end of the email page, while in the back end it forwards the victim to a non-secure link. This feature is found only in phishing emails.

5.5 Intelligent model for detection and protection

5.5.1 Using fuzzy logic approach

Since phishing is a type of social engineering attack, it is the exploitation of the vulnerability in human nature rather than of technological weakness. The solution is a combination of utilising tools and a rigorous human learning approach to avoid different types of attacks such as email phishing, vishing (voice phishing) and smishing (SMS phishing).

CHAPTER FIVE

Most of the existing solutions are technical in nature, and are mainly tools installed on the user's computer to monitor and filter phishing emails. We suggest that investment in the human element itself as a preventive strategy combined with proper utilisation of tools yields better results.

The first step that should be taken into consideration is the implementation of a proficient security awareness program that can help users to avoid all the phishing techniques. Such programs will not completely stop the effectiveness of the phishing attack, but will reduce it. Awareness programs are usually categorised as proactive solutions; therefore they are more effective and cost less than reactive solutions.

In addition to awareness development, one can also consider an intelligent system to detect the level of vulnerability, in turn helping to make decisions in regard to a phishing attack. This section focuses on a similar scheme of methodology to build an effective and preventive anti-phishing tool:

1. A set of 408 phishing (Nazario Oct 2008) and another 600 non-phishing emails were collected to implement the proposed methodology.
2. All six features discussed in the previous section were used to distinguish between legitimate and phishing emails according to their relevance.
3. Any incoming emails are separated into two parts, front and back end; the front end is the visible part of the email that users normally read, while the back end is the source code of the email.

Following diagram shows this process:

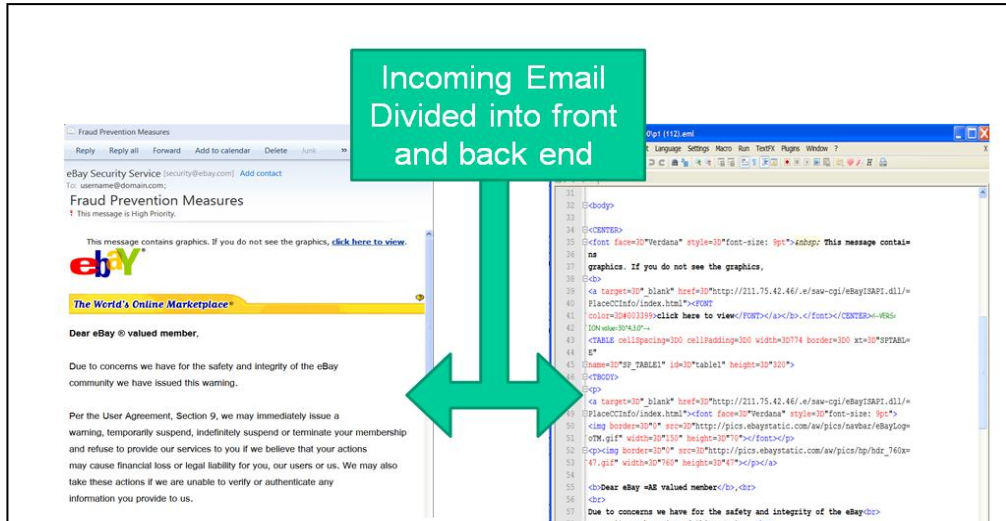


Figure 37 : Separating front end and back end of incoming email

4. A VB script was written to extract those features. Initially, the pilot program parses emails on two levels; the content level (front end), which is the body of the email, and the back end, which is the source code. It extracts all the features discussed above and then gives the email scores for each feature (rate level) as shown in figure 38. The resulting scores are used to assist in further automated phases of assessing whether the email is a phishing not. The implementation developed using VBA for script programming and MS Access 2007 for the backend database.

CHAPTER FIVE

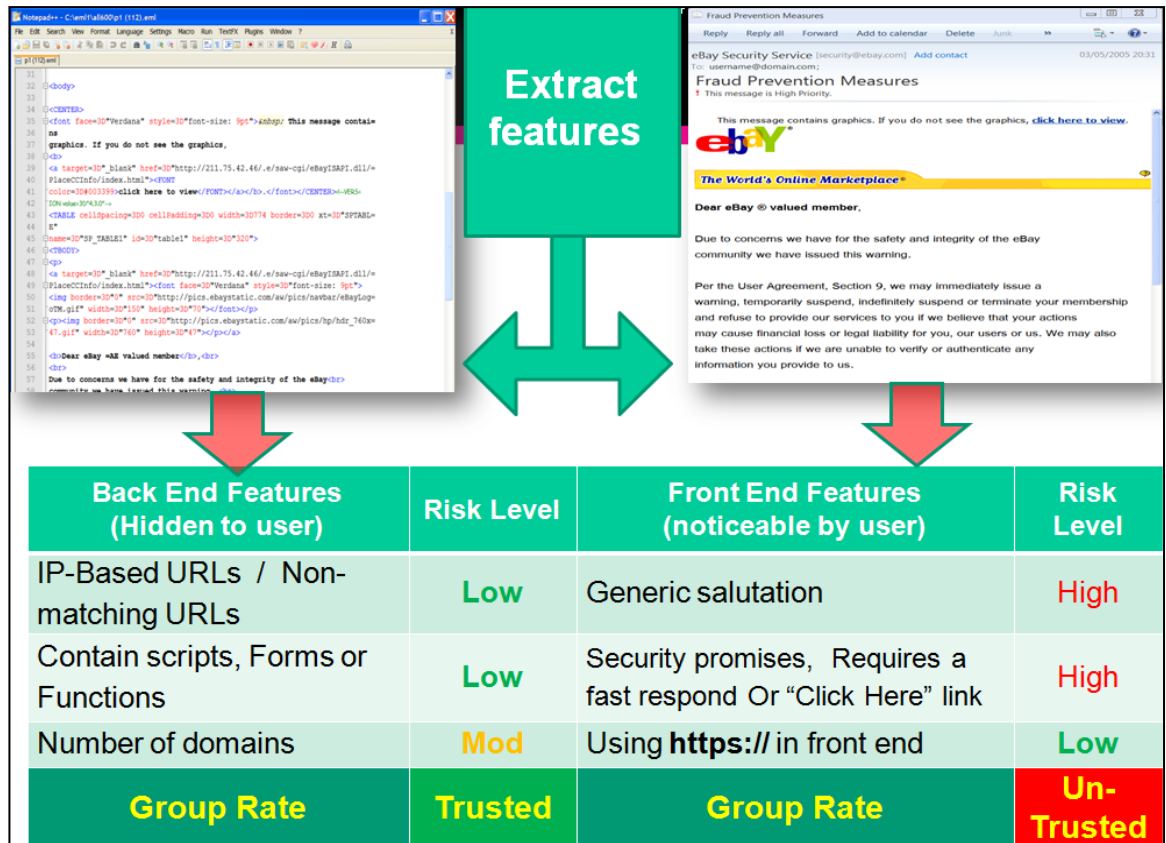


Figure 38 : Using script to extract features of each layer then rate each layer

Following are the linguistic descriptors used to represent the phishing features indicators:

Feature	Case	Risk Rate	
Back End Features	IP-based URLs / Non-matching URLs	Contains IP address at URL (regardless of non-matching URLs) or Completely non-matching URLs	High
			Moderate
		No IP address and all links exist at front end.	Low
	Contain scripts, Forms or Functions	"Onmouseover" script	High
		Forms or any kind of other scripts or functions	Moderate
		No any kind of scripts, Forms or Functions	Low
Number of domains	More than two domains	High	
	Two domains	Moderate	
	One domain	Low	

CHAPTER FIVE

Front End Features	Generic salutation	generic salutation (dear customer, dear valued member, etc)	High
		Contains the first name (e.g. Dear John) *	Moderate
		Contains both the first and last name or the customer name (e.g. Dear John Mick)	Low
	Security promises, requires a fast respond Or “Click Here” link	More than 10 words	High
		From 3 to 12	Moderate
		Up to 5 words	Low
	Using https:// in front end	https at front and no https at the back end	High
		https at the end only	Moderate
		Match https at front and back ends	Low

* Sometimes the first name can be extracted from the prefix part of the user’s email.

