A SURVEY ABOUT THE INTEGRATION OF SOCIAL ENGINEERING ATTACKS WITH CYBER SECURITY EXPLOITING TURKISH VULNERABILITIES IN TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS INSTITUTE
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ADEM TOSUN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR MASTER'S DEGREE

IN

THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2015

A SURVEY ABOUT THE INTEGRATION OF SOCIAL ENGINEERING ATTACKS WITH CYBER SECURITY EXPLOITING TURKISH VULNERABILITIES IN TURKEY

Submitted by **Adem TOSUN** in partial fulfillment of the requirements for the **Master's Degree in Department of Information Systems, Middle East Technical University** by,

Prof. Dr. Nazife BAYKAL _____
Director, **Informatics Institute**

Prof. Dr. Yasemin Yardımcı ÇETİN _____
Head of Department, **Information Systems**

Prof. Dr. Nazife BAYKAL _____
Supervisor, **Information Systems, METU**

Examining Committee Members:

Prof. Dr. Nazife BAYKAL _____
Information Systems, METU

Assist. Prof. Dr. Erhan EREN _____
Information Systems, METU

Prof. Dr. Kemal BIÇAKÇI _____
Computer Engineering Dept.TOBB University of Economics and Technology

Assist. Prof. Dr. Aybar Can ACAR _____
Bioinformatics, Medical Informatics, Information Systems, METU

Assist. Prof. Dr. Cengiz ACARTÜRK _____
Cognitive Science, METU

Date: 15.09.2015

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Adem TOSUN

Signature:

ABSTRACT

A SURVEY ABOUT THE INTEGRATION OF SOCIAL ENGINEERING ATTACKS WITH CYBER SECURITY EXPLOITING TURKISH VULNERABILITIES IN TURKEY

TOSUN, Adem
M.S., Department of Information Systems
Supervisor: Prof. Dr. Nazife Baykal

September 2015, 97 pages

Many organizations have been seeking for comprehensive and applicable security policies to regulate their security aspects. As it is a well-known issue, the weakest link of chain in Cyber security is human being and it cannot be measured easily as its being intangible. Organizations may invest millions of dollars to build technically secure systems by installing high level trusted software programs or devices. History has shown that these kind of measures neither has been that much successful or effective in protecting the systems nor prevented social engineering kinds of attacks which may lead to a compromised system without any need to lose much time and risk for a hacker. The purpose of this thesis is to investigate which successful tactic and techniques are successfully being used to compromise systems by manipulating or hacking human software rather than software systems and find out results of these attacks. In addition, the weakness of human software will be analyzed and dominant factors will be figured out. At the end of this thesis, how security policies should be made, which issues better be considered in addition to technical solutions and what the most weaknesses of participants will be revealed to provide a higher level secure systems for organizations. The effects and popularity of social engineering attacks will also be discussed at the end of the study and some countermeasures will be given to managers to prevent such social engineering attacks towards their workers.

Keywords: Cyber Security Policies, Social Engineering, Hacking People Techniques, Social Engineering Attack Types, Security, Weaknesses of Human, Secure Systems, Cyber Education, Ways Company More Secure, High Level Security, Hack Human Software

ÖZ

İNSAN ZAFİYETLERİNİ İSTİSMAR EDEREK YAPILAN SOSYAL MÜHENDİSLİK SALDIRILARININ SİBER GÜVENLİK İLE İLİŞKİLENDİRİLMESİ - TÜRKİYE ÖRNEĞİ

TOSUN, Adem
Yüksek Lisans, Bilişim Sistemleri
Tez Yöneticisi: Prof. Dr. Nazife Baykal

Eylül 2015, 97 sayfa

Günümüzde birçok şirket ve devlet kurumları, siber alanda güvenliklerini sağlayacak kapsamlı ve uygulanabilir bir siber güvenlik politikası için arayış içindedirler. Siber Güvenlik alanında en zayıf halka olan "insan" unsurunun siber alandaki güvenlik anlayış ve seviyesinin soyut bir kavram olması nedeniyle ölçümü oldukça zordur. Bu nedenle şirket ve devlet kurumlarının büyük bir yüzdesi yüksek güvenlik önlemler getiren sistemler için milyon dolar seviyesinde bütçeler ayırmakta olup bu konuda da imtina etmemektedirler. Ancak; siber güvenlik alanında yaşanılan olaylar açıkça göstermiştir ki, sadece donanımsal ve yazılımsal güvenlik tedbirleri özellikle sosyal mühendislik taktik ve teknikleri kullanılarak yapılan saldırılarda tek başlarına yetersiz ve etkisiz kalmaktadır. Çünkü bu tip sosyal mühendislik saldırıları, Hackerlerin zararlı kod yazarak hedeflerindeki şirket ve kurumların sistemlerini ele geçirmeye oranla fazla zaman harcamadan ve fazla "yakalanma" riskine girmeden hedef sistemleri ele geçirmeyi amaç edinmektedir. Bu tezimin ana amacı, hangi taktik ve tekniklerin, güvenlik yazılımlarını "kırmak" yerine insanların zayıf yönlerini istismar ederek veya insanları manipüle ederek hedef sistemleri ele geçirmeye olanak sağladığını tespit ederek bu alanda insanların zafiyetlerini ortaya çıkarmaktır. Araştırmam sonucunda katılımcıların hangi alanlarda zafiyeti olduğu konusunda tespit ettiğim husus ve tedbirlerin, şirket ve kurumların siber güvenlik seviyeleri konusunda artı katkıda bulunacağını değerlendiriyorum.

Anahtar Kelimeler: Siber güvenlik, sosyal mühendislik, İnsan kandırma sanatları, sosyal mühendislik saldırı türleri, insan zafiyetleri, İnsan Manipülasyonu,

DEDICATION

To METU, and my Family

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Prof Dr. Nazife BAYKAL for her extensive support, guidance and patience throughout my thesis studies. I am grateful for what she has done for me so far.

And I would like to thank my beloved wife Oya Sarkan Tosun and my sweet kids Ataberk Tosun and Elif Doğa Tosun for their boundless love, patience and support during the thesis period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SE	Social Engineering
IT	Information Technology
RSE	Reverse Social Engineering
NLP	Neuro-Linguistic Programming
AV	Anti-Virus

Table 1 – List of Abbreviations

CHAPTER 1

1 INTRODUCTION

There are several techniques that can be used to breach the cyber security defenses of any organization. Attacking through "the human" approach, often termed Social Engineering; a technique used by computer hackers based on getting people to unknowingly assist the attacker in successfully accomplishing his/her breach attempt into the target system; is one of these techniques.

None of us will give our username and passwords after being asked a question like "Hi; could you please give me your username and password?" At least after such a question, we would feel ourselves kind of suspicious to the person who wants to get an "access right" into our private area. We have to consider today world's attackers are professionals in their domains and they know how to get into other people's mind and "hacking" them. They will be able to manipulate the "weakest link" as they want without any alert, detection or system alarm only after they break the "secure chain" of the target system.

In psychology, human being is eager to "trust" and "share" his/her feelings with others. We normally believe this habit makes us feel satisfied, pleased, self-confident, and happy. For instance if something goes wrong with the life, we feel ourselves to share our problems with people we trust to feel better and safe. Knowing this natural "trust and sharing" habit, social engineers are willing to get our critical information by hiding their real intent by abusing our weak and sensitive moments. In order to get the control of their target, the key point is gaining the trust in any way.

1.1 RESEARCH QUESTION

Traditional hacking and attacks like sending malicious code to the target system are mostly technical-based. These attack types are directed to the targeting system itself or its applications trying to exploit the vulnerabilities of the software and hardware systems. However, the effectiveness of these technical-based attacks has decreased as the technical and technological countermeasures are gradually being adopted by more and more organizations. This situation has encouraged technical hackers to choose the alternative path; a non-technical method called social engineering, targeting the vulnerabilities of both people and technology. As a result, this is being considered as one of the biggest cyber security threats faced by many organizations and individuals today. (Sapuan, Emo, & Irty, 2012)

Nowadays security companies have been testing the cyber security level of their customers' system in terms of technical vulnerabilities. There has been implemented "social engineering" tests but this does not go further than just "phishing" technique. Unfortunately

after some period of time, when the users have knowledge of IT policies of the organization and these kinds of awareness tests, they pretend to behave as they should according to the security policies after being sent such emails. Moreover; after the system users applied any kind of questionnaire or interview, they already know which option they should mark or choose; and as a result these kind of tests does not reflect the real picture of the awareness level of the organizations.

In this research, rather than applying just phishing technique or applying a questionnaire, my research team and I added some more techniques towards the participants like baiting, vishing, and contacting personally. Our goals were here putting the users into a real scenario without their knowledge of being tested at that moment and see their responses and reactions against these social engineering types of attacks. We also chose some popular approaches used by many social engineers towards our participants to measure what kind of subjects are popular among the system users and open to successful attacks. Before applying our approaches, we normally made some investigations about our participants and got some information about their private life from their social media pages. We did such a research to choose which approach will be fit for the target. In this way we aimed to determine which approach will be used against which participant to increase our success likelihood; just like a social engineer does. By this way, we could able to see which vulnerabilities are most common among people and to figure out most popular weaknesses of them. In the end we were able to build some decision trees for a social engineer to increase the success level of his attacks. This made us able to see which paths could be used by social engineers to exploit the system users' personal vulnerabilities.

This thesis includes not only information about common Social Engineering attack types but also potential cost of these attacks to the organizations. It discusses the various forms of Social Engineering technique and tactics, and how social engineers take advantage of human vulnerabilities. It also discusses some ways about countermeasures to fight against these kinds of attacks, and highlights the importance of awareness trainings and a strict security policy in the organization to prevent such attacks.

1.2 THE COMMON MISTAKE – "I AM SAFE" SYNDROME

Social engineers are always looking and waiting for the weakest moments of their targets as mentioned before. This means they need to gather detailed information about their targets. It is crystal clear that without investigating about them, social engineers can't breach into their world. Even a crumb of information can also lead to high-level intelligence. For instance if a social engineer is able to get information of "the boss's vacation schedule" there can be a scenario like "pretending to be a close friend of the boss who was just passing by and wanted to see how the boss is" and with a fake business card and a suit, the attacker will be able to make his/her secretary believe him to be his close friend. After having the trust – because social engineers know that secretaries are there for helping people - he can ask the secretary to insert a USB stick into the computer to print out a document to deliver the boss when s/he comes back. For the secretary, rather than plugging that USB given by the attacker into the

company's computer, it would be better to say "Sir, welcome to our system. You can do whatever you want with this authorization that I gave you a few seconds ago". This scenario is not that far from reality or inapplicable for a company; easy and clean job.

Figure 1 – "I'm Safe" Syndrome

Most of the time; while IT personnel or managerial people getting deep into high level technical precautions on software and hardware systems; they may ignore or omit the easiest pitfalls which may make their systems vulnerable to attacks. It is just like not being able to see clear the closer while concentrating on looking too far. Actually not taking in consideration of the weakest component of systems – human users – of the security chain is one of a critical mistake for many companies. Discovered vulnerabilities of the users can be manipulated easily without spending that much risk and time by an attacker with some carefully chosen approaches with right techniques.

After taking technical measures and spending thousands of dollars on hardware and software systems, the "I'm safe now!" feeling takes place in many administrative people or system users. As long as this dangerous habit takes place in users' or administrators' mind, it clearly means that one of security doors is wide open for outsiders and these moments may be exploited by a social engineer with less effort than a normal time.

This "I'm safe now" syndrome makes systems users or administrative people feel relaxed and behave ignorant to many security policies. And normally these kinds of behaviors damage the security level of companies. History has shown that there have been many breaches to systems just because of users' being ignorant to security policies and trusting technically taken precautions more than they should. This syndrome generally ends up with exploited systems on very critical times and it generally becomes too late to turn back or fix the failure.

1.3 SOCIAL ENGINEERING: CONCEPT AND SOLUTIONS

> *"It is much easier to trick someone into giving a password for a system than to spend the effort to crack into the system."*
>
> *Kevin Mitnick*

As it was stated by Tim Thornburgh in 2004, the key to maintaining the confidentiality, integrity, and availability of information systems is controlling who accesses which information. This is accomplished by being able to identify the user, and ensuring that the user has the proper right to access a given resource.

There have always been those that attempt to by-pass this security mechanism by guile or brute force. In the past, those who use guile have been called confidence men and con artists. Today, these people are called social engineers, but the tactics remain the same even if the objectives have changed. (Thornburgh, 2004)

Social engineering continues to be an increasing attack type for the propagation of malicious programs. In most articles, social engineering's definitions begin with some sort of definition like "the art and science of getting people to comply to your wishes" (Sarah Granger, 2001), "process of deceiving people into giving away access or confidential information, is a formidable threat to most secured networks" (Hasan, Prajapati, & Vohara, 2010), or "getting needed information; for example, a username and password; from a person rather than breaking into a system" (Hadnagy, 2010).

Social engineering can be any and all of these things. The one thing that everyone seems to agree upon is that social engineering is generally a hackers' clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system (Sarah Granger, 2001). Social Engineering (SE) is also a blend of science, art and psychology. While it is amazing and complex, it can be also very simple to apply to breach into target systems (social-engineer.org, 2015).

Social engineering attacks are usually performed by outsiders; people who doesn't work for the organization. But this does not mean there is no risk for insiders. The attackers mostly use psychological tricks to exploit their target systems by abusing "system users" to give them the information they need. These attack types mostly accomplished successfully without taking many potential risks or losing time to hack the already technically secured systems.

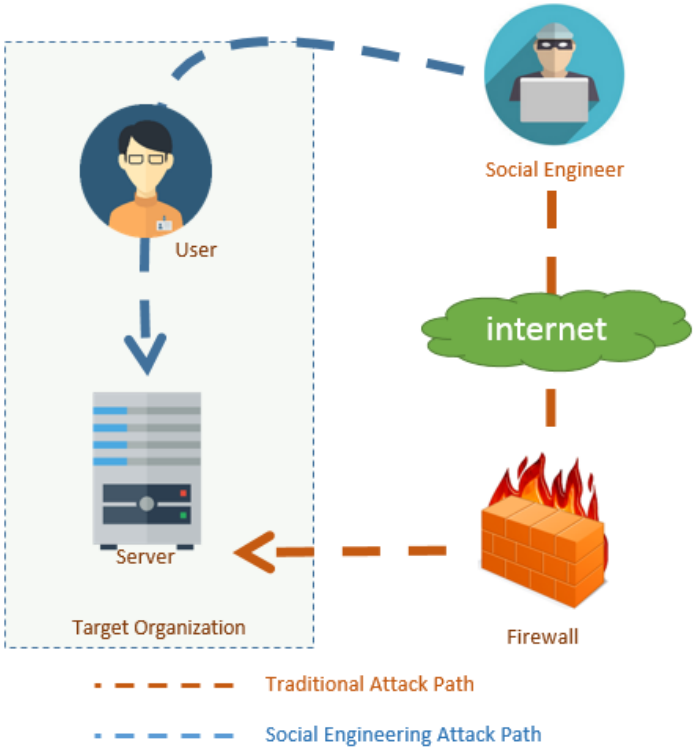

Figure 2 – Social Engineering Attack Path

As it is depicted in the figure 2, rather than trying to hack the systems through internet connection and trying to pass the firewalls or other security measures taken by the target organization; social engineers choose the shorter and less risky way, trying to hack the system users. As famous social engineer Kevin Mitnick mentions above, this second way will take less time and be less risky too.

Many of us think computer-network breaches are purely from technical paths. Technical flaws or vulnerabilities in computer systems and networks may be exploited or abused by the intruders or outsiders most of the time. Because mostly every update in the system gives births to new kinds of flaws or vulnerabilities, the technical precautions are never enough to meet fully secure system needs. In addition, social engineering types of attacks also play a crucial part in exploiting the systems. These attack types mostly aims to help an attacker to navigate through the technical software and hardware security barriers and precautions without any or less need of codes or technical flaws in target systems. The attacker aims to learn the username and passwords from his/her victims or get the credentials to get the control of their target systems without any alarm by using social engineering tactic and techniques. Before their attacks, social engineers make deep investigations about their victims' vulnerabilities or weaknesses. After waiting for the right time and moment, the attacker applies his/her chosen approach with the proper technique.

Social Engineers mostly exploit the vulnerabilities of their target systems by system users' lack of security awareness, inattention to details about cyber security policies, ignorance of potential catastrophic consequences, or the gullibility of theirs.

1.4 THE CYCLE OF SOCIAL ENGINEERING ATTACKS

Social engineers have four phases when performing their attacks.

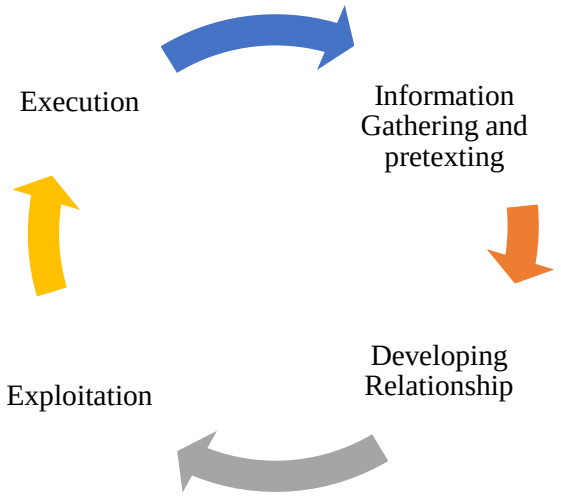

Figure 3 – Social Engineering Cycle

As mentioned above; the first step is information gathering and pretexting. In this phase social engineers do their best to gather enough information about their targets. They use many tools, programs, social media and websites to discover their victims' personality, habits, likes, dislikes etc. In the end, social engineer ends up with some meaningful information about the victim to be exploited.

The next step is developing relationship with the target somehow. These techniques vary according to the victim, the situation, and the environment. This relationship could be based on trust, respect, fear, reciprocation, and help, for some favor or many more reasons. (Kvedar, Nettis, & Fulton, 2010)

After contacting the victim, the next step is exploitation. Social engineer tries to exploit the built relationship after s/he believes it is the right time. The attacker will prepare his technique and tactics in more detailed in this phase as s/he has much knowledge about his/her victim.

The last step in the cycle is execution. In this phase the attacker puts his tactics and techniques into action. S/he may choose getting what s/he wants and get out the system or staying in the system until being detected to get more information s/he will need later. They usually choose the second option most of the time. This cycle may be applied to the same person to get more information or another victim for a fresh new star. (Scott Pinzon, 2007)

1.5 SOME COMMON SOCIAL ENGINEERING ATTACK TYPES

The easiest way to breach into a system is to simply ask permission from one who is in charge at the moment. No matter how much encryption and software security precautions have been implemented, a network is never completely secure against technical or non-technical attacks. The weakest link, the human component, can never be ignored when it comes to fully secured systems. It does not matter how many virtual private networks (VPNs), firewalls, antiviruses, anti-malware software or encrypting devices are in action if employees are willing to give access to their systems to anyone who asks for it unknowingly or by purpose. (Andrew Whitaker, 2009)

A social engineer is the one who uses deception, persuasion, or influence tactics and techniques to get information from these weakest links at the right moment. The fact that "there is a sucker born every minute" gives social engineers the opportunity to breach into many of secure systems. If the right technique with the right approach is applied to the right person, that means a high probable successful attack against the organization.

Being social engineer is about understanding and manipulating human psychology and having a methodical way of using someone to either give sensitive, critical information or grant unauthorized access to the attacker. In other words, this is not about being a good liar; it is about being an engineer who discovers ways to influence people for his/her advantage to get into secure systems more easily without losing so much time and without taking high risks.

1.5.1 Social Engineering in Reverse (RSE)

Reverse social engineering (RSE) has three steps as it is shown in the Figure 4 below.

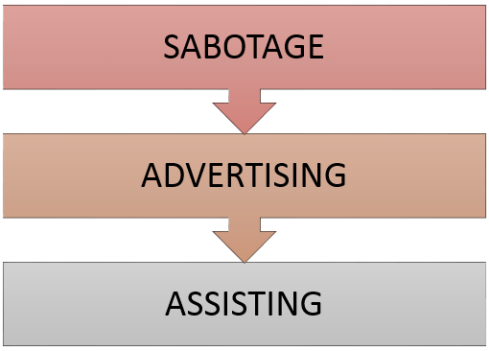

Figure 4 – Reverse social engineering (RSE) steps

In the first step, a social engineer finds a way to sabotage the target network by doing a technical attack against target system or simply sending an email telling they are infected by a virus or malware.

After waiting for proper time, the attacker advertises his/her services as a security consultant or behaves as if s/he is from a company, which is founded to fight against unauthorized system breaches.

After the target organization sees the advertisement, contacts the social engineer and applies to the social engineer about fixing the error in their systems. This actually means letting the attacker to work on their network as he wants. Once in, the social engineer gives the impression of fixing the problem (assisting) as he knows already what is wrong about the system. But the attacker will really do something malicious in fact, such as stealing confidential data, planting keyloggers or giving credentials for himself to reach the system.

Shortly in RSE; the social engineer creates a problem in the targeted network and is placing himself/herself in a position to help against the situation. Then after solving the problem, s/he becomes the organization's trustable security member as it is shown in the figure below.

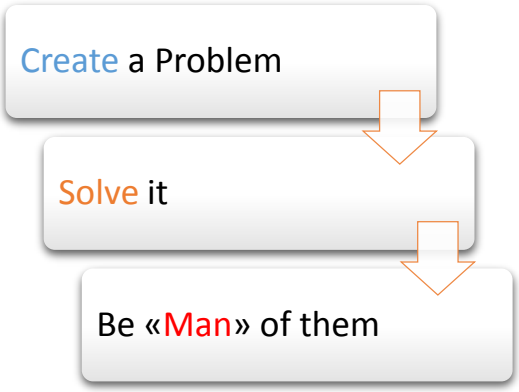

Figure 5 – Easiest way to Manipulate Human

In this way; the attacker does not have to produce a new tactic or technique to get the control of the target system. The attacker just creates a problem by his own and solves the problem already created by himself to exploit the target system. In the end, s/he appears to be a "good, helpful" man for the company. When the right time comes, the attacker will not hesitate to use all his right to gain his/her goals.

1.5.2 Piggyback Rides

With *piggybacking technique*, a social engineer pretends as an authorized employee and walks into a secure building or facility by following someone who has access right to that building. A classic example of this attack is; a social engineer appears at the front door of a secure facility on a rainy day, carrying a heavy box. As an authorized employee walks up, the social engineer takes advantage of human kindness habit by saying, "Could you please open the door for me? I can't reach my badge because of this box." Because people generally want to help others, the authorized employee opens the secured door and grants access to the attacker by his own hands. And Social engineer found himself in the facility without any effort except the heavy box.

Another common example of this is to show up in the employee smoking areas which are usually outside of the organization. The social engineer stands outside smoking with other employees; and when the employees finish smoking, s/he will simply walk right behind them into the building, bypassing any physical security control such as card readers.

The key point here is that; while all these things are happening against the system, there is no system alert, there is no alarm or no sign for an abnormal behavior.

1.5.3 Techie Talk

In this attack type social engineer behaves as a help desk operator trying to find out how secure passwords are being used by the users. They make calls to employees and persuades them to change their password with a "strong" one. The attacker here uses very technical terms that most of the users most probably does not know or have any idea about. After they update their passwords, they simply ask the new password to "check" whether the password is strong enough or not.

After he waits some time to check while saving the password into his database, the user does not suspect anything. Even this makes employees think that the IT personnel is really doing a great job against the security attacks for the company.

1.5.4 Phishing

In this technique, social engineer sends an email to a person who appears to come from a official site, such as PayPal Inc., Ebay Inc., company IT personnel or a banking site, asking someone to visit a website and input sensitive information such as a username and password combination. The website appears to be the official website, but is instead a site created by the attacker with the same looking.

Here is an example from an actual phishing email where the attacker impersonated an employee of PayPal Inc.:

"It has come to our attention that 98 percent of all fraudulent transactions are caused by members using stolen credit cards to purchase or sell non-existent items. Thus, we require our members to add a debit/check card to their billing records as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. Your debit/check card will only be used to identify you. If you could please take 5-10 minutes out of your online experience and renew your records, you will not run into any future problems with the PayPal service. However, failure to confirm your records will result in your account suspension." (Andrew Whitaker, 2009)

This e-mail goes on like providing a link to a fake but exactly same looking website for the e-mail recipient to input the credit card information. PayPal Inc. is mostly chosen site because its being a pool of a credit cards all around the world and most used site while paying anything.

These phishing attacks don't have to include not only directing the user any other website, but also sending some malicious codes or programs. Most common attack type that can be seen under this type is sending ".exe" files and making the users run on their computers.

Figure 6 – Credit Card Phishing

In the figure above, it is clearly seen that the attacker seem to be a well-intentioned man who helps people whether their credit card info has been stolen or not. Here the attacker wrote the "stolen" word in all capitals because he wants to attract the victims' attention. And with asking a question like "Has your credit card number STOLEN on the Internet?" he is trying to make people curious. In addition the attacker designs the window very simple as all people can understand. He also uses "scale" which is used to represent the justice and law. All these symbols and words carefully chosen to make careless people give their credit card number and its expiry date. With this information, the attacker will have a pool of credit card numbers by which he can buy many stuff from amazon.com easily.

This attack may seem so simple but many users are giving their credit card information after seeing this screen on their mailbox. There are some comments after giving their credit cards from users in the figure below.

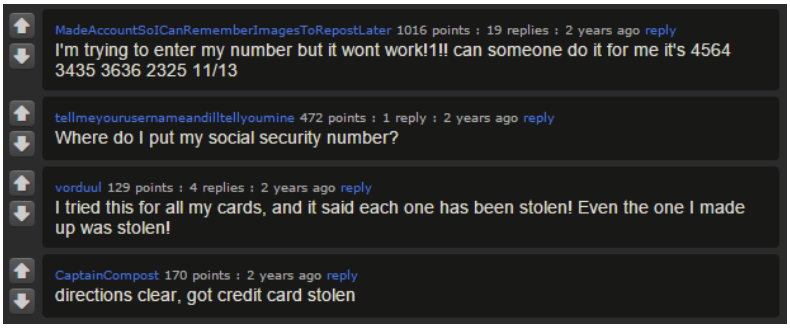

Figure 7 – Credit card Phishing Comments

In the figure above, just 3 of the 135 comments can be seen. As it can be seen from the comments, there have been some people who wanted to give more information to check it like their social security number. These people did not know anything about that "check it" button in fact saves their credit card information into the attacker's database. ("Hmmm has my credit card number been stolen," 2015)

In the research section of this thesis, it can be easily seen we had the similar results from our participants while the research period.

1.5.5 Whaling

In this attack type the social engineers' targets are executives, high-profile targets like administrators. Personal information about these people can be accessed and found already on many social media sites or companies' official websites. For instance, a company may have bios of its executives on their corporate website. This information may be used by a social engineer to the corporate officer as all the info is verified by the company itself already.

If the bio tells chief financial officer graduated from X University and enjoys playing basketball (some executives actually put even their hobbies in their bios), a social engineer may abuse this information. S/he may send an email to that corporate officer as if from the university alumni chapter offering him to come to a special alumni basketball tournament for graduates. The executive will likely think the invitation is real and valid because it would seem authentic. The email may go on to ask the person to access a website to enter credit card information to reserve a good spot in the tournament.

Because of the vast amount of information about corporate officers and other high-profile targets, whaling is becoming increasingly popular. This information makes it so easy for social engineers to target those in a convincing manner with verified information. They can attack to specific targets knowing their interests or dislikes even by using carelessly given information.

1.5.6 Vishing

Vishing is an attack type that uses the phone to perform the equivalent of a phishing attack. In this attack; rather than waiting for the response from the victim, the attacker is able to arrange himself/herself according to reactions s/he takes from the victim.

The social engineer has an initiative about managing the conversation and opportunity to convince the victim. Even the voice tone of the victim on phone will give a clue to social engineer about his/her next steps to reach his/her goal from the target company.

A common example, and highly effective, is performing this with the help of a pre-recorded message. When the phone is answered, the recorded message may say that the call is from the person's bank and that their credit card may be compromised. The "victims" are asked to call a number to resolve the issue. After the user calls the number, they hear another automated message that mentions the victim to enter his or her credit card number, PIN, address, and whatever else the social engineer may want or need.

If a social engineer decides to manage the dialogue by himself/herself, then using office background sounds will make his job easier. So that victims will be more convinced about they are talking to legitimate people from the company or bank whatever.

Another popular variation of a vishing attack is sending a text message to the victim instead of calling the person directly. This may be considered as another type of phishing attacks. Nowadays most of us are familiar with these kinds of messages. In Turkey, because Police Department is one of the highly trusted organizations, social engineers use this department's name to get information they need including money. They impersonate this department's personnel and try to get some critical information or directly what they need to obtain.

Vishing may be used with other attack types to support them. So the victim of the engineer will be more convinced about he should do something about the situation s/he faces. If any time limit is given to the victim, the probability of success increases significantly.

1.5.7 Social Media Networking

Social networking sites such as facebook or twitter are a social engineer's pool of information. A social engineer can discover so many details about their targets from these kinds of sites by clicking on some pages only.

People share information about where they work, what they like to do, which music bands they like, how they feel at the moment, what they dislike or afraid from and more. A social engineer can abuse these posted information against their victims obtained from their own pages. People's being eager to share their private life so openly from their social pages makes social engineers' hands so powerful. People are even sharing where they are at the moment and updating their location in every second. So if a social engineer knows his/her victim is nearby, s/he can put his/her tactics into action against them directly. Out of the victim's territory and work environment, the social engineer will be more comfortable and free while trying his/her chance to get what s/he wants.

This approach may be used in a number of ways:

- Sending email impersonating a friend listed on the victim's page,
- Viewing pictures of a person to discover popular hang-outs and then showing up nearby or just at the same areas,
- Discovering the person's age, school, previous companies, place of birth, and which can all be used to target the person,
- Adding the victim as a friend to build up an online relationship with a person in order to build trust.

The social engineer then will not hesitate to use the information s/he got against the victim which could be used to launch another attack.

1.5.8 NLP

As stated by Hadnagy in 2010, a good social engineer has a strong grasp on how to manipulate or hack the human software. *Neuro-linguistic programming* (NLP) is one of the powerful psychological approaches used by many social engineers to manipulate their victims. When this technique is applied right, it eases to manipulate the target.

NLP deals with a person's neurological processes, language, and learned behavior responses. While NLP was originally designed to be used in therapeutic goals, it is being used by social engineers to manipulate and hack human mind to make their victims (Hadnagy, 2010).

In this technique, the social engineer will seek ways to use his/her body language and a careful selection of words to give subconscious messages to the person s/he is trying to manipulate. S/he begins by matching his/her body language with the victim's body language. S/he also matches his/her breathing rate, voice level, accent, and vocabulary with the victim. Doing so, he tries to build rapport on a subconscious level. S/he may then give other subconscious messages by changing his/her body language, smiling and lightly touching the person on their shoulder or arm, and using words that denote positive thoughts, emotions, and images. All of these tactile, visual, and verbal actions (called *anchoring* and *reframing* in NLP terms) give subconscious messages that influence the person to have positive feelings and gain a sense of rapport with the social engineer. After that point, s/he can then direct to the communication to what s/he is after, such as gathering information about a company's secrets or critical information.

Figure 8 – A pen used in NLP technique

The attackers may use even a shiny, loud sound-making pen to discover which feeling is dominant in the victim's brain. And after the engineer discovers the dominant feeling, s/he then uses proper words according to the victim. For instance if the social engineer discovers the audial part is dominant in victim's brain, his/her offers will be like "It **sounds** great right?" or if visual side discovered dominant, then his supportive expressions be like "It **seems** awesome right?". The social engineer uses the same approach if tactile side is dominant s/he will use "It **feels** safe right?" The social engineer chooses his/her verbs according to the victim.

In short, in this technique the attacker arranges himself/herself according to his/her victim and trying to behave in a way which will suit the victim's personality and behaviors. In this

way the attacker is trying to increase the success level of his/her attacks to gain the targeted goal of hers/his.

1.5.9 Opposite Gender Attraction

Using human attraction is about getting someone interested in the social engineer and giving the victim the impression that his or her feelings are reciprocated. This leaves the person vulnerable to attacks from gathering critical information about the organization to pick-pocketing keys of a building while the victim is not paying attention.

If a social engineer discovers about his/her victim to have vulnerability about being attracted by opposite gender, s/he will use this technique against the target to get what s/he wants with high probability of success.

1.5.10 Friendly Meetings and Talks

If a social engineer wants to learn more about the targeted company or organization, s/he may seek for a moment that s/he can be out with the target person who likes to go to bars or entertainment centers. The social engineer may follow people home from their work to see which ones go to bars after work, or may look people up on social networking sites to see if there are pictures or any other information that may reveal the names of bars or clubs that they often visit. Armed with this information, the social engineer may build up a conversation with the victim at the bar/coffee shop and try to reveal some critical information.

There are many ways a social engineer may take to accomplish this mission. Once the social engineer learns which bar/coffee shop his target person often visits, s/he may arrive early to strike up conversation with the bartender. S/he may bribe the bartender with some cash in exchange for making sure that there always drinks ready for him without any alcohol. This way the social engineer stays sober and can focus on his/her objective while the target person gets drunk.

Later that night, the social engineer may strike up a conversation with the target person, and attempt to get his target person drunk. Once the target is drunk, the social engineer can bring up the topic of work and proceed to get information that the person would otherwise never share such as how to get into a building, passwords, trade secrets, and more.

Another positive effect of being such an environment is social engineer's being more comfortable compared to office environment. The victim will not be his/her workspace where s/he will be more confident and strict to corporate rules.

After giving some clues about the common social engineering attack types, it is time to get into popular social engineering techniques in our time. The following techniques are being used while attack types to get into victims' world.

1.6 SOME POPULAR SOCIAL ENGINEERING TECHNIQUES

It is kind of a brainstorming activity for a social engineer about manipulating people and making others behave as they want. Here in this section, some most widely used techniques will be given.

1.6.1 Lying

We have to be aware that not all people are honest and frank. Most of the people evaluate others depending on their own inner qualities, their own qualifications. So if a person don't have the habit of lying, s/he probably will not expect others to lie either. This is a normal natural behavior of a human.

As mentioned in previous sections, social engineers gain information about their victims and they use the information they obtained against his/her victims. They don't question themselves whether their behavior is in moral limits or not. They are just focused on their goals. This habit leads them to pretext very professionally. After sometime, to manipulate others they may use lying technique that should not be seen as a something weird. (Verizon, 2012)

1.6.2 Saying Partially Truth

Another technique is saying the truth but omitting certain parts of it. This is a good technique for the ones who are not used to lie and cannot keep track of all the lies they have told before. They just specify the certain truths and they don't say anything else about all of the situations and possibilities.

Here the main idea of the attacker is gaining the trust first. After approving they are thinking the in the same way with the victim, they put their actions according to their real malicious intentions. But until that stage, they clearly know that they should make their victims think they are telling the truth.

1.6.3 Giving a Reason

If the attacker gives a rationalization and uses the **magic word** "because" it is much more likely for a victim to behave as wanted from him/her even if the reason is nonsense.

According to a study performed by InfoSec Institute in 2014, following chart was obtained about showing the importance of the word "because".

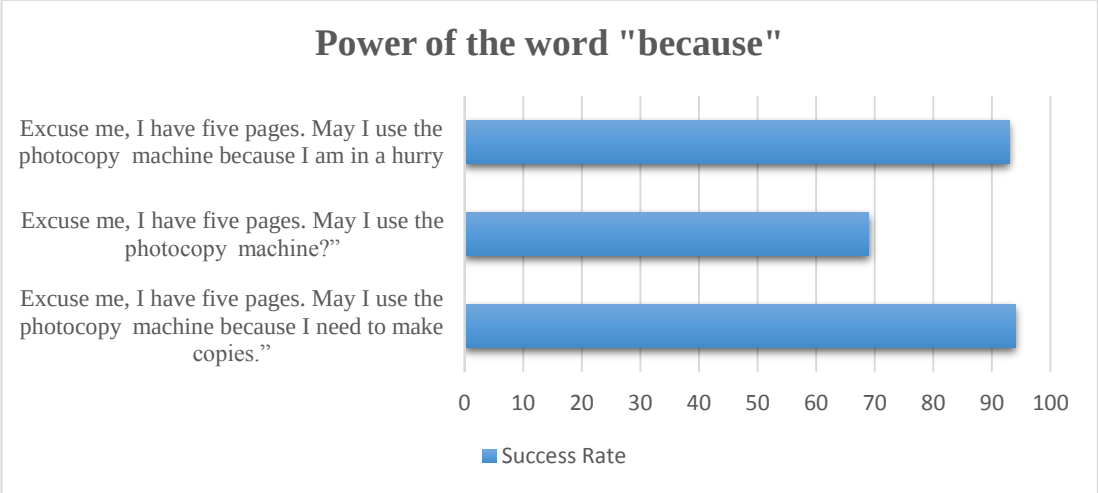

Figure 9 – Success Rate of using just "because" word

Here it will be better to extend the meaning of the magic word "**because**". There has been a study involving rationalization. The experiment takes place in a library and in the line to use the photocopy machine in particular. There are many people in a line to make copies of their papers and a person comes and asks them to cut in line.

In the first group, the person who wants to cut in line asks the others:

- "Excuse me, I have five pages. May I use the photocopy machine *because* I'm in a rush,"

After this offer, 94% of the participants allow him to copy his pages before them.

In a different group the same person asks:

- "Excuse me. I have five pages. May I use the photocopy machine,"

After such an offer without any reason; only 60% allows him to cut in line. They don't agree to allow the new guy make copies and complaining him they are waiting for the same reason just he mentioned.

In the last group, the same person asks again:

- "Excuse me, I have five pages. May I use the photocopy machine because I need to make copies"

After hearing such a weird reason 93% people allows him to cut in line.

This clearly shows that the use of "**because**" is sufficient enough for people to think that as if he has a valid reason to cut in line and they do not even process the reason itself. (Infosec Institute, 2014)

1.6.4 Evasion and Diversion

Evasion and diversion are two common techniques being used by social engineers. In this technique; the attacker evades questions trying to respond either by changing the topic or telling something vague or irrelevant as an answer to divert the attention of the question.

In addition they can pretend innocence, anger, or confusion to trick the victim or try to establish guilt in the target so he can feel the need to exonerate himself from the situation.

1.6.5 Reciprocation

This trick involves giving a gift or doing some kind of favor to the victim to which he will feel obliged to respond. Here the social engineer tries to make an emotional connection between himself and the victim.

This technique has some crucial points while applying in case the victim feels the engineer is bribing him/her. If the victim feels the engineer has a bad intention, then s/he will not be friendly to the engineer normally. S/he waits some time but not too much as well because the sense of reciprocation can expire if the prospective victim stops feeling indebted.

1.6.6 Using Humor

Most of the social engineers have some "instant" jokes prepared in advance to make their victims laugh and make them feel comfortable and happy during the relationship-building phase. As most people enjoy the company of people with a good sense of humor, the likelihood of the successful attack increases when this kind of technique is used.

Another advantage of this technique is, if something goes wrong, the engineer have a chance to convert the problematic situation into a funny case. The attack is more invisible as its being full of humor.

1.6.7 Yes-Yes Technique

It's important for a social engineer to place his/her targets in a positive state of mind. If s/he manages to do this, it will mean a high probable success.

In this technique the victim are being asked too many questions which are most probably answered by "yes". For instance "you want to be successful in this life, right?", "you want to live in better conditions when you are retired, right?" kind of questions are being asked to the victim and waits him to answer with "yes". After many questions, the attacker asks the main question like "so, you want to work with our company, right?" or "as you trust us, you can

let us test your system tomorrow, right?" and normally expects from his victim to say "yes" again.

1.6.8 Throw a Ball Technique

In this attack type, the victim is given many great opportunities and is being forced to dream about what he can have in the future by the attacker. Until making sure of the emotional connection is provided between the victim and the dreams; the attacker waits. The attacker shows up somehow saying because of the circumstances happened, they are not able to do all the stuff he talked about. The attacker exactly knows that after making the victim connected with the stuff, it will be hard to turn back after going that far. So the victim accepts the attacker's new offer.

1.7 THE FOUR MOST IMPORTANT ASPECTS OF HUMAN VULNERABILITIES

Social engineers mostly exploit one or more of four psychological issues reside in human according to SANS Institute (SANS Institute, 2004) as it is shown in the figure below.

Figure 10 – Most Important Aspects of Human Vulnerabilities

1.7.1 Fear

Fear is one of the most exploited human traits of all. This can vary from phishing, vishing, pretexting to other techniques used by many attackers that usually create on the victim an instant sense of act. This trait may be exploited like claiming the victim that his/her

username and password has been hacked, stolen, or there are suspicious activities in his bank account or something similar.

Fear can be thought as putting the victim in a small box and if s/he does not act immediately, they will find themselves in front of the judge soon. There can be scenarios like threatening the victim with losing job or judicial sanctions.

This trait in human being is significantly important for a social engineer indeed. In Chapter 4, the findings section of this thesis, it will be clearly seen how successful abusing this trait can be. Because most of the people are afraid of even hearing about judge or court, they feel themselves to act immediately. After being threatened it will be hard for them to stay calm. Furthermore if the threatening includes the family members of the victim, it means a high probability of success to achieve the goal for the attacker.

1.7.2 Desire to Help

The next most exploited trait is "desire to help" or "being kind towards others". This attack type is mostly applied by two ways: piggybacking or impersonation.

The piggybacking method has already been discussed above. The attacker may dress up as a cleaner. As s/he has lots of stuff to handle and carry, s/he stops the authorized stuff as they are entering the target department and asking them to keep the door open for him/her. In most cases the authorized stuff simply lets him/her go without checking the cleaner for his badge or entry pass. This is all because of desire to help trait in human nature, just like we would have liked it if somebody did the same for us. In addition, there are some scenarios like letting the cleaners inside the building while the users are out of their departments. The main reason of such behavior is to make room for the cleaners to do their job better but any evil-minded people who want to harm the organization may abuse this trait.

It does not have to be cleaning tools and a maintenance guy. The social engineer can be dressed up as a delivery guy even and carry a big, heavy box. He may even utilize name-dropping technique and mention that the delivery is for the boss or some high rank guys in the company. When people hear their boss's name, they simply drop their wings towards the attacker and let the attackers in.

Another way to exploit the desire to help is impersonating an insider. This has already been discussed above as well. The impersonation usually used after some other techniques such as reconnaissance methods or dumpster diving. After getting the needed information for the attack, the social engineer puts his steps into action to reach his/her goals.

1.7.3 Carelessness

The careless trait of human can be exploited too as most of the people often feel indifferent to the security policy rules in their organizations. Dumpster diving; which involves investigating the trash and reunion or puts the waste together again to make it useful information such as thrown out documents with signatures without being shredded; can be a good example of attacks against this trait. (Andrew Whitaker, 2009)

The exploitation of this trait is usually just a step of a more complicated attack. This trait is usually abused as a part of the exploration phase to gather necessary information to make the attack more successful success rate.

Password theft can be seen as another example of this exploit. Many companies often force their employees to change their passwords on a regular basis according to their security policies. While applying this policy, they have strict rules about new password's strength that at least involves some letters, special characters, or numbers. This situation makes employees struggle to remember their updated password after each change. After sometime they can't keep track of their own passwords. Most of the employees unfortunately find a solution to this problem by writing their updated passwords on a piece of paper. They mostly forget to hide the paper too or put the paper to a place where easy to guess and find like under the keyboard. This behavior of most employees makes password theft easy, as the attacker just would have to check only the surroundings of the office computer – such as chair, the desk drawer, under the keyboard etc. Another technique that system users do is installing a program that stores the updated usernames and passwords downloaded from Internet, most probably P2P programs. In this way, they are giving a great, perfect chance for an attacker to have updated usernames and passwords.

1.7.4 Comfort Zone

The next trait that social engineers exploit is about their victims' comfort zone. People feel secure at their workplace as home. This feeling makes them to be less perceptive towards possible threats, scams that may exploit this sense of security. Their guard will be down when an attacker takes advantage of their feeling secure.

A common abuse of this trait is impersonating an insider. The most common impersonation is of the IT staff. The reason of choosing IT staff is people generally do not have much knowledge of how IT systems are maintained or they are ignorant in this area in a way. (Greitzer et al., 2014) When employees see a person wearing a shirt like IT staff, people will most probably assume that s/he is working in IT department. As a result their guard will be down normally. After gaining the trust of victim in this way, s/he can easily ask to do some critical software updates on the victim's computer. Out of the victim's knowledge the attacker may give herself/himself remote access right.

Another scenario can be like the attacker asking the employees for their password to check if they use high level secure password, which sounds totally normal. There have been some occasions even after such an attack; the employees thank the attacker for his being nice and helpful for his/her security.

Shoulder surfing is another method used by many social engineers by which they can abuse others' comfort zone. Actually this technique involves both the exploitation of comfort zone and his carelessness at the same time. People mostly do not check their backs. They don't consider someone would stand behind and watch them while they are typing on the keyboard their username and passwords when concentrated on duties. Feeling secure because of their comfort zone at workplace can also be seen as some of the reasons that can be exploited here.

Another attack type that social engineers can do is stealing a laptop, external hard drive, USB, badge, wallet, purse, smartphone, or other work-related machines such as gadgets and entry passes. Most of the social engineers mostly choose Friday to steal this kind of stuff because that will give some more time for the social engineer to be discovered. The main reason of such behavior is the possibility of the victim's notice will be on Monday morning and weekend's approach.

Physical security is another comfort zone threat. For instance, in smoking areas, people often leave the gate open so they can go out for a smoke without having to swipe their card again and again. Employees are going out for just couple of minutes but that definitely leaves a window or doors for penetration.

1.8 QUALITIFICATIONS OF A SOCIAL ENGINEER

In order to manipulate the victim successfully and get the goal of attacks, the social engineer has to have the ability to hide his malicious intentions. They also have to know the weaknesses of the targets in order to play his game wisely on the victim. In the end, he will be able to decide which the technique he is going to carry out on the target. He also must be cruel enough not to have any hesitation on harming the victim in the stage of relationship-development. Their friendship is just until they get their goal in their hands. After that point s/he does not care about the anything else.

A social engineer prefers to arrange the sincerity level of their relationships with his/her environment. They never shuts a door so hard because they are aware of one day they may have to come back to that door. Behaving in this way, s/he will have a right to ask for any information or help when they need. They like buying gifts, they know how to steal people's hearts. They are so kind to others indeed to kill the suspicious feelings people may feel. They attack when they gain the full trust and that is their most cruel side. They know that big secrets are hidden under the small details; so they pay great attention to this issue. S/He behaves very serious while working but s/he also makes jokes to cheer up himself/herself and others. They never avoid to make use of his great effort for others just to exploit them one day when needed. One can say "communication expert" for them for sure. They mostly have a personality like greeting people, acting calm and friendly and walking through the

building as if you know exactly where you are going without looking around all the time at windows, doors or hallways (Hadnagy, 2010).

CHAPTER 2

2 LITERATURE REVIEW

2.1 SOCIAL ENGINEERING AND CYBER SECURITY

Social Engineering (SE) defined as "any act that influences a person to take an action that may or may not be in their best interest." (social-engineer.org, 2015)

Since Social Engineering (SE) comprises simple but at the same time complex techniques, there has been lots of examples of its usage in history. These tactic and techniques are not always negative indeed. It merits a closer look at how it is used in different scenarios. After seeing things behind the scene, it can be easy to notice that many social engineers to part their targets from data, money, information and more are often using the similar techniques.

Social engineering is a non-technical method of intrusion hackers' use that relies heavily on human interaction. It is one of the greatest threats that organizations face today because this issue often involves tricking people into breaking normal security procedures.

Since SE attacks are being applied to many organizations in our time, there have been held many researches about this attack type. After getting deeper into many documents, reports, journals or experiences, the following items are involved mostly all of the attacks somehow directly or indirectly.

Social Engineering mostly benefits from the following:

- Influence,
- Misdirection,
- Profiling,
- Information gathering,
- Psychology,
- Manipulation,
- Elicitation,
- Science,
- Communications Modeling,
- Body language,
- Facial Expressions,
- Pretexting,
- Emotional Hijacking,
- Rapport,
- Art,
- Sociology.

One can understand from the list above that Social Engineering has always been interacted with many fields. This picture does not mean that social engineering is a science or an art. Here I want to emphasize that social engineering benefits from these science fields or techniques. Even; there are many examples of usage of these tactics by most of the countries to train their agents, spies in order to win the battle without much effort. There are many examples of this situation in history that without any bullet, some countries conquer the other using well-trained spies.

As we live in the information era, even the wars have been being held in intangible, abstract and cyber fields. And this has been very popular nowadays as this attack type does not require not only trained troops, life risks or ammunition but also it is possible to hide yourself easily from your enemy. All these reasons make cyber wars very attractive for many countries today.

As in many cyber defense conferences mentioned; attacks may be in both technical and non-technical fields. Social Engineering is placed in the "non-technical" part of this classification and described as a "weapon type" in warfare literature.

Security expert Andrew Whitaker explains both the technical and non-technical techniques used by social engineers today to gain trust and manipulate people for their benefit.

2.2 SE: TO WHOM AND FOR WHAT?

Social engineering attack types these techniques are simply targeted to the victim directly or to people who are close to the victim. Social Engineers mostly choose:

a. Victim himself/herself
b. Family
c. Friends
d. Social Environment
e. Boss
f. Spouse to reach their goals (Kvedar et al., 2010).

Social engineers know that when the right attack is applied to right people, probability of success level their attacks will be higher. When it comes to why they perform these attacks, there are many reasons and motivation behind and can be classified as shown below.

a. Personal Satisfaction
b. Making Money
c. Civilian Harm
d. Breaching Companies
e. Stealing Data
f. Cyber Crimes

g. Cyber Warfare
h. Research

For a social engineer, deciding on which technique will be applied to which people is very critical question. S/he has to make detailed investigation about their victims in every aspect. After getting the information needed, according to the goal, it will be the time to put the investigations into action. According to the feedback of the attacks, it is very clear that the attacker will update his/her path for better results.

2.3 PERSONALITY TRAITS OF TURKISH SOCIETY

Many studies have been done to reveal the adjectives of Turkish personality traits and to define people in the Turkey.

According to a research in this field studied by Tülin Gençöz and Öznur Öncül in 2012, following results are obtained about Turkish people traits.