Table 16: Features extracted from phishing email

5. The first phase of the proposed tool is building a set of fuzzy logic (FL) rules to get an accurate assessment of a phishing email’s set. These were then utilised to develop a FL-based expert system. In brief, a FL expert system is a collection of membership functions and rules that are utilised to reason about data (J. Buckley and Tucker). The inference process in FL goes through four steps (Cox 2001) to achieve the outcome:
 - I. **Fuzzification**, the membership function values defined on the input variables is applied to their actual values to determine the degree of truth for each rule premise.
 - II. **Inference**, the truth value for the premise of each rule is computed, and applied to the conclusion part of that rule. This results in one fuzzy subset to be assigned to each output variable for each rule.

CHAPTER FIVE

- III. **Composition**, all of the fuzzy subsets assigned to each output variable are combined together to form a single fuzzy subset for each output variable.
- IV. **Defuzzification** (optional), mainly used when converting the fuzzy output set to a crisp number.

The rule-based system has three input parameters and one output. It contains all “IF-THEN” rules for the proposed tool. The result of building FL rules for six features is that each feature has three linguistic variables (*Low, Moderate and High*) and it will need a complicated process of 3^6 rules, i.e. 729 rules. This may affect the speed of the proposed tool. Due to the large number of aforementioned rules, the evaluation process is divided into two layers with two groups in the first layer (*Back End* and *Front End groups*). The first layer is to rate each group separately. This layer is called the rule-based layer. Each group has three linguistic variables with a total number of 27 rules. Therefore, 54 rules are built to evaluate the *Back End* and *Front End* groups separately.

For each group, three output fuzzy sets are defined: (*Trusted, Doubtful and Un-Trusted*)

The fuzzy rules were built based on analysing 600 phishing emails by extracting the six features from each email. Some interesting facts have been found such as:

- 1) Any incoming email contains a public salutation such as “Dear” is most likely a phishing email since service providers contact their customers by official names.
- 2) Any email urge people to click on a link is most likely a phishing email.

CHAPTER FIVE

- 3) If the email explicitly contains a link such as “https://”, it is most likely to be a trick to give the impression of secure link.

The following table is the 27 fuzzy rules for *Back End* group risk probability:

Rule #	Domains conflict (IP, Non-matching URLs ,	Contains (Scripts ,Functions and forms)	Multi domain (not registered)	Safety Rate (Trusted) (Doubtful) (Un Trusted)
1	High	High	High	Un Trusted
2	High	High	Mod	Un Trusted
3	High	High	Low	(Doubtful)
4	High	Mod	High	Un Trusted
5	High	Mod	Mod	Un Trusted
6	High	Mod	Low	(Doubtful)
7	High	Low	High	Un Trusted
8	High	Low	Mod	(Doubtful)
9	High	Low	Low	(Doubtful)
10	Mod	High	High	Un Trusted
11	Mod	High	Mod	Un Trusted
12	Mod	High	Low	Un Trusted
13	Mod	Mod	High	(Doubtful)
14	Mod	Mod	Mod	(Doubtful)
15	Mod	Mod	Low	Trusted
16	Mod	Low	High	(Doubtful)
17	Mod	Low	Mod	(Doubtful)
18	Mod	Low	Low	Trusted
19	Low	High	High	(Doubtful)
20	Low	High	Mod	(Doubtful)
21	Low	High	Low	Trusted
22	Low	Mod	High	(Doubtful)
23	Low	Mod	Mod	Trusted
24	Low	Mod	Low	(Doubtful)
25	Low	Low	High	(Doubtful)

CHAPTER FIVE

26	Low	Low	Mod	Trusted
27	Low	Low	Low	Trusted

Table 17: Back end features rules

Following table contains the fuzzy rules for *Front End* group risk probability:

Rule #	Salutation (contains Name)	Warning, action to take, menace and Click here , Security promises	Https	Safety Rate (Trusted) (Doubtful) (Un Trusted)
1	High	High	High	Un Trusted
2	High	High	Mod	Un Trusted
3	High	High	Low	Un Trusted
4	High	Mod	High	Un Trusted
5	High	Mod	Mod	(Doubtful)
6	High	Mod	Low	(Doubtful)
7	High	Low	High	Un Trusted
8	High	Low	Mod	(Doubtful)
9	High	Low	Low	Trusted
10	Mod	High	High	Un Trusted
11	Mod	High	Mod	(Doubtful)
12	Mod	High	Low	(Doubtful)
13	Mod	Mod	High	Un Trusted
14	Mod	Mod	Mod	(Doubtful)
15	Mod	Mod	Low	Trusted
16	Mod	Low	High	Un Trusted
17	Mod	Low	Mod	(Doubtful)
18	Mod	Low	Low	Trusted
19	Low	High	High	(Doubtful)
20	Low	High	Mod	Trusted
21	Low	High	Low	Trusted
22	Low	Mod	High	Trusted
23	Low	Mod	Mod	(Doubtful)
24	Low	Mod	Low	Trusted

CHAPTER FIVE

25	Low	Low	High	(Doubtful)
26	Low	Low	Mod	Trusted
27	Low	Low	Low	Trusted

Table 18: Front end features rules

The output of both groups is the input of the second layer which is the rule-based two. Finally, a set of nine rules are built in that layer to evaluate the email for the final rating

The following table is the second layer of the rule-based; two inputs are used for final email rating.

Rule #	Back End Group	Front End Group	Final Evaluation
1	Trusted	Trusted	Safe
2	Trusted	Doubtful	Safe
3	Trusted	Un Trusted	Partially Safe
4	Doubtful	Trusted	Partially Safe
5	Doubtful	Doubtful	Partially Safe
6	Doubtful	Un Trusted	Phishy
7	Un Trusted	Trusted	Partially Safe
8	Un Trusted	Doubtful	Phishy
9	Un Trusted	Un Trusted	Phishy

Table 19: Rule Based 2 for Final Email Evaluation

The three-dimensional plot for rule base 2 is displayed as below:

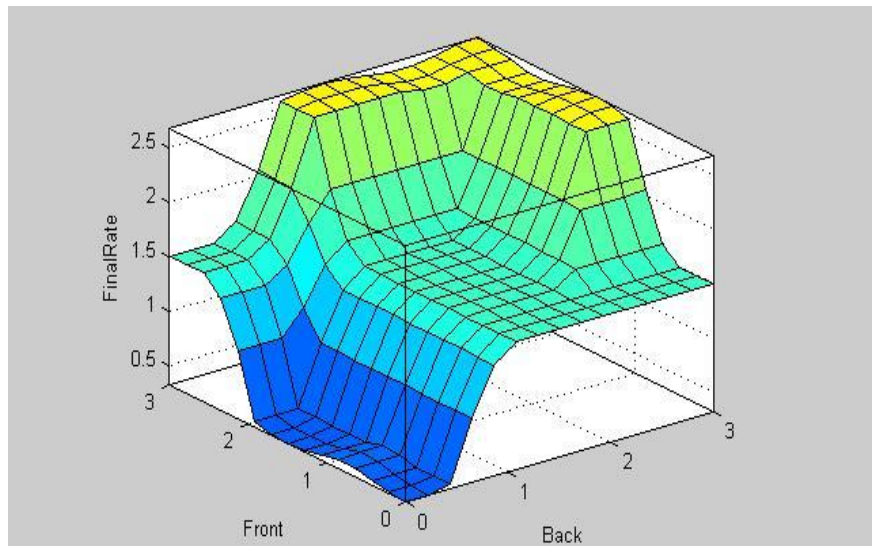


Figure 39: Three-dimensional plots for rule base 2

5.5.2 Experiment and results

In order to gain a clear idea about how phishing works and what effect it has on its victims, each email has been divided into two parts; Front end, which is the email body (content part that the user can normally read) and back end (which is the source code of the email and hidden from the user). First of all, the features mentioned in part IV are extracted from both front and back ends, and then each feature is assigned a value of risk (*High, Moderate* or *Low*) by rating the front end. It is much easier to explain to users the reasons why the emails are risky; thus it helps to prevent users becoming victims when they use unprotected environments. Secondly, the output of each group is passed into the rule-based 2 layer (table 1) to find the final rating of the email. Each email is rated as *Safe, Partially Safe* or *Phishy*.