	I	II	III	IV	V	VI
I. Extraversion						
Timid (Çekingen)	**.81**	−.01	.01	.09	−.24	.16
Withdrawn (İçine kapanık)	**.79**	−.02	−.05	.11	−.15	.16
Shy (Utangaç)	**.70**	.08	.10	.07	−.26	.12
Talkative (Konuşkan)	**−.70**	.10	.31	.13	.13	.14
Lethargic (Durgun)	**.66**	−.15	−.06	.05	−.13	.02
Enterprising (Girişken)	**−.65**	.22	.29	−.02	.31	.10
Cold (Soğuk)	**.64**	−.08	−.35	.11	.14	.08
Passive (Pasif)	**.63**	−.24	−.19	.08	−.16	.19
II. Conscientiousness						
Self-disciplined (Disiplinli)	−.05	**.77**	−.01	−.01	.15	−.01
Tidy (Düzenli)	−.01	**.73**	.10	−.06	−.03	−.06
Hard-working (Çalışkan)	−.11	**.69**	.10	−.08	.19	−.07
Prudent (Tedbirli)	.05	**.69**	.16	−.06	.09	.03
Fussy (Titiz)	.00	**.69**	.17	.00	.00	−.05
Determined (Azimli)	−.17	**.65**	.14	−.05	.30	.05
Irresponsible (Sorumsuz)	.22	**−.61**	−.03	.11	.06	.38
Lazy (Üşengeç)	.30	**−.49**	.01	.31	−.02	.07
III. Agreeableness						
Sincere (İçten)	−.09	.06	**.68**	−.06	.22	−.32
Compassionate (Sevecen)	−.27	.09	**.67**	−.03	.11	.04
Genial (Canayakın)	−.39	.10	**.66**	.05	.17	−.03
Well intentioned (İyi niyetli)	.08	.10	**.65**	−.10	.18	−.33
Philanthropic (Yardımsever)	−.01	.05	**.63**	−.08	.10	−.21
Tolerant (Hoşgörülü)	.01	.08	**.60**	−.20	.13	−.09
Sharer (Paylaşımcı)	−.21	.10	**.57**	−.09	−.00	−.21
Sensitive (Duyarlı)	−.05	.29	**.53**	−.08	.01	−.16
IV. Neuroticism						
Nervous (Sinirli)	.09	−.03	−.15	**.84**	.01	−.01
Aggressive (Agresif)	.10	−.09	−.23	**.78**	.07	.01
Angry (Kızgın)	.11	−.05	−.22	**.76**	−.06	.06
Temperamental (Huysuz)	.12	−.15	−.23	**.63**	.05	.06
Impatient (Sabırsız)	−.11	−.15	.06	**.60**	−.11	.13
Capricious (Kaprisli)	.04	−.04	−.08	**.59**	.01	.24
Impetuous (Aceleci)	−.22	.01	.11	**.52**	−.08	.10
Touchy (Alıngan)	.29	.09	.14	**.46**	−.28	.17
Worried (Kaygılı)	.26	−.08	.05	**.44**	−.40	.10
V. Openness to Experience						
Self-confident (Kendinden emin)	−.27	.21	.11	−.11	**.70**	−.13
Self-assured (Kendine güvenen)	−.38	.22	.05	.00	**.68**	−.08
Brave (Cesur)	−.31	−.01	.11	.09	**.66**	−.06
Creative (Yaratıcı)	−.07	.17	.24	−.06	**.63**	.08
Capable (Kabiliyetli)	.02	.21	.31	−.04	**.63**	−.03
VI. Negative Valence						
Ill-mannered (Görgüsüz)	.12	−.11	−.20	.03	−.10	**.66**
Pretentious (Yapmacık)	.06	−.09	−.16	.05	−.17	**.64**
Rude (Terbiyesiz)	.03	−.23	−.19	.14	.06	**.64**
Backstabbing (İçten pazarlıklı)	.08	.04	−.25	.05	.05	**.63**
Greedy (Aç gözlü)	−.01	.01	−.10	.22	−.03	**.59**
Hidebound (Sabit fikirli)	.15	.06	−.01	.32	.02	**.40**
Eigenvalue	5.13	4.21	4.17	4.13	3.38	2.95
Explained Variance (%)	11.39	9.36	9.26	9.17	7.52	6.55

Notes. (1) I: Extraversion, II: Conscientiousness, III: Agreeableness, IV: Neuroticism, V: Openness to Experience, VI: Negative Valence.
(2) In parenthesis, original Turkish items are provided.
(3) The factor loadings printed in bold represent the factors on which the items are accepted.

Figure 11 – Basic Personality Traits Inventory Items – Turkey Example

These findings revealed 45 person-descriptive adjectives that accounted for the well-known five basic personality dimensions (i.e., Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experience) and the 6th dimension, which was named Negative Valence, in accordance with the relevant suggestions in the literature (Durrett & Trull, 2005).

According to the results; for the Turkish society, general preference and politeness is an expression of positive qualities by others, while awareness about and expression of negative qualities by oneself is very important (Gençöz & Öncül, 2012). Thus, people in Turkey do not often welcome expressions of personal pride; rather, they reinforce group pride or positive appraisals from others. Positive qualities should be appreciated by others according to them, whereas people should decently accept and be able to express their failures and shortcomings when necessary.

As the figure above clearly shows, most of the Turkish society is:

- Timid, withdrawn and talk-active under Extraversion dimension;
- Self-disciplined, tidy and hard-working under Conscientiousness dimension;
- Sincere, compassionate, genial, well intentioned, philanthropic, tolerant and sharer under agreeableness dimension;
- Nervous, aggressive, angry, temperamental and impatient under neuroticism dimension;
- Self-confident, self-assured, brave, creative, capable under openness to experience dimension,
- And also sometimes ill-mannered, Pretentious, Rude, Backstabbing, Greedy and Hidebound under Negative Valence.

2.4 TRUSTED ORGANIZATIONS IN TURKEY

For social engineers, winning the trust of their victims is the key point. Their all attacks will be put in action after getting the trust of theirs. As trust issue is being this much important; it will not be so surprising for a social engineer to use already trusted organizations' names while their attacks.

A phishing attack just like sending from a Military department or vishing attack using the Police Department's name will clearly increase the success of the attempts of the social engineer as we already all witness nowadays.

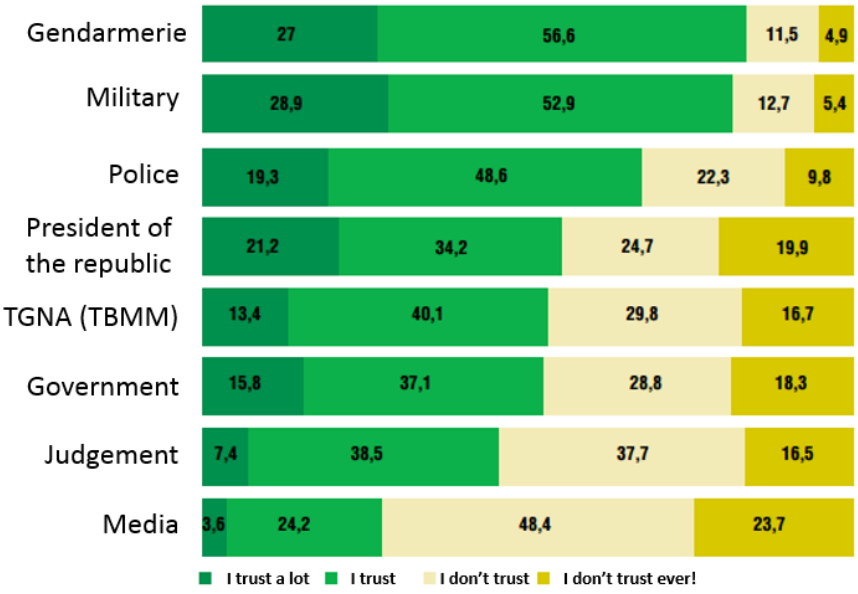

Figure 12 – Organizations Turkish people trust

When looked at the Global Turkey questionnaire held in 2015; it is clearly seen that Gendarmerie and the Military are the most trusted organizations. (Global Politika ve Strateji, 2015)

Here the most surprising result is, it is too low percentage about trusting the judgement in Turkey. I believe that this is the reason when threatened to sue in judgement; our participants feel themselves to act against immediately because they don't trust the judgement. This shows there is a serious gap between justice and the participants. This is actually makes people to choose other ways to get their fair shake rather than via using courts or judgement. Another surprising result is about media. In the questionnaire, although it is shown that media is the last organ people trust in Turkey according to the report.

2.5 CURRENT RESEARCH TO ASSESS THE END-USER AWARENESS LEVEL

There are many companies or organizations that are founded for the purpose of evaluating the security level of other companies or organizations. These companies apply some tests to evaluate the technical security level of the company. But when it comes to measuring the security level against non-technical attack types, these tests does not meet the need. Because it is intangible, it always has been a hard job for organizations to assess their awareness level against social engineering types of attack. Most of these companies are still applying just

phishing or vishing techniques to their system users in order to identify the awareness level of their workers.

There are some researches done about presenting an assessment of user awareness level in many companies. Phishing is the most popular technique among all social engineering attack types that are mostly in form of email phishing attacks.

The important point here is that, phishing and vishing techniques are insufficient to evaluate the awareness level of the company. There are some other researches done by filling out some forms or questionnaires. Phishing or vishing may give a general idea about awareness level but forms or questionnaires does not clearly reflect the real picture as the users will already know which choice or answer is the right one in terms of the security policies.

Like most of the research emphasize, social engineering attack types got popular in our time as it is shown in the figure below. (Sapuan et al., 2012)

Threat Initiator	Motivation	Attack Action	Method
Hacktivism (hacker, cracker, Phreaker, script kiddies)	• Ego, fame • Destruction of system or information	• DoS / DDoS • System intrusion • Website defacement • DNS attack	• Hacking • **Social engineering**
Computer Criminal	• Theft of data • Monetary gain • Privacy compromise • Illegal information disclosure • Unauthorized data alteration	• Cyber stalking • Fraudulent act (man-in-the-middle, spoofing)	• Hacking • **Social engineering**
Insider (disgruntled, poorly trained, dishonest, malicious, negligent, former employee)	• Revenge • Monetary gain • Intelligence	• Unauthorized access • Computer abuse • Fraud • Theft of proprietary information (both logical and physical) • Bribery • System sabotage	• Malicious code (logic bomb, Trojan, malcode inserted as part of the software development process) • **Social engineering**
Industrial Espionage	• Competitive advantage	• Unauthorized access • Information theft • System Penetration	• Hacking • **Social engineering**

Figure 13 – Summary of security Threats and Attack Methods

As it is clearly seen in the figure, social engineering methods are being used under the umbrella of many attack types and threats. This table also proves that knowing the awareness level of a company against these kinds of attacks is very crucial information for administrators.

Another research done in University of Plymouth as about sending their participants some emails and asking them whether the emails seem legitimate or not. The result of the research is shown below. (Karakasiliotis, Furnell, & Papadaki, 2006)

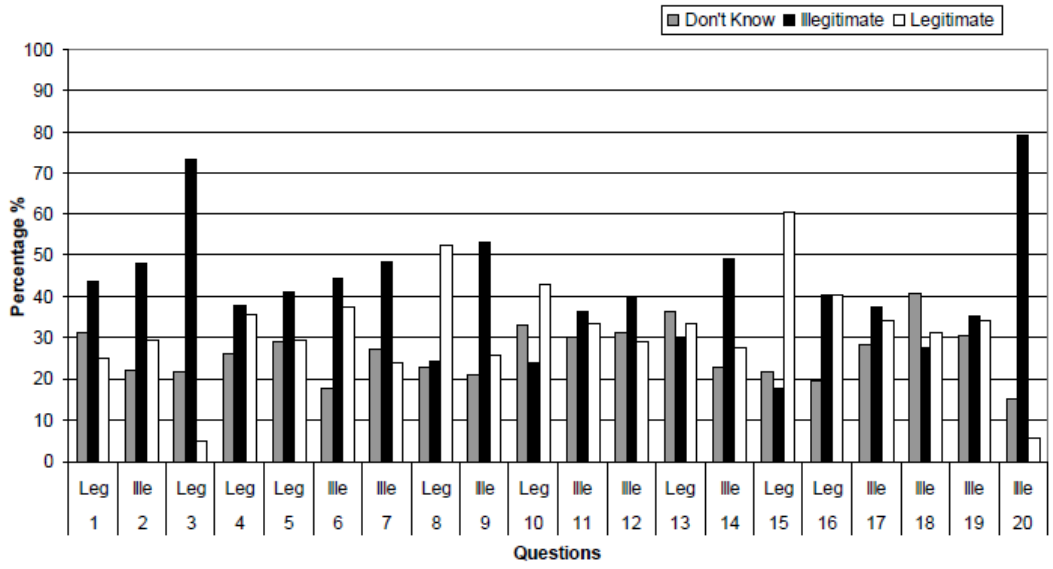

Figure 14 – A Research Result About Evaluating The End-User Awareness Level

In this figure, it is shown 20 mail types; some of which are legitimate, some are not. Vertical lines indicate what participants' decisions. One immediate observation is that, in most cases, opinions were very much divided. Furthermore, in some cases the majority view was dramatically wrong. This clearly shows that many users typically face a hard task to differentiate between a genuine email and a bogus one based upon the message content alone (Karakasiliotis et al., 2006).

Another research done by Symantec in December 2009 was done to see the State of Phishing around the world. According to the report, the following chart is obtained (Hasan et al., 2010).

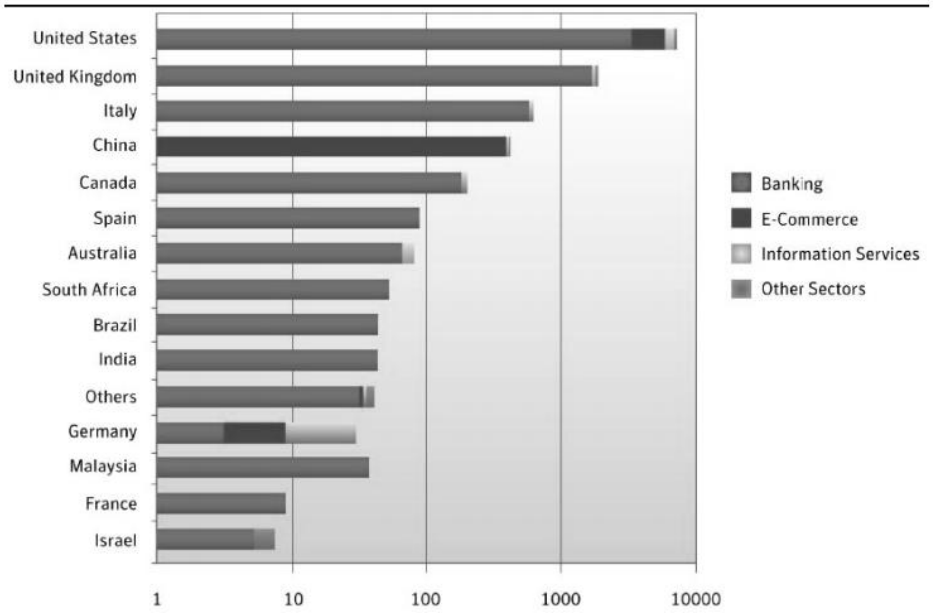

Figure 15 – State of Phishing: Monthly Report: December 2009 by Symantec

In this figure, which subjects are dominant for which country is tried to be figured out. For instance it is clearly seen that China has a great vulnerability towards e-commerce types of emails or Germany has more vulnerability in information services compared to others. According to this report, one can easily say that nearly all of countries listed in the figure have high-level vulnerabilities in banking sector.

One of the most common technique under social engineering umbrella is vishing and following graphic shows the success level of this technique (Mataracioglu & Ozkan, 2011).

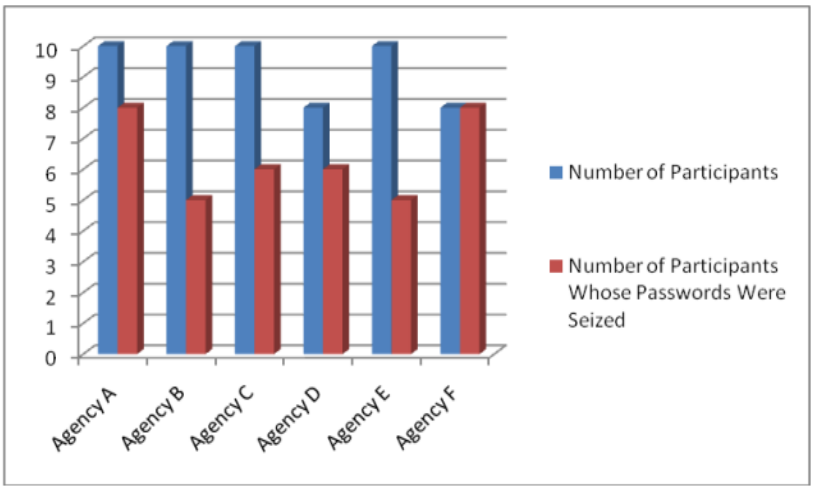

Figure 16 – Results of vishing attacks against some companies in Turkey

As it is clearly seen from the picture above, the research, which was done by vishing technique, had great success to obtain participants' passwords. The aim of the research was to figure that the employees in many public agencies have a lack of information security awareness and they compromise the information security principles which should be necessarily applied for any public agencies (Mataracioglu & Ozkan, 2011).

CHAPTER 3

3 RESEARCH DESIGN

3.1 RESEARCH METHOD

In this research, in order to evaluate the awareness level of participants against social engineering attack types, rather than applying just phishing or vishing technique, my research team and I added some more techniques against the participants like baiting and contacting personally too. Our goal was here to put the users into the real scenario without their information of their being tested at that moment and measure their real responses against social engineering types of attacks.

To figure out the success level of social engineering tactic and techniques about breaching into systems, we've done this research for 10 months in Turkey in 2014 with my 4 colleagues; one of us was female. We planned to have a female member in our team because we wanted to evaluate the opposite gender attraction effect on towards our participants too.

Participants

Age	Participants
18-25	1321
26-35	1151
36-60	1522
	3994

Table 2 – Age of the Participants

Many various tactics and different approach methods were applied on people from different education levels and different age ranges. Participants were divided into three in terms of their ages according to their roles in their companies like newbies; ones have active roles and the ones with managerial positions.

After the attacks applied none of gained information is stored somewhere and no data recorded. The results classified as "successful" or "unsuccessful" manner. The reason of this classification is just to see whether the attacker was able to breach the system or not. The results were surprising indeed with its high percentage of success when the right techniques were applied to right people.

Education Levels

Education Level	Participants
Under graduate	1343
Graduate - Post Graduate- PhD	2651
	3994

Table 3 – Education levels of the Participants

In this research, 3994 attack attempts were applied towards the participants from different education levels, ages and genders. The participants consist of from different regions of Turkey in order to represent the homogeneous distribution and the most of the society.

3.2 METHODS USED IN THE STUDY

There were lots of ways to manage to get some valuable information from people who are working in organizations or universities of course but we chose the ways that we could apply more easily and get the result. The techniques we chose are seen in the figure below.

Figure 17 – Techniques used in this study

These techniques were applied to participants in different approaches as shown in the figure below according to the participants' likes, dislikes, hobbies, or personalities.

Approaches Used				
Approach	**Phishing**	**Vishing**	**Baiting**	**Contacting**

Fear/Threaten	1	1	0	0
Fake ID	0	0	0	1
Job Offer	1	1	0	1
Promotion/money	1	1	0	0
Sports	1	0	0	0
Vacation	1	0	0	0
Prize/Gift	1	1	0	0
Free Program	1	0	1	0
Foreign Language	1	1	1	1
Comparing	0	1	0	1
System Check	1	1	0	1
Curiosity	1	0	1	0
Emotional Blackmail	0	0	0	1
Total	**10**	**7**	**3**	**6**

Table 4 – Used Approaches in Research

Normally to reveal the real picture of the awareness level of our participants, we did not use every approach with every technique. In the table above, the yellow (light) cells show the intersection of the column (used approach method) and rows (used technique) were applied together against the targets; and the red (dark) cells represent the opposite. According to this table, following results will be obtained. For instance in approach-technique correlation chart, sports and baiting will be shown as empty because that would be nonsense to invite people to their favorite team's match with a USB or CD/DVD. So in following charts, the empty cells does not mean it is successful or unsuccessful.

In this research, four main techniques are used which are phishing, vishing, baiting and contacting personally. Other techniques were also used accordingly with these main techniques. In order to discover the weakest point of our participants, we chose the approach methods shown below.

- Designing a fake ID and trying to getting access to critical areas,
- Threatening to sue while talking face to face or vishing about their computer is sending out some malicious code,
- Blaming the user as they had done something intentionally,
- Tailgating with a car saying "we are together with the one that has just passed",
- Doing emotional blackmail with a little child saying, "we are in a hurry and my kid is really hungry now. Could you please help me about just sending a document which is in this USB?"
- Comparing with other security personnel or lying about previous entrances,
- Emotional blackmail and hijacking,
- Offering a job or a new position,
- Pretending to be an IT personnel and checking the system,

- Phishing and sending malicious code,
- Offering promotion,
- Using opposite gender on vishing attacks,
- Teaching foreign language very fast,
- Free education or training,
- Arousing curiosity and interest with some labels like “TOP SECRET”,
- Offering higher salary, money or bribe,
- Filling out a form which has some parts about personal information,
- Installing a free program like “SalaryCalculator.exe”,
- Offering free vacation,
- Offering free gifts,
- Sending news, gifts, invitations related to victim’s favorite sport team,
- Exploiting the religion according to victim’s personality,
- Exploiting politics or pretending to support the same political approach,
- Shoulder surfing,
- Dumpster diving.

In this research, one or more techniques, subjects, and approach methods were chosen according to victim’s personality in order to increase the chance of our success just like a social engineer do. All these techniques; because pretexting is always a must, held on mostly on phishing, vishing, baiting and meeting techniques. Some pretexting stories were made up according to peoples’ interest in time manner. For instance getting information about most of the company workers were complaining about high rate taxes in the company, so we built up a story about “solving” the tax problem and send an email about the subject.

In order to get realistic results from this research, the participants were chosen in a way that it could represent the society all. So students from a high quality popular university that represents high-medium level educated people and staff working for some government organizations from all over the country with high, medium, and low level education were chosen as participants. With this approach, it was possible to represent the majority of the society with homogeneous distribution. Besides in this way the study was not limited with not only from high level educated staff but also low and normal standard level educated people from different ages.

3.3 PARTICIPANTS’ QUALIFICATION AND CLASSIFICATION

Some details about the participants are given below in charts.

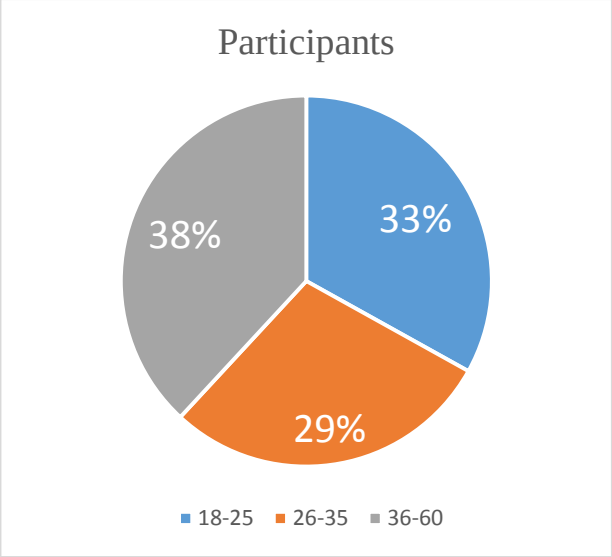

Figure 18 – Age Distribution of Participants

In Turkey, the average graduation age from a university is 22. After graduating from universities, many students getting employed in private sector or government. These people are working as "freshman" in their companies. For the worst case it takes 4 years to learn the job in details. After getting talent in their fields, people gets some more critical positions and active roles in their companies or ministries. Approximately after age 35, people gets to know much more in their fields and starts to give "decisions" for their working places and taking managerial or administrative positions in their organizations. After age 35 the needs are changing dramatically. Rather than being aware of their companies or ministries, people start to plan for themselves and concentrate on more detailed future plans. With this approach, normally, the decisions, interests and approaches change too.

Most of the participants were selected from mostly 26-35 age range because this age range people has more active roles in many government organizations and companies. The tests were also applied to 18-25 age range to see the vulnerabilities of newly graduated students or newbies of the companies and ministries.

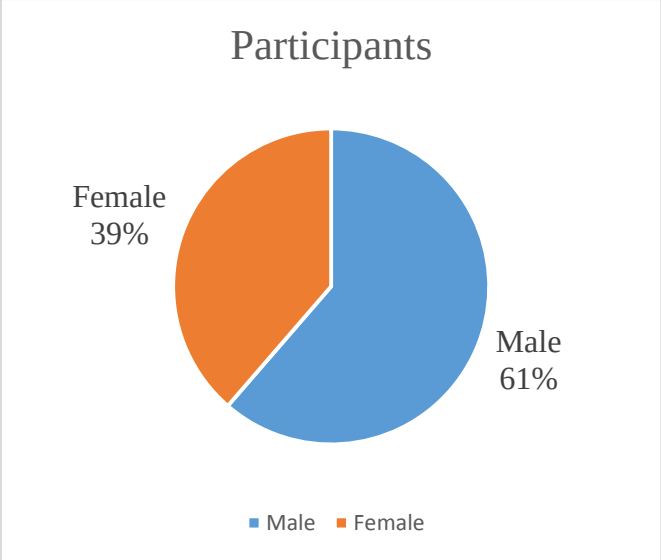

Figure 19 – Gender Distribution in Participants

The participants consist of mostly male people. The social engineering techniques were applied according to the genders too. For instance while the approaches about shopping or vacation were mostly applied to women considering that they are more into these issues. Approaches about sports and new positions were mostly applied to men in order to see the how we can abuse the vulnerabilities according to gender of the group.

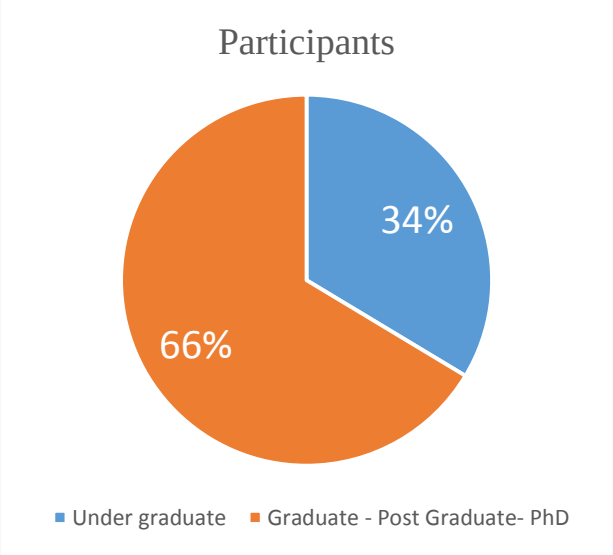

Figure 20 – Education level distribution in participants

This study applied to people who have different education levels too. In order to make the study reflect more realistic results, the group was divided into undergraduate and graduate. The reason not to split the group into more sections is there is no so much difference between for instance a post-graduated man and a man with PhD. Because social engineers are interested into the personalities, the divisions were chosen to represent the society best.

CHAPTER 4

4 FINDINGS

In this chapter, the results of our research will be shared in detailed manner. First the results of the attempts for each technique and approach will be given, and then these results will be analyzed in details with using statistical techniques.

4.1 Phishing Test Results

Following table shows the results of success level in phishing attack type, including the participants' qualifications and education levels.

Phishing

Participants			Results		
Age	**Education**	**Subject**	**# mails**	**Succ.**	**UnSucc.**
18-25	UnderGraduate	Promotion/money	200	152	48
18-25	UnderGraduate	Prize/Gift	80	13	67
18-25	UnderGraduate	Job Offer	220	51	169
18-25	UnderGraduate	Promotion/money	15	9	6
18-25	UnderGraduate	Job Offer	10	2	8
18-25	UnderGraduate	Free Program	250	140	110
18-25	UnderGraduate	Fear/Threaten	96	85	11
18-25	UnderGraduate	Vacation	55	3	52
18-25	UnderGraduate	Prize/Gift	25	8	17
18-25	UnderGraduate	Promotion/money	70	42	28
18-25	UnderGraduate	Sports	25	2	23
18-25	UnderGraduate	Foreign Language	30	19	11
18-25	UnderGraduate	System Check	40	33	7
18-25	UnderGraduate	Curiosity	15	8	7
26-35	Graduate - Post Graduate- PhD	Promotion/money	150	89	61
26-35	Graduate - Post Graduate- PhD	Promotion/money	15	9	6
26-35	Graduate - Post Graduate- PhD	Free Program	150	15	135

Participants			Results		
Age	**Education**	**Subject**	**# mails**	**Succ.**	**UnSucc.**
26-35	Graduate - Post Graduate- PhD	Free Program	160	12	148
26-35	Graduate - Post Graduate- PhD	Fear/Threaten	84	71	13
26-35	Graduate - Post Graduate- PhD	Fear/Threaten	75	67	8
26-35	Graduate - Post Graduate- PhD	Vacation	55	2	53
26-35	Graduate - Post Graduate- PhD	Prize/Gift	25	3	22
26-35	Graduate - Post Graduate- PhD	Promotion/money	25	14	11
26-35	Graduate - Post Graduate- PhD	Sports	25	1	24
26-35	Graduate - Post Graduate- PhD	Job Offer	30	13	17
26-35	Graduate - Post Graduate- PhD	Foreign Language	30	11	19
26-35	Graduate - Post Graduate- PhD	System Check	40	28	12
26-35	Graduate - Post Graduate- PhD	Curiosity	15	8	7
36-60	Graduate - Post Graduate- PhD	Promotion/money	155	102	53
36-60	Graduate - Post Graduate- PhD	Free Program	473	240	233
36-60	Graduate - Post Graduate- PhD	Free Program	400	239	161
36-60	Graduate - Post Graduate- PhD	Fear/Threaten	75	72	3
36-60	Graduate - Post Graduate- PhD	Job Offer	30	8	22
36-60	Graduate - Post Graduate- PhD	Sports	20	1	19
36-60	Graduate - Post Graduate- PhD	Vacation	20	2	18
36-60	Graduate - Post Graduate- PhD	Prize/Gift	40	14	26
36-60	Graduate - Post Graduate- PhD	Foreign Language	30	12	18
36-60	Graduate - Post Graduate- PhD	System Check	40	27	13
36-60	Graduate - Post Graduate- PhD	Curiosity	15	8	7
			3308	**1635**	**1673**

Table 5 – Phishing Attack Test Results

In this table; it is clearly seen from 3308 phishing attack attempts towards different education level and aged people, while 1635 attempts were successful, 1673 attempts were ignored by the participants. These results' classification and observations will be given in Chapter 5, Conclusions section.

4.2 Vishing Test Results

Following table shows the results of success level in vishing attack type, including the participants' qualifications and education levels.

Vishing

Participants			Results		
Age	**Education**	**Subject**	**call #**	**Succ.**	**Unsucc.**
18-25	UnderGraduate	System Check	16	12	4
18-25	UnderGraduate	Job Offer	10	6	4
18-25	UnderGraduate	Promotion/money	7	6	1
18-25	UnderGraduate	Fear/Threaten	18	16	2
18-25	UnderGraduate	Prize/Gift	12	8	4
18-25	UnderGraduate	Foreign Language	16	11	5
18-25	UnderGraduate	Comparing	16	12	4
26-35	Graduate - Post Graduate- PhD	System Check	13	9	4
26-35	Graduate - Post Graduate- PhD	System Check	17	11	6
26-35	Graduate - Post Graduate- PhD	Fear/Threaten	23	20	3
26-35	Graduate - Post Graduate- PhD	Job Offer	15	3	12
26-35	Graduate - Post Graduate- PhD	Promotion/money	9	8	1
26-35	Graduate - Post Graduate- PhD	Prize/Gift	11	4	7
26-35	Graduate - Post Graduate- PhD	Foreign Language	15	8	7
26-35	Graduate - Post Graduate- PhD	Comparing	15	11	4
36-60	Graduate - Post Graduate- PhD	System Check	20	16	4
36-60	Graduate - Post Graduate- PhD	Job Offer	13	7	6
36-60	Graduate - Post Graduate- PhD	Promotion/money	13	11	2
36-60	Graduate - Post Graduate- PhD	Prize/Gift	7	3	4
36-60	Graduate - Post Graduate- PhD	Fear/Threaten	20	18	2
36-60	Graduate - Post Graduate- PhD	Foreign Language	16	9	7
36-60	Graduate - Post Graduate- PhD	Comparing	16	11	5
			318	**220**	**98**

Table 6 – Vishing Attack Test Results

In this table; it is clearly seen from 318 vishing attack attempts towards different education level and aged people, while 220 attempts were successful, 98 were unsuccessful. Although we force those 98 people they did not allow us to get the data we were seeking for. These results' classification and observations will be given in Chapter 5, Conclusions section.

4.3 Baiting Test Results

Following table shows the results of success level in baiting attack type, including the participants' qualifications and education levels.

Baiting

Participants			Results		
Age	**Education**	**Subject**	**# of people**	**Succ.**	**Unsucc.**
18-25	UnderGraduate	Curiosity	8	4	4
18-25	UnderGraduate	Free Program	10	6	4
18-25	UnderGraduate	Foreign Language	12	7	5
26-35	Graduate - Post Graduate- PhD	Curiosity	11	7	4
26-35	Graduate - Post Graduate- PhD	Free Program	15	9	6
26-35	Graduate - Post Graduate- PhD	Foreign Language	13	6	7
36-60	Graduate - Post Graduate- PhD	Curiosity	8	2	6
36-60	Graduate - Post Graduate- PhD	Free Program	15	8	7
36-60	Graduate - Post Graduate- PhD	Foreign Language	12	5	7
			104	**54**	**50**

Table 7 – Baiting Attack Test Results

In this table; it is clearly seen from 104 baiting attack attempts towards different education level and aged people, while 54 attempts were successful, 50 were unsuccessful. While doing these attacks, we mostly chose the places where people mostly visit or we left the stuff on their desks. These results' classification and observations will be given in Chapter 5, Conclusions section.

4.4 Contacting Test Results

Following table shows the results of success level in contacting personally attack type, including the participants' qualifications and education levels.

Contacting

Participants			Results		
Age	**Education**	**Subject**	**# of people**	**Succ.**	**Unsucc.**
18-25	UnderGraduate	Fake ID	20	18	2
18-25	UnderGraduate	Job Offer	16	12	4
18-25	UnderGraduate	Foreign Language	13	12	1
18-25	UnderGraduate	System Check	16	15	1
26-35	Graduate - Post Graduate- PhD	Fake ID	6	5	1
26-35	Graduate - Post Graduate- PhD	Job Offer	15	12	3
26-35	Graduate - Post Graduate- PhD	Foreign Language	14	10	4
26-35	Graduate - Post Graduate- PhD	Comparing	12	9	3
26-35	Graduate - Post Graduate- PhD	System Check	23	22	1
26-35	Graduate - Post Graduate- PhD	Emotional Blackmail	23	16	7
26-35	UnderGraduate	Fake ID	7	6	1
26-35	UnderGraduate	Comparing	7	5	2
26-35	UnderGraduate	Emotional Blackmail	8	7	1
36-60	Graduate - Post Graduate- PhD	Fake ID	5	4	1
36-60	Graduate - Post Graduate- PhD	Job Offer	14	13	1
36-60	Graduate - Post Graduate- PhD	Foreign Language	11	10	1
36-60	Graduate - Post Graduate- PhD	Comparing	14	13	1
36-60	Graduate - Post Graduate- PhD	System Check	25	22	3
36-60	Graduate - Post Graduate- PhD	Emotional Blackmail	15	14	1
			264	**225**	**39**

Table 8 – Contacting Personally Attack Test Results

In this table; it is clearly seen from 264 baiting attack attempts towards different education level and aged people, while 225 attempts were successful, only 39 were unsuccessful. While doing these attacks, we first made a very detailed search about our participants and

especially paid attention to use the right body language. These results' classification and observations will be given in Chapter 5, Conclusions section.

4.5 Technique Success Rate Results

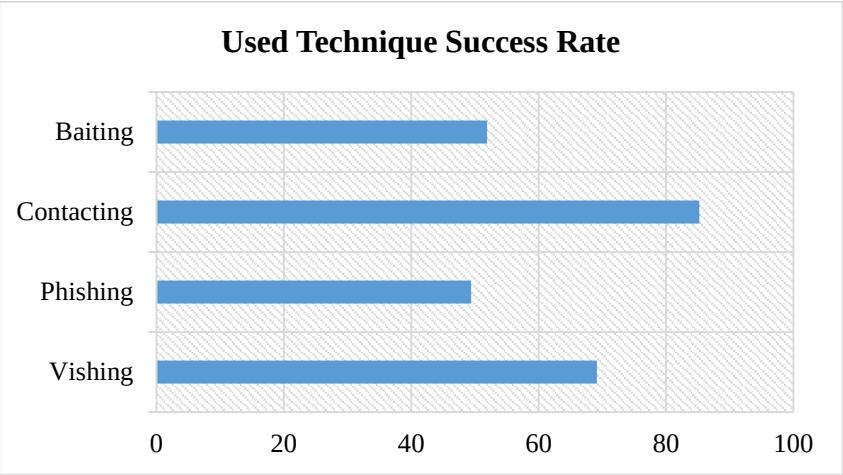

Figure 21 – Success Rate of usage of SE Techniques

In this study, one of our goals was to reveal which technique leads social engineers to success. It was clearly seen that talking personally and vishing technique was much more successful techniques compared to phishing or baiting using USB/CD. The reason of this result is just because in talking personally or vishing technique, the attacker can arrange himself/herself according to his/her target and has a chance to select the right behavior according to victim's responses. This makes attacker's success rate to higher levels. In phishing or baiting, the attackers builds up a trap and wait what to happen. On the other hand in contacting personally or vishing, the attacker can decide how to go on or how to behave and clarify the next step in his/her mind.

4.6 Approach Success Rate Results

The success of used approach methods are shown below in the figure. To repeat, these approaches are not applied randomly. We tried to apply the "right" method against the "right" participant according to their interests, likes, dislikes etc.

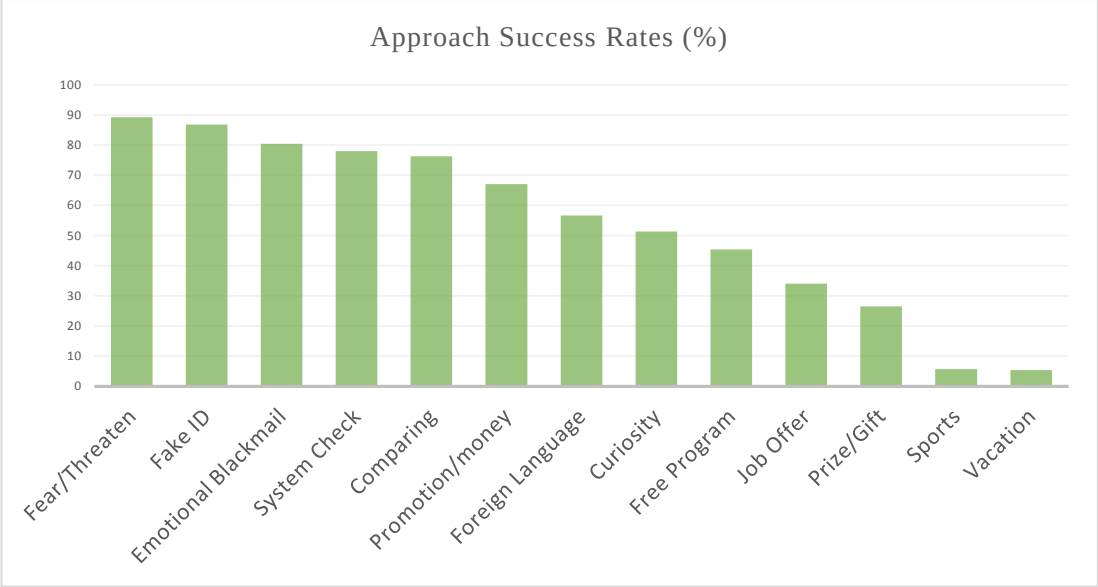

Figure 22 – Approach Success Rates

Using a fake ID card or threatening had most successful ratio in my study. None of any security guard was suspicious about our well-designed fake IDs except limited ones. This shows it would be easy for someone who has well-designed fake ID, would successfully breach into a system or facility with 87 percent of chance which is very risky for many companies, institutes or ministries.

Another thing that needs attention is about "threatening or blaming". After hearing some words like "judge, court, punishment", people drops their wings. In the research, it was seen that offering some gifts, talking about sports team, free programs, offering more salary or promotions, vacations, language training etc. does not work for a social engineer. The reason of this result is; these tactics has been too old and most people already know about these tricks and got talented. But when it comes to threatening, blaming or emotional blackmail and tailgating; the attack attempts are still successful about in these areas. When people are threatened with jail supported by time limit and pressure, they behave exactly how the social engineer wants. Again in this research, when it comes to tailgating attack, people were keeping the door open for the ones who were just walking behind of them as being polite. There have been some people who talked the security guards to allow our team member as if they know him before although they don't know anything about them. This trait showed us Turkish people trust others so easily in a short period of time.

4.7 Approach - Technique Success Rate Results

Approaches					
Approach	**Phishing**	**Vishing**	**Baiting**	**Contacting**	**Sum**
Fear/Threaten	330	61	0	0	**391**
Fake ID	0	0	0	38	**38**
Job Offer	290	38	0	45	**373**
Promotion/money	630	29	0	0	**659**
Sports	70	0	0	0	**70**
Vacation	130	0	0	0	**130**
Prize/Gift	170	30	0	0	**200**
Free Program	1433	0	40	0	**1473**
Foreign Language	90	47	37	38	**212**
Comparing	0	47	0	33	**80**
System Check	120	66	0	64	**250**
Curiosity	45	0	27	0	**72**
Emotional Blackmail	0	0	0	46	**46**
	3308	**318**	**104**	**264**	**3994**

Table 9 – Approach – Technique applied

Approaches Success					
Approach	**Phishing**	**Vishing**	**Baiting**	**Contacting**	**Sum**
Fear/Threaten	295	54	0	0	**349**
Fake ID	0	0	0	33	**33**
Job Offer	74	16	0	37	**127**
Promotion/money	417	25	0	0	**442**
Sports	4	0	0	0	**4**
Vacation	7	0	0	0	**7**
Prize/Gift	38	15	0	0	**53**
Free Program	646	0	23	0	**669**
Foreign Language	42	28	18	32	**120**
Comparing	0	34	0	27	**61**
System Check	88	48	0	59	**195**
Curiosity	24	0	13	0	**37**
Emotional Blackmail	0	0	0	37	**37**
	1635	**220**	**54**	**225**	**2134**

Table 10 – Approach – Technique Success

The graph below shows the relation between approaches and techniques used. In all fields "contacting personally" technique was the most successful approach type among all.

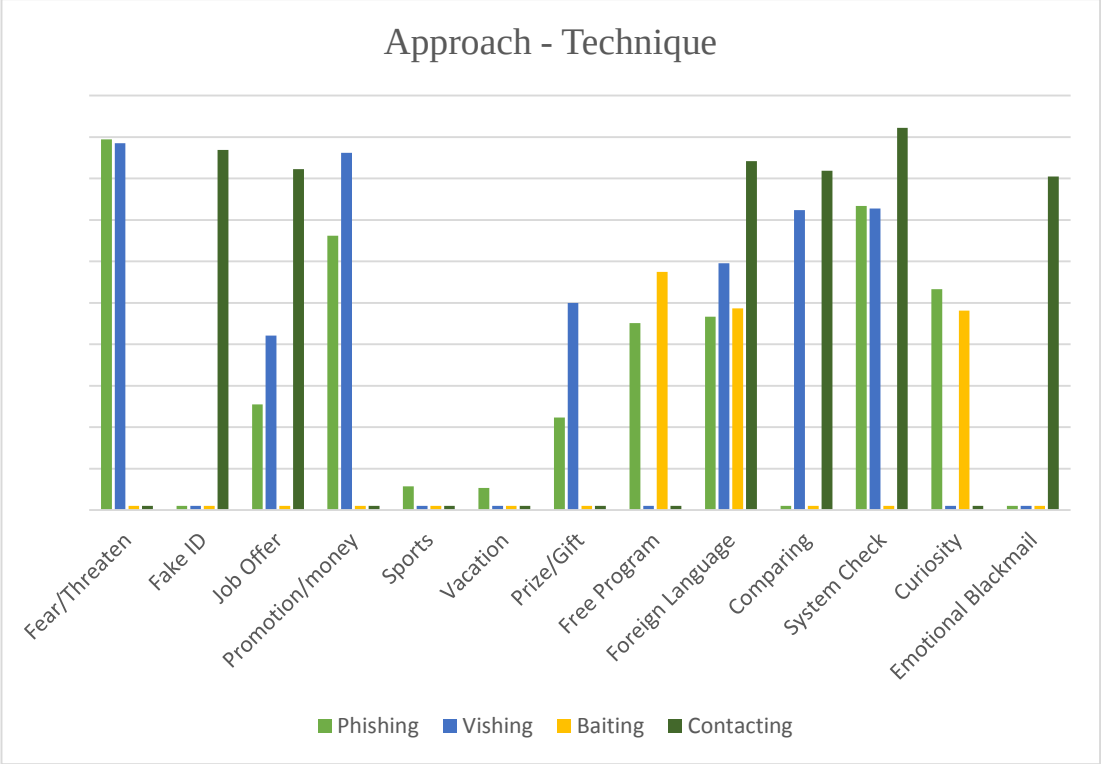

Figure 23 – Approach–Technique Success Relation

The underlying reason of this success rate is, it is supported by interacting with users by using body language, micro expressions or NLP techniques. The social engineer chooses his way of acting according to the responses coming from the victim.

Phishing technique was successful to some extend and mostly used for "as a part of" social engineering attacks. It can be clearly seen in this graph that threating, blaming or using fake id leads to successful attempts. And here one of the new leading successful attempt is "system checking" trick. Most people gave their usernames and passwords to attackers when it is said it would be used for system check accompanied by blaming or threatening approach.

Another important and most used approach is blaming while especially contacting with the victim personally. This can be applied like "insulting" the victim saying "hey! How can't you know me?!" The social engineer blames in this way or threatens the victim afterwards. Time limit and psychological pressure is a strong catalytic instrument for social engineers in this type of attacks.

In this study, another revealed vulnerability for some security guards is when a person is given responsibility in more crowded areas; s/he behaves stricter and applies to all rules without any exception. The strange and interesting thing is; when the same person is given a responsibility on his/her own, they are sometimes eager to take initiative about giving decision and they can ignore some rules against the security policies. When users are given more flexibility as they may decide according to their instinct, the probability of success of attack types increases.

4.8 Age-Technique Success Rate Results

Age - Techniques				
Technique	**18-25**	**26-35**	**36-60**	**Sum**
Phishing	1131	879	1298	**3308**
Vishing	95	118	105	**318**
Baiting	30	39	35	**104**
Contacting	65	115	84	**264**
	1321	**1151**	**1522**	**3994**

Table 11 – Age – Technique Applied

Age - Technique Success				
Technique	**18-25**	**26-35**	**36-60**	**Sum**
Phishing	567	343	725	**1635**
Vishing	71	74	75	**220**
Baiting	17	22	15	**54**
Contacting	57	92	76	**225**
	712	**531**	**891**	**2134**

Table 12 – Age – Technique Success

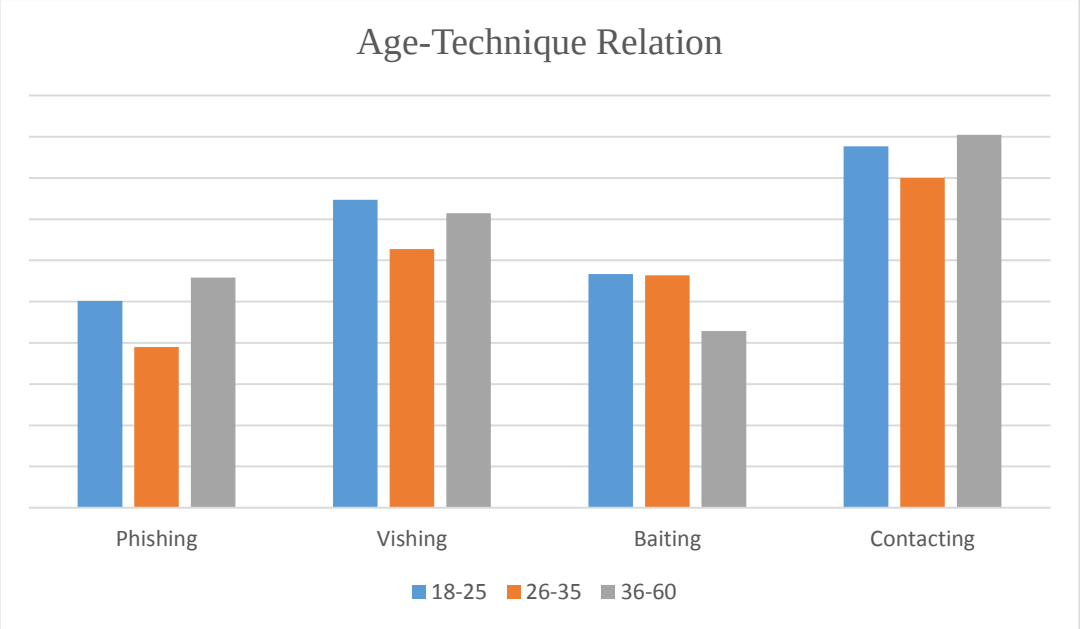

Figure 24 – Age- Technique Success Relation

According to results of the study, as this graph shows we can't say "this range of age has clear vulnerabilities in this field". Most of the time people over 36 were great targets in this study. Over age 36, people are more eager to "trust" to others or most of them are new to the digital world. Because they don't have knowledge about the digital world, they behave as attackers wants unintentionally and unknowingly. It can be said that less than 25 age, people mostly behave just because of their curiosity. 26-35 range people are most the ones who are talented and know much more about these attack types. Because most of them are educated and eager to discover.