CHAPTER FIVE

By examining an initial number of healthy and phishing emails, the proposed tool rated 33% of the emails as suspicious phishing emails (*Partially Safe*) and 67% as *Phishy*, while 95% of the healthy emails passed as *Safe* emails with 5% rated *Partially Safe* as shown in Figure 40.

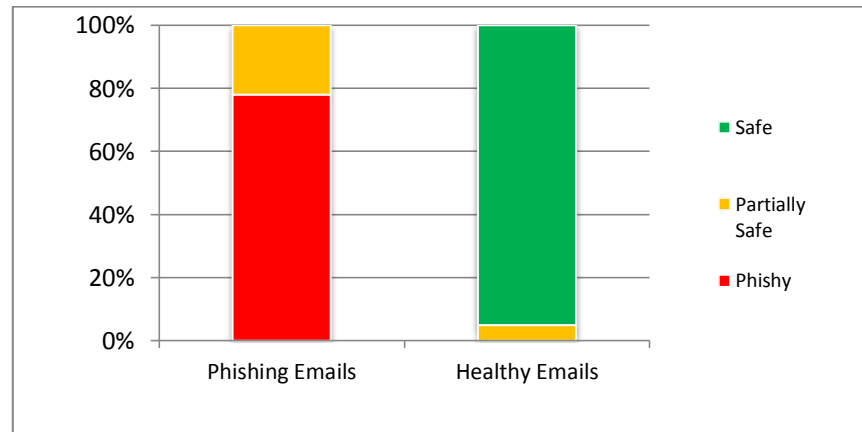


Figure 40: Results of evaluating phishing and healthy emails

In order to improve the accuracy of the proposed tool, the results of our experiments were compared with *Microsoft Windows Live Mail 2009*, which is an existing mail tool containing an anti-phishing detector. Testing the same dataset of phishing emails, *Microsoft Windows Live Mail 2009* flagged 58% as suspicious phishing emails while 42% were not detected. Figure 41 shows the comparison between the proposed tool and *Microsoft Windows live mail 2009*.

CHAPTER FIVE

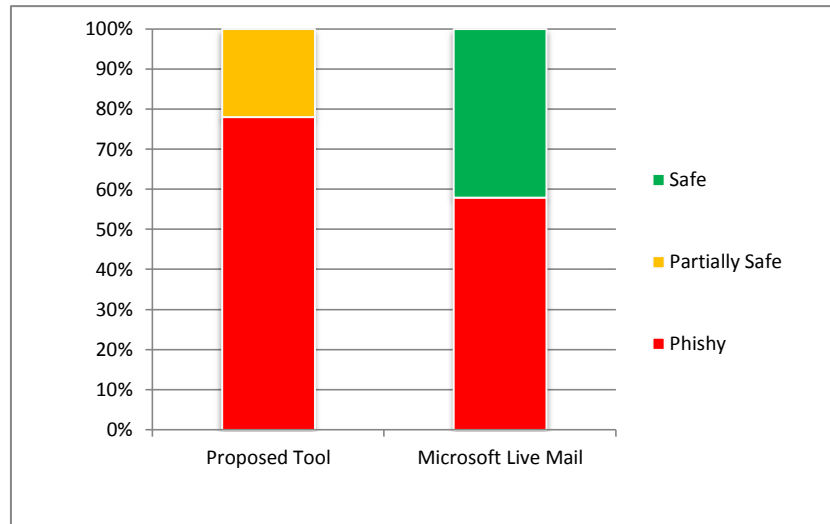


Figure 41: Results of comparison the proposed tool with Microsoft Windows live mail 2009

The following diagram 41 shows a comparison results between Thunderbird email client and Avira Anti-virus based on testing another new set of 408 phishing emails. Those emails are different from the 1200 emails used to extract the rules of the proposed anti-phishing tool.

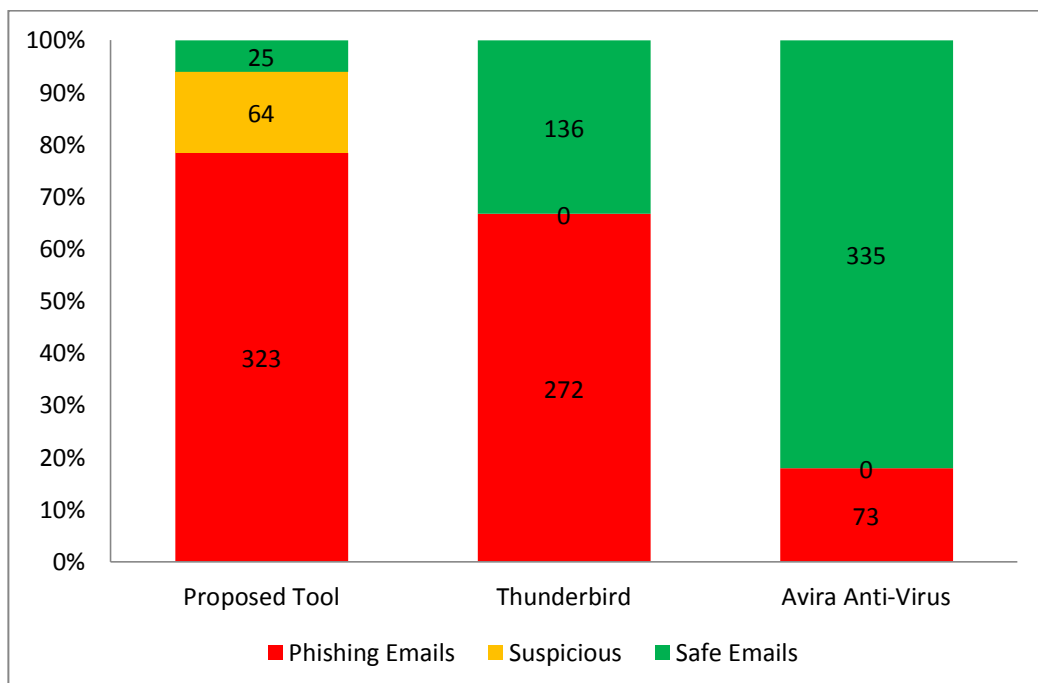


Figure 42: Results of comparison the proposed tool with Thunder bird and Avira Anti-virus

CHAPTER FIVE

Finally, 94% of the phishing emails were found to deceive users at the front end layer of the incoming email (the visible part of the email); so by implementing a sufficient awareness security program, people will be able to detect phishing emails easily, as figure 43 shows the results of evaluating the front end vs. the back end.

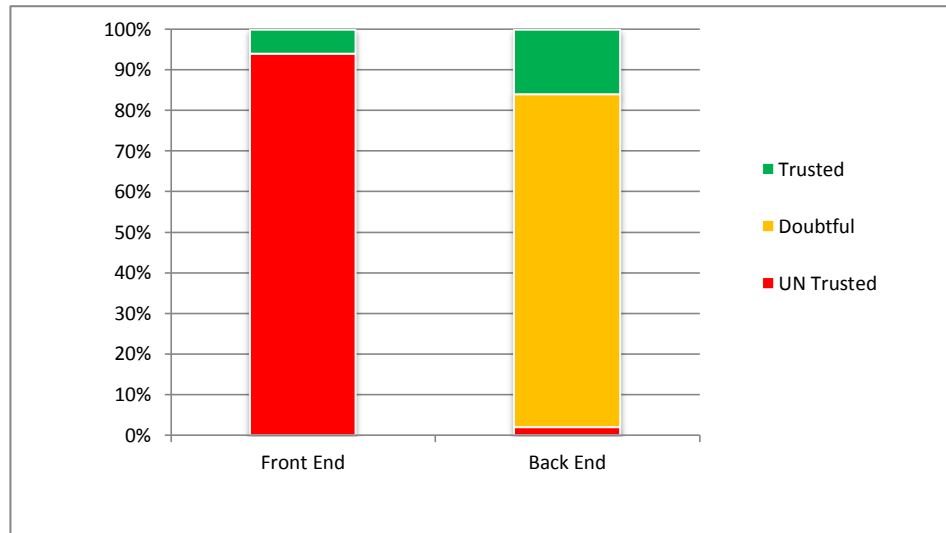


Figure 43 : Front End vs. Back End

According to the analysis of the phishing emails, the end-user will be made aware of three main features:

1. Since the phishers do not have the database of the victims, the user should notice his/her registered name at the salutation line of the incoming email.
2. Asking the user for a fast response and offering many security promises could be a trick to convince the victim that they are aiming to visit a secure website for a critical issue.
3. Including “http://” link on the front end of the email could be a trick to deceive the user.

CHAPTER FIVE

Diagram 44 shows the interface of the phishing email captured tool, noting that emails can be categorised as Inbox (safe), suspicious, and phishing.

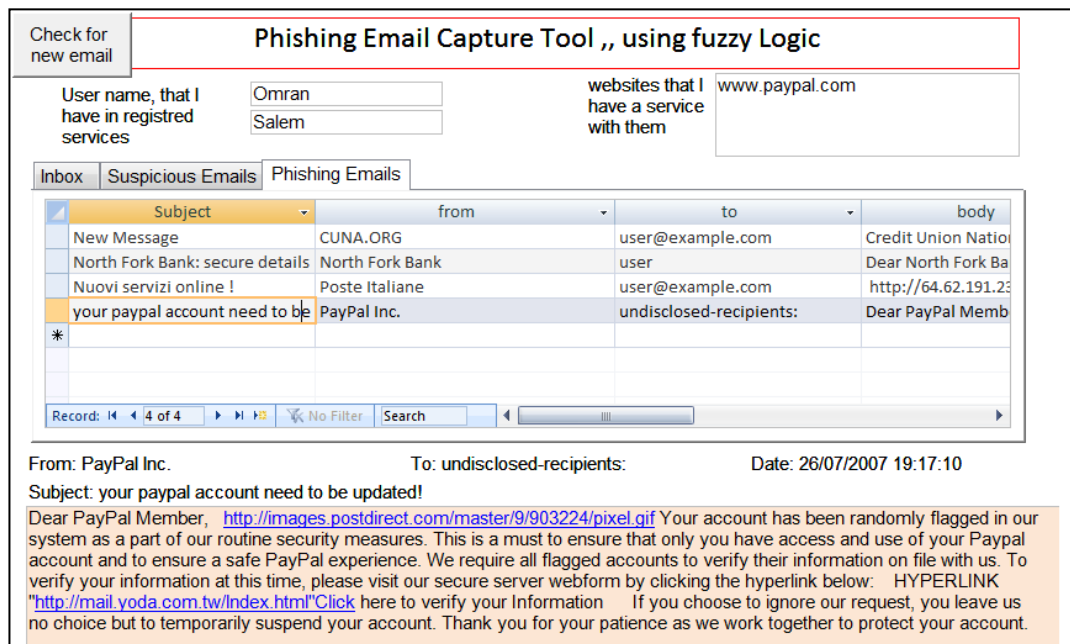


Figure 44 : Phishing emails capture module

In this module, the spoofed link is removed automatically inside the incoming email; this is a kind of enforcing policy to protect nonchalant users who usually try unfamiliar links.

5.6 Conclusion

This chapter presents an examination of the social engineering issues and technical aspects of detection of and protection against phishing, vishing and smishing. A detailed literature survey is used to provide an analysis of different contexts of vulnerability of the user and to demonstrate the existing state of technology. Particular attention has been paid to email phishing as it is considered one of the most common attacks on individual vulnerability. It is clearly demonstrated that, by determining the main differences between the legitimate emails and the phishing, one can reduce the risk

CHAPTER FIVE

of this type of attack. In addition, a fuzzy logic-based intelligent expert system has been explored to evaluate its suitability for real-time detection and protection. A new approach of dividing phishing e-mails into layers and groups is used. This has helped to simplify the implementation of fuzzy rules in a speedy and efficient way by rating each group individually.

6 Conclusion and Future Work

Information security is an important aspect for preserving confidentiality, availability and integrity against various threats. Several studies and reviews suggest that hazards against information have been growing rapidly and occur on daily basis. Furthermore, as human element is considered as the weakest link in security process, social engineering attacks are targeting people who are exposed in the systems. In this study, we have declared, analysed and proposed solutions for two major types of social engineering attacks, shoulder surfing and phishing emails.

Expert systems are used widely in different fields nowadays. Recently, computer solutions including intrusion detection systems, anti-virus, learning systems, decision making algorithms etc, depends on various expert systems such as knowledge based systems, fuzzy logic, data mining, neural networks and a wide range of artificial intelligence techniques.

Based on fuzzy logic expert system, a security framework has been developed in order to integrate people, procedures and physical information security controls to reduce the impact of social engineering attacks. The proposed tools enforce the security policies and popup concise educational messages to help users understand the reasons for the decisions taken by the intelligent tools.

The case studies in Chapter three implies that underestimation the importance of security policies or implementing insufficient procedures and rules could increase the vulnerabilities of the system by exposing it to severe threats, such as malware, virus and phishing attacks. Applying sufficient security policies and enforce it in some cases along with awareness and education programs, threats will defiantly mitigated. It is

CHAPTER SIX

considerable importance to integrate the mentioned security policies into a consistent security system followed with a security audit process to address and insure the continuity of the running systems.

In chapter four, the proposed model has been implemented through an intelligent tool (PTool) to measure the strength of passwords using Fuzzy rule sets that may help to prevent dictionary, brute-force and shoulder surfing attacks simultaneously. Length of password and dictionary based are the main factors used by existing tools to measure password strength. In this research, Entropy has been added as a new factor to measure a given password by taking into consideration the sequences of keyboard patterns and repeated characters. Finally, the performance of the proposed tool has been compared with major providers around the world, such as Microsoft, Yahoo and Google, in order to demonstrate its merits and capabilities Awareness is presented in this module through guidance and messages that explain the reasons behind password rate. Furthermore, refusing weak passwords is considered as enforcing policy to avoid system vulnerability.

In chapter five, we examine the social engineering issues and technical aspects related to detection and protection against phishing, vishing and smishing, which are considered to be one of the most common attacks on individual vulnerability. It is clearly demonstrated that by determining the main differences between the legitimate emails and the phishing, one can reduce the risk of this type of attack. In addition, a fuzzy logic-based intelligent expert system has been explored to evaluate the suitability of real-time detection and protection. A new approach of dividing phishing e-mails into layers and groups is used. This has helped to simplify implementing fuzzy rules in a speedy and efficient way by rating each group individually, incoming emails are

CHAPTER SIX

categorised into safe, suspicious and phishy emails. Users are aware of such attacks by popup guidance messages that show the suspicious parts of the phishing emails.

Future work

Firstly, the proposed model should be assessed as an integrated framework to people, procedures and security controls. The assessment should especially focus on the awareness and education part, which is related to people. The reliability of the proposed model will be measured through assessment schemes, which will be conducted before and after the model is implemented.

Secondly, the qualitative approach used to examine phishing email attacks is improved by using a quantitative approach. Accordingly, the degree of phishing email will be presented by numeric value based on the level of attack.

Thirdly, the awareness and education part should be taken into consideration as an important entity of the security process. The feedback of the survey in section 3.5 shows that people appreciate this kind of awareness. Thus, future modules should contain additional dose of education in different forms.

Finally, the model should be tested in different social engineering attacks, such as phones phishing, tailgating and other frauds emails.