4.9 Age-Approach Success Rate Results

Age – Approach				
Approach	**18-25**	**26-35**	**36-60**	**Sum**
Fear/Threaten	114	182	95	391
Fake ID	20	13	5	38
Job Offer	256	60	57	373
Promotion/money	292	199	168	659
Sports	25	25	20	70
Vacation	55	55	20	130
Prize/Gift	117	36	47	200

Age – Approach				
Approach	**18-25**	**26-35**	**36-60**	**Sum**
Free Program	260	325	888	1473
Foreign Language	71	72	69	212
Comparing	16	34	30	80
System Check	72	93	85	250
Curiosity	23	26	23	72
Emotional Blackmail	0	31	15	46
	1321	**1151**	**1522**	**3994**

Table 13 – Age- Approach Applied

Age - Approach Success				
Approach	**18-25**	**26-35**	**36-60**	**Sum**
Fear/Threaten	101	158	90	349
Fake ID	18	11	4	33
Job Offer	71	28	28	127
Promotion/money	209	120	113	442
Sports	2	1	1	4
Vacation	3	2	2	7
Prize/Gift	29	7	17	53
Free Program	146	36	487	669
Foreign Language	49	35	36	120
Comparing	12	25	24	61
System Check	60	70	65	195
Curiosity	12	15	10	37
Emotional Blackmail	0	23	14	37
	712	**531**	**891**	**2134**

Table 14 – Age- Approach Success

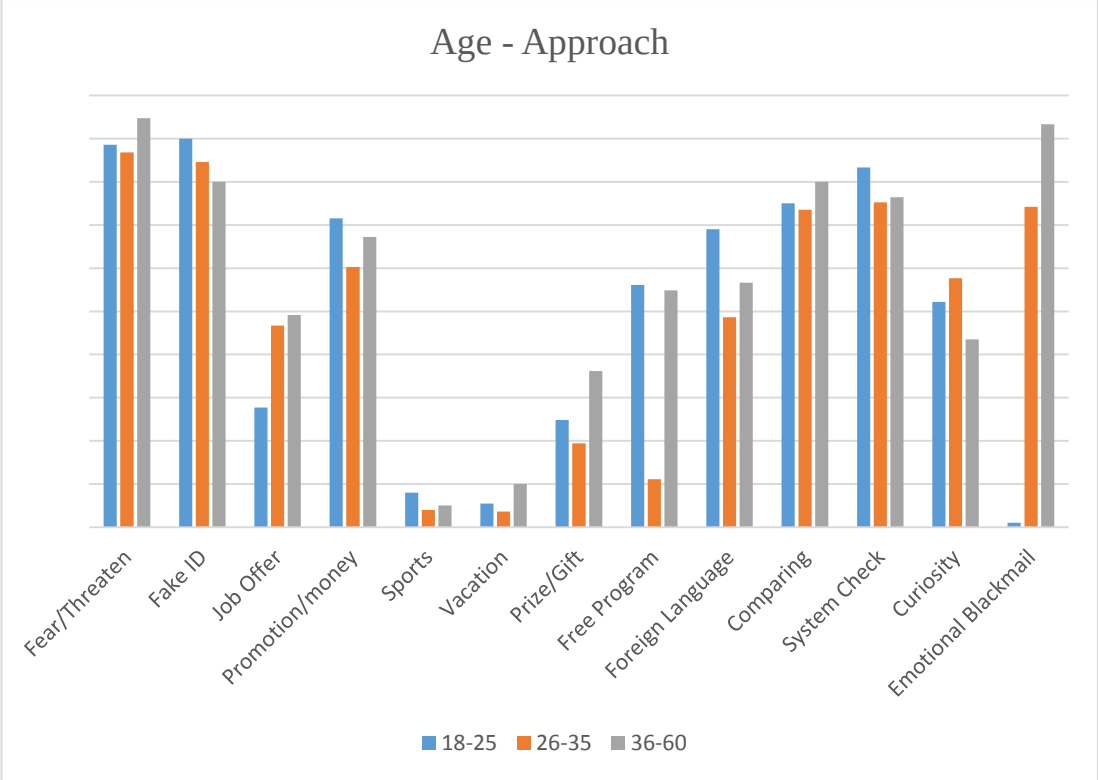

Figure 25 – Age-Approach Success Relation

When the results were classified according to ages and approaches, as this graph shows, again system checking, comparing, blaming, and threating are the most successful attack types for all ranges of ages. As most of older people in organizations are mostly satisfied with life and talented, they are were good at blocking the attacks like fake ID, curiosity when compared to younger people. On the other hand the younger people are eager to make their life higher quality so they are open to any offer that can make this dream come true. As a result, they have some vulnerabilities about free programs, promotions and money offers, system check tricks and fake IDs.

4.10 Education - Technique Success Rate Results

Education - Techniques			
Technique	**Undergraduate**	**Graduate - Post Graduate- PhD**	**Sum**
Phishing	1131	2177	3308
Vishing	95	223	318
Baiting	30	74	104
Contacting	87	177	264
	1343	**2651**	**3994**

Table 15 – Education - Technique Applied

Education - Techniques, Success			
Technique	**Undergraduate**	**Graduate - Post Graduate- PhD**	**Sum**
Phishing	567	1068	1635
Vishing	71	149	220
Baiting	17	37	54
Contacting	75	150	225
	730	**1404**	**2134**

Table 16 – Education - Technique Success

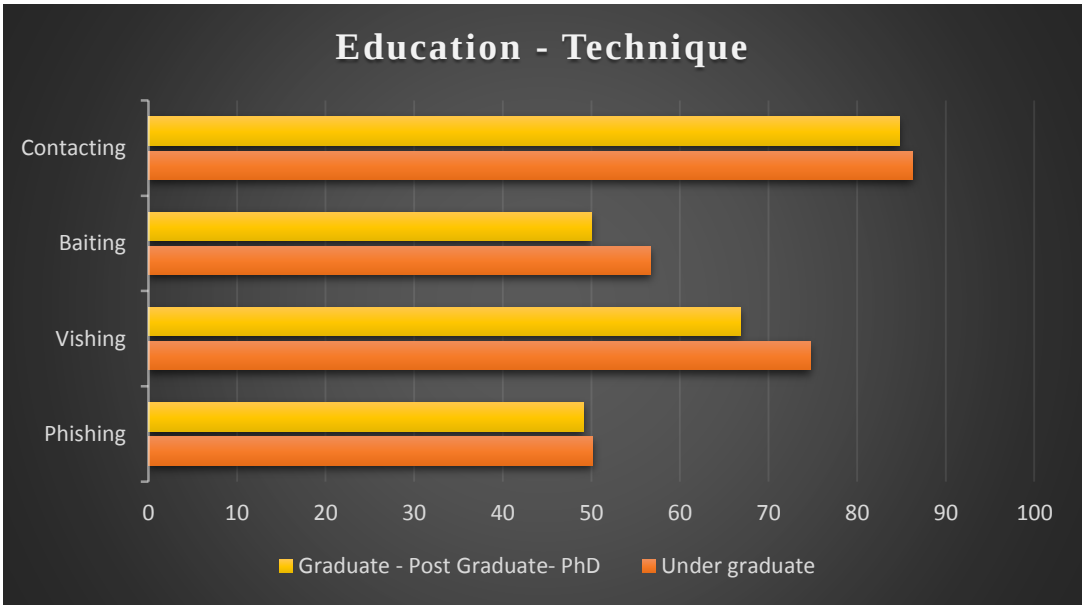

Figure 26 – Education-Technique Success Relation

When compared the results according to education level, normally the higher people are educated, the lower success level for social engineers. As users know more and educated enough, they are more aware of the risks that their companies or organizations may face. Mostly people with lower educated; their awareness level is low and can be cheated more easily. And the thing is, this information is valid for all the social engineering techniques applied towards the targets.

4.11 Education – Approach Success Rate Results

Education - Approach - SUM			
Approach	**Undergraduate**	**Graduate - Post Graduate- PhD**	**Sum**
Fear/Threaten	114	277	**391**
Fake ID	27	11	**38**
Job Offer	256	117	**373**
Promotion/money	292	367	**659**
Sports	25	45	**70**
Vacation	55	75	**130**
Prize/Gift	117	83	**200**
Free Program	260	1213	**1473**
Foreign Language	71	141	**212**
Comparing	23	57	**80**
System Check	72	178	**250**

Education - Approach - SUM			
Approach	**Undergraduate**	**Graduate - Post Graduate- PhD**	**Sum**
Curiosity	23	49	**72**
Emotional Blackmail	8	38	**46**
	1343	**2651**	**3994**

Table 17 – Education – Approach Applied

Education - Approach - SUM, Success			
Approach	**Undergraduate**	**Graduate - Post Graduate- PhD**	**Sum**
Fear/Threaten	101	248	**349**
Fake ID	24	9	**33**
Job Offer	71	56	**127**
Promotion/money	209	233	**442**
Sports	2	2	**4**
Vacation	3	4	**7**
Prize/Gift	29	24	**53**
Free Program	146	523	**669**
Foreign Language	49	71	**120**
Comparing	17	44	**61**
System Check	60	135	**195**
Curiosity	12	25	**37**
Emotional Blackmail	7	30	**37**
	730	**1404**	**2134**

Table 18 – Education – Approach Success

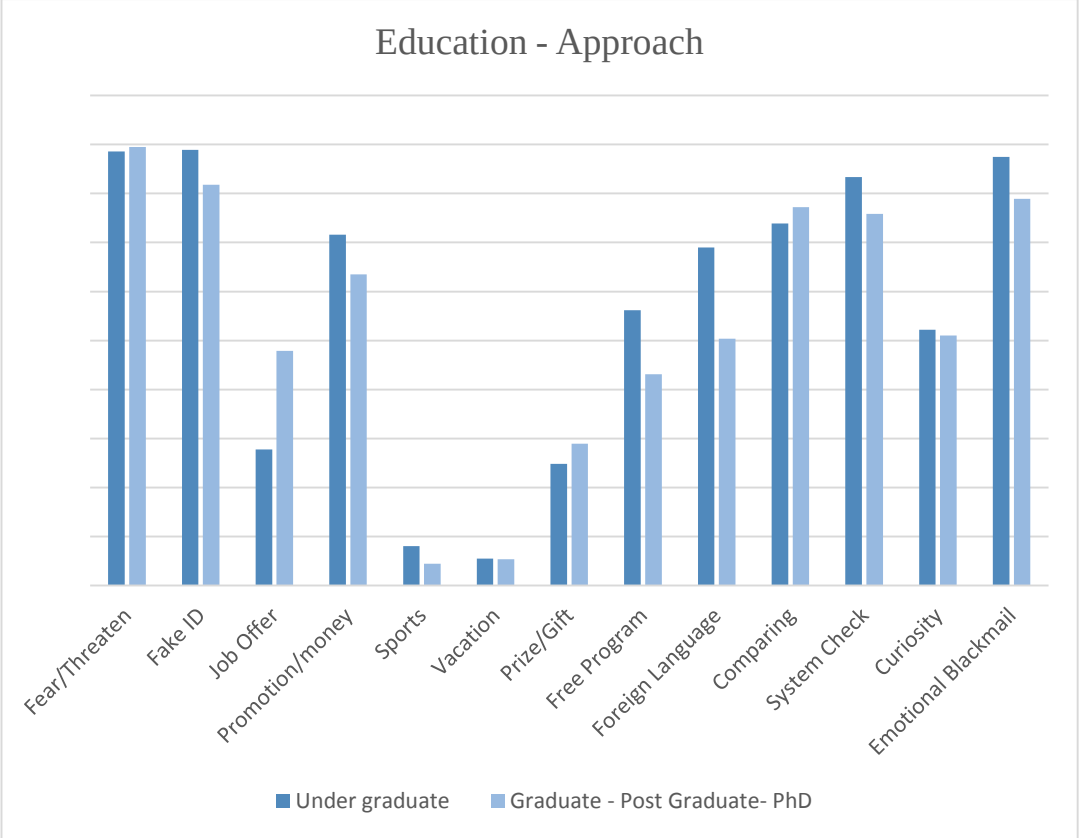

Figure 27 – Education-Approach Success Relation

This graph shows the relationship between education levels and approach ways. Among the successful attempts, mostly under-graduate people were abused by the attacks normally. This graph is clearly showing that the higher educated people are, the more aware they are again. There are some approach methods that higher educated people were abused but there is no significant difference between those as it will be analyzed in chapter 5, conclusion part.

CHAPTER 5

5 CONCLUSIONS

5.1 STATISTICAL EVALUATION OF RESEARCH RESULTS

In order to evaluate the results of our research, we've applied some statistical analysis about the results we obtained. We applied "Tree Structured Data Analysis" method to our findings in order to see the possible pathways of a social engineering attack types according to the data we got.

Classification and regression trees are becoming increasingly popular for partitioning data and identifying local structure in small and large datasets. Classification trees include those models in which the dependent variables are categorical (Wilkinson, 1992). Because the data we obtained from our research falls under the categorical data type; we chose this way to figure out the possible pathways of a social engineer.

IBM® SPSS® Decision Trees helped us better identify our groups, discover the relationships between the techniques and approaches used and predict the attack types and approach ways that could be chosen by a social engineer.

After having the decision trees, the possible paths and their success possibilities will be discussed. The nodes in decision trees resemble the paths that have significant difference from other paths. So, each node can be thought of as a cluster of objects (cases), which is to be split by further branches in the tree. The node that has more than one item, meaning there is no significant difference between those items. This significance test is done by the IBM® SPSS® program using chi-square test technique (Wilkinson, 1992) to classify the items in that node.

5.1.1 Techniques Analysis

In this part; the techniques used in the research will be analyzed and possible paths will be figured out most of which probably would be traced by a social engineer.

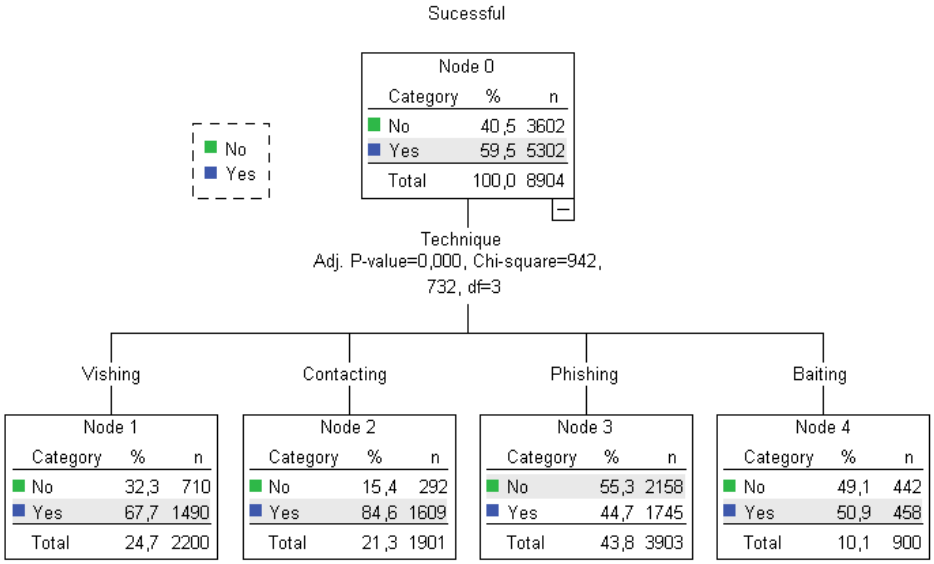

Figure 28 – Statistical Analysis on Used Techniques

As it is shown in the figure above; the p value of the chi-square test is 0.000, which shows clearly there is a significant difference between using these techniques. This result means choosing which technique will be applied is a decision point for a social engineer to reach his/her goals. The attacker has to choose his/her technique according to his/her victim and the situation. In order to choose the right technique, s/he has to get enough information about his/her target. This means if a social engineer applies the right attack type to the right person on the right time, s/he will most probably be successful with a success probability of 59.5%.

When examined the nodes, the most successful method is “contacting” among the techniques used in the research. The success order of other techniques is vishing, baiting and phishing respectively. Here we can clearly see that the techniques that benefits from contacting personally and has initiative to manage the attack are the most successful ones. So; for a social engineer, rather than building up a trap and waiting, taking control of the attack will be a most probable choice to exploit the target system.

5.1.2 Approach Analysis

Here; the approaches used in the research will be analyzed and possible paths will be figured out most of which probably would be traced by a social engineer.

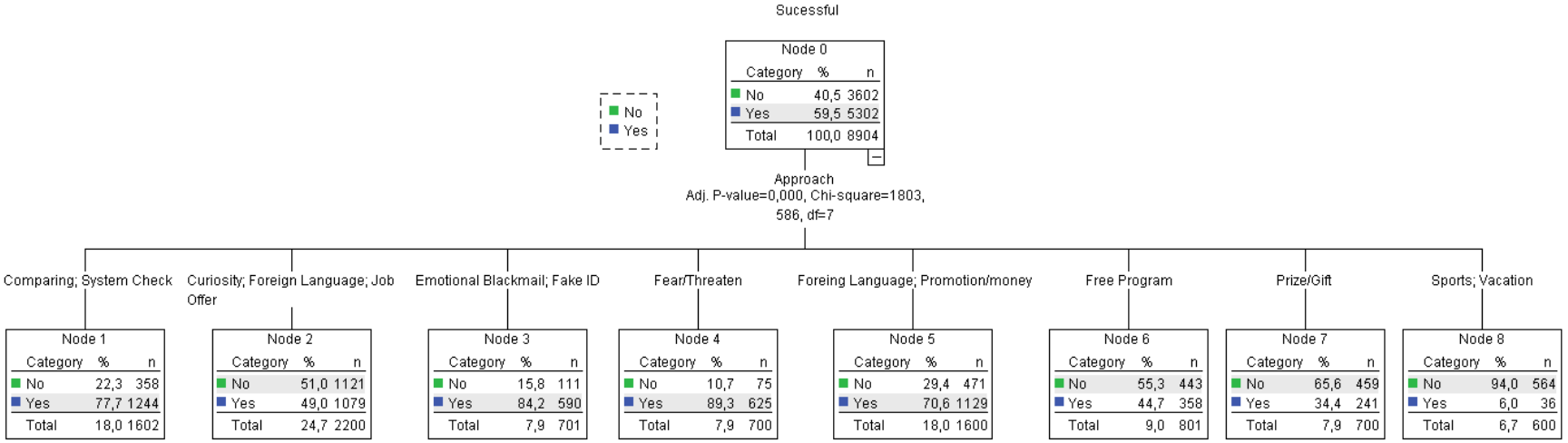

Figure 29 – Statistical Analysis on Used Approaches

As it is shown in the figure above; the p value of the chi-square test is 0.000, which shows there is significant differences between the nodes that are consist of techniques. Here each node resembles a decision point for a social engineer to reach his/her goals. We can see there are some nodes that have more than one approach. These nodes means there is no significant difference between those approaches and will be successful with similar percentage of probability. The attacker has to choose his/her approach according to his/her victim and the situation.

The nodes that have high probable success are the first, third and the fourth nodes. The highest success level among all these is the node, which is, consist of fear and threatening approach with an 89.3% relative success probability. Then the next successful node is the one that includes Emotional blackmailing and fake ID. Comparing people with others and calling for a system check come as next successful approaches for the participants in our research among all approaches.

While these approaches are the most successful ones, the last node which is consist of offering a vacation or inviting to a football match are the least successful approaches with a 6% probability of success compared to rest approaches. As it is seen in the figure, this path most probably will not be chosen by the social engineer according to our data.

Looking at the decision nodes in terms of used approach ways, a social engineer will most probably choose a path which includes fear, threatening, emotional blackmailing, using fake ID, comparing people with others or system check. The attacker normally chooses one or more approach ways according to his opportunities and capabilities against the target.

5.1.3 Age Analysis

Here; it will be revealed whether the age of a target is important or not for a social engineering attack.

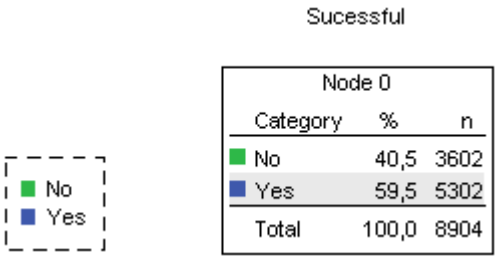

Figure 30 – Statistical Analysis on Age

As it is shown in the figure above, there is no significant difference between age groups. This figure means it will no differ that much to attack to only one age range people for a social engineer. So; every range of people can be target of social engineering attack types.

5.1.4 Education Level Analysis

Here; it will be shown whether the education level of a target is important or not for a social engineering attack.

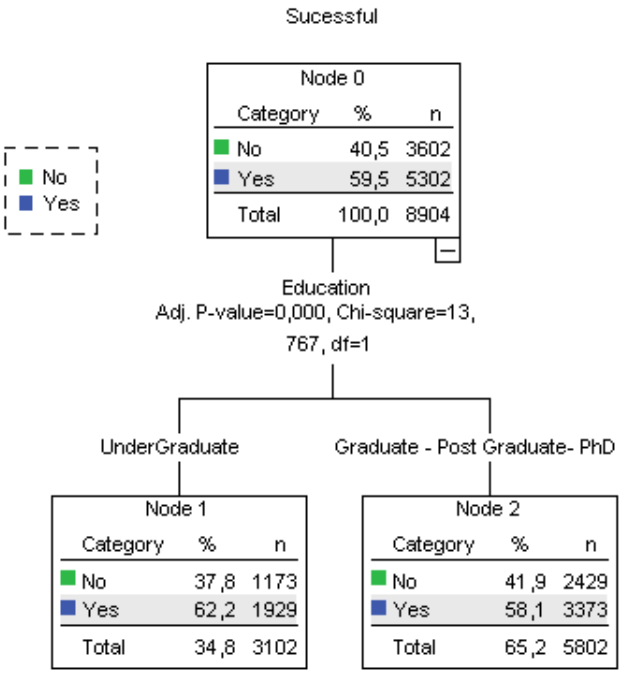

Figure 31 – Statistical Analysis on Education Levels

As it is shown in the figure above, there is a significant difference between the education levels. For a social engineer, it would be a better choice to apply his/her attacks towards people who have lower education levels. If the attacker does so, his/her attack will be successful with a percentage of 62.2% compared to higher education levels. The social engineer will most probably select his/her targets according to his opportunities and targets but, as the figure above shows, s/he will do his/her best to attack lower educated people as much as possible s/he can.

5.1.5 Technique – Approach Analysis

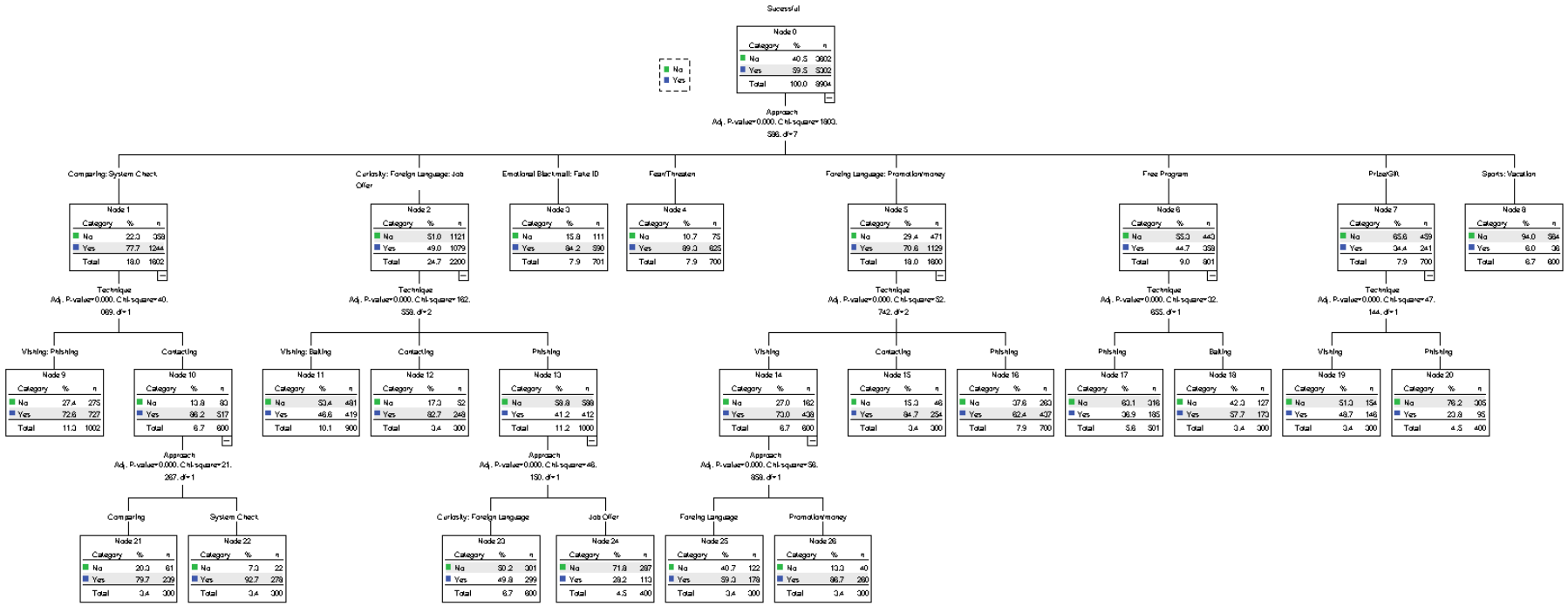

Figure 32 – Statistical Analysis on Technique - Approach

The figure shows that when a social engineer considers about technique and approach together, he will have some decision points. There are some nodes again which consist of more than one node, showing there is no significant difference between those.

According to the results we got here, if a social engineer chooses a method, s/he would also consider about other issues too that will affect his/her decision. The figure above considers just approach method and used technique. Here if a social engineer will most probably choose the first path – comparing, system check – and then s/he should then consider which technique will be used with this approach. As the figure shows, the next most successful methods for those approach types are vishing, phishing and contacting personally. Among the techniques, while contacting personally has 86.2 % of relative success probability, the vishing and phishing has only 72.8 % relative success probability compared to rest. Normally after choosing the "contracting personally" technique, the results shows that s/he should consider again about the approach s/he is going to apply. If the attacker chooses to contact the target, he will have two more paths, which are comparing with them or system checking. As the system checking has higher percentage of relative success probability (92.7%) s/he will most probably use this path if his/her opportunities permit. If the attacker would choose the other path, the vishing or phishing technique, then he would not consider about the approach again as it does not differ that much. He just would choose one of the approach way, comparing or system checking.

Another path that the figure shows here, the one that has the most relative success probability with 89.3%, is fear and threatening node. Because it has high percentage of success in all techniques used, it will not differ that much to focus on any technique for the attacker. The same approach will be valid for the third node, emotional blackmail and fake ID. But when it comes to a node fifth node, the social engineer would consider about two more steps to success.