REFERENCES

- (2001). E-mail related crimes, The Cyber Regulations Appellate Tribunal
- (2005). "What is SpoofStick?", from <http://www.spoofstick.com/>.
- (2007). from http://pages.ebay.com/ebay_toolbar/.
- Adams, A. and M. Sasse (1999). "Users are not the enemy." Commun. ACM **42**(12): 46.
- Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology, CRC Press.
- APWG (2007). Phishing Activity Trends, Report for the Month of February, 2007.
- APWG, A.-P. W. G. (2012). "Report a Suspected Phishing Site." Retrieved 17/10/2010, from http://www.antiphishing.org/report_phishing.html.
- Association, C. F. C. P. (July 2008) "Social Engineering ".
- Barrett, N. (2003). "Penetration testing and social engineering: Hacking the weakest link." Information Security Technical Report **8**(4): 56.
- Basnet, R., S. Mukkamala, et al. (2008). Detection of Phishing Attacks: A Machine Learning Approach
- Soft Computing Applications in Industry. B. Prasad, Springer Berlin / Heidelberg. **226**: 373-383.
- Berg., C. J. (2006). High-Assurance Design: Architecting Secure and Reliable Enterprise Applications, Addison Wesley Professional.
- Bergadano, F., B. Crispo, et al. (1997). Proactive password checking with decision trees Proceedings of the 4th ACM conference on Computer and communications security Zurich, Switzerland ACM Press.
- Bidgoli, H. (2008). Handbook of Computer Networks: Distributed networks, network planning, control, management, and new trends and applications, John Wiley & Sons, Inc.
- Bonneau, J. (2012) "Thescience of guessing: analyzing an anonymized corpus of 70 million passwords."
- Brodie, C. (2008). The Importance of Security Awareness Training. Information Security Reading Room. S. Institute. USA.
- Brooks, J. (2006). Anti-Phishing Best Practices: Keys to Aggressively and Effectively Protecting Your Organization from Phishing Attacks, Cyveillance

- Buckley, J. W., M. H. Buckley, et al. (1976). "Research Methodology and Business Decisions." National Association of Accountants and the Society of Industrial Accountants of Canada.
- Carlson, N. (May 2012). Facebook Now Has 901 Million Monthly Users, With 526 Million Coming Back Every Day, San Francisco Times.
- Center, L. S. (2006, Wednesday 19th April 2006). "Password Recovery Speeds, How long will your password stand up." from <http://www.lockdown.co.uk/?pg=combi&s=articles>.
- CertainKey. (2006). "Passphrase Strength Analyser." from <http://www.certainkey.com/demos/password/>.
- Charles Cresson Wood and D. Lineman (2009). Information Security Policies Made Easy Version 11, Information Shield, Inc.
- Charles E. Frank and L. A. Werner (2007). "Getting A Hook On Phishing." Information Systems Education Journal 5(36).
- Christine E. Drake, J. J. O., and Eugene J. Koontz (2004). "Anatomy of a Phishing Email ", from citeseer.ist.psu.edu/734697.html.
- Clinch, J. (May 2009) "ITIL V3 and Information Security."
- Collis, J. and R. Hussey (2003). Business Research: a practical guide for undergraduate and postgraduate students, Basingstoke: Palgrave Macmillan.
- Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days?, Laura Pritchard.
- Corporation, T. B. C. o. C. i. a. w. M. (2003). Guide to IT Security.
- Cox, E. (2001). "FL and Measures of Certainty in E-Commerce Expert System." Scianta Intelligence, Chapel Hill.
- D'Arcy, J., A. Hovav, et al. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." Info. Sys. Research 20(1): 79-98.
- Dieterle, D. (2010) "Cracking 14 Character Complex Passwords in 5 Seconds."
- Dong-Mei, Z., W. Jing-Hong, et al. (2005). Using Fuzzy Logic and Entropy Theory to Risk Assessment of the Information Security.
- Downs, J. S., M. Holbrook, et al. (2007). Behavioral response to phishing risk. Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, Pennsylvania, ACM: 37-44.
- Emirsk (2009) "Social Engineering: People Hacking."

- Engelmore, R. S. and E. Feigenbaum (1993). KNOWLEDGE-BASED SYSTEMS IN JAPAN, JTEC.
- Engin, K. and K. Christopher (2005). Protecting Users Against Phishing Attacks with AntiPhish. Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05) Volume 1 - Volume 01, IEEE Computer Society.
- Engin Kirda, C. K. (2005). "Protecting Users Against Phishing Attacks." The Computer Journal.
- FBI (2007). Something Vishy, Be Aware of a New Online Scam
- FTC, F. T. C. (February 2006). "Pretexting: Your Personal Information Revealed " Retrieved 29/06/2011, 2011, from <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre10.shtm>.
- Gehringer, E. F. (2002). Choosing passwords: security and human factors.
- George, S. (2001) "Enhancing Defenses Against Social Engineering."
- Gordon, J. L. and L. Jorgensen. (1998). "Artificial Intelligence : Technologies." from <http://www.akri.org/ai/techs.htm>.
- Granger, S. (2001). "Social Engineering Fundamentals, Part I: Hacker Tactics ".
- Gregg, M. (2006). CISSP Exam Cram 2, QUE Certification.
- Gulati, R. (2003). "The Threats of social engineering and your defense against it." SANS Institute.
- Guyot, L. (2003). "Essential Information Security For Corporate Employees." Information Security Reading Room, <http://www.sans.org>.
- Hausman, K., D. Barrett, et al. (2003). Security+ Exam Cram, QUE Certification.
- Herold, R. (2010). Managing an Information Security and Privacy Awareness and Training Program, CRC Press.
- <http://www.computeruser.com/>. (2006). "Social Engineering Definition." from <http://www.computeruser.com/resources/dictionary/definition.html?lookup=8057>.
- Ian Fette, N. S., Anthony Tomasic (June 2006). learning to detect phishing emails, Carnegie Mellon University Technical Report CMU-ISRI-06-112. .
- Ihara, S. (1993). Information theory for continuous systems, World Scientific.
- ISO (2005). ISO/IEC FDIS 17799 – Information technology – security techniques – code of practice for information security management (2nd edition), International Organization for Standardization.

- J. Buckley and D. Tucker "Second generation fuzzy expert system." Fuzzy Sets and Systems **31:271{284,1989}**.
- James, L. (2006). "Phishing Exposed." from searchexchange.com.
- Jeffrey M. Stanton, Kathryn R. Stama, et al. (2005). "Analysis of end user security behaviors." Computers & Security **24(2): 124–133**.
- Jianxin Jeff, Y. (2001). A note on proactive password checking. Proceedings of the 2001 workshop on New security paradigms. Cloudcroft, New Mexico, ACM Press.
- Johansson, J. M. (2004). "The Great Debates: Pass Phrases vs. Passwords." from <http://www.microsoft.com/technet/community/columns/secgmt/sm1204.msp>.
- Jones, C. (2004). "Social Engineering: Understanding and Auditing." SANS institute.
- Kaehler, S. D. (1998). "FUZZY LOGIC - AN INTRODUCTION." from http://www.seattlerobotics.org/encoder/mar98/fuz/fl_part1.html.
- Kapp, J. (2000). "How to Conduct A Security Audit." (120).
- Kenneth Allendoerfer (2005). Human Factors Considerations for Passwords and Other User Identification Techniques 35.
- Kruger, H. A. and W. D. Kearney (2006). "A prototype for assessing information security awareness." Computers & Security **25(4): 289-296**.
- Larcom, G. and A. J. Elbirt (2006). "Gone phishing." Technology and Society Magazine, IEEE **25(3): 52**.
- Lin Chun-Li, Sun Hung-Min, et al. (2001). "Attacks and solutions on strong-password authentication." IEICE Transactions on Communications e Series B **E84B(9): 2622-2627**.
- Liu, W., H. Guanglin, et al. (2005). Phishing Webpage Detection. Proceedings of the Eighth International Conference on Document Analysis and Recognition, IEEE Computer Society.
- Lo, E. C. and M. Marchand (2004). Security audit: A case study, Niagara Falls, Canada, IEEE Inc., Piscataway, NJ 08855-1331, United States.
- Luo, J., S. M. Bridges, et al. (2001). Fuzzy frequent episodes for real-time intrusion detection, Melbourne, Australia, Institute of Electrical and Electronics Engineers Inc.
- M. Chandrasekaran, K. Karayanan, et al. (2006). Towards phishing e-mail detection based on their structural properties. New York, State Cyber Security Conference.
- Mark Wilson and J. Hash (2003). Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology. **15/10/2010**.