5.1.6 Technique – Age Analysis

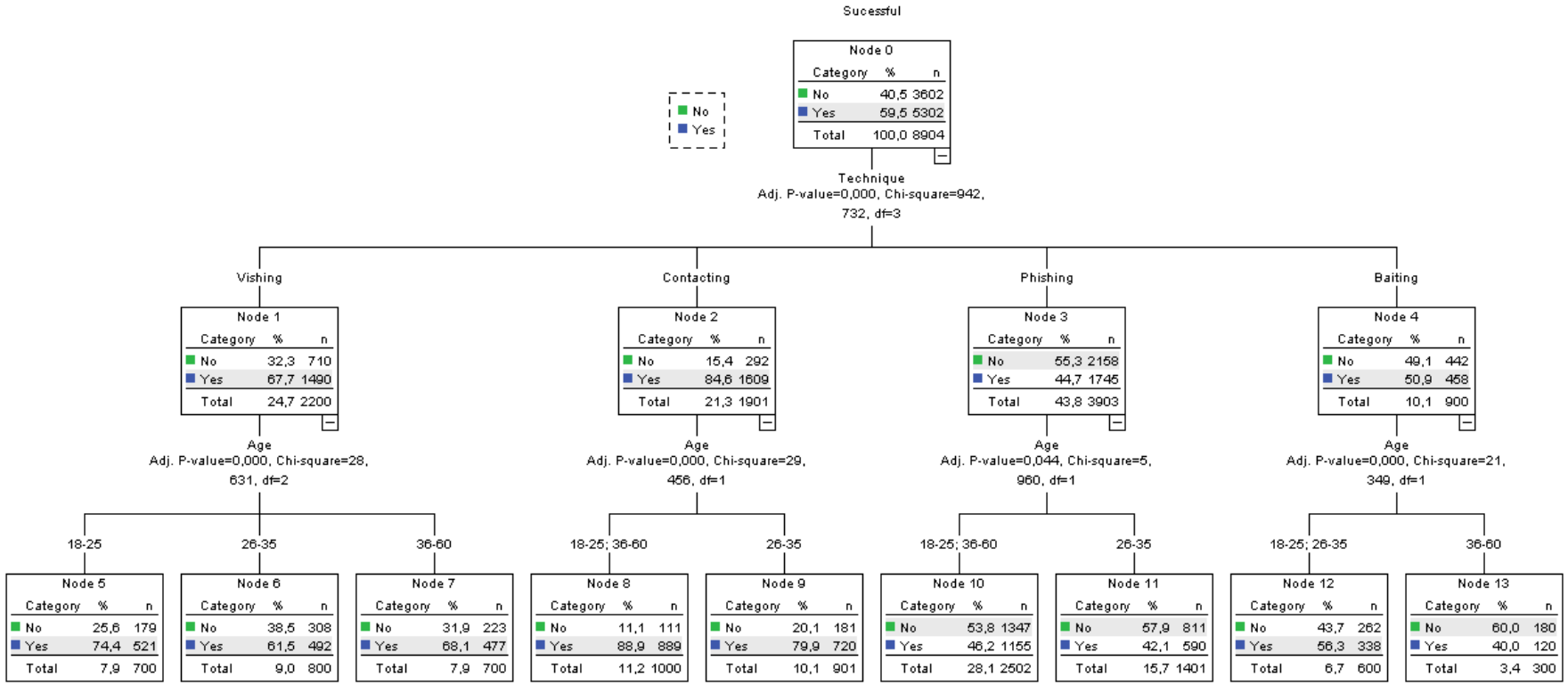

Figure 33 – Statistical Analysis on Technique - Approach

The figure shows that when a social engineer considers about technique and the age of his/her targets together, s/he will have some more decision points. There are some nodes again here that consist of more than one item, showing there is no significant difference between those. The figure above considers just technique and age ranges of the participants.

Here if a social engineer chooses the first path – vishing – then s/he should then consider which age range of people should be seen as a potential target for a better attack. As the figure shows, the node with the highest relative success probability with 74.4% is 18-25 age range people for vishing technique. If a social engineer has just an opportunity to call the targets or if s/he plans to attack the targets by vishing, s/he will probably choose to call younger people to get some critical information.

Similarly, according to our data, if the attacker choses contacting, then s/he has to consider about which age of range people can be more vulnerable targets. It is shown in the figure that, there is no significant difference between 18-25 age of range and 36-60 range of people when it comes to contacting personally. While youngest and oldest range of people are great targets for this technique – with 88.9% relative success probability – 26-35 age range of people are "bad" targets for a social engineer.

5.1.7 Technique – Education Level Analysis

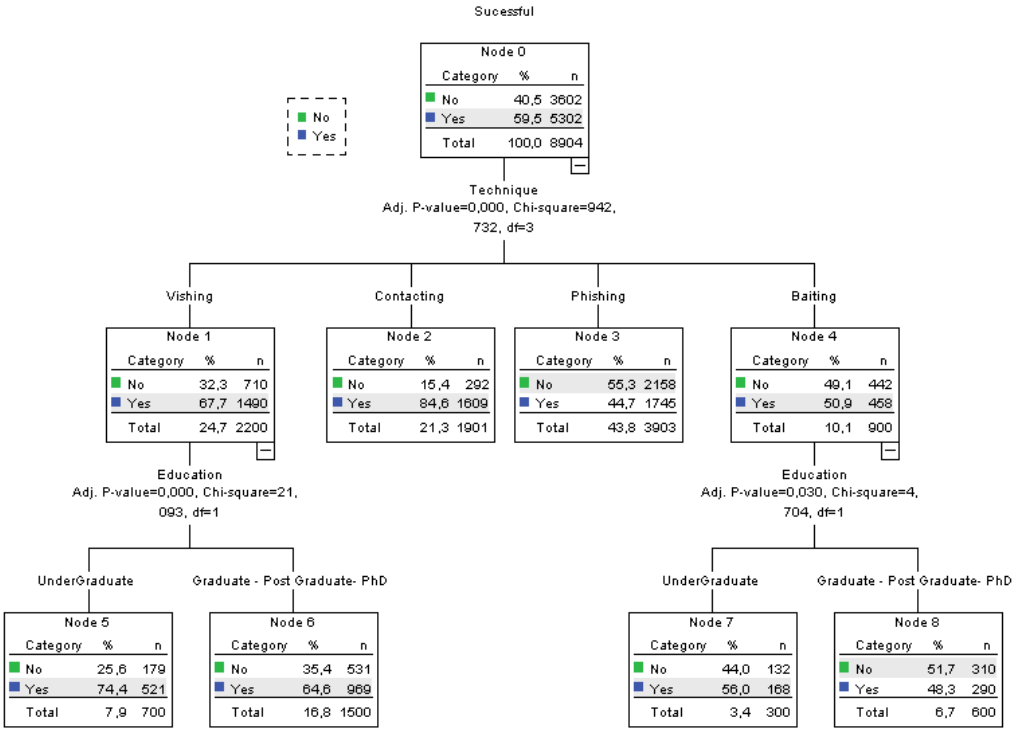

Figure 34 – Statistical Analysis on Technique – Approach

The figure shows that when a social engineer considers about just technique and the education level of his/her targets together, he will have some more decision points also.

Here, as the figure shows, while the social engineer better consider the educational status of his/her target when s/he is using vishing and baiting techniques, s/he does not need to focus on the educational status of the target if phishing and contacting personally is used.

If a social engineer chooses the first path – vishing – then s/he should then consider about which education level of people should be targeted to make the attack with higher probability of success. As the results of the test shows, the node with the highest relative success probability (74.4%) is people at undergraduate educational level, who are university students or newbies in universities and organizations. If a social engineer has just an opportunity to call the targets or if s/he plans to attack the targets by vishing, s/he will probably choose to call the people who have lower education level to get some critical information.

Similarly, according to the figure, if the attacker choses contacting, then s/he does not have to focus on only one education level because it has no significant difference between undergraduate and graduate people.

When the results are examined carefully, it will be seen mostly the undergraduate people are more vulnerable to social engineering attack types compared to higher educated ones. Although it seems so; there are some techniques in which there is no that much difference for social engineers in terms of target's education level. The figure clearly shows that when it comes to phishing or contacting personally, the educational level does not that much change the success of the social engineering attack types. So this result shows that the general belief in society "if someone is highly educated, then it means it will not be easy to apply a successful attack on him" misperception is wrong in some attack types like contacting and phishing. The key point here is; just knowing about the vulnerabilities or having critical information about the target is not about just the educational level. So as a result, it will be better not to have "I am safe" syndrome when it comes to social engineering attack types, which are focusing on human vulnerabilities, that all of the people have.

5.1.8 Approach – Education Level Analysis

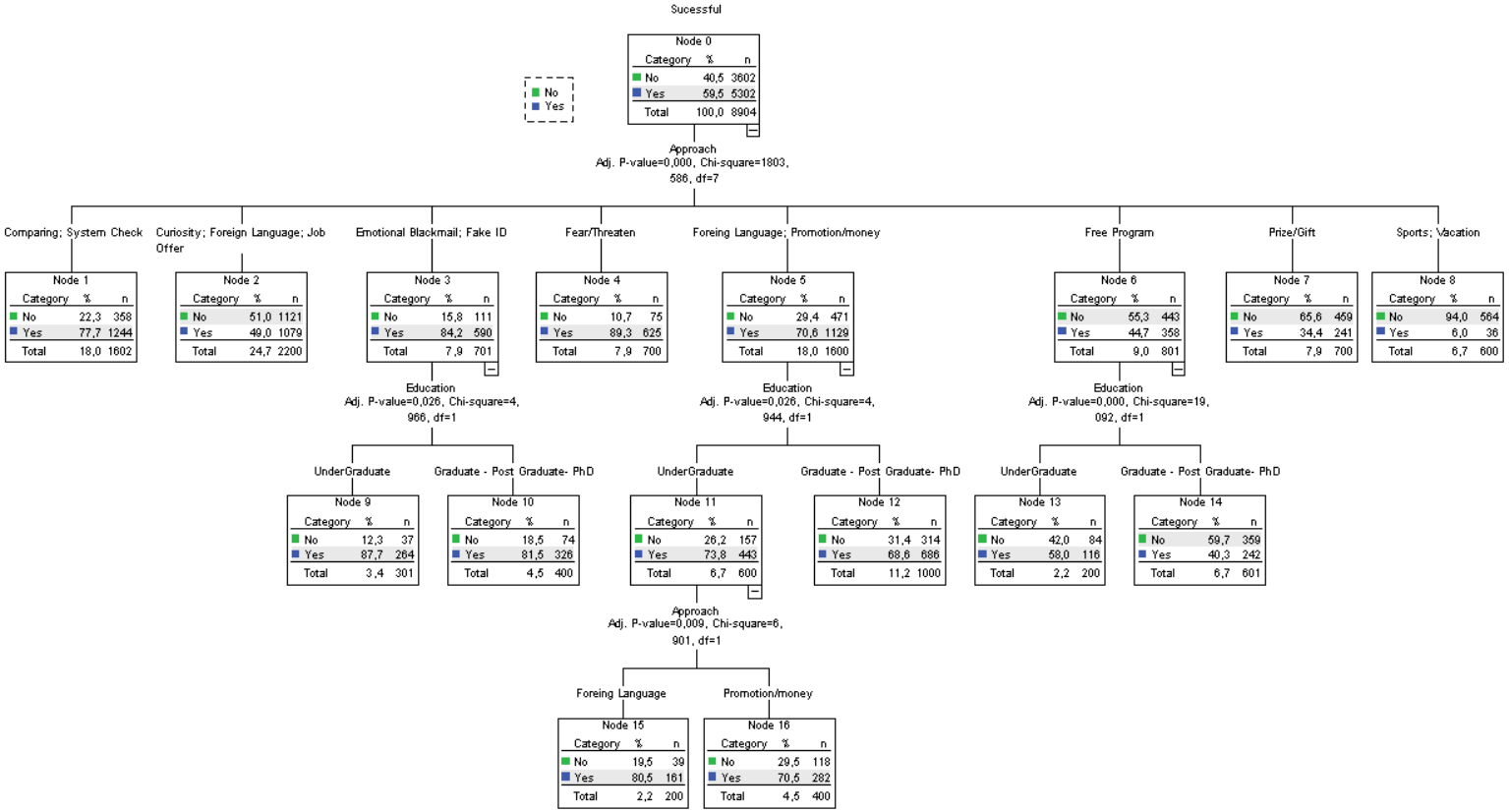

Figure 35 – Statistical Analysis on Approach – Education

The figure shows that when a social engineer considers about the chosen approach way and the education level of his/her targets together, he will have some more decision points also.

Here, as the figure shows, while the social engineer better consider the educational status of his/her target when s/he is using emotional blackmailing, fake ID technique, foreign language learning, promotion/money, and installing a free program, s/he does not need to focus on the educational status of the target if the other methods shown in the figure will be used.

According to the test results, lower educated people are more vulnerable to social engineering attack types. It will be so important for a social engineer to focus on the nodes that need to be considered on which education level will be chosen. But there are also some approach ways which do not need to be considered about focusing on education levels of the target like system checking, comparing, fear-threatening, sports and vacation offering.

For instance if a social engineer knows that in a department, there are some people who are eager to learn a foreign language or has some weaknesses on money, s/he then better consider the educational level of the people who can be potential targets. If the target has higher education level, then there will be no other decision point for the engineer; on contrary if the target has lower education, then the attacker will consider which approach would be better. As it is shown in the figure, the foreign language learning approach has more relative success probability (80.5%) than offering promotion or money. So the most probable path under the foreign language or promotion/money node will end up with applying foreign language learning approach on undergraduate people in that department. This is actually how a social engineer plans his acts before the attack.

Similarly, according to the figure, if one of the "fear/threatening", "comparing / system checking", or "prize/gift" approach way was chosen by the attacker, then s/he does not have to focus on only one education level because it has no significant difference between undergraduate and graduate people.

When the results are examined carefully, it will be seen mostly the undergraduate people are more vulnerable to social engineering attack types compared to higher educated ones. Although it seems so; there are some approaches in which there is no that much difference for social engineers in terms of target's education level. The figure clearly shows that when it comes to approaches like "fear/threatening" or "sports/vacation", the educational level does not that much change in terms of the success of social engineering attack types. The key point here is just knowing about the vulnerabilities or having critical information about the target; is not about just the educational level of the potential targets.

5.1.9 Approach – Age Analysis

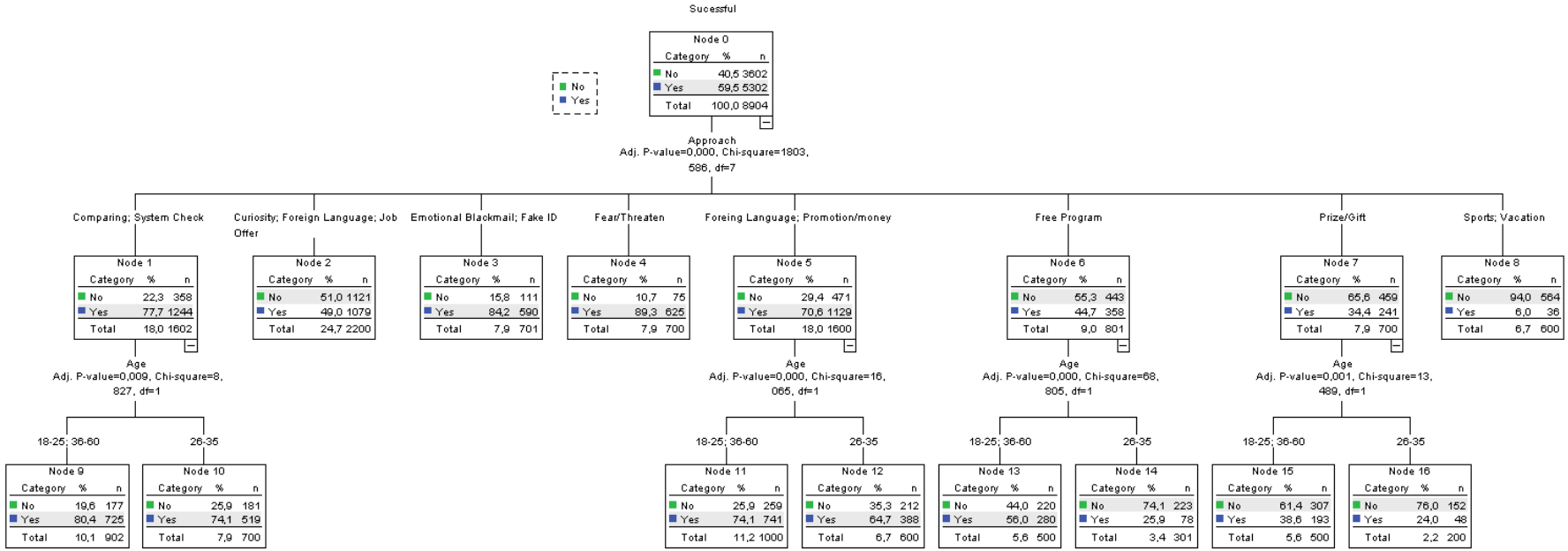

Figure 36 – Statistical Analysis on Approach – Education

The figure shows that when a social engineer considers about the chosen approach way and the age range of his/her targets together, he will have some more decision points also.

Here, as the figure shows, while the social engineer better consider the age range of his/her target when s/he is using comparing, system checking, foreign language learning, installing a free program, and giving prize of gift, s/he does not need to focus on the age range of the target if the other methods shown in the figure will be used.

According to the test results 18-25 and 36-60 range of people are more vulnerable to social engineering attack types. It will be so important for a social engineer to focus on the nodes that need to be considered on which age range will be chosen. But there are also some approach ways that do not need to be focused on age of the target like emotional blackmailing, comparing, fear/threatening, sports and vacation offering.

For instance if a social engineer decides to attack to an organization by "system checking" approach, s/he then better consider the age range of the people who are potential targets. If the target belongs to 18-25 and 36-60 age range, then the attacker will know the attack will be more probably successful when compared to 26-35 age range people. So the most probable path under the comparing – system check node will end up with applying either any of the approach on 18-25 and 36-60 age range rather than 26-35 age range.

Similarly, according to the figure, if one of the "fear/threatening", or "emotional blackmail / fake ID" approach way was chosen by the attacker, then s/he does not have to focus on only one age range because it has no significant difference between older or younger people.

When the results are examined carefully, it will be seen mostly the middle aged people are more aware to social engineering attack types. Although it seems so; there are some approaches in which there is no that much difference for social engineers in terms of target's age. The figure shows that when it comes to approaches like "fear/threatening" or "sports/vacation", the age does not change the relative success of the social engineering attacks that much. Having detailed information about the vulnerabilities of targets or having critical information about the target is the key point here again.

5.1.10 Age – Education Level Analysis

Here; it will be shown what the possible paths will be when age and education levels are considered together by a social engineer.

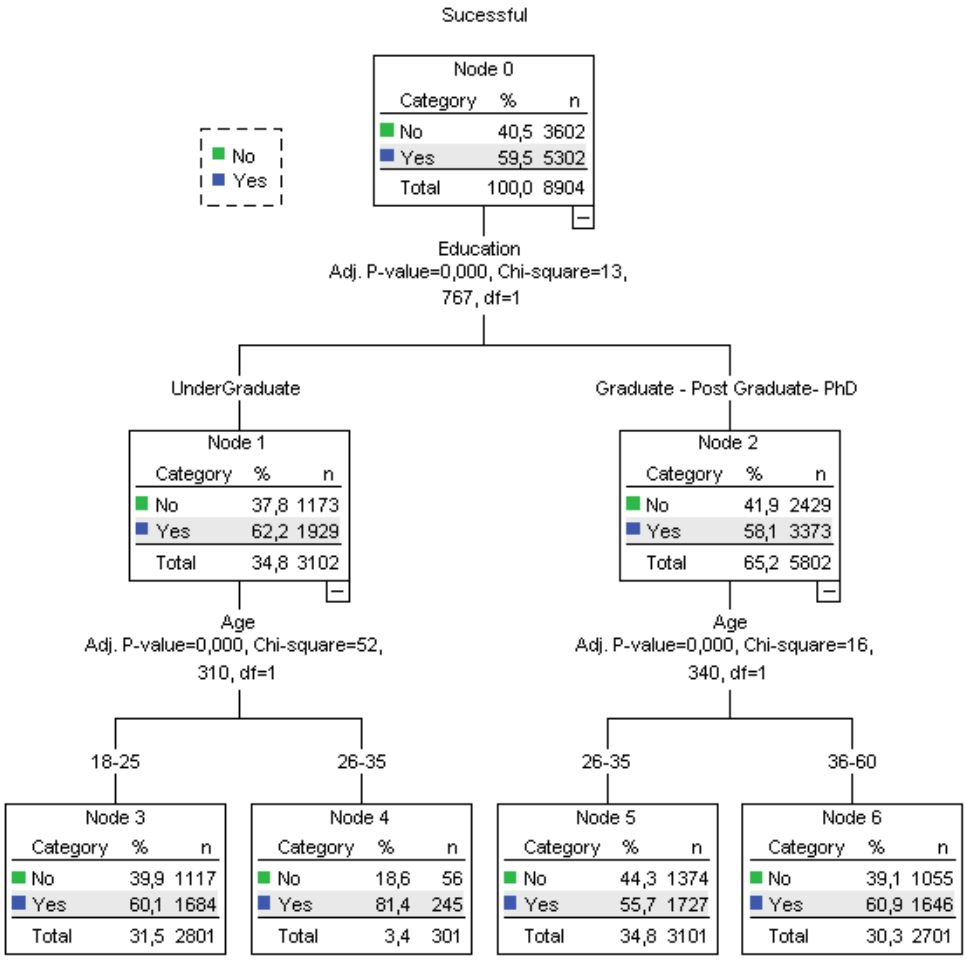

Figure 37 – Statistical Analysis on Age – Education

Here as it is shown in the figure above, when considered age ranges and the education levels, first decision point is whether the attack will be applied to undergraduate people or higher educated ones. Here the relative success probability of an attack towards lower educated people is higher than the high-educated people with a 62.2% relative success ratio. This issue changes according to the target of the social engineer. If he has a chance to choose one of each, he will clearly focus on undergraduate people to get higher probability of success.

If he does not have such a chance to choose, then his/her decisions will change according to target. If the target is lower educated, then his attacks will be on 26-35 age range people; if not, 36-60 age range people will be his potential target.

5.1.11 Technique – Approach – Age Analysis

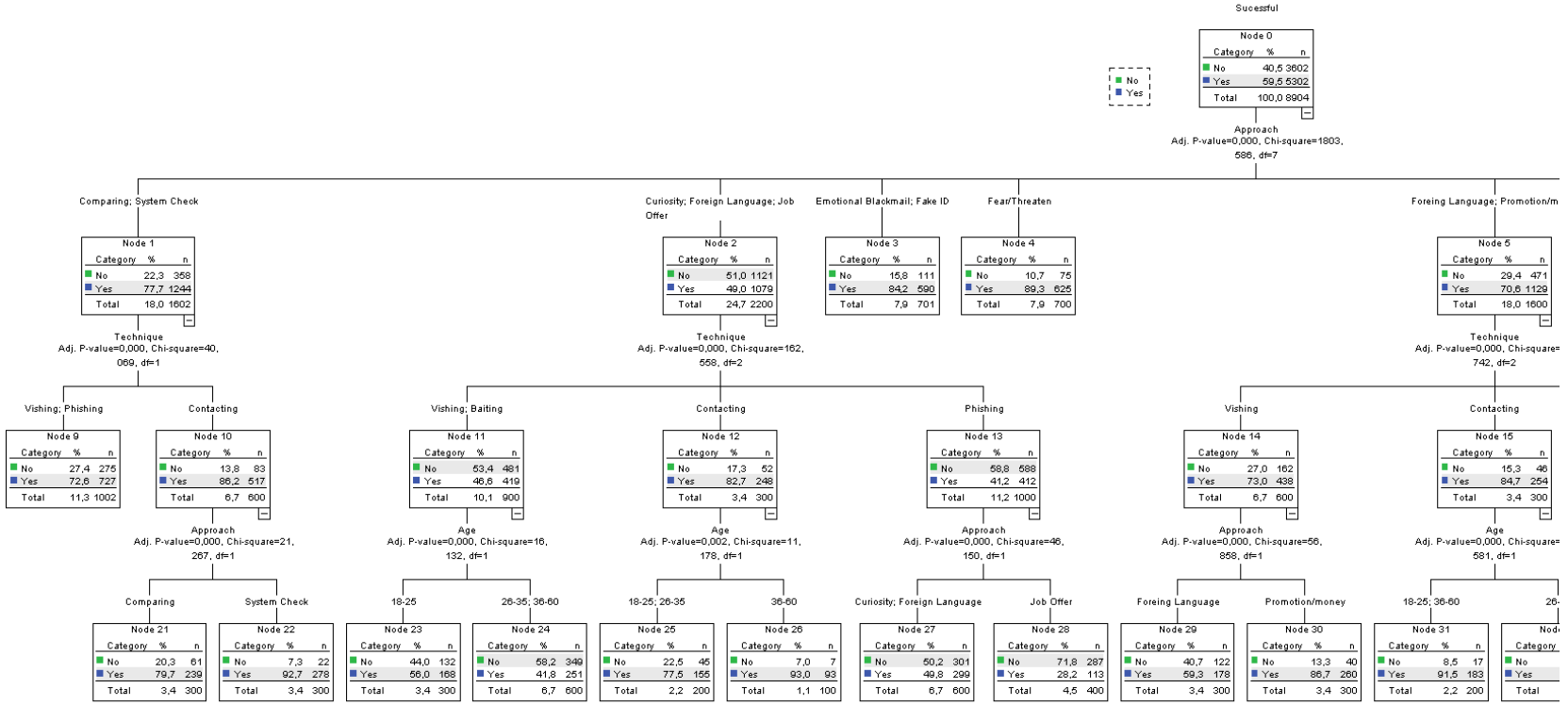

Figure 38 – Statistical Analysis on Technique – Approach – Age (1)

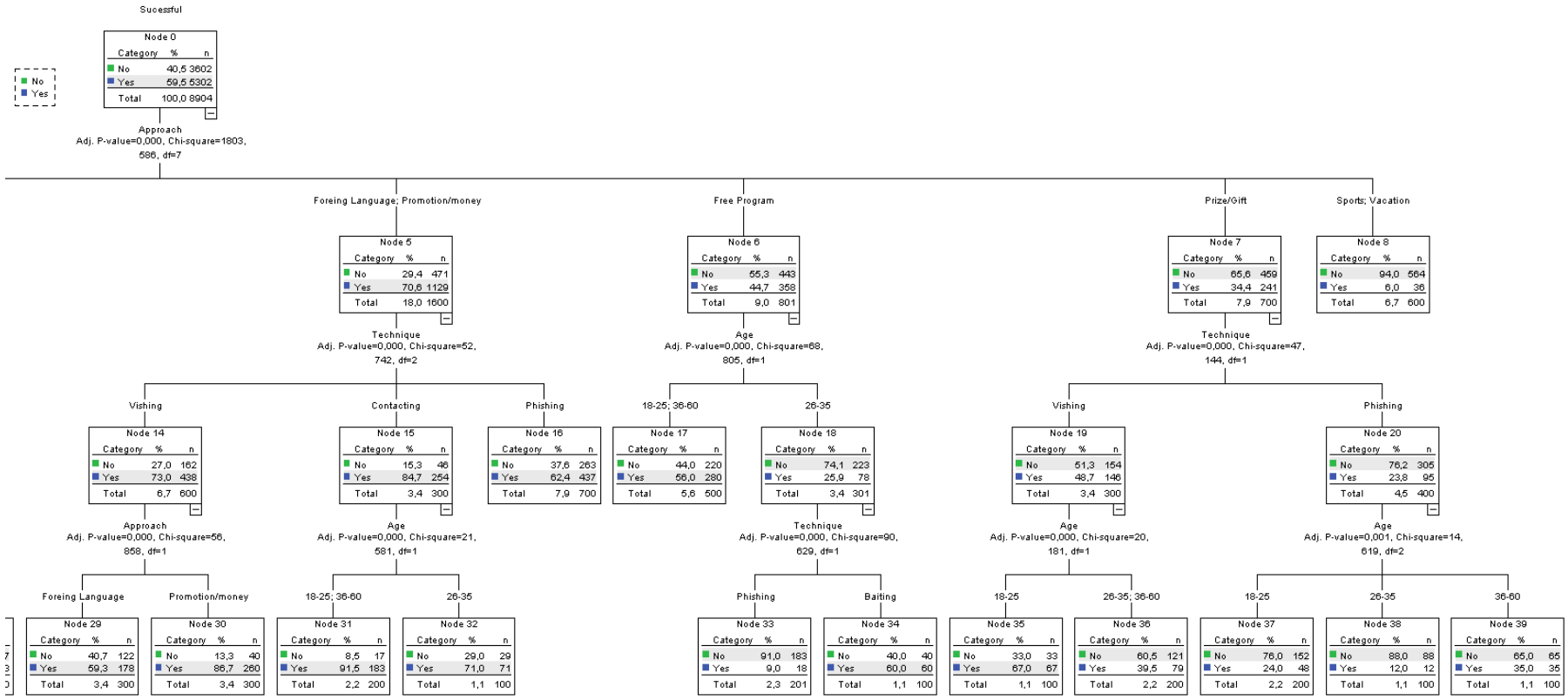

Figure 39 – Statistical Analysis on Technique – Approach – Age (2)

The figure shows what will be the possible paths when technique, approach way and age range are considered together by a social engineer.

Here, as the figure shows, social engineers have many decision points in front of him/her. And one can clearly see that there are some approaches that has no connection with age or technique used like emotional blackmailing, using fake ID, threatening, offering vacation, or inviting to a favourite teams' match. Among all these approach ways the most successful one is fear/threatening. The next successful ones are emotional blackmailing and using fake ID. Offering vacation, or inviting to a favourite teams' match does not work that much as the figure shows its relative success probability, just 6%. If social engineer decides other nodes, then that means he will consider about many other factors some of which has two or three steps more for being successful in the attack.

According to the test results, there is no such a technique that works great on a specific age range or with some other approach ways. Every decision path has its own characteristics. This means the chosen approach, technique and the age range will differ according to the target, which has high diversity.

For instance if a social engineer decides to attack to an organization by "system checking" or "comparing" after considering approach, technique and the age factors; s/he then better consider the which technique will suit for the target. According to results above, if vishing or phishing chosen by the attacker, then there will be no further decision node for him/her. But instead if s/he decides on attacking by contacting the target personally, then he will consider the approach way again. Looking at the figure, we can say that the attacker better to choose system-checking approach with a 92.7 % relative success probability. In this path there was no need to consider about the age range of the target. But that is not the case always as in the following example.

If the social engineer decides that sending malicious code with a help of a free program fits best for him, he will think about that node. As the figure shows clearly, first step of him will be considering the age range. If the targets are not consist of middle age range people, then there is no more steps to decision. He will just start to his attack. On the contrary; if the target is a middle age one, then the attacker will consider about which technique s/he will use; phishing or baiting. According to results, baiting will be a better choice for him. So rather than sending an email to the target, he will prepare a CD/DVD or USB which includes malicious codes and leave that near the target, if possible his/her table.

As it is shown in the decision tree of a social engineer according to our results, there are many possible paths. The paths will be chosen according to the opportunities of the social engineer, targets and environment even. Because the circumstances will differ, the chosen path will normally change too.

5.1.12 Approach – Age – Education Analysis

The figure below shows what possible paths will be when approach, age range and education levels are considered together by a social engineer.

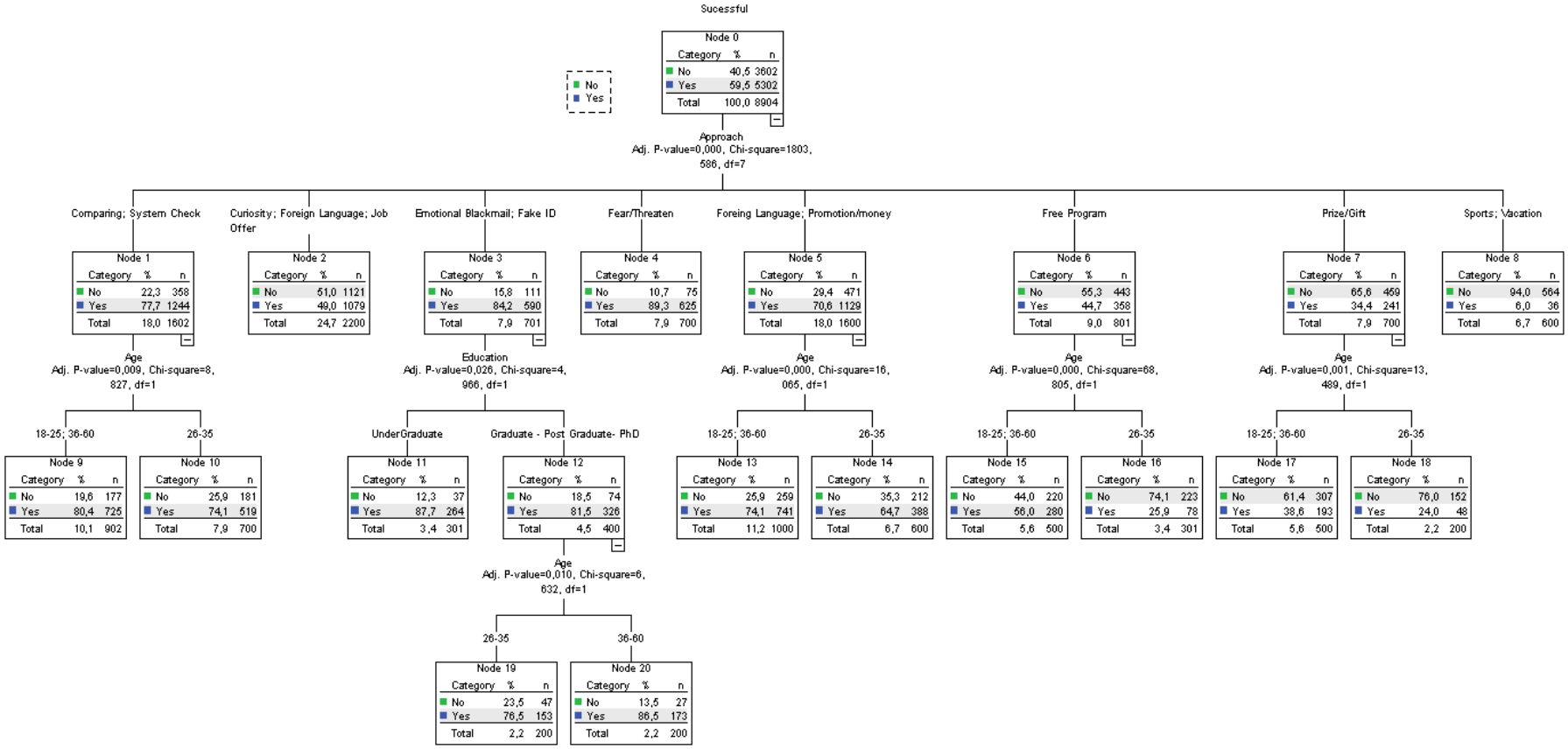

Figure 40 – Statistical Analysis on Approach – Age – Education

Here, as the figure shows, social engineers have many decision points in front of him/her when considered age, approach and education levels. And one can clearly see that there are some approaches that has no connection with age or education level like threating, creating curiosity, offering vacation, or inviting to a favourite teams' match. Among all these approach ways the most successful one is fear/threatening again. Offering vacation, or inviting to a favourite teams' match does not work that much as the figure shows its relative success probability, just 6%. If social engineer decides other nodes, then that means he will consider about many other factors some of which has two or three steps more for being successful in the attack.

According to the test results, there is no such a technique that works great on a specific age range or education levels. Every decision path has its own characteristics. This means the chosen approach, technique and the age range will differ according to the target, which has high diversity.

For instance if a social engineer decides to attack to an organization by "system checking" or "comparing" by considering approach, education levels and the age factors; s/he then better consider the which age range will suit to be a target. Looking at the figure, we can say that he better to choose 18-25 or 36-60 age range people, with 80.4 % relative success probability rather than 26-35 age range. In this path there was no need to consider about the education level of the target. But that is not the case always as in the following example.

If the social engineer decides emotional blackmailing as an attack approach, first step of his will be considering the education level of the target. If the target is undergraduate, then there is no more steps to his/her decision. He will just start to his attack. On the contrary; if the target has higher education level, then will consider about the age range; 26-35 age range or 36-60 age range. According to results, 36-60 age range will be a better choice for him.

As it is shown in the decision tree of a social engineer according to our results, there are many possible paths. The paths will be chosen according to the opportunities of the social engineer, targets and environment even. Because the circumstances will differ, the chosen path will normally change too.

Another result that can be obtained from the decision tree is, when it comes to consider approach, age range and education levels together; while making a decision, under only "emotional blackmail; fake ID" node, the education level is considered to make a decision. Rest of all approaches, considering on just age range was enough to decide the highest relative successful probable path.

5.1.13 Technique – Age – Education Analysis

The figure below shows what possible paths will be when technique, age range and education levels are considered together by a social engineer.

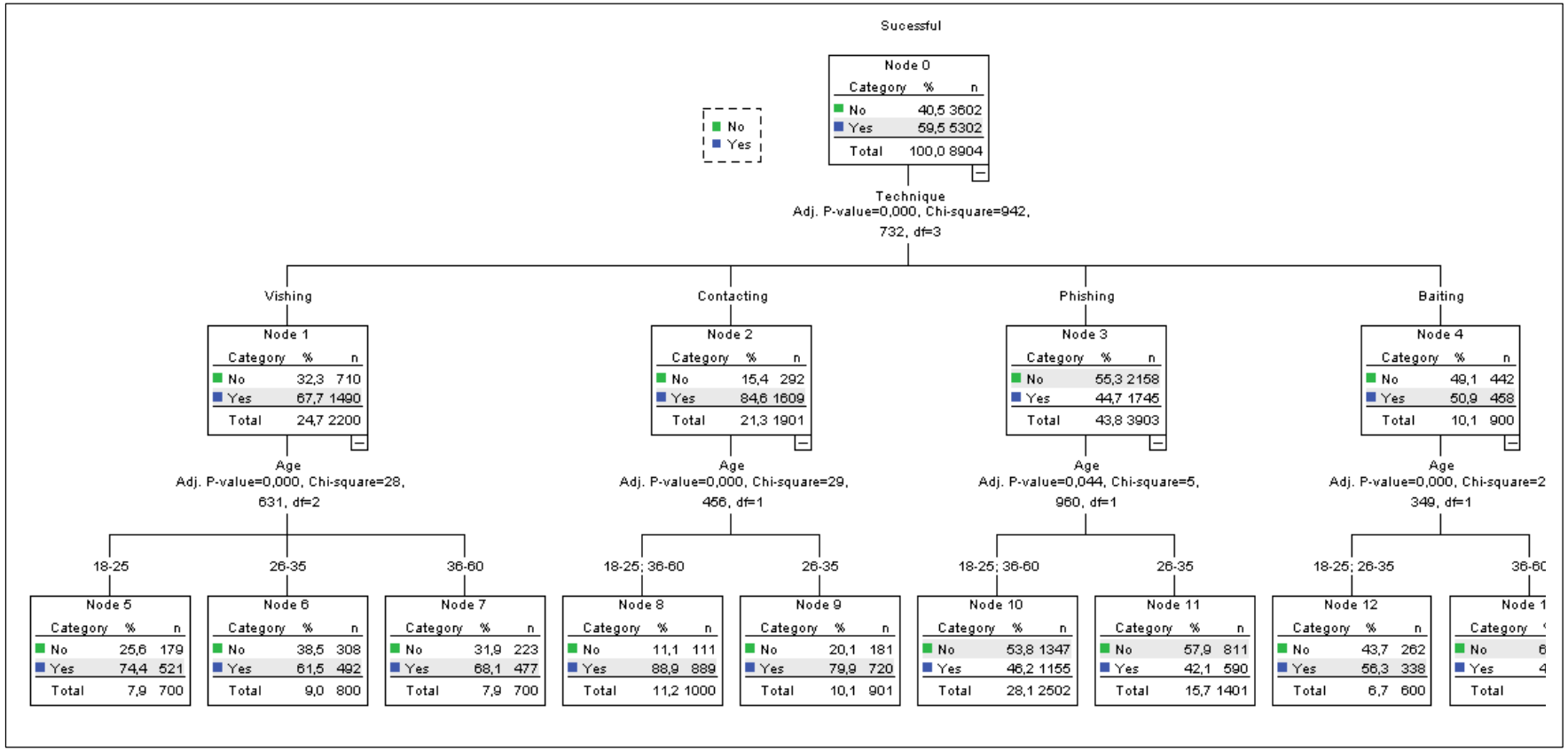

Figure 41 – Statistical Analysis on Technique – Age – Education

Here, as the figure shows, social engineers have many decision points in front of him/her when considered age, technique and education levels. And one can clearly see from the figure that all the selected technique has its own characteristics and there is no consideration about the education levels. The most successful technique is shown as "contacting personally" and the least successful method is depicted as "phishing" as shown in the figure.

For instance if a social engineer decides to attack to an organization by using "contacting personally", s/he then better to consider the which age range will suit to be a target. Looking at the figure, we can say that he better to choose 18-25 or 36-60 age range people, with 88.9 % relative success probability rather than 26-35 age range. In this path there was no need to consider about the education level of the target.

As it is shown in the decision tree of a social engineer according to our results, there are many possible paths. The paths will be chosen according to the opportunities of the social engineer, targets and environment even. Because the circumstances will differ, the chosen path will normally change too.

Another result that can be obtained from the decision tree is, if either contacting or phishing used as a technique, the 18-25 and 36-60 age range people are more vulnerable. When baiting is used in an attack, this time 18-25 and 26-35 age range people are more vulnerable. But when it comes to vishing technique, 18-25 age range people are the most vulnerable group against social engineering attacks.

5.1.14 Technique – Approach – Education Analysis

The figure below shows what the possible paths will be when technique, approach and education levels are considered together by a social engineer.

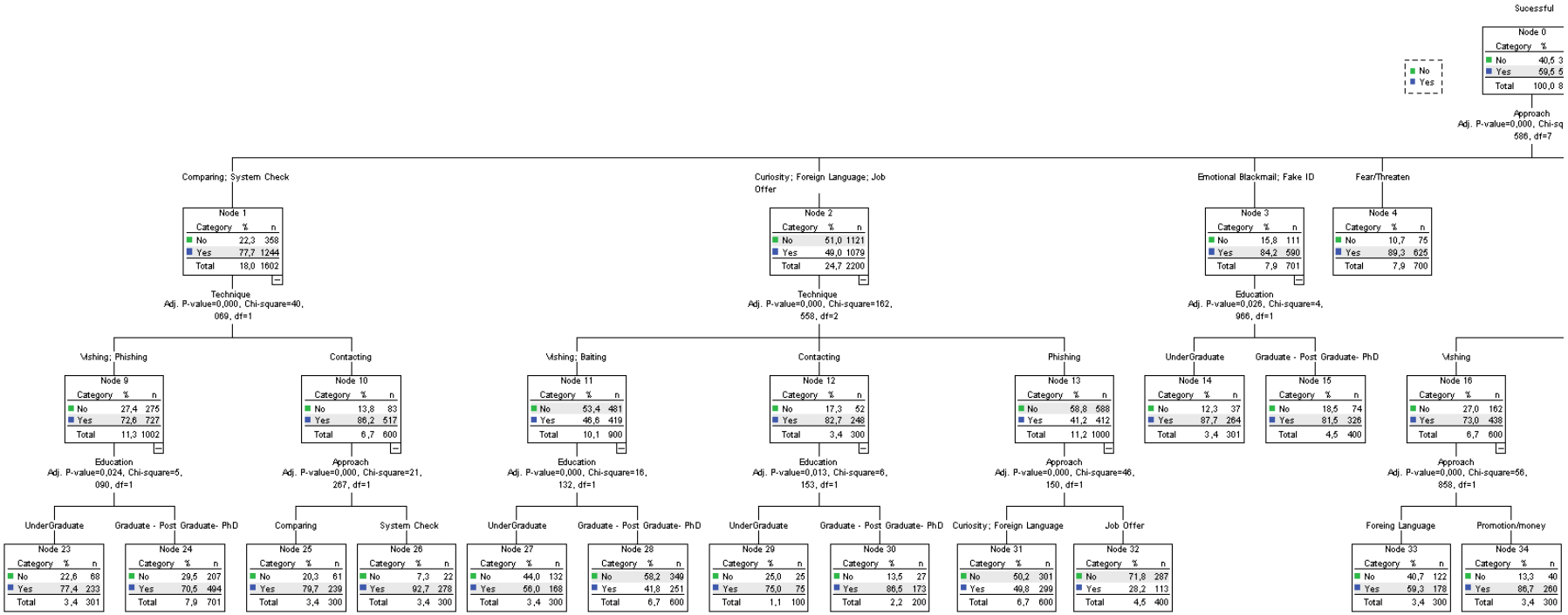

Figure 42 – Statistical Analysis on Technique – Approach – Education Level (1)

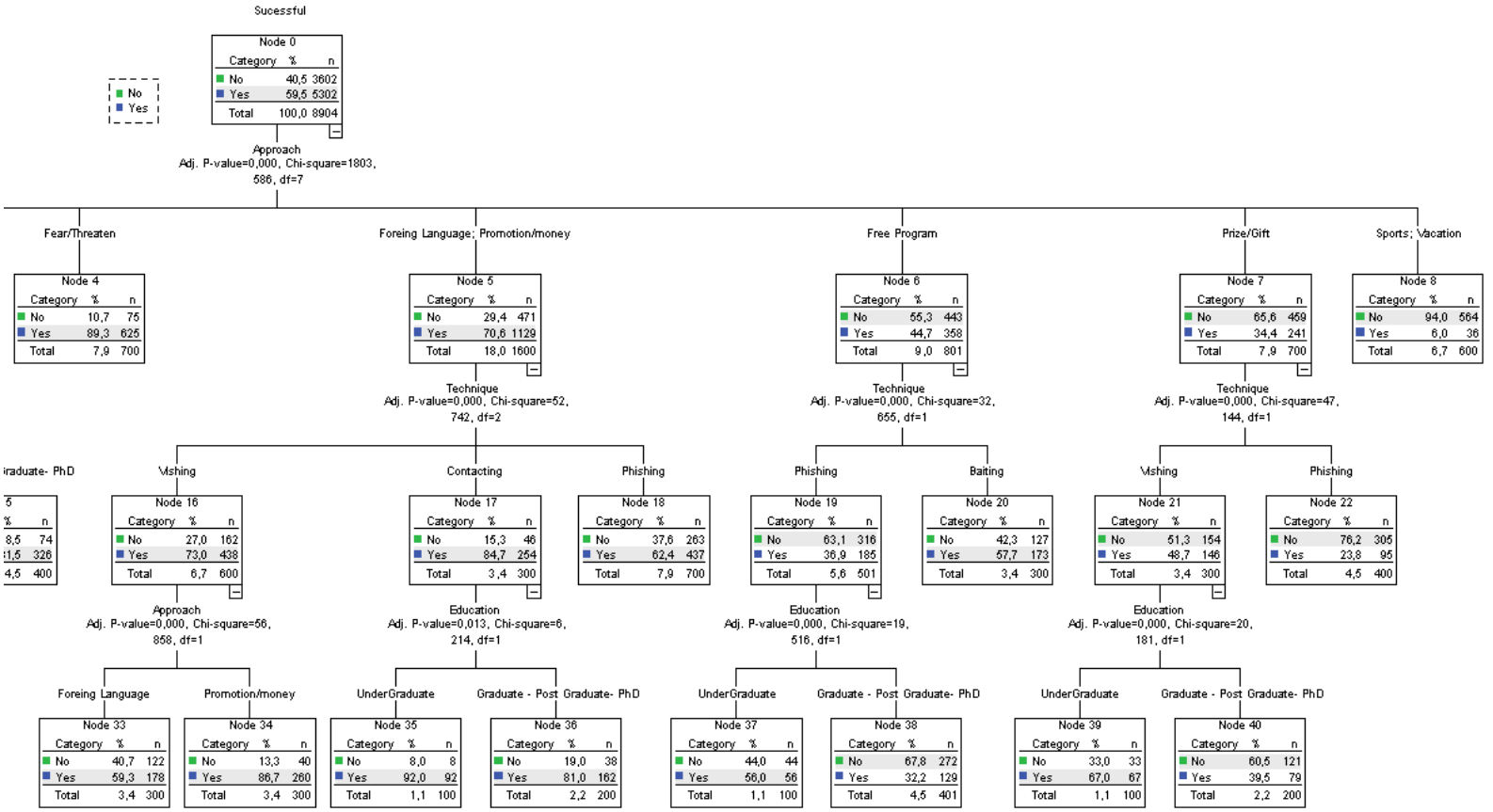

Figure 43 – Statistical Analysis on Technique – Approach – Education Level (2)

Here, as the figure shows, social engineers have many decision points in front of him/her when technique, approach way and age range are considered together.

One can clearly see that there are some approaches that has no connection with education level or technique used in threatening, offering vacation, or inviting to a favourite teams' match approaches. Among all these approach ways the most successful one is fear/threatening. Offering vacation, or inviting to a favourite teams' match does not work that much as the figure shows its relative success probability, just 6%. If social engineer decides other nodes, then that means he will consider about many other factors some of which has two or three steps more for being successful in the attack.

According to the test results, there is no such a technique that works great on a specific education level or with some other approach ways. Every decision path has its own characteristics. This means the chosen approach, technique and education level will differ according to the target, which has high diversity.

For instance if a social engineer decides to attack to an organization by "system checking" or "comparing" by considering approach, technique and the education level factors; s/he then better consider the which technique will suit for the target. According to results above, if vishing or phishing chosen by the attacker, then s/he will consider the education level of the target. But instead if s/he decides on attacking by contacting the target personally, then he will consider about the approach way again. Looking at the figure, we can say that he better to choose system-checking approach with a 92.7 % relative success probability.

Another result can be understood from the figure above is, the nodes that need second consideration, are all about the technique; not about the education level. Education level has always been the last factor to be considered when necessary.

As it is shown in the decision tree of a social engineer according to our results, there are many possible paths. The paths will be chosen according to the opportunities of the social engineer, targets and environment even. Because the circumstances will differ, the chosen path will normally change too.

5.1.15 Technique – Approach – Education – Age Analysis

The figure below shows what the possible paths will be when technique, approach, age range and education levels are considered together by a social engineer.