- Michael E. Whitman, H. J. M. (2010). Management of Information Security, Course Technology, Cengage Learning.
- Microsoft (2006). "How to protect insiders from social engineering threats."
- Microsoft, C. (2006). "Password Checker." from <http://www.microsoft.com/protect/yourself/password/checker.mspx>.
- Microsoft, C. (2006). "Recognize phishing scams and fraudulent e-mails." Retrieved 25/09/2009, from <http://www.microsoft.com/athome/security/email/phishing.mspx>.
- Microsoft, C. (2011). "Password Checker " Retrieved 22/06/2011, from <https://www.microsoft.com/security/pc-security/password-checker.aspx>.
- Micrsoft. (2009). "Protect yourself from Conficker." from <http://www.microsoft.com/en-gb/security/pc-security/conficker.aspx>.
- Miller, G. A. (1956). "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information." Psychological Review: 81-97.
- Milus, S. (2004). "The Institutional Need for Comprehensive Auditing Strategies." Information Systems Audit and Control Association 6.
- Mitnick, K. D. and W. L. Simon (2002). The Art of Deception, wiley.
- Mozilla. (2010). "Thunderbird Phishing Protection." from <http://www.mozilla.org/en-US/thunderbird/features/>.
- Namestnikov, Y. (2010). "Information Security Threats in the First Quarter of 2010." from http://www.securelist.com/en/analysis/204792120/Information_Security_Threats_in_the_First_Quarter_of_2010.
- Nazario, J. (Oct 2008). "Phishing Corpus." from <http://monkey.org/~jose/wiki/doku.php?id=PhishingCorpus>.
- Negnevitsky, M. (2005). Artificial Intelligence - A guide to Intelligent Systems, Addison Wesley.
- Nigel, D. and J. Arun (2002). "Connectionist Password Quality Tester." IEEE Transactions on Knowledge and Data Engineering 14(4): 920-922.
- NIIT (2004). Introduction to Information Security Risk Management, Prentic Hall of India.
- O'sullivan, A. (2009) "Online banking fraud on the rise."
- Okenyi, P. O. and T. J. Owens (2007). "On the Anatomy of Human Hacking." Information Systems Security 16(6): 302-314.
- Olzak, T. (2011) "Enterprise Security: A practitioner's guide."

- Orgill, G. L., G. W. Romney, et al. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems Proceedings of the 5th conference on Information technology education, Salt Lake City, UT, USA ACM Press.
- Page, P. (2003). Security Auditing A Continuous Process, SANS Institute.
- Panko, R. R. (2003). Corporate Computer and Network Security, Pearson Education.
- Peter Hoonakker, N. B. a. P. C. (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. HUMAN FACTORS and ERGONOMICS SOCIETY 53rd ANNUAL MEETING, USA.
- RCMP (2012). E-mail Fraud / Phishing Royal Canadian Mounted Police.
- Redmon, K. C. (2006). "Mitigation of Social Engineering Attacks in Corporate America." <http://www.infosecwriters.com>.
- Research, I.-T. (2004). Security Auditing An Eight-Step Guide, Info-Tech Research Group.
- Rigby, B. (July 2012) "Hotmail relaunched as social-friendly Outlook ".
- Sapronov, K. (2005). "The human factor and information security."
- Scarfone, K. and M. Souppaya (2009). Guide to Enterprise Password Management.
- Schneier, B. (1996). Applied Cryptography Wiley.
- Schneier, B. (2000). Secrets & Lies : Digital Security in a Networked World, Wiley.
- Schneier, B. (2004). "Customers, passwords, and Web sites." Security & Privacy Magazine, IEEE **2**(4): 88.
- Shah, J. (April 2007). "Online Crime Migrates to Mobile Phones." Sage **1**(2).
- Shannon, C. (1951). "Prediction and Entropy of Printed English." Bell System Technical Journal **30**(1): 50-64.
- Shi, X., W. Li, et al. (2004). "Model approach to fuzzy security audit." Journal of Information and Computation Science **1**(2): 299-303.
- Sniper, S. (2012). "Active Facebook Phishing Warning! - Friends posting links to your wall which urge you to watch a video. ." Retrieved 01/07/2012, from <http://scamsniper.blogspot.co.uk/2011/02/active-facebook-phishing-warning.html>.
- Symantec, C. (April 2012, 31/5/2012). "Internet Security Threat Repor." 2012, from http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=tal_number_of_vulnerabilities.

- Symantec, I. (2009). "How to Remove the Conficker Worm Virus - Information and Removal." 2010, from <http://www.norton-security-store.com/help/remove-conficker-worm.html>.
- Symantic (2002). **Managing Security Incidents in the Enterprise.**
- Technology, N. (2006, 4/10/2006). "The Advent of Uncrackable Passwords." from http://neosmart.net/downloads/research/Uncrackable_Passwords.pdf.
- Thornburgh, T. (2004). Social engineering: the "Dark Art" Proceedings of the 1st annual conference on Information security curriculum development, ACM Press.
- Tyler Moore and R. Clayton (2007). An Empirical Analysis of the Current State of Phishing Attack and Defence. In Proceedings of the 2007 Workshop on the Economics of Information Security (WEIS).
- Tzer-Shyong, C., J. Fuh-Gwo, et al. (2006). Hacking Tricks Toward Security on Network Environments.
- US-CERT (2011). National Cyber Alert System.
- Vijaya M.S, Jamuna K.S, and Karpagavalli S.. 2009. Password Strength Prediction Using Supervised Machine Learning Techniques. In Proceedings of the 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT '09). IEEE Computer Society, Washington, DC, USA, 401-405
- Wenyin, L., D. Xiaotie, et al. (2006). "An antiphishing strategy based on visual similarity assessment." IEEE Internet Computing **10**(2): 58.
- Whitman, M. E. and H. J. Mattord (2012). Principles of Information Security, Course Technology, Cengage Learning.
- Wiedenbeck, S., J. Waters, et al. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. Proceedings of the working conference on Advanced visual interfaces. Venezia, Italy, ACM: 177-184.
- William E. Burr, Donna F. Dodson, et al. (2006). Electronic Authentication Guideline. C. S. Division, NIST
- Wilshusen, G. C. (2011). Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems.
- Wold, J. (March 2006). "Security Awareness Training For Small Businesses." THE ISSA JOURNAL.
- Xiaoyuan, S., Z. Ying, et al. (2005). Graphical passwords: a survey.
- Yue Zhang, S. E., Lorrie Cranor, and Jason Hong (2007). Phinding Phish Evaluating Anti-Phishing Tools. 14th Annual Network & Distributed System Security Symposium (NDSS 2007), San Diego, CA.

APPENDICES

6.1 Published Contributions

- a. **Salem O S**, Hossain M A and Kamala M : “Awareness Program and AI based Tool to reduce risk of phishing attacks”, *International Symposium on Frontier of Computer Science, Engineering and Applications– IEEE, (CSEA 2010)– June 29 to July 1 – Bradford, United Kingdom.*
- b. **Salem O S**, Hossain M A and Kamala M : “Phishing, Vishing and Smishing – Detection and Protection Scheme”, *International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2009) - October 21-23– Fes, Morocco*
- c. **Salem O S**, Hossain M A and Kamala M (2008): "Intelligent Measuring Tools for Password Strength", *International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 18-21 March, Kathmandu, Nepal.*
- d. **Salem O S**, Hossain M A and Kamala M (2008): "Intelligent System to Measure the Strength of Authentication", *IEEE, 3rd International Conference, Information and Communication Technologies: From Theory to Applications. (ICTTA 2008), 7-11 April, ICTTA460., Damascus, Syria*

6.2 Feedback of the survey conducted at section 3.5

Timestamp	Gender	Job	Education Level	Country of resident	did you hear about phishing problem before?	how much spoofed website that I show you looks like legitimate one?	one objective of this study is to aware you about this problem, do you think it was useful study?	how do you think we can reduce the risk of this problem (phishing)?	if you know this problem before, tell me your experience with it please s in few words..
7/7/2012 0:27:34	Female	Not Working	University Graduate	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/9/2012 10:11:03	Male	Employee	High Study	Saudi Arabia	I'm not sure about it	slightly different	yes, very useful	Anti-phishing tools and security software	They hijacked my friend yahoo email and he lost his data
7/7/2012 0:27:52	Male	Student	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	التدريب وبرامج الحماية ضرورية جدا
7/7/2012 11:50:24	Male	Student	High Study	UK	First time I hear about it	they are very similar	yes, very useful	Both of them	
<p>سمعت عن مشاكل مشابهة ، ولكن لم تكن لدي فكرة واضحة عنها . هذا أوضح وأبسط شرح اطلعت عليه لهذه المشكلة . سأحاول أن أكون حريصاً في المستقبل . جزاك الله خيراً .</p>									

APPENDIX - B

7/7/2012 12:34:01	Male	Student	High Study	Jordan	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
7/7/2012 13:02:43	Female	Student	School	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/7/2012 13:02:57	Female	Student	School	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/7/2012 13:16:36	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
I learnt about this problem from messages which i received from my bank highlighting this problem. There was a software that was distributed by my bank website to help avoid phishing website. I think it was called trusteeer.									
7/7/2012 13:43:56	Male	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/7/2012 16:23:41	Male	Employee	High Study	Saudi Arabia	I'm not sure about it	they are very similar	yes,, it was ok	Both of them	
7/8/2012 5:59:06	Male	Employee	University Graduate	Jordan	I'm not sure about it	they are very similar	yes,, it was ok	Both of them	
7/11/2012 15:16:40	Male	Student	High Study	Other	yes I know it very well	slightly different	yes, very useful	Both of them	
there are some software that can identify these phishing pages. one of the very simple techiques is that it checks the link from the HTML page itself. the link looks like that visible displayed part. it applies matching tecniques on the "real destination page" and the "visible displayed part". it alerts the user if the following conditions are met: 1- if the "real destination page" and the "visible displayed part" are not matching at all. for instance "visible displayed part" is : facebook and "real destination page" is: www.omra. bla bla 2- if the "real destination page" is not secured website (sometimes denoted by https). 3- if some java scripts are to be executed by the "real destination page". Thanks. and one more thing do not forget to add Egypt in the countries combobox or Morsi will be upset :) Walid Adly:) just kidding.									
7/8/2012 6:44:09	Male	Employee	University Graduate	Jordan	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
7/8/2012 7:03:33	Male	Employee	High Study	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
أعلم أن هناك صفحات تشبه صفحات Hotmail كانت تظهر للمستخدم من خلال بريد إلكتروني عادي جدا وعلى شكل إعلان تجاري، ثم يكتشف المستخدم بعد فترة انه تم سرقة بريده الإلكتروني وإرسال رسائل منه إلى الأصدقاء لطلب مساعدة أو ما شابه.									
7/12/2012	Male	Employee	High	UK	yes I know it very	slightly different	yes, very useful	By Training and	

APPENDIX - B

0:49:43			Study		well			awarness programs	
<p>Yes, I have been hacked by receiveing a link through yahoo, sent automatically from my friend through his messenger to all people in his list in which I was one of them.</p> <p>Although, I am a techincal person, however this was the firt time have been fooled by such a trick. I actually was tempted by the title of the link which made me click on the link then I got a page which is exactly the same as Yahoo login detail, I was kind enough to enter my Yahoo email address, after second my Yahoo been taken by somebody else and he started to talk to my family through the messenger.</p> <p>Although I was lucky enough by having a recovery email which manged to bring back. However, to me, this is one of the most dangrous type of spoofing.</p> <p>Thanks</p> <p>Mohammed</p>									
7/8/2012 12:07:48	Male	Student	High Study	UK	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/12/2012 18:44:34	Female	Student	High Study	UK	yes I know it very well	slightly different	yes, very useful	Both of them	
7/8/2012 12:21:30	Male	Student	School	UAE	yes I know it very well	they are very similar	yes, very useful	Both of them	
(facebook, hotmail) اذا تلقيت رسالة من اي موقع لا اعرفه او من كلا الموقعين اقوم بحذف الرسالة بعد قراء عنوانها..									
7/8/2012 13:16:39	Male	Student	School	Jordan	I'm not sure about it	they are very similar	yes, very useful	Anti-phishing tools and security software	
7/8/2012 14:12:30	Male	Employee	University Graduate	Saudi Arabia	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
Part of my work is to sell security solutions and this is only an example of the things we present to our prospects.									
7/14/2012 13:27:47	Male	Student	School	Jordan	I'm not sure about it	slightly different	yes, very useful	Both of them	
7/8/2012 14:15:06	Male	Student	High Study	Saudi Arabia	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/8/2012 14:18:14	Female	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Anti-phishing tools and	

APPENDIX - B

								security software	
7/8/2012 14:19:55	Female	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/8/2012 15:26:27	Male	Employee	University Graduate	Canada	First time I hear about it	they are very similar	yes, very useful	By Training and awareness programs	
7/8/2012 15:42:57	Female	Student	University Graduate	USA	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
7/23/2012 15:18:31	Male	Employee	High Study	UK	yes I know it very well	slightly different	yes, very useful	Both of them	I never responded to such emails. As i know the risk of responding
7/8/2012 16:03:49	Male	Student	High Study	Jordan	yes I know it very well	they are very similar	yes, very useful	Anti-phishing tools and security software	
7/26/2012 13:21:37	Male	Student	University Graduate	Jordan	First time I hear about it	They are not similar	yes, very useful	Both of them	
7/8/2012 16:04:41	Male	Not Working	High Study	Jordan	yes I know it very well	they are very similar	yes, very useful	Both of them	
بعض الهاكرز يلجؤون لإرسال روابط مشابهة لصفحات مواقع التواصل من أجل كتابة اسم المستخدم وكلمة السر مرة أخرى ليتم السيطرة عليها من قبل الهاكرز واختراق حسابك.									
7/26/2012 18:40:56	Male	Student	High Study	UK	First time I hear about it	They are not similar	yes, very useful	Both of them	
7/8/2012 16:55:11	Male	Student	High Study	UAE	yes I know it very well	they are very similar	yes,, it was ok	By Training and awareness programs	
هذه المشاكل تكون عادة تأتي من أناس لا نعرفهم على الفيسبوك حيث يطلبون منا أن نصوت لهم! المتصفحات الجديدة تظهر لك أن هذه الصفحة هي عملية نصيد و ليست موقع رسمي!									

APPENDIX - B

7/8/2012 17:24:25	Male	Student	School	Jordan	yes I know it very well	they are very similar	yes, very useful	Both of them	
تعرضت لهذه المشكلة مرة وسرق حسابي على الفيس بوك ولاكن استرجعته عن طريق الايميل افضل ان يجعل الشخص باسورد غير متشابه في كل حساباته									
7/8/2012 17:31:24	Male	Employee	High Study	Canada	yes I know it very well	they are very similar	No, it wasn't	Both of them	
7/8/2012 18:52:11	Female	Employee	University Graduate	Saudi Arabia	I'm not sure about it	they are very similar	yes, very useful	Both of them	
تم إرسال معلومات عنها بوسائط اتصالات مختلفة ، وقرأت عنها في الصحف ، ولكن لم اكن اتوقع ان تكون بالدقة هذه، شكراً لك ، عسى ان يفيدك ما قدمنا ، وفق الله الجميع									
7/8/2012 19:38:50	Male	Employee	High Study	Other	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
Yes I knew it. When I have suspicions about any website link recieved by email, I rarely clicked on it. Also, I clicked on the link, then normally I check to see if the webpage like is changed or not.									
7/8/2012 19:41:00	Male	Student	School	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/8/2012 19:54:43	Male	Buisnessman	High Study	Jordan	yes I know it very well	they are very similar	yes, very useful	Both of them	
I have read some about this problem specially with facebook; when i thought my account was hacked, and i heard about not just phishing but also , someone might add you on facebook as a friend and after you accept him/her they will share a link on your wall that if you click it or share it they hack you, i think its similar to phishing but i am only a user not an expert, this was helpfull thank you, Jazakom Allah Khairan									
7/8/2012 22:10:20	Male	Employee	University Graduate	UAE	yes I know it very well	they are very similar	yes, very useful	Both of them	
if you put the mouse on the fake link, you can see the actual website on the bottom of the browser when you place the mouse above the link,, this is how i find out that the email/link is fake. for example (in your examples before) when i placed the mouse on the "www.hotmail.com" link (without clicking) i found out that the website is actually ww.omran.....etc i also usually check the email address when the email is suspicious; the name is similar to my friend's name but the email ID is not I wish you all the best,,									
7/8/2012 22:38:14	Female	Not Working	University Graduate	UAE	I'm not sure about it	they are very similar	yes, very useful	Both of them	
Really i heard about this problem before but the thing i didnt know is that they have made the same pages of the social networks which makes people trust them.									

APPENDIX - B

According to me I usually dont open any suspicious email except some cases like sending email for a specific destination									
7/8/2012 22:39:29	Male	Student	School	UAE	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/9/2012 0:16:51	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/9/2012 8:25:17	Male	Employee	University Graduate	Kuwait	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
7/9/2012 10:50:35	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/9/2012 16:12:05	Male	Employee	School	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
Thank You for this. Although I was aware of phishing before, I do feel that this type of study is useful to raise awareness of the problem, and the threats attached to it. Thanks, Farzan									
7/9/2012 20:37:43	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	I always look at the site address.
7/10/2012 0:11:30	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes,, it was ok	Both of them	
7/10/2012 10:28:37	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Anti-phishing tools and security software	
Friend of mine was affected where he lost his e-mail because of that. After contacting the e-mail company we have managed to get it back.									
7/7/2012 13:00:56	Male	Student	University Graduate	UK	I'm not sure about it	slightly different	yes, very useful	Both of them	
7/10/2012 11:28:45	Male	Student	Diploma	UAE	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/10/2012 20:45:03	Male	Employee	University Graduate	UAE	yes I know it very well	they are very similar	yes, very useful	Both of them	usually when I receive

APPENDIX - B

									such emails, I trash them.
7/10/2012 21:43:27	Male	Employee	University Graduate	UK	First time I hear about it	they are very similar	yes, very useful	By Training and awareness programs	
7/11/2012 7:04:55	Male	Employee	High Study	Saudi Arabia	First time I hear about it	they are very similar	yes, very useful	By Training and awareness programs	
7/11/2012 13:07:54	Male	Student	School	UK	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/7/2012 23:36:20	Male	Employee	University Graduate	Jordan	yes I know it very well	slightly different	yes, very useful	Both of them	
7/11/2012 15:46:36	Female	Employee	High Study	Saudi Arabia	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/11/2012 15:58:15	Female	Employee	High Study	UK	yes I know it very well	they are very similar	No, it wasn't	Both of them	
7/12/2012 17:22:08	Male	Student	High Study	Other	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/8/2012 8:31:17	Male	Student	School	Jordan	yes I know it very well	slightly different	yes,, it was ok	Both of them	
هناك الكثير من المنتديات التي لا تعد ولا تحصى تساعد علا انشاء مثل هذه الصفحات وهنا تكمن المشكلة بحيث انه اصبح الموضوع لا يحتاج لان تكون هاكل محترف لتستطيع الاحتيال من هذا المجال.									
7/8/2012 9:52:15	Male	Student	High Study	UK	yes I know it very well	slightly different	yes, very useful	By Training and awareness programs	
حدثت هذه المشكلة عندنا حاول بعض شباب الجيش الإلكتروني التابع لنظام الأسد اختراق صفحات الناشطين . وكانت محاولتهم ناجحة على الأشخاص الذين لديهم حساب على الهوتميل و لم تنجح على الذين لديهم حساب على جي ميل . ربما يعود السبب إلى أن شركة الجي ميل أقوى حماية من الهوتميل ، وشكرا، الله يفتح عليكم ويسرلكم .									
7/12/2012 21:25:07	Male	Student	High Study	UK	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/12/2012 23:10:59	Female	Not Working	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/13/2012 16:45:31	Male	Student	High Study	UK	yes I know it very well	they are very similar	yes,, it was ok	Both of them	

APPENDIX - B

I have read about this problem when I started receiving some email which was asking for passwords.									
7/16/2012 2:02:36	Male	Employee	High Study	Saudi Arabia	I'm not sure about it	they are very similar	yes, very useful	Both of them	
7/16/2012 7:44:10	Male	Employee	High Study	UAE	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/16/2012 12:38:46	Male	Employee	School	Jordan	First time I hear about it	they are very similar	yes, very useful	By Training and awarness programs	أشكر ككثيرا... لقد استفدت منك كثيرا يا عزيزي
7/16/2012 18:52:40	Male	Student	High Study	Jordan	First time I hear about it	they are very similar	yes,, it was ok	Both of them	
7/8/2012 15:20:58	Male	Student	School	UAE	yes I know it very well	slightly different	yes, very useful	Both of them	
7/16/2012 19:33:26	Male	Student	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/18/2012 19:26:50	Male	Student	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/22/2012 14:48:57	Male	Employee	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
so great study, its give good awarness message to users, i like it									
7/25/2012 20:58:22	Male	Employee	High Study	Jordan	yes I know it very well	they are very similar	yes, very useful	Both of them	
the facebook page shocked me,,its look like it,, i was think its really facebook page excellent study									
7/26/2012 6:35:57	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	تجربة رائعة اعتقد أنه يجب تعميمها لنشر الاستفادة
7/26/2012 6:40:50	Male	Buisnessman	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/26/2012 18:40:32	Male	Employee	University Graduate	Jordan	yes I know it very well	they are very similar	yes, very useful	Both of them	
7/26/2012	Male	Student	High	UK	First time I hear	they are very	yes, very useful	Both of them	

APPENDIX - B

18:47:27			Study		about it	similar			
7/27/2012 17:51:10	Male	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/29/2012 3:30:57	Female	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/8/2012 19:42:04	Male	Student	Diploma	USA	yes I know it very well	slightly different	yes, very useful	Both of them	
I had friends who received spoofed paypal emails from people who wanted to buy their items. so the person receives fake email from "paypal" telling them that money has been put into their account and the person who is uneducated about this topic does not log in to the real paypal to check, he sent out the item and got scammed.									
7/29/2012 6:41:39	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/29/2012 19:18:51	Male	Student	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/29/2012 19:19:46	Male	Employee	High Study	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/29/2012 20:02:13	Male	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/29/2012 22:39:07	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/9/2012 6:39:38	Male	Student	School	UAE	yes I know it very well	slightly different	yes, very useful	Both of them	
7/30/2012 1:38:32	Female	Employee	High Study	UK	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/10/2012 20:50:46	Male	Employee	University Graduate	Jordan	I'm not sure about it	slightly different	yes, very useful	Both of them	
7/10/2012 21:00:42	Male	Employee	University Graduate	UAE	yes I know it very well	slightly different	yes,, it was ok	By Training and awarness programs	
7/14/2012 16:07:57	Female	Student	High Study	Jordan	I'm not sure about it	slightly different	yes, very useful	Both of them	
7/15/2012 8:47:09	Female	Employee	University Graduate	Jordan	yes I know it very well	slightly different	yes,, it was ok	Both of them	

APPENDIX - B

7/30/2012 1:40:50	Female	Employee	University Graduate	UK	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/30/2012 6:02:11	Male	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
7/30/2012 18:19:48	Male	Buisnessman	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/1/2012 3:16:45	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/1/2012 3:17:01	Female	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/1/2012 3:17:18	Male	Employee	High Study	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/1/2012 3:19:13	Female	Employee	University Graduate	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
8/1/2012 3:20:13	Male	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	By Training and awarness programs	
8/1/2012 3:22:36	Female	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 5:45:28	Male	Buisnessman	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 5:53:56	Male	Student	High Study	UK	yes I know it very well	they are very similar	yes, very useful	Both of them	
Phishing is an illegal activity that the hacker tricks people into divulging sensitive information, such as bank and credit card accounts, its forbidden to such attack,, and its so important to aware propel about this kind of security problems, thanks for this experiment. Wael									
8/2/2012 20:05:01	Male	Student	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 20:06:06	Female	Employee	High Study	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 20:20:04	Female	Student	School	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 22:08:16	Female	Buisnessman	Diploma	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	

APPENDIX - B

8/2/2012 22:09:44	Male	Employee	High Study	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	
8/2/2012 22:10:55	Female	Student	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 22:11:42	Male	Employee	University Graduate	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/2/2012 23:05:39	Male	Employee	Diploma	Jordan	I'm not sure about it	they are very similar	yes, very useful	Anti-phishing tools and security software	
8/2/2012 23:09:05	Female	Employee	Diploma	Jordan	First time I hear about it	they are very similar	yes, very useful	Both of them	
8/3/2012 3:16:53	Female	Student	University Graduate	Jordan	First time I hear about it	they are very similar	yes,, it was ok	Both of them	
8/3/2012 5:46:46	Male	Employee	Diploma	Jordan	I'm not sure about it	they are very similar	yes, very useful	Both of them	