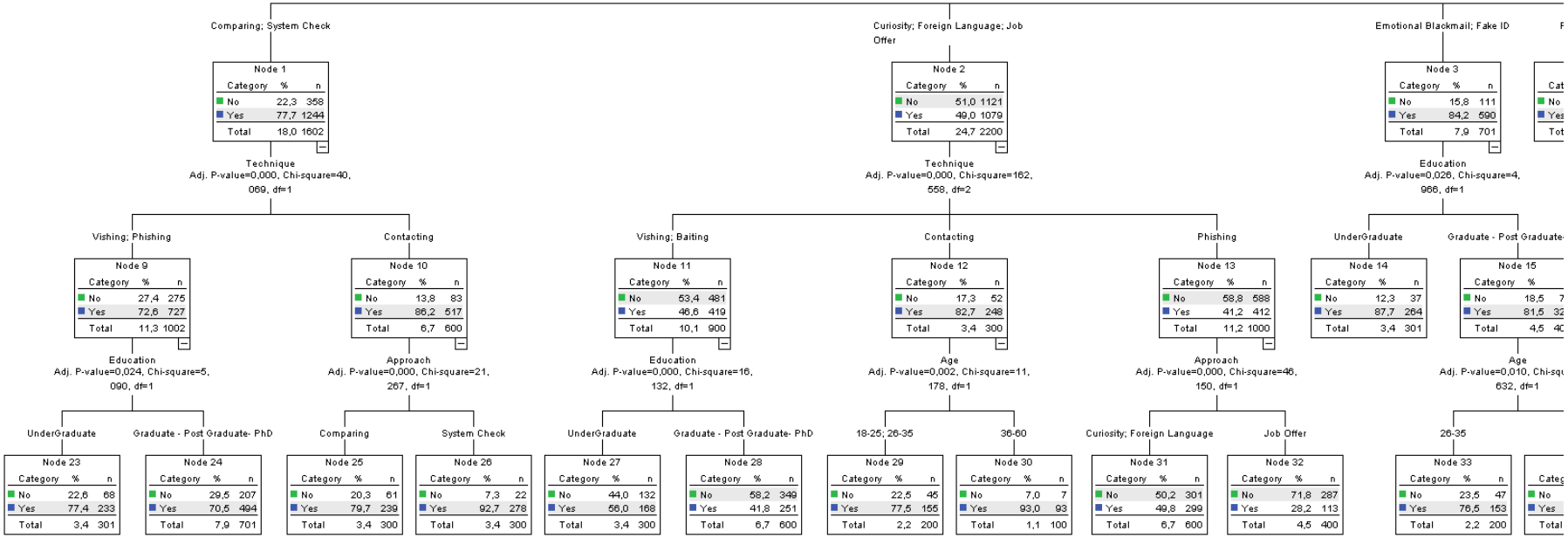

Figure 44 – Statistical Analysis on Technique – Approach – Age – Education Level (1)

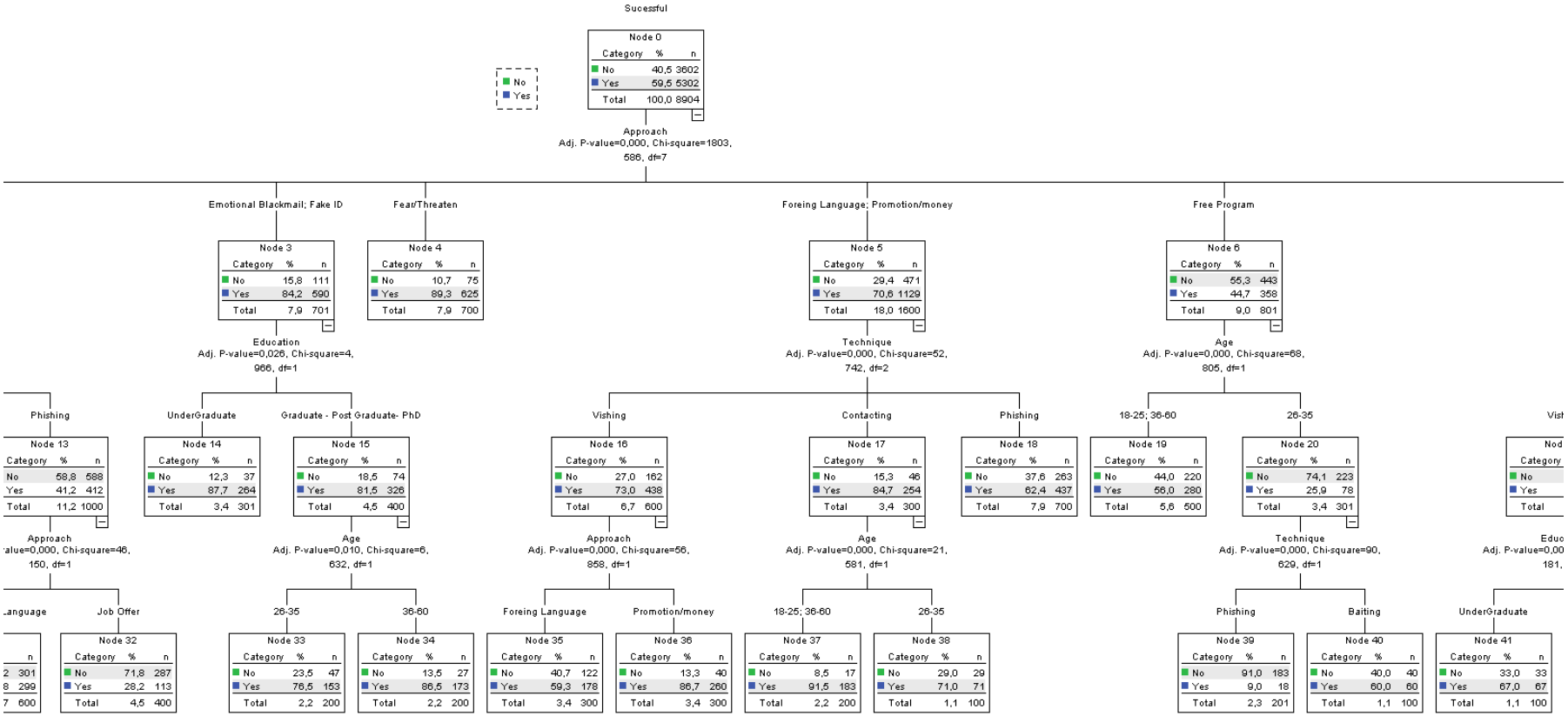

Figure 45 – Statistical Analysis on Technique – Approach – Age – Education Level (2)

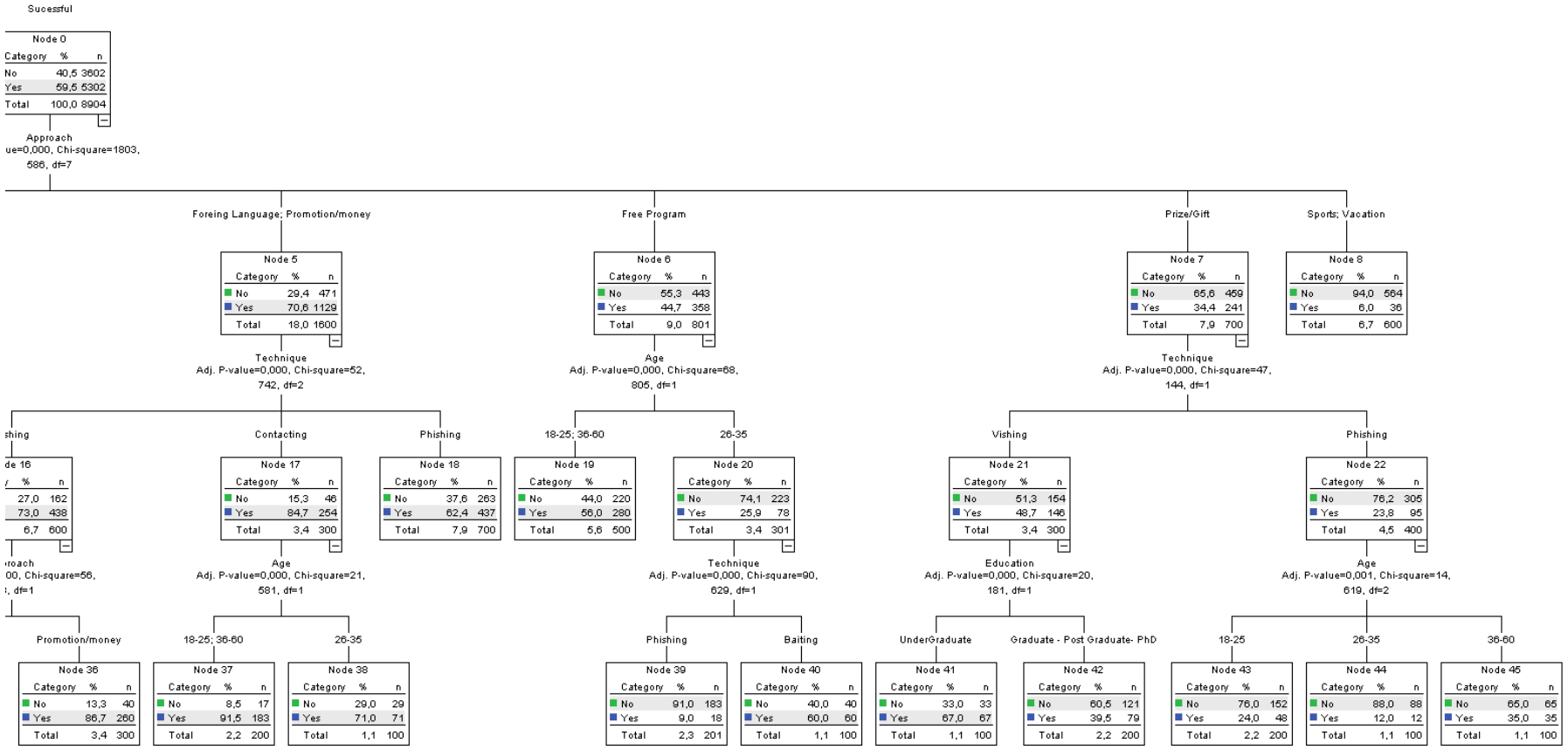

Figure 46 – Statistical Analysis on Technique – Approach – Age – Education Level (3)

Here, as the figure shows, social engineers have many decision points in front of him/her when technique, approach way, education level, and age range are considered together.

One can clearly see that there are some approaches that have no connection with education level or technique used like threatening, offering vacation, or inviting to a favourite teams' match. Among all these approach ways the most successful one is fear/threatening. Offering vacation, or inviting to a favourite teams' match does not work that much as the figure shows its relative success probability, just 6%. If social engineer decides other nodes, then that means he will consider about many other factors some of which has two or three steps more for being successful in the attack.

According to the test results, there is no such a technique that works great on a specific education level or with some other approach ways. Every decision path has its own characteristics. This means the chosen approach, technique and education level will differ according to the target, which has high diversity.

For instance if a social engineer decides to attack to an organization by "system checking" or "comparing" by considering approach, technique, age range and the education level factors; s/he then better consider the which technique will suit for the target. According to results above, if vishing or phishing chosen by the attacker, then s/he will consider the education level of the target. But instead if s/he decides on attacking by contacting the target personally, then he will think about the approach way again. Looking at the figure, we can say that he better to choose system-checking approach with a 92.7 % relative success probability. Here although age range was under the consideration, there was no need to use that here.

As it is shown in the decision tree of a social engineer, according to our results, there are many possible paths. The paths will be chosen according to the opportunities of the social engineer, targets and environment even. Because the circumstances will differ, the chosen path will normally change too. Other possible paths that could be chosen by the attacker can be seen in the figures above.

5.2 COUNTER MEASURES

Now that we are clear on what social engineers can accomplish, it will be better to review what can be done to keep them out of the organizations. According to the results above, the following counter measures may be taken to lessen the likelihood of the attack types related to social engineering. As mentioned in the report, social engineers are not just sending emails and waits for their victim to click on a link.

- **Build strong corporate security policy:** If the rules are clear and strict, it will be easier to control your security level. The rules being obscure will let the employees to take initiatives about giving decisions that may end up with a successful attack. The security policy of an organization should include every detail about each position about cyber security. There must also be some measures taken if a user ignores any of the security rules. These kinds of measures will affect the behaviors of the employees and will increase the security level of the organization.

- **Be careful about any email from untrusted sources:** After receiving an email that seems from someone not familiar, better to just right click and delete. If you believe the mail is sent from someone who you know, then check out the links s/he is trying to direct. The links may be directed to a fake site that is under control of the attacker. You can check it with keeping the mouse on the link without clicking it, looking left bottom corner of the page. Don't forget the phishing technique is the easiest way to get some information for a social engineer.

- **Do not trust easily:** If someone is really too "good" towards you without any reason, better you feel suspicious about him/her. Think always that no one is eager to solve your problems and take you to your favourite team's football match for free. Be aware always there can be some people around who may try to access your system that you are responsible for.

- **Do not hesitate to ask or talk to them:** Just doing your job and being polite to others without getting out of the security policies will be enough for some tailgating like attacks. It is clearly declared in security policies about under what circumstances you cannot or should not let a stranger into the building you are responsible for. Don't forget that you are a member of a system. In order to protect that system, do your job very carefully with no exceptions. If someone comes and says he is in a hurry and does not have time, just don't change your attitude. Keep doing your job and never be rude to anyone incase s/he is right. They may wait for your checking for the credentials. Don't behave so brave against these kind of people.

- **Always keep your stuff safe:** Your laptop, desktop, files, documents should be locked somewhere or their security should be considered when you are out. You should consider this even when you want to smoke outside or just to see a colleague in the same room. While leaving your desk keeping stuff secure should be a habit. Just one more glance will do the job.

- **Update your anti-virus software:** No AV solution can defend against every threat that seeks to jeopardize users' information, but they can help protect against some. So better to take the countermeasures as much as we can. Against technical attacks, this measure will help the system to be more secured to some extent.

- **Test your people**: There should be a mechanism that tests the awareness level of the personnel including the administrators. Actually they are the one who has more critical information about the organization. That pool of information will make them a potential target for a social engineer. Actually social engineers are seeking for valuable information they would abuse. According to test results, there should be training programs concentrating on vulnerabilities that will help to increase the awareness level of people.

- **Don't work on private stuff in public spaces:** This will make you a great target of a social engineer. If you've got to work on private stuff in public, consider a laptop privacy filter. Of course bear in mind that an experienced shoulder surfer will see a privacy filter and rightly assume you're working on something sensitive. In the end you will be one of a social engineer's target. So better not to work private issues in public places like coffee shops or bars. Keep your stuff secure in your organizations with physical or non-physical measures like locking your stuff or using strong passwords.

- **Be aware of the social media profile**: If you use social media, be careful about the profile you present and tone it down if necessary. Keep in mind that someone with bad intention may exploit any of information there. Just filter the information you present with "necessity" manner. Social media is social engineers' paradise. They don't need to make any investigation or choose many complex and risky techniques to gather information about their victims with the help of these sites. Many people love to share everything in detail even what they are doing in every moment. And there are many also who love to share negative issues about their organizations. Those kind of information will make a social engineer to know about the vulnerabilities much more about the company. So these kind of shares will make the social engineer's job easier.

- **Be careful about the stickers and badges:** If you are working in a critical organization like police department, don't leave your stickers or batch around, including your car's windshield. Any social engineer may copy it or know what your position is in your company. That will be a great opportunity for a social engineer to have some knowledge about your company and your position there. This does not have to be a critical information indeed. This ignorance even may lead a social engineer to pretend as if he knows you giving your name and position to the security guards. Don't use stuff that makes clear your identity. Don't wear company logos and remove extraneous markings and information from your mobile computing devices, especially if your company name might entice an adversary.

- **Be careful about your talks about work:** You don't have to talk about your work with strangers when you are out of your organization. If you have to talk about the work you do, then be careful about the words you use, because, a social engineer may abuse those against you or your organization.

- **Shred unnecessary document:** Shred everything you don't need any more or the documents especially if they are classified. While shredding, choose a good device otherwise those pieces may be combined again with some simple programs if not shredded well. Don't put documents in the trash in one piece. This will protect you against dumpster diving attack types to some extent.

- **Keep your stuff physically secured**: Keep in mind that no matter how secure your locking systems may be, you should always keep your keys out of sight of the bad guys. This

will even be a negative perception if a social engineer is around. It will give an idea about security level is high in the organization and that will affect the attacker's behaviors and decisions. Using multiple cameras with fully overlapping views may also dissuade the attacker and may prevent some attacks to some extent. Even fake cameras will do a great job against physical attacks.

- **Shut down shoulder surfers' watch with your angles:** Don't put yourself in situations that invite shoulder surfers. Position your back to the wall when using your machine, and never leave it unattended. When entering sensitive data, create some sort of barrier between the keys and wandering eyes. This might require you to reposition your body, or create a shield with your spare hand.

- **Be careful against tailgaters:** Block the tailgaters and don't let them in. If someone you don't recognize attempts to tailgate behind you, just don't allow and ask for the credentials. Keep in mind that asking for authorization is not a rude behavior. In addition, be careful at the smoking areas, as those places are more prone to these kinds of attack types. Bear in mind that this attack type may also be applied by using cars too.

- **P2P software:** Many social engineers have been using P2P programs, as they know what the people seeking for. Because it is a free platform, most people love to use these programs that provide free service. If you have to use some programs, you better be careful before doing so. Not using this kind of sharing programs is the best way normally.

5.3 RESERACH CONTRIBUTION, LIMITATIONS AND FUTURE WORK

Over the past several years, the incidents of social engineering tactics used in cases of fraud and data breaches have continued to increase. IT personnel should discuss the "security issues" under umbrella of brainstorming activities. They better figure out what can be a good reason for a social engineer to enter their system. Along with a list of possible goals of that engineer, preventative measures and training should be implemented. Only thinking like a social engineer will be more productive and successful precaution for the companies, ministries and organizations.

For many directors, managers, chiefs etc. if there is a good technical precaution then it means their system is secure against the attacks. Moreover; there is no such a 100% secure system in cyber world. Considering that cyber-attack types are being updated in every second, feeling secure will be so optimistic approach towards these attacks. This situation can be defined as "I'm safe" syndrome that many people have in most of the organizations. Although this syndrome's reason may vary from having not much knowledge in this field to trust issues, the main idea and the result is the same. As they "feel safe" it becomes hard to think of alternatives and their facing a compromised system one day becomes inevitable. In addition; regarding that social engineering; simpler, easier but highly effective technique; is being applied professionally nowadays, this syndrome makes the systems more vulnerable.

Social Engineering tactic and techniques are being applied towards the target victims in a chained steps manner. The basic issue which lays down under these kinds of non-technical attack types is gathering information which can be obtained in many ways. After getting

needed information for an attack, there is no need for waiting for a social engineer to exploit the target system.

Social Engineers have been abusing the four most important vulnerabilities in human being, which are careless trait, comfort zone, desire to help and fear. If they can take advantage of at least one of these vulnerabilities, it means a high probable success attack. As it was clearly shown in the findings section of this thesis, the "fear" part is dominant for our participants. Furthermore; considering that Turkish society does not trust the "judgement" according to the report shown in section 2.4, it will be make social engineers to focus on this vulnerability in Turkey.

According to the research results applied; the most important findings are listed below:

- Gathering valuable and necessary information is the first step of many successful social engineering attacks. Without pretexting, these kinds of attacks will not be that much successful.
- Participants get afraid when they heard a sentence like "there will be a prosecution in court in following days" and they force themselves to act immediately, which mostly ended up with a successful attack.
- Among the attack types; rather than baiting or phishing, talking personally and vishing are more successful results because these techniques are giving a chance to social engineer to adjust his/her behaviors according to target's responses and reactions.
- Blaming, threatening and showing a fake id worked on our participants. The security personnel sometimes even took the investigation stage as a losing time. Rather than investigating, trusting and taking risk sounded more logical for many participants in the research.
- Promotion, money offers, rewards are good incentives. The attacks, which were applied to these fields, had highly successful rates. This behavior is related to "comparing" trait because this is a chance for people to be pointed by others' fingers.
- Offers like "sending the target to vacation" which requires time to get use of, are not good incentives. Participants mostly prefer the "shortest way to success" and they don't like to wait. Offers like "learning a foreign language in 3 days" were more attractive for the participants when compared to offering for a vacation with family members.
- According to research results, the success is not related to how aged the victim is or how high level education s/he took. Because social engineering is about the vulnerabilities of human operating system, it comprises generally people as a whole. This means "people who got higher level education, they are susceptible to cyber-attack types" hypothesis can be wrong in some cases. Indeed some social engineering attack types like "whaling" are directly applied to higher level educated people and the success ratio is not that low. "I'm safe" syndrome can be seen as a reason for this success level.
- There is a significant relationship between the approach way towards the target and used techniques. So this means it is so important for a social engineer to choose the right technique for the right person to make a successful attack. This result also shows that there are exactly some methods for some techniques and each approach way are being chosen according to the technique used. It is also very crucial here to

mention that gathering information about the target will make it clear which technique and approach will be applied.

- Participants were too understandable, respectful to others but did not like to work under time pressure. When it comes to finish even a little task, if they are given some limited time, they ignored some precautions they should apply although they knew their stuff very good.
- Even the reason would be nonsense, as it was shown in the context, it makes the social engineering attack types more successful. People are waiting for any reason to change their behaviors.
- When compared by others, many participants ignored the security policies and took risks. When a security guard was being compared by someone else, some guards changed their decisions and allowed the attacker to get into their facilities. This comparison includes the time concept too. For instance after giving a reason like "I had already be able to get inside of the facility 2 days ago", there have been many participants changed their ideas and even did not bother with checking the attackers' credentials.

The limitation of this thesis was the number of people we could reach. We were able to reach just 3994 people in 10 months during our research. So the results and findings are valid for our participants; not generalizing the Turkish society. But we did our best to test from every education level and age of range as much as we could to resemble the society.

In this thesis, cultural characteristics and differences were not included. The research was limited by Turkey, in Ankara. Including cultural characteristics and revealing the differences between them in terms of social engineering attack types can be seen as a future work of this thesis. Investigating these findings under cultural characteristics will contribute many international organizations in a positive way about social engineering attacks.

REFERENCES

Andrew Whitaker. (2009). *Top 10 Social Engineering Tactics*. Retrieved from http://www.informit.com/articles/printerfriendly/1350956

Durrett, C., & Trull, T. J. (2005). An evaluation of evaluative personality terms: a comparison of the big seven and five-factor model in predicting psychopathology. *Psychological Assessment*, *17*(3), 359–368.

Gençöz, T., & Öncül, Ö. (2012). Examination of Personality Characteristics in a Turkish Sample: Development of Basic Personality Traits Inventory. *The Journal of General Psychology*, *139*(3), 194–216.

Global Politika ve Strateji. (2015). *Türkiye Toplumsal Eğilimler Anketi*. Ankara.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshops*, 236–250.

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. *The Art of Human Hacking*,

Hasan, M., Prajapati, N., & Vohara, S. (2010). Case Study on Social Engineering. *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks*, *2*(2), 17–23.

Hmmm has my credit card number been stolen. (2015), http://imgur.com/gallery/N5084p6

Infosec Institute. (2014). Guerilla Psychology and Tactical Approaches to Social Engineering. Retrieved from http://resources.infosecinstitute.com/guerilla-psychology-tactical-approaches-social-engineering-part/

Karakasiliotis, a., Furnell, S., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. *Information Warfare and Security Conference*, 60.

Kvedar, D., Nettis, M., & Fulton, S. P. (2010). the Use of Formal Social Engineering Techniques To Identify Weaknesses During a Computer Vulnerability Competition. *Journal of Computing Sciences in Colleges*, *26*(2),

Mataracioglu, T., & Ozkan, S. (2011). User Awareness Measurement Through Social Engineering, 1–7.

SANS Institute. (2004). Global Information Assurance Certification Paper. Retrieved July 23, 2015,

Sapuan, M., Emo, R. E. M., & Irty, G. a M. E. D. (2012). Social Engineering-Based Attacks: Model and New Zealand Perspective, 847–853.

Sarah Granger. (2001). Social Engineering Fundamentals.

Scott Pinzon, K. D. M. (2007). No Tech Hacking. Retrieved July 23, 2015,

social-engineer.org. (2015). What is Social Engineering.

Thornburgh, T. (2004). Social engineering: the dark art. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 133–135.

Verizon. (2012). *Verizon 2012 Data Breach Investigations Report*.

Wilkinson, L. (1992). Tree structured data analysis: AID, CHAID and CART. *Proceedings of Sawtooth Software*, 1–10.

CIRRICULUM VITAE

Name: Adem TOSUN

E-mail: h015859@yahoo.com

1. DEGREES

2011 Computer Engineering Certificate, Hacettepe University, Ankara TR
Thesis Title: ISRAM: Information Security Risk Analysis Method
2005 Turkish Military Academy, Ankara, TR

TEZ FOTOKOPİ İZİN FORMU / THESIS PHOTOCOPY PERMISSION FORM

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐
Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☐
Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐
Enformatik Enstitüsü / Graduate School of Informatics ☑
Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname : TOSUN
Adı / Name : Adem
Bölümü / Department : INFORMATION SYSTEMS

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English):

A SURVEY ABOUT THE INTEGRATION OF SOCIAL ENGINEERING ATTACKS AND CYBER SECURITY POLICIES EXPLOITING CULTURAL VULNERABILITIES IN TURKEY

TEZİN TÜRÜ / DEGREE: Yüksek Lisans ☑ Doktora ☐

1. **Tezimin tamamı dünya çapında erişime açılsın ve kaynak gösterilmek şartıyla tezimin bir kısmı veya tamamının fotokopisi alınsın.** / Release the entire work immediately for access worldwide and photocopy whether all or part of my thesis providing that cited. ☐

2. **Tezimin tamamı yalnızca Orta Doğu Teknik Üniversitesi kullanıcılarının erişimine açılsın. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.)** / Release the entire work for Middle East Technical University access only. (With this option your work will not be listed in any research sources, and no one outside METU will be able to provide both electronic and paper copies through the Library.) ☐

3. **Tezim bir (1) yıl süreyle erişime kapalı olsun. (Bu seçenekle tezinizin fotokopisi ya da elektronik kopyası Kütüphane aracılığı ile ODTÜ dışına dağıtılmayacaktır.)** / Secure the entire work for patent and/or proprietary purposes for a period of one year ☑

YAZARIN İMZAZI / Signature: **TARİH** / Date: