Social Engineering and Awareness Training

Capstone

Jose A. Arroyo Cruz

Walsh College Master of Science Information Assurance

December 6, 2010

Tables Contents

Introduction

The rapid growth of strong technological control measures used to protect information technologies has forced attackers into exploiting creative ways to fulfill their purpose. The creative attacks are centered on the not so technological aspects of information technology, which are “humans”, often called the weakest link. Network users are being targeted to provide essential information, which would ease a technical attack. In the information security field, social engineering is defined as: “an attack in which an attacker uses human interaction to obtain or compromise information about an organization or its computer system.” (US-CERT, 2009)

“On Wednesday, a man dressed as an armored truck employee with the company AT Systems walked into a BB&T bank in Wheaton about 11 a.m., was handed more than $500,000 in cash and walked out, a source familiar with the case said. It wasn't until the actual AT Systems employees arrived at the bank, at 11501 Georgia Ave the next day, that bank officials realized they'd been had” (Schneier, 2008). It is very probable that bank had many security controls like: metal detectors, security cameras, security officer, and man trap doors among others. None of these technical controls stopped the thief from stealing five hundred thousand dollars from the bank like if nothing ever happened. The art of deception can be found in many ways and thanks to the human response most of the social engineering skills are very successful. The authors of *A Case Study in Social Engineering Techniques for Persuasion* (Hasan, Prajapati, & Vohara, 2010) compile a very good set of skills found in a social engineer. Types of skills required by a social engineer:

1. Impersonating staff: this is the art of inventing a scenario to persuade a target to release information or perform an action
2. Playing on user sympathy: the social engineer may pretend to be a worker from outside, “the nature of people is to help someone that is in trouble.”
3. Intimidation: social engineers may need to turn to stronger stuff like intimidation depending on the response of the target.
4. Hoaxing: a hoax is an attempt to trick people into believing something false is real.

5. Creating confusion: this one involves creating a problem and then take advantage of it.
6. Dumpster diving: checking junk mail or routine mail looking for information. Usually in trashcans or corporation's dumpsters.
7. Reverse social engineering: get others to ask you questions instead of you asking them.
8. Email: the use of an interesting subject line can trigger an emotion that leads to accidental participation from the target.
9. Phishing: in this technique version of a scam, the consumer receives and email design in a way that looks like an email from a legitimate company, mainly to change passwords, or retype personal information in order to protect the account

Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. (US-CERT, 2009) A recent phishing scam event happened on Comerica bank in Michigan when a spoofed email from another corporation gave the cyber criminal enough information to wire transfer 1.9 million dollars out of Comerica to different accounts. In *The Curious Case of EMI vs. Comerica* (Navetta, 2010) the author explains how an EMI employee received a phishing attack tricking him to give out his login credential. EMI employee mentioned that the fake email allegedly looked very similar to the emails sent by Comerica Bank. Comerica uses a strong authentication mechanism to authenticate users, a token-based 2-way factor authentication system that was not enough to stop the attack. This control mechanism is what they call in the technical field an industry standard, meaning almost every bank uses the same method of authentication because of its secure factor. "This case raises several interesting legal issues. In fact, this case could ultimately illuminate how courts view the scope of a "reasonable security duty." (Navetta, 2010) If the bank of Comerica was using all highly recommended industry standards as their control mechanism, and the phishing scam was performed on EMI, why are they still

liable? I guess we are going to have to pay close attention to this case; which by the time of the completion of this report, the case has not been yet resolved.

Social engineering bypasses all software and hardware security controls by targeting humans; which are the computer users, making it very difficult to control information leakage. Experts believe that awareness and training are necessary tools for fighting social engineering attacks. This research is part of an effort of understanding security awareness programs and why are they not been effective.

Background

The world has known about social engineering techniques since the time of Greek mythology. The Trojan horse is a good example that represents how effective can be to trick someone, and according to some, Prometheus is one if the oldest social engineer. "According to Greek mythology, humanity's proficiency in social engineering today is probably a direct result of its greatest mentor: Prometheus, who was so skilled in this craft that he could trick Zeus, the king of gods." (Dang, 2008) Prometheus was recognized for his ways and tricks. The creation of man is accredited to him by molding him out of clay. This trick was known as the "Trick at Mecone", here Prometheus offered Zeus with two choices, to finish once and for all the disagreement between mortals and gods. One of he choices was ox meat stuffed inside an ox's stomach, and the other was an ox bone covered with shining fat. Zeus chose the second option and as a result humankind would only have to make sacrifices to bones and fat gods. Zeus selection freed humankind from having to make sacrifices to the gods. Even though this is just a myth someone must have thought of this and passed it along. Meaning that those malicious intentions of tricking someone to comply with your wishes go back to the eight century. Somehow it can be said that the world has failed to mitigate social engineering attacks. Kevin Mitnick tells the story that goes back to 1978 about a man called Mark Rifkin, "... pulled the biggest bank heist in history- and done it without using a gun, even without a computer." (Mitnick, 2002, p.4). One would think that living in the information

age[1], organizations would be more aware of such old methods to compromise an information system. It has been proven that as time progresses, the human factor still remains the weakest link in organizations.

Every year, there is a hacking conference where all sorts of security professionals and enthusiast meet to talk about the latest news on information security and hacking. The conference is called Defcon. The 18th meet took place this year in Las Vegas, called Defcon 18. In Defcon 18 the people of social-engineer.org, lead by Christopher Hadnagy[2], who is a subject matter expert, organized a social engineering capture the flag (CTF) contest. In this event the Fortune 500 companies were the target; and from the results, the contestants found very little resistance to social engineering attacks. The goal of the capture the flag event in Las Vegas was to create a higher level of awareness to this type of threat. What makes this event important is the fact that it was the first time that social engineering tactics have been put in display for the public.

In this CTF event the contestants where assigned a company and where given two weeks to perform information gathering using passive techniques to built an organization profile. No direct contact was allowed during this time. The direct contact was going to take place in the conference and each contestant was allowed 25 minutes to call target and collect as many flags as possible. To make the contest as less invasive as possible the flags that were targeted had to be non-sensitive information flags. Each flag was appointed with a value according to the level of difficulty.

There are several things that make social engineering a big threat to an organization, and the ease of information gathering is one of them. Corporations spend a lot of time and money into protecting information: intrusion detection systems (IDS)/ intrusion prevention systems (IPS) systems, firewalls, corporate anti-virus systems, employee training and constant monitoring, amongst others. However they have failed to constrain all the information that is available in the Internet. Finding enough information to create an organizational profile before a social engineering attack has become much easier now with information sources that are available to everybody. Sources like Twitter,

---

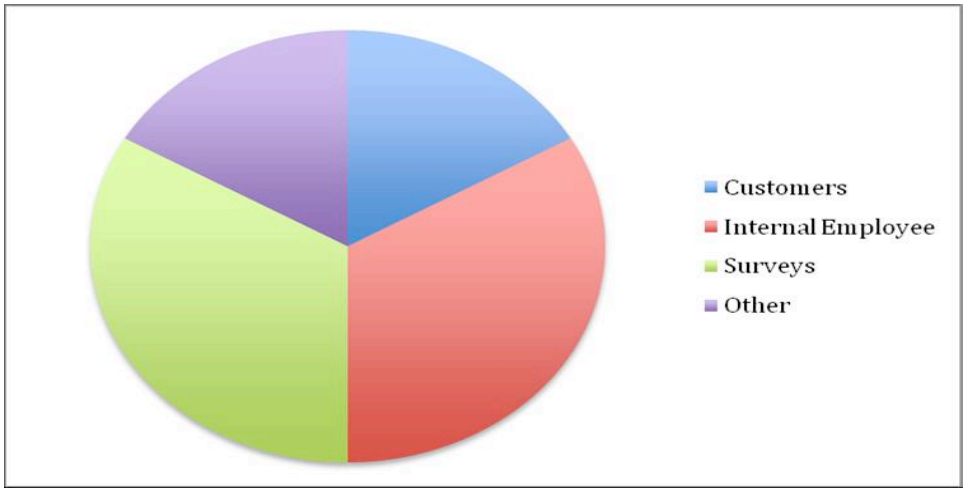
[1] Information Age is the period beginning around 1970 and noted for the abundant publication, consumption, and manipulation of information, especially by computers and computer networks. (TheFreeDictionary, 2009)

[2] Christopher Hadnagy is a professional social engineer and author of *Social Engineering: The Art of Human Hacking*

Google, LinkedIn, and Facebook are some of the most commonly used tools to passively create organizational profiles that would be later used by a social engineer to carry out their attacks. In the Defcon 18 CTF event, information gathering using these mechanisms was crucial. From the social media perspective one of the services that has been overlooked is LinkedIn. LinkedIn is mainly used for professional networking. LinkedIn provides complete layouts of company profiles providing relevant information for a social engineer. "LinkedIn is a service that has not received as much popular attention, but in the context of the CTF event was far more useful than any other single information source." (Hadnagy, 2010) This depicts the fact that there is much information leakage found in the social media network; and since this is a new growing industry, organizations have implemented very little control mechanisms over this subject.

Once a social engineer collects all the information needed, he can design an attack based on the information gathered from the specific target. In Defcon 18 the phone call pretext method was the main attraction. In figure 1 we can see a graphical representation of the most successfully used pretext:

Figure 1: Successful pretext used in CTF

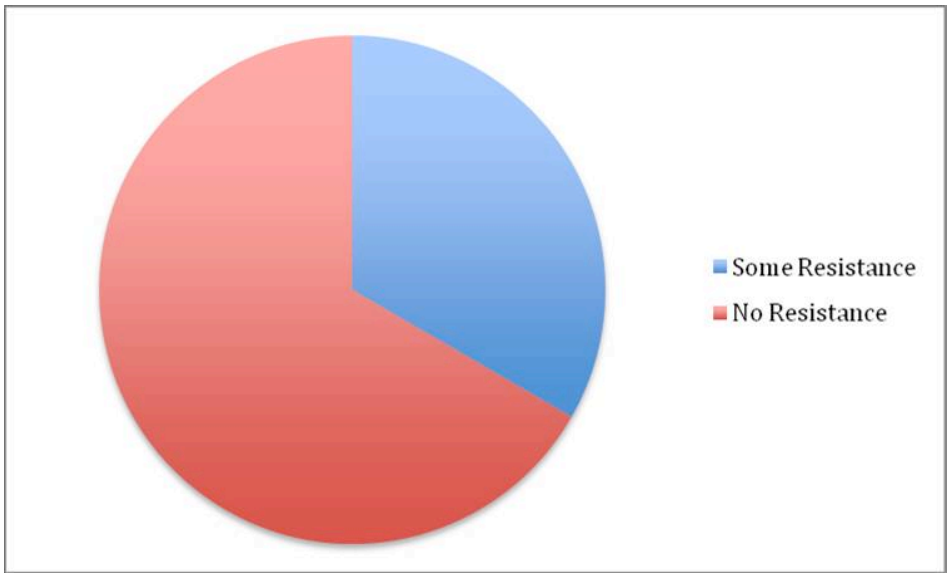


As you can see form the chart internal employees are the main contributors to this attack vector followed by the typical "fill out this survey to win a iPad" phishing scam. The biggest contribution made by this event is pointing out that in this day of age; the year 2010, Fortune 500 companies (BP, Shell, Google, Proctor & Gamble, Microsoft,

Apple, Cisco, Ford, Coke, Pepsi, Wal-Mart, Symantec, Philip Morris, Dell, and Verizon) with information awareness training and expensive technical control mechanism failed to provide a control against one of the fastest growing form of attacks, known as social engineering.

"Unfortunately throughout the course of the contest, the number of times contestants encountered any degree of resistance was rather minimal. In tallying these results we took a very liberal approach on classification of resistance. According to our analysis, the results show that in the calls that were made, awareness training was not effective within the targeted organizations." (Hadnagy, 2010) Figure two is a graphical representation of the amount of resistance found in the CTF event.

Figure 2: Resistance Found on CTF pretext based attack



It is evident that very little resistance was found over these attacks. The fact that this event is so recent brings great relevance to this capstone project. It is very clear that security awareness, even though implemented, is not effective. The intention of this project is to go deeper into understanding why is security awareness is not reaching the end user.

Kevin Mitnick in his book *The Art of Deception* (2002), talks about the effectiveness of technological controls and how they promote malicious attackers into performing social engineering attacks. The *Anti-Phishing Work Group 2010* (APWG,

2010) report indicated that the financial industry is still the leading target of phishing scams. Earlier, it was mentioned how Comerica Bank is on a legal case due to a phishing scam, and it all started with a user clicking on the wrong link in an email. People are not just the problem; it is important to understand they are part of the solution "many losses are not caused by a lack of technology or faulty technology but rather by users of technology and faulty human behavior" (Rotvold, 2008).

There are some surveys that target the decision makers on corporations, these surveys provide a clear perspective of the way corporations are reacting to information security trends. These surveys are: "Computer Crime and Security Survey" and "Global Information Security Survey". The main target in these surveys are chief information officers (CIO) and chief security officers (CSO) from but not limited to the United States. What makes this survey interesting is the fact that security awareness is analyzed from different perspectives. They also capture the level of understanding that all security professionals have on awareness, policies and procedures within their organization. The relevance of "The Global Information Security Survey"; and the "Computer Crime and Security Surveys", to this capstone project is that they all investigate how chief information officer act upon specific information security issues. The difference in these surveys and the capstone project is that the capstone project focuses more on the knowledge that users really need to identify a social engineering attack.

One of the surveys that we are going to be comparing is Ernst & Young Global Information Security Survey (GISS), this survey puts emphasis in new tendencies, although not directly associated with social engineering, it can be said that the new trends will ease social engineering attacks. "Over the last year, we have witnessed a significant increase in the use of external service providers and the business adoption of new technologies such as: cloud computing, social networking and Web 2.0." (Ernst & Young, 2010) 60% of the respondents in the survey believe that their level of risk will increase do to this trend. This is most alarming when you read that only 46% of the respondents acknowledge their investment in information security is increasing.

If the rest of the respondents are not doing any change, it means that 33% of them know that the risks is increasing and are not doing anything about it. If you combine the

results from this survey and compare it with the findings in the Defcon event, it could be said that lack of awareness is not the reason for lack of action against increasing risk. There was one question on the Ernst & Young survey that really hit the jackpot: "Compared to the previous year, does your organization plan to spend more or relative the same amount over the next year for the following activities?" (Ernst & Young, 2010) There were two specific responses that have great relevance to this project with very interesting results: security awareness training and security testing. 53% of the respondents said that their security awareness program was going to suffer no changes versus a forty two percent said they will adapt their security awareness program to the new trends.

The other activity that needs to be highlighted is security testing. Here, 58% of the respondents mentioned that they were not going to change their security testing methods, while a 36% said that they would adapt their security testing mechanism to meet new trends. This means that corporations understand the trends, but not necessarily will adapt to them. The main question that comes to mind is: if these chief information officers know the risk of the new trends; and possible solutions, why are they not adapting? Is it because of financial crisis or confidence on their actual control mechanisms? These are some of the things that this project will be paying attention to when it comes to providing possible solutions to the problem. The 2010 Ernst & Young survey was focused on social media networks and mobile computing. Even though the survey is not social engineering related, both social media networks and mobile computing are tools used by the social engineer. From the capture the flag event in Las Vegas, we learned that social media networks are one of the key elements used by social engineers to gather information about their targets. Now, when it comes to mobile media, the relevance relies in that mobile media is the tool used by some users to access social media networks. "In January 2010, 25.1 million mobile users accessed Facebook via their mobile browser, up 112 percent from the previous year."(comScore, 2010)

Social media networks are on a constant rise, "Active unique users of social networks are also up nearly 30% globally, rising from 244.2 million to 314.5 million collectively." (Nielsen, 2010) A representation of this in found on figure three.

Figure 3: Social Network traffic Feb 2010

Global* Social Network Traffic / Feb 2010			
Web Site	% Reach of Active Social Users	Sessions per Person	Time per Person (hh:mm:ss)
Facebook	52%	19.16	5:52:00
Myspace.com	15%	6.66	0:59:33
Twitter.com	10%	5.81	0:36:43
LinkedIn	6%	3.15	0:12:47
Classmates Online	5%	3.29	0:13:55

Source: The Nielsen Company

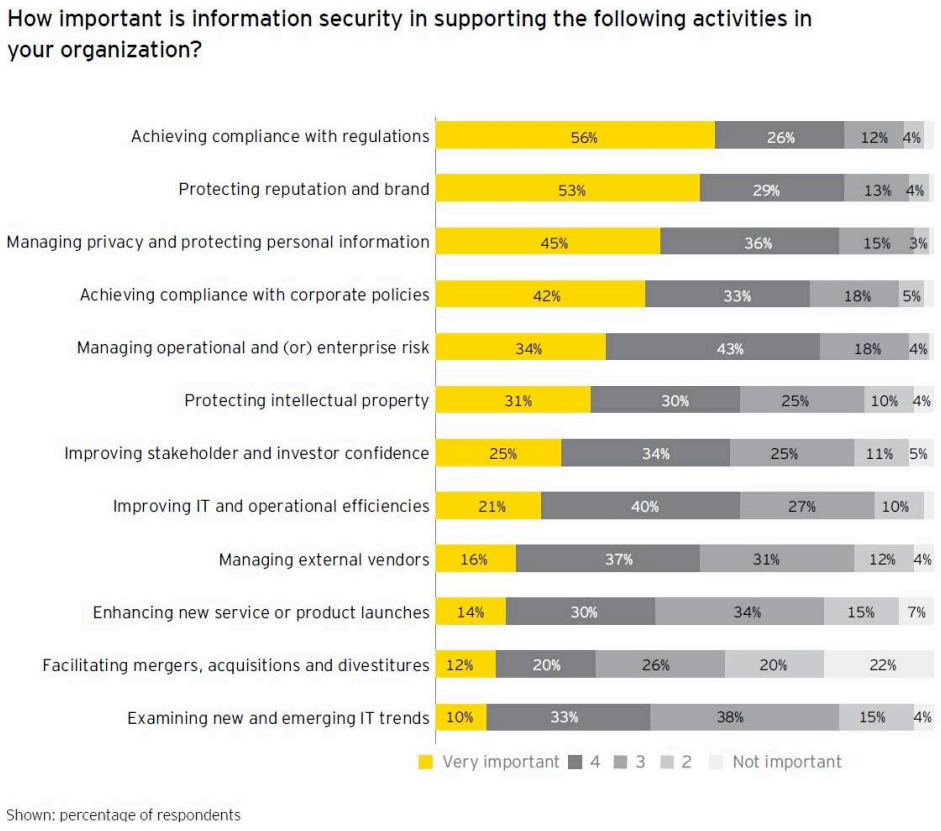
*United States, Brazil, Australia, Japan, France, Germany, Italy, Spain, Switzerland, United Kingdom

Unique audience represents active usage, not overall membership of social networks

Some organizations understand the high level of potential customers inside these networks and are starting to use them for strategic purposes to achieve business goals. “More than one-third (35%) of employers in the U.S. use social media to promote their company, according to a new Career Builder survey.” (Grasz, 2010) The question that we need to ask is: are they implementing the use of social media networks safely and responsibly? Ernst & Young reported that 33% of the respondents on their survey understand that social networking is a challenge to control and deliver proper security initiatives. Meaning that social networking is hard to control; and even though they understand there is a big risk, only a few organizations are actually doing something about it. If we take a deeper look at LinkedIn (the number one source for the CTF event in Las Vegas), there is a great deal of information that can be gathered from this site. A few examples are: tactical research data, complete organization charts, complete identity information, phone numbers, operating systems in use, network hardware in use, and name dropping, amongst others. Sometimes is just a matter of connecting the dots; if an organization has a profile where most of their network administrators are Cisco certified and Cisco experts; there is a big possibility that Cisco is the vendor used for network infrastructure in this organization. It is evident that most of the chief information officers are somehow not paying attention to the new trends when “only ten percent of respondents indicated that examining IT trends was a very important activity for the information security function to perform” (Ernst & Young, 2010). Figure 4 below shows some of the activities that are relevant to organizations where compliance with regulations and protecting brand reputations are the winners. These responses could be

very disturbing, and can be found counterproductive. If you do not know what it is that you need to protect against, then there is no need to bother with protecting reputation or complying with regulations. Security is an ongoing process and keeping the organization protected should be an everyday task. Compliance vs. security has been a never-ending debate in the information security world.

Figure 4: Security Activities in the organization.



As mentioned before the purpose of this paper is to comprehend the effectiveness of security awareness training in corporations, and understand why are they not been effective against social engineering attacks. Chief information officers are the decision makers and the people responsible for protecting information on their organizations; Ernst & Young's survey has showed us that even when a majority of them understand the new risks they face. In this survey 15% of the respondents said that they do not have an information awareness program, a 76% of them mentioned that their information awareness program reviews general awareness security topics, and only 21% of them

measure the overall effectiveness of the awareness program. Every organization has different needs and resources, it is important for the organization to understand their specific requirements. Each key area of an organization needs to be involved in the process of creating this security awareness training. It is important that every organization understands and identifies possible gaps in the security awareness program. Identifying these gaps should be an on-going process to improve security awareness, and also to test the organizations capability to withstand an attack. This will offer important details on the effectiveness of the organization's security awareness program and provide for improvement. Maintaining an updated security program will promote security and give the organization a better security posture.

A study conducted by Glenda Rotvold[3] revealed interesting results on organization's security culture and awareness program. 60% of the survey participants mentioned that their organizations have security awareness training, out of those sixty, 44% mentioned that attendance was mandatory. The majority of the respondents on Rotvold's survey stated that the most common methods to deliver training were used: face-to-face training sessions, email messages, and online training both in the intranet and the web. "Training sessions were offered primarily once a year, typically conducted by information systems (IS) or security staff and were usually flexible enough to incorporate new issues or needs. Results indicated that training was not typically customized for different organizational groups." (Rotvold, 2008) From the Ernst & Young's survey we learned that there was no adaptation of the awareness training. In Rotvold's survey, the trend of not customizing the awareness training is the same. Many security professionals agree that customizing the awareness training to benefit individual departments is one of many ways to improve the effectiveness of the awareness training. If the user can relate the information that is been given to him on the training and adapt it to his everyday routine, he can incorporate better the control mechanisms taught. In this survey, 72% of the respondents mentioned that they have received security awareness training. This is very relevant to this project because from the information gathered, it can be concluded

[3] Glenda Rotvold is a Ph.D from the University of North Dakota and author of *How to create a Security Culture in Your Organization.*

that the majority of the organizations have some sort of information awareness training even if it just covers generic security awareness.

In Rotvold's report, 20% of the respondents said to have a policy regarding social engineering and fourteen percent of them say this policy is in use. Having a security policy is considered to be an essential information security activity. A security policy is defined as: "the rules, privileges, roles, and responsibilities that apply to the users in managing all the information." (Hansche, 2007) There is no use on having a security policy if the network users are not aware of it and understand it. For the security policy to be effective, users must understand how to comply, understand the consequences of not complying, and agree to them. In Rotvold's survey "A substantial percentage of respondents reported that there were penalties or consequences for security breaches, including social engineering (48.8 %); however, 41.5 % did not know if there were consequences, and only 9.8 percent reported no consequences." (Rotvold, 2008) Even though this study found that there is a positive perception amongst respondent to what their organization is doing about information security, many respondents felt that they would like to receive more information security training from their organization. Another interesting aspect about Rotvold's findings is that the respondents felt that it was everybody's responsibility to help the organization with protecting its assets and complying with information security control measures. Most network users understand the importance of information awareness, and they feel they want more information from the organization to help them recognize possible risks and protect against them. The big irony is what we learned from the Ernst & Young's results, and that is most of the chief information officers will stay with their generic security awareness training and will not adapt to new trends. When you put all this information together it makes much more sense why Fortune 500 organizations failed so badly when put into the test by social engineering attacks in the recent Capture the Flag event in Defcon 18, in Las Vegas.

The responsibility of the organization security posture lies on upper management. This is the reason why Ernst & Young's survey reveals interesting information about how upper management handles current information security in many organizations. The security policy established by an organization should have the blessing of their senior management. This policy will help the organization create a security program. In the

capture the flag event in Las Vegas, it was recorded that very little resistance was found on the pretext based attacks. In the cases where the attacker found resistance from one employee, it would just take another call to a different employee to be able to capture the required flag.

One of the elements that should be included in the security program is incident handling. Incident handling cannot be just on responses to technical attack vectors. An example could be the Fortune 500 companies tested on the CTF event; assuming that those companies had an incident-handling program, would they have been able to control these attacks? There is a possibility that on the repeated cases where the phone calls had to go to a second attempt, these may have been failure attempts if the employees where alerted of the suspicious phone calls. With an incident response plan, those strange phone calls would have been reported and the rest of the employees alerted. The key question is: did the employees have enough tools to identify the attack? The fact of the matter is that contestant in the event found very little resistance to the pretext based attacks. It is clear that even if an incident response plan is established, it still comes down to identifying the call as a suspicious one. Here is where we go back to awareness training. It is very likely that many of the pretext-based attacks in the CTF at Defcon went unreported; this is because the users did not have the capability to identify a social engineering attack.

In 2005, the state Office of Cyber Security & Critical Infrastructure (NYS-CSCIC) started working on an awareness program that would revolutionize awareness on the city of New York. The program was focusing on phishing scam. Participating with NYS-CSCIC were the Anti-Phishing Working Group, AT&T, and the SANS Institute. Together they ran this first anti-phishing pilot project. This pilot project had two main goals: to better protect the agency against phishing scams, and to test the effectiveness of the security training. The project consisted on providing the end user with training and then testing their ability to identify a phishing scam. "The mock phishing scam exercise involved sending an e-mail to the group that appeared to be coming from a legitimate source, the agency's Information Security Office, and contained a link to the NYS-CSCIC Web site that were instructed to visit to check the security of their password." (Harber,

2009) The interesting thing about this method is that the end-user was recently warned about the problems prior to been tested. This method would capture the effectiveness of the training program and users ability to retain the information given. The results were quite interesting, 17% of the participants followed the illegitimate links in the mocked emails and 15% tried to change their passwords. The end users who follow the link where given a fail to comply message and taken back to the training. William Pelgrin; chief cyber security officer for New York understood that the program was very effective and use the results to improve the awareness course, "Cybersecurity awareness is about cultural change" he says.

In the year 2008 the same office implemented a 10-module computer base training program. This program contained interactive exercises on topics like the phishing scam previously tested. To further reach out into this problem the computer-based training introduced by NYS-CSCIC included another 10 interactive models on updated topics like social engineering, security accountability, and security threats amongst other important topics. Having succeeded with reaching its goal, a server version of this training was made available to other government agencies within the state through the Multi-State Information Sharing and Analysis Center.

This event has great relevance to this project because it demonstrates to a point the effectiveness of this type of methodology of maintaining an updated version of the awareness training with direct interaction with the user. As time progresses, technology changes and evolves. If organizations maintain a constant on training while technology is evolving, then training will definitely stay behind to a point of not been effective anymore. Information owners should be the ones regulating the access to their resources and what the users can do with that resource.

In another Global State of Information Security Survey (GSIS) we got the answers to some of the questions we ask. This survey was performed by: PricewaterhouseCooper (PWC) from CIO magazine. Very similar to Ernst & Young's survey, this survey also focuses on chief information officers from around the world. In 2011, around twelve thousand eight hundred CIO's participated on the survey. Earlier we asked if chief information officers trusted their security implementations or was it the economic crisis holding back decisions towards a better security posture. The GSIS

survey performed by PricewaterhouseCooper evidenced that financial restraint is withholding information security evolution in many organizations. Below is figure five with a comparison of security budgets for previous years:

Figure 5 : Most important drivers

Figure 2: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organization. [2]

	2007	2008	2009	2010	Three-year % change*
Economic conditions	n/a	n/a	39%	49%	n/a
Business continuity/disaster recovery	68%	57%	41%	40%	-41%
Company reputation	44%	39%	32%	35%	-20%
Internal policy compliance	51%	46%	38%	34%	-33%
Regulatory compliance	54%	44%	37%	33%	-39%

[2] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Source: The 2011 Global State of Information Security Survey®

As you can see from the chart many companies have accepted the risk for economic reasons. If we combine the respondents from Ernst & Young's and the ones from PWC, we can note that CIO's around the world are putting emphasis to many aspects of security and are not considering social engineering a threat. PWC survey reported that 49% of the respondents where not focusing on security because of the economic condition of the organization, while a 40% of the respondents are focusing on business continuity and disaster recovery. Accepting the risk is probably very dangerous to many companies, it would be very interesting to see further investigations that would compare the risk assessments performed by these companies. This would provide a clear view as to what are the priorities within each organization. From this survey the CIO's where asked to provide information on how is security justified in their organization and the results expressed were quite amazing. Figure six is the representation of the respondent's security justification.

Figure 6 : Justification

Figure 3: Percentage of respondents who identify the following factors when asked to reveal how information security is justified in their organization. [3]

	2007	2008	2009	2010	Three-year % change*
Legal/regulatory environment	58%	47%	43%	43%	-26%
Client requirement	34%	31%	34%	41%	+21%
Professional judgment	45%	46%	40%	40%	-11%
Potential liability/exposure	49%	40%	37%	38%	-22%
Common industry practice	42%	37%	34%	38%	-10%
Risk reduction score	36%	31%	31%	30%	-17%
Potential revenue impact	30%	27%	26%	27%	-10%

[3] Not all factors shown. Does not add up to 100%. Respondents were allowed to indicate multiple factors.
* This calculation measures the difference between response levels over a three-year period from 2007 to 2010.

Source: The 2011 Global State of Information Security Survey®

It almost seems like if regulations would not exist many corporations would not be security oriented, especially when a 41% of the security justifications are because of client's requirements. This is the main reason why this type of survey is important, to understand what is really going on behind corporate walls and the reason why they make some of their decisions. It is clear from the chart that legal and regulatory environments are the number one justification for information security.

After all this research the question remains: how many chief information officers understand that social engineering is a great threat to many organizations? Companies can comply with all regulations, have all sorts of technical control mechanism put in place and still be vulnerable to a social engineering attack; where in some occasions without any use of technology results could be devastating. The main problem seems to be organizational focus, many organizations are using the same strategies year after year and no adaptation to new threats is taking place. "For the second year in a row, the focus on data protection is the single most common strategy worldwide." (PWC, 2010) On top of that, many organizations are facing economic crisis and accepting that they are reducing security budget. 47% of the respondents mentioned that the main reason for reducing on security activities is capital expenditures. All this information has great relevance to this project, because social engineering requires very little to no technology to be able to compromise a network. If the majority of the organizations are leaving their

defense mechanism as they are, if no adaptation of trends are taking place, if no larger activity for security awareness are happening, and on top of that, if organizations are not investing on security, then many social engineers will find it very easy to conduct their attacks and be successful, something already proven in the CTF at Defcon 18.

PWC survey pointed out a very important aspect of the situation, 49% of the respondents mentioned that they had an updated security awareness program, meaning that an incredible 51% do not have an updated awareness program. This information can be combined with the fact that no further research is performed when actual events happened. There are many areas that go unheard-of. This is another great contributor to the problem because if an organization cannot learn from their current events, they will never correct them either. It is crucial to understand your network and the events that happen on it, to properly put in place control mechanisms that are effective, which is the main reason why a risk analysis is performed. There is a clear pattern that should not be overlooked. It is evident that social media is changing the world, and the way people communicate using mobile devices is changing everything. People are using social media to let the world know, who they are, what they are doing, where are they located and their areas of expertise. All this information is free and very easy to obtain. At the same time corporations are supporting this movement because of the business potentials.

Chart 1: Negative Events

Respondents who reported negative security events (PricewaterhouseCooper 2010)	
Don't know how many security events have occurred in the past 12 months	23%
Don't know what type of security events occurred, whether exploitation was via USB, mobile device or social engineering	33%
Don't know the source of the event like, supplier, former employee, hacker or current employee	34%

Chart 1 illustrates how many attacks can go unnoticed and unheard-of. If there is no stable security culture in the organization, many more things can bypass security and cause other disastrous effects. PWC survey findings are no different from any of the other

survey mentioned in this project. Many organizations are incorporating WEB 2.0 technologies and social media networks into their environments and not many of them are implementing it safely. On PWC survey, 40% of the respondents mentioned that they where implementing social media to help business, and only 23% of them have security policies to control the use of them. Again, many organizations are starting to use new ways of communicating with their clients but not necessarily making sure these new ways are safe for the organizations operation. Assessing end-users is a great tool not only to force the awareness, but also to test with real life scenarios if the awareness program is being effective. Just like the example in New York, improving the methodology will also maintain the end user aware.

Social engineering is very successful because of the natural human desired to help. It involves both physical and technological tricks to increase the trust of the target. In order to improve the chances of a successful attack, the attacker must exploit all possible human characteristics. Dr. Robert Cialdini[4] in his book *Influenced,* talks about various human behavior tendencies that may influence compliance of a special request. These are: authority, scarcity, liking, reciprocation, consistency, and social proof.

1. *Authority* = "We have a deep-seated sense of duty to authority, Tests demonstrate that adults will do extreme things when instructed to do so by an authority figure"
2. *Scarcity* = "Opportunities seem more valuable to us when their availability is limited"
3. *Liking* = "We prefer to say yes to someone we know and like"
4. *Reciprocation* = "We want to repay, in kind, what another person has provided us"
5. *Consistency:* "desire to be (and to appear) consistent with what we have already done"
6. *Social proof* = "One means we use to determine what is correct is to find out what other people think is correct...We view a behavior as more correct in a given situation to the degree that we see others performing it"

"Similarly, within the field of information technology, Stevens (2000) refers to beha

[4] Robert Cialdini : Ph.D Professor Emeritus of Psychology and Marketing at Arizona State University

vioral traits such as 'conformity' and the 'desire to be helpful', while Jordan and Goudey (2005) refer to factors of 'inexperience' and 'curiosity' that may be exploited. In phishing attacks, these influential methods can be implemented through the technique of semantic deception (Fetteat al.2006), which is achieved through the language used in the text body of an email." (Karakasilios, 2006). It is very interesting how "inexperience" and "curiosity" are included and mentioned as human factors that can be exploited. These could very likely be called in the technical field as the human exploits. All of these techniques and studies in the field of psychology that refer to human behavior are the features used by social engineers to access what Christopher Hadnagy[5] calls "the HumanOS".

These psychological methods can be exploited through the use of technology; the phishing technique uses both, human factor and technological one to meet its goal. People worry about their bank accounts, email accounts, and all other services offered in the Internet that carries personal information. When an email says there is a problem with one of these accounts and a need for a password reset needs to take people tend to perform what it is asked for. Also to put your personal information on a site to clear it and let them know that it is really you, most people follow these commands to feel they are doing the something to protect their information. Even though there are anti-phishing scam campaigns, people still tend to fall for it and follow the link. These links, found in the emails telling them to perform something specific, carry an uniform resource locator (URL) to a bogus site or a site that looks very close to the sender's site, usually banks or online retail stores.

"Visual deception in phishing attacks can be achieved through many ploys to make the email appear legitimate, such as masking a fraudulent URL (Huseby, 2004) and stealing HTML code from a genuine web site in order to create a bogus one by mirroring it (Drake et al. 2004). Images with banners and logos can also be used to create a more plausible appearance." (Karakasiliotis, 2006)

This capstone project goal is to make a clear point that "this is the year 2010" and these old methodologies are still being used and are still an effective method for social engineers. The research presented by Karakasiliotis is of great relevance to this research.

---

[5] Christopher Hadnagy author of *The Art of Human Hacking* and security expert in charge of CTF in Defcon in 18

Karakasiliotis designed a survey with a series of legitimate and illegitimate emails and confronted his participants to verify if they can identify the content. This capstone project used a very similar method of testing its participants; the difference stands in knowing the participant. This project wants to research what type of computer knowledge these participants have, if they have taken an awareness course before and what is their level of education. Karakasiliotis survey inspired the survey designed for this capstone project, because understanding why the participant thinks the emails are legitimate or illegitimate helps the researcher come to a better conclusion about the problem. Karakasiliotis' research drew very interesting conclusions back in 2006, this capstone project wanted to provide information about how many users really know what to look for in a email now in the year 2010. This research is putting great emphasis on the year because it understands that as time passes by, end users should be a little more aware of these old trends and corporations by now should have full adaptation to these trends. Karakasiliotis send a range of email messages that typical Internet users received from vendors, and banks amongst others. "The 20 email questions were composed from 11 illegitimate and nine legitimate messages, and were gathered from a combination of websites showing phishing related examples, as well as emails that the authors had personally received." (Karakasiliotis, 2006) Here are the categories used for this survey:

1. Identifiable recipient: Did the message include something that addressed the recipient by name or some other characteristic (e.g. part of an account number) that could assist to verify whether or not the sender was in possession of valid details about them?
2. Identifiable sender: Did the message body indicate the name of a specific individual that a recipient could attempt to contact (i.e. instead of a generic claim such as 'XYZ security team' etc).
3. Images / logos: Did the message include graphical content that could help to improve the appearance, emphasize brand identity, etc?
4. Untidy layout: Was the message presented in an unprofessional manner (e.g. line br eaks in the middle of sentences)?

5. Typos / language errors: Did the message contain any spelling mistakes or grammat ical errors?
6. URL / link: Did the message seek to encourage the recipient to follow a hyperlink?

The results from this survey will reveal crucial information that will help design a better information awareness course. In the year 2006, when this survey took place, only 42% of the respondents where able to identify emails correctly, 32% of them identified them incorrectly and 26% were unable to identify the emails. Figure eight represents a chart of the respondent's classifications.

Figure 8: Overall classifications

	Correctly classified	Incorrectly classified	Don't Know
Legitimate messages	36	37	27
Illegitimate messages	45	28	26
Overall	42	32	26

Table 2: Classification of messages by participants

Clearly, less than half of the respondents where able to identify the legitimacy of the emails providing a clear conclusion that more training needs to go into this topic. Karakasiliotis survey pays close attention at the ability of the participant to identify from visual factors or technical details. Visuals like logos, banners, trademarks, footer, fonts and copyright symbols to be able to identify legitimacy. On the other hand, http, https, and specific URL structure as a more technical way to approach the legitimacy. In this case the overall results where quite interesting, 40 respondents used visual factors and 52 made judgment based on the technical aspect. More participants paying attention to the technical side of the identification process lets this research know that it is possible to provide the end-users a technical training where they would identify specific aspects of the email so they represent better defense to the network at the long run. "Also from an analysis of influential techniques, it seems that messages that involve asser ting authority or exploiting the recipient's desire to be helpful are most likely to be miscla ssified, compared to those attempting to exert influence based upon social proof or scarcit

y, which participants were more able to classify correctly." (Karakasiliotis, 2006) This aspect of the study is very important because as mentioned before, social engineers study their target prior to launching an attack. They will capture information and understand many important aspects of their target that will help them elaborate a successful attack. This is particularly the reason why awareness training should target specific issues instead of a general idea.

The 2006 CSI/FBI Computer Crime Survey reported around $52 million dollars in total losses, and out of the total email attacks represented $1.8 million dollars in loss. Having a problem that would constitute millions in loss would be something that should catch someone's attention, as well as to correcting the problem. The anti-phishing workgroup report of the first half of 2009 reported that during February and June the number of phishing sites fluctuated around the 30,000; which is nearly 12% lower than the all time set of 55,643, but still remains the second highest number, meaning that these attacks will still remain very common. As a matter of fact, Symantec (a company that specializes in Antivirus) believes that social engineering trends will continue to grow during the year 2010. "More and more, attackers are going directly after end users and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred by the fact that it is the actual user being targeted, not necessarily vulnerabilities in a machine. Symantec estimates that the number of attempted attacks using social engineering techniques will increase in 2010." (Symantec, 2010) Symantec also mentioned that social networking third-party applications would also be a high target during this year. The main problem with type of flaw is that there are very little organizations willing to do something about it, mainly because they believe that social engineering is an attack vector that requires a lot of preparation, and only inexperienced hackers use it.

According to a company called MANDIANT that is not true. They published a report explaining the new anatomy of a modern hack. These companies mention that their study is based on seven years of front-lines breach investigations for the public and private sector. "MANDIANT uses the newly vogue term Advanced Persistent Threat (APT) to describe the attacks detailed in the report. The company defines APT as an

"orchestrated deployment of sophisticated and perpetual attacks that have systematically compromised computer networks in the public and private sector for years." (Hulme, 2010) MANDIANT reports that during the phase two of the attack (Initial Intrusion into the Network) the attacker will very likely use a combination of efforts to gain access to the network. These include commonly used tools like social engineering, combined with email, which they call "spear phishing". This method will combine spoofed emails targeted to a small number of specific individual within the organization. The spoofed emails will contain specific exploits from most common vulnerabilities like Microsoft and Adobe. This vendors explain how a complete attack is orchestrated, mentioning that social engineering is one of the techniques used to gain access to a system. Even though the author seems to have not found any new trend on the way, MANDIANT reported the new anatomy. He mentions "What we do have are highly-motivated, well trained and funded adversaries using social engineering, attack tools, software flaws, and low-and-slow attack strategies that we've been grappling with for more than a decade now." (Hulme, 2010) There is an inside joke amongst the IT community called "the layer 8" problem; the end user, it cannot be taken for granted because it still remains for many organizations its weakest link.

The last but not least report that will be mentioned in this research is the Computer Crime and Security Survey performed 2010. The Computer Security Institute conducts a yearly report that provides status of the majority of the reported incidents. This report will provide updated information about on ongoing attacks. This survey is conducted on 5,412 security practitioners where 21.5% are in the consulting business, 10.6% are in the finance sector, and 10.9% in information technology among others. Similar to the other surveys presented in this research the majority of the respondents have to comply with industry regulations like HIPAA, SOX, Payment Card Industry Security PCI, and Federal Information Security Management Act among others. This report is of great relevance to this research because it provides updated information on the most recent attacks that organizations are experiencing. This updated information provides a real perspective of the problem being exposed by this capstone project.

The attacks reported by CSI include many vectors, form these vectors some may be caused by social engineering and others regular attacks. Here are the reported attacks

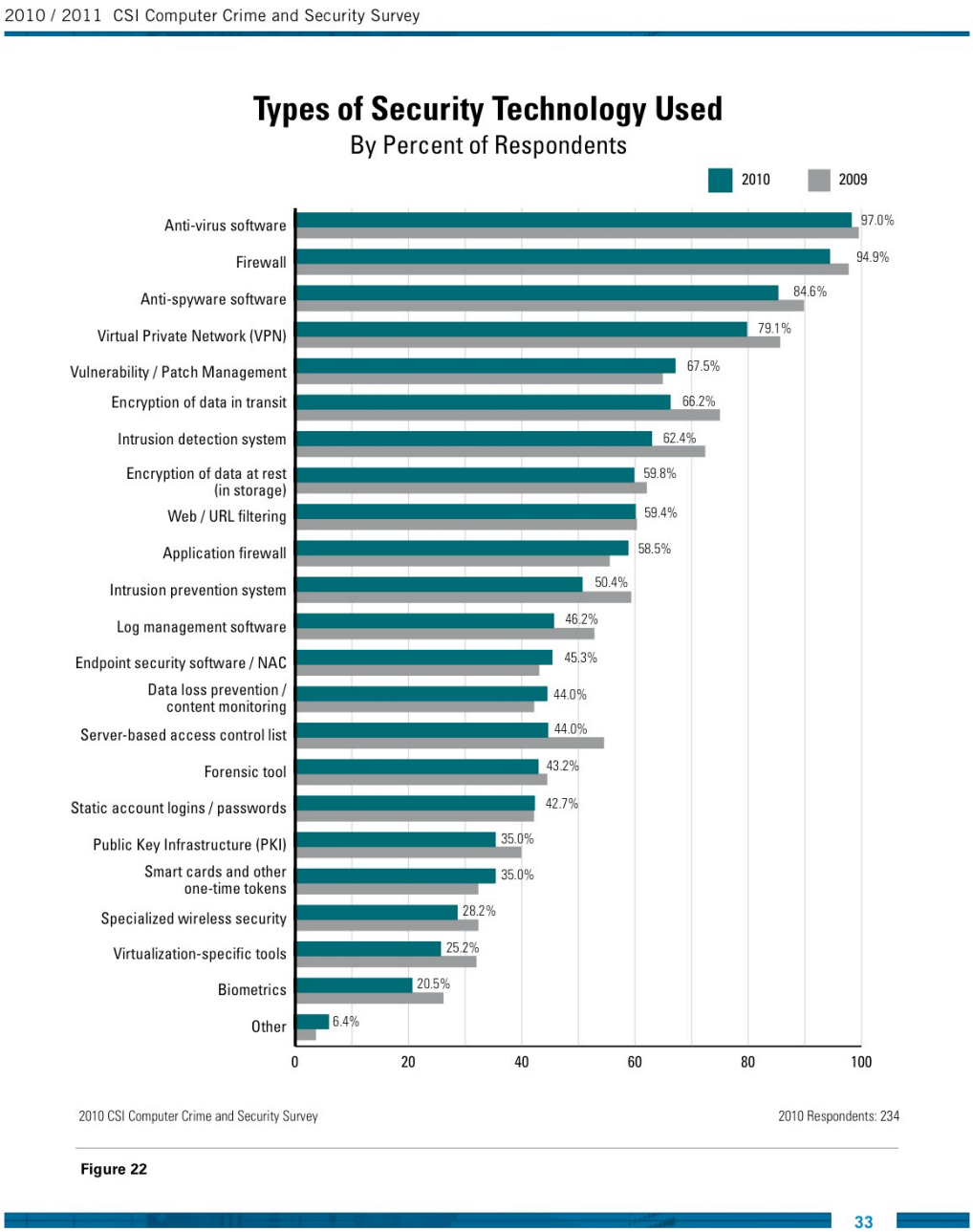
with higher rate of occurrence:

1. Malware Infection 67%
2. Phishing messages 39%
3. Laptop theft or loss 34%
4. Bots within the organization 29%
5. Insider Abuse of internet access or email 25%
6. Exploit of client web browser 10%

Even when malwares still remains the most common attack used, the phishing events increased 5% from the 2009 report. The insider abuse of Internet access and email has a high rate also with a 25% and the exploitation of web browse has a 10%. These three have in common the fact that they can all be associated with social engineering attacks. Another interesting fact about the report that bring great relevance to this project is that in 2009 CSI reported that the majority of the financial loss was caused by insiders strongly accentuating the fact that human error causes high loss. “87.1 percent of respondents said that 20 percent or less of their losses should be attributed to malicious insiders. 66.1 percent of respondents said that 20 percent or less of their losses were attributed to non-malicious insiders.” (CSI, 2010) Most of these contestants also reported about the actions taken when an attack takes place. 62.3% of them mentioned that patching vulnerabilities to software is their main course of action. A 42% mentioned that they provide additional security awareness training to end-users as an action taken. This is a very positive result when confronted with the fact that the majority of the attacks are caused by malware infection. Another established fact that is also mentioned in other surveys is that the majority of the contestants (60.4%) revealed that their organizations have an established formal security policy. Although we already know that a policy can help provide a control mechanism we also know it does not mitigate the problem and a combination of efforts must be made to control the threat. The majority of the contestants (50%) when asked about the investment on security awareness being adequate actually acknowledge that it was to little. This information provides an already establish point that many corporations are aware of the problem. One of the most relevant

information is the amount of technology controls used, figure 9 provides a visual guide to the types of security controls used by the respondents.

Figure 9: Types of Security Technology Used



It is clear that organizations have many technology security controls but humans will continue to be the networks weakest link. The CSI survey provides results for a question

that gives some kind of hope to the rest of the findings we have gathered through the research. This question was added to the survey in 2009 on and continued to be in use this year. The contestants where asked what techniques where used to evaluate the effectiveness of awareness training. In 2009: 12.6% had no information awareness training, 40.8% of the contestants had information awareness training but did not measure its effectiveness and 15.3% provide social engineering techniques in the training. In 2010: 14.9% have no awareness training, 34.1% have information awareness training but did not measure it and 21.2% have social engineering training with a method to measure its effectiveness. The observation is evident that the number of unmeasured training decrease, and the number of social engineering specific training increased. This data provides positive inputs, one of the main suggestions that this research wants to provide is the fact that it is imperative to valuate awareness training and find mechanism to know if the training is working for the organization and if not to re-evaluate and adapt the things thank the training is lacking to better improve it.

Investigative Methodology

This capstone project understands that security awareness is one of the most valuable tools an organization has to counteract an overlooked weakness amongst organizations. Having a general awareness program will not provide the necessary elements required to fulfill the goal. To provide a better control mechanism for social engineering attacks, users need be properly informed about the techniques used in both technical and non-technical attacks. This experiment wants to prove that in the year 2010, when almost everybody is a computer user with a high level of education, the majority of the network users cannot identify a link or the legitimacy of an email. The experiment was designed based on an online survey and it included three main sections. The first section collected demographic details about respondents, computer knowledge, education and their Internet usage. This is followed by the main part of the survey, which consisted of a small quiz composed of nine questions, each presenting the participant with an email message or a URL, and asking them to judge its legitimacy. In each case, respondents could choose one of

three options (‘illegitimate’, ‘legitimate’ and ‘don’ know’). If they choose illegitimate, then they were asked why did they think the email presented was illegitimate. The last part of the survey tries to understand a little more about network user specifics: has the participant ever taken any awareness course, have they heard specific terms like phishing, and other tricky questions found on Appendix A. This survey would test how much the participant is really aware off.

A variety of email samples from Helping Haiti, Amazon password reset, to banks asking user information were used in this scenario all taken from the anti-phishing work group web site (http://www.antiphishing.org/). One of the key elements that make phishing scams so successful is the combination of human factor with the inability of the user to identifying a legitimate or illegitimate URL. As part of this investigation we have incorporated a series of uniform resource locators (URL) for the participants to identify just like in the email: in each case, respondents could chose one of three options (‘illegitimate’, ‘legitimate’ and ‘don’t know’), and if they choose illegitimate, then they were asked why did they think it was illegitimate. The fake URL’s where also taken from the anti-phishing workgroup web site (http://www.antiphishing.org/).

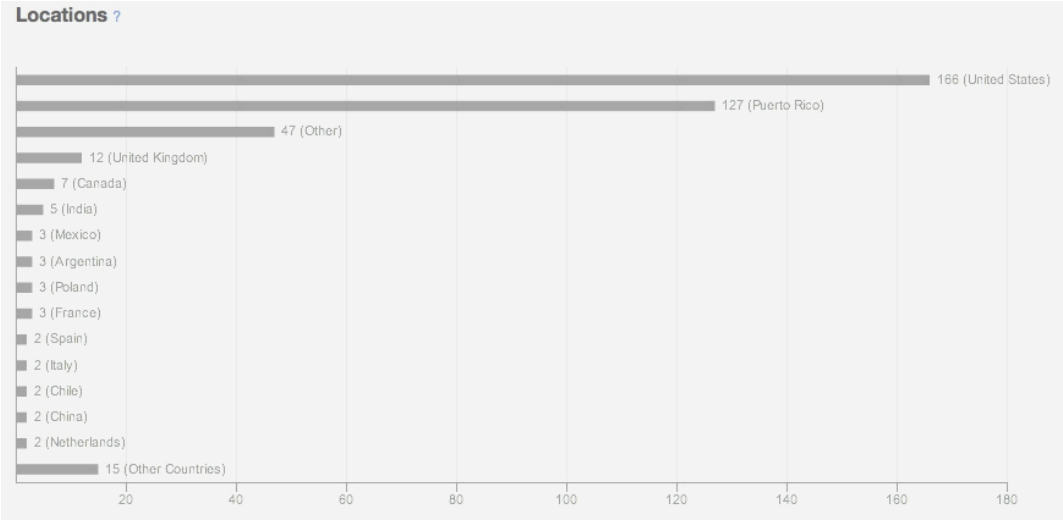
Only two URL’s where legitimate in the small quiz and the rest of the examples were illegitimate. The central idea is to understand why users think these emails are illegitimate and learn if they really understand what to look for in an email. Since most of the problems in a phishing scam come from clicking on an incorrect link, this survey decided to include URL identification as part of the tested items.

Experimental Results and Analysis

Although a total of 225 participants started the survey, only 152 participants fully completed the survey over the course of two weeks. Walsh College Qualtric’s system was able to translate the survey, so it was provided in both English and Spanish. This survey was intended primarily to study actual network users in different corporations. Do to the research topic many corporations decline help by disseminating this survey to their network users. This limitation completely changed the goal of this capstone project and

having time limitations caused this survey to be propagated publicly instead of directly to network users. Facebook, LinkedIn, Twitter, and email systems where used to propagate the survey. The URL redirection service http://bit.ly was used to track survey's hits and locations. Figure 10 represents a chart on the places where the survey was clicked.

Figure 10: Bit.ly link tracking



According to our findings the total participants included 17 different nationalities with the majority of the participants being from United States and Puerto Rico. This included a mix gender of 70% male and 30% female. The majority of the participant's age ranged from 30 to 49 years of age with a 51%, 39% from the range of 10-29 and 9% from the ages 50 to 69. On an interesting note the majority of the participants (45%) had a bachelor's degree, and a significant amount had higher education, like a masters degree with a 27%. For the purpose of this research this data is very important, to a degree the level of education of the users means they are more capable of understanding a better-detailed awareness course than those without an education. Although further research is needed to prove this point, it is suggested that better distribution of the awareness courses can benefit the organization. "Training is not equally distributed among employees. Older, low skilled workers, and to some extent female workers, typically receive less training than other groups of employees. However, we do not find any clear-cut evidence that returns to training varies with gender, educational or skills levels, which suggests that inequalities do not arise because of differences in returns to training, but are more a

consequence of inequalities of the distribution of training investments." (Hansson, B. 2008) The participants worked in a variety of sectors and the most notable are: 25% over all services, 17% students, 13% government, 11% self employed, 7% Financial, and 6% unemployed, among others. The majority of these users expressed to be Microsoft users with a 67%, Apple users ranged in a 14% while a 12% for open source users. The rest of the participants claimed to use them all, or both Microsoft and Apple. People with some sort of college degree tend to be more "computer savvy" than others. There are studies that determine that level of education can go hand-to-hand with the type of computer used. One factor could be that people with education have been more exposed to computer usage than people without an education. Further research could provide more evidence of this matter but for the scope of the project we feel that the type of operating systems used is important to understand the type of computer user. "Nielsen/NetRatings said that 70.2 percent of Mac users online have a college degree, compared with 54.2 percent of all Web surfers." (CNET, 2002)

The majority of the participants mentioned that they use computer every day both at home and at work. The purpose of usage varies, but email system was the majority. Figure 11 represents those numbers:

Figure 11: Computer Usage

#	Answer	Response	%
1	News	159	83%
2	Work research	121	63%
3	Personal research	147	77%
4	Investments	26	14%
5	Shopping	116	61%
6	Auctions	49	26%
7	Email	177	93%
8	Chat/communities	94	49%
9	Banking	113	59%
10	Social Media	124	65%
11	Job Hunt	72	38%
12	Entertainment	131	69%
13	Other	12	6%

The second part of the survey was the quiz with the URL and emails. As mentioned before this part was composed of nine questions, there where four emails to identify and five URLs. All the emails in the survey where illegitimate and out of the five URL exposed only two were legitimate. If the participant identified the email or the URL as an illegitimate one, he/she was challenged with a text box to explain his/her reasoning. A quick observation from the over all results: out of the nine questions exposed on four of them (13, 15,21, and 29) the majority of the participants where correct about the email or URL and sustained their answer as to why. This means that 56% of the overall quiz caused some type of trouble for the participant to identify correctly. In question 17 the majority of the participants (57%) indicated that the URL was illegitimate but out of that majority only 52% of them could sustain their answer setting back this majority to a 28%. In the rest of the quiz less that half of the participants indicated the correct answer and even that lesser half could not sustain their answer. See figure 12 below.

Figure 12 : Provides the overall responses:

Question #	Type	Identification	Total Responses	%
13	**Can you recognize this email?**	**Illegitimate**	96	52.00%
		I don't know	36	20.00%
		Legitimate	52	28.00%
15	**----------**	**Illegitimate**	127	73.00%
	----------	**I don't know**	31	18.00%
	----------...	**Legitimate**	15	9.00%
17	**Can you identify a URL? http://paypalsecurity.co.uk/security/protectyourdata.asp**	**Illegitimate**	98	58.00%
		I don't know	48	28.00%
		Legitimate	24	14.00%
19	**Can you identify a URL? http://203.144.234.138/us/safedata/index.html**	**Illegitimate**	82	49.00%
		I don't know	76	45.00%
		Legitimate	10	6.00%
21	**Can you identify a URL? https://paypal.com**	**Illegitimate**	27	16.00%
		I don't know	20	12.00%
		Legitimate	120	72.00%
23	**Can you recognize this email?**	**Illegitimate**	65	40.00%
		I don't know	59	36.00%
		Legitimate	40	24.00%
25	**Can you identify a URL? https://security.ebay.passwordreset.com/**	**Illegitimate**	76	47.00%
		I don't know	52	32.00%
		Legitimate	33	20.00%
27	**Can you recognize an email?**	**I don't read Spanish**	35	22.00%
		Illegitimate	78	49.00%
		I don't know	14	9.00%
		Legitimate	32	20.00%
29	**Can you identify a URL? http://cars.com**	**Illegitimate**	14	9.00%
		I don't know	50	31.00%
		Legitimate	95	60.00%
		Total	225	

Another observation was the confusion of “http” and “www”. The http means that the browser will use http protocol to communicate with that specific site, and the www is only a naming standard. This means the server is a web server, in DNS there would be “A” type records pointing to that site's IP for both site name & site name prefixed with www. In this case both sites were legitimate but still a very small percentage of the participants had trouble identifying it. A 3% error needs to be taken in consideration do to the nature of this quiz; taken over the Internet, because people tend to look for the right answer instead of answering what they really know. As mentioned before in this research; the main suggestion is for users to have a specific awareness course, were detailed information in relevance to their job is specified. Users need to be aware of the difference in terminology and how to properly identify them, only this will provide and effective countermeasure against phishing attacks. The table 2 (below) depicts out of the overall respondents, only the ones that answered “illegitimate” and what percentage of those answers where sustained.

Table 2: Sustained Answered

	Question #	Type	Correct Answer	ID as Illegitimate	Correctly ID
1	13	Email	Illegitimate	52%	87%
2	15	Email	Illegitimate	73%	94%
3	17	URL	Illegitimate	57%	52%
4	19	URL	Illegitimate	49%	73%
5	21	URL	Legitimate	16%	72%
6	23	Email	Illegitimate	39%	79%
7	25	URL	Illegitimate	47%	72%
8	27	Email	Illegitimate	49%	87%
9	29	URL	Legitimate	8%	61%

The majority of these emails where correctly identified due to:

1. Spelling errors
2. Sender address
3. Why confirm identity?
4. Content of the email seems fishy
5. Email layout
6. Lacks original Logo
7. Domain name not properly formatted
8. Recognized email from the news
9. Lack of traceable information

The results did reveal that the participants had some level of difficulty and where more inclined to misclassify emails even when this survey itself was fishy. The URL on question number 17 was one of the most controversial one.

http://payplasecurity.co.uk/security/protectyoudata.asp

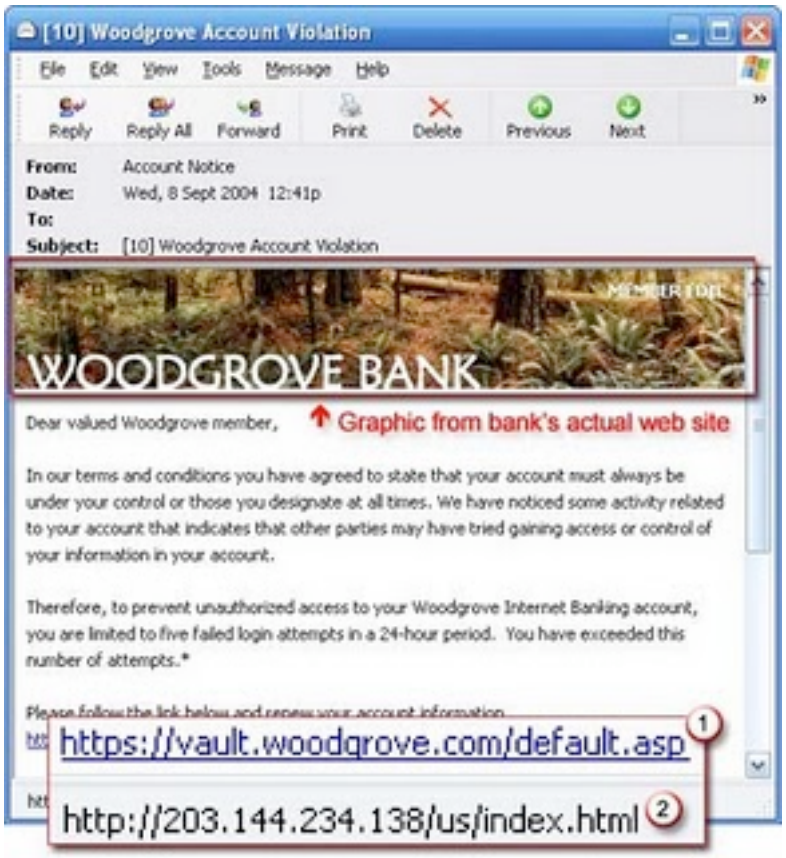
In this question 57% of the participants said that the URL was illegitimate, but when asked to sustain their answers the majority of them said that the reason was because it lacks the "s" on the "http://". The question with the IP address on the URL also generated interesting results.

http://203.144.234.138/us/safedata/index.html

In this question 46% of the participants did not know whether the URL was legitimate or not and out of the 49% who mentioned it was illegitimate only 73% of them provided the correct reasoning. Many said it lacked .COM, other said the URL is not working; some said they don't trust anything without an https. The pattern with the URL questions is that the participants try the link before answering if it is fake or not, meaning that these participants did not know how to properly identified the URL and had to actually try them to identify their legitimacy. This is just like not knowing; the other problem is that the URLs presented in the survey are usually hidden behind the code of

what it looks like a legitimate link like in figure 12. This means that the user really needs to know where to look to be able to identify the legitimacy. An information awareness course should target these inputs and properly test users to understand their comprehension on the matter; this awareness training should also be cyclic. This way it can be segmented and all technical information does not have to be given at the same time, which could be very overwhelming if not properly handled. To better protect the enterprise it is important to provide an accurate and user focused security awareness training. It is also important to measure its effectiveness, by testing the user. This method will provide a measurement for the awareness course, points out what the awareness course is lacking, and the areas that need improvement. Just like performed in this research, surveys, exams, and audits are just a few of the assessment tools that can be used to evaluate the awareness course given by the corporation.

Figure 12: Example Phishing



Now that we have analyzed the data and we have identified the participant's weaknesses, it is time to take an awareness approach at the observations. It is evident that most of the participants have found some of the emails and URL suspicious, the problem strides that in a real social engineering attack the social engineer would have enough information about its target that he would make no mistake on sending an email that the target would fall for. So if you take the spelling errors off, the fake logos and the "I do not have an account on Amazon" you are left with the possibility of an attacker finding something the target would follow. This is where awareness comes in, identifying those specific areas where a users lacks knowledge and providing the end-user with the necessary tools to fight off this growing problem. While most of the social engineering attacks can occur over the phone or via email a really motivated social engineer might physically end up in the target's arena looking for more leads on the target. This is why all those possibilities need to be covered and end-users need to understand the possibilities.

On the third part of the survey more specific questions about the social engineering topic where asked. Among these question was the: "have you ever taken an information awareness course". In this case 47% of the participants indicated that they had taken an awareness course. This small amount of users that have taken an information awareness course represent just a tiny portion of the status of most computer users, taken than 20% of the participants work in services, 11% in the government, 11% self employed and 17% where students among others. Insisting on the numbers the majority of these participants had already indicated that they uses computers both at home and at work every day and that email systems was the most common purpose of the usage. As mentioned earlier the intention of this survey was to study organizations with information awareness course and organizations without it. Since this survey found very little support from organizations the scope was limited to general public. Among the participants from the general public there is a good grasp of professionals from different areas, which still depict a good status of how many computer users are a little more informed. There was one question that asked the participants if they had received an email in the past six month asking for information that they had identified as a fraudulent email, 59% of the participants mentioned that yes they have recently received this type of

emails. This means that these attacks are still commonly used and even though some are just regular spam, one never knows when an elaborated email coming from a social engineer might show up in the inbox.

Not everything is lost, 64% of our participants have heard about social engineering and understood what it was when asked. Also 65% of them had a working environment that was governed by a network security policy. To go deeper into the study we decided to cross tabulate the quiz responses to the amount of participants who had taken an information awareness course. This will point out all the participants that answered correctly and whether or not they had some sort of awareness about these subjects, keeping in mind that the overall results stated that less than half of the participants had taken an information awareness course before. Figure 12 shows a representation of this cross tabulation.

The rows in this chart represented in figure 12 provide the questions asked in the quiz, and the columns represent those who have taken an awareness course. The highlighted items represent the correct answers correlated with the awareness. Keeping in mind that in some of the questions the participants were not able to sustain their answer the general feeling is that the majority of the participants in this survey that answered the questions correctly had an information awareness course. For the purpose of the investigation it is clear that awareness training is an effective mechanism against these types of attacks, we understand that some of the users were not able to really identify key items when asked why where they legitimated or not; which means that some changes need to be made to the training to adapt new trends and specific attacks.

The overall message is that the people that had mentioned taking an information awareness course have better probabilities of identifying an attack, if the knowledge of these individuals were to be improve improved by providing them with a more details awareness course .

Figure 12: shows the cross tabulation

		Have you ever taken an information awareness course?			
		Yes	Maybe	No	Total
Can you recognize this email?	Illegitimate	39 40.63%	5 5.21%	37 38.54%	96 100.00%
	I don't know	9 25.00%	2 5.56%	16 44.44%	36 100.00%
	Legitimate	23 44.23%	0 0.00%	22 42.31%	52 100.00%
.....	Illegitimate	56 44.09%	3 2.36%	56 44.09%	127 100.00%
	I don't know	8 25.81%	4 12.90%	13 41.94%	31 100.00%
	Legitimate	7 46.67%	0 0.00%	6 40.00%	15 100.00%
Can you identify a URL? http://paypalsecurity.co.uk/security/protectyourdata.asp	Illegitimate	49 50.00%	3 3.06%	39 39.80%	98 100.00%
	I don't know	14 29.17%	0 0.00%	28 58.33%	48 100.00%
	Legitimate	8 33.33%	4 16.67%	8 33.33%	24 100.00%
Can you identify a URL? http://203.144.234.138/us/safedata/index.html	Illegitimate	48 58.54%	4 4.88%	26 31.71%	82 100.00%
	I don't know	21 27.63%	1 1.32%	43 56.58%	76 100.00%
	Legitimate	2 20.00%	2 20.00%	6 60.00%	10 100.00%
Can you identify a URL? https://paypal.com	Illegitimate	10 37.04%	1 3.70%	15 55.56%	27 100.00%
	I don't know	3 15.00%	1 5.00%	13 65.00%	20 100.00%
	Legitimate	58 48.33%	5 4.17%	47 39.17%	120 100.00%
Can you recognize this email?	Illegitimate	31 47.69%	3 4.62%	24 36.92%	65 100.00%
	I don't know	21 35.59%	3 5.08%	32 54.24%	59 100.00%
	Legitimate	19 47.50%	1 2.50%	19 47.50%	40 100.00%
Can you identify a URL? https://security.ebay.passwordreset.com/	Illegitimate	44 57.89%	2 2.63%	28 36.84%	76 100.00%
	I don't know	10 19.23%	3 5.77%	34 65.38%	52 100.00%
	Legitimate	17 51.52%	2 6.06%	13 39.39%	33 100.00%
Can you recognize an email?	I don't read Spanish	19 54.29%	1 2.86%	15 42.86%	35 100.00%
	Illegitimate	39 50.00%	5 6.41%	33 42.31%	78 100.00%
	I don't know	3 21.43%	1 7.14%	8 57.14%	14 100.00%
	Legitimate	10 31.25%	0 0.00%	19 59.38%	32 100.00%
Can you identify a URL? http://cars.com	Illegitimate	4 28.57%	1 7.14%	9 64.29%	14 100.00%
	I don't know	13 26.00%	3 6.00%	31 62.00%	50 100.00%
	Legitimate	54 56.84%	3 3.16%	35 36.84%	95 100.00%
	Total	71 31.56%	7 3.11%	75 33.33%	225 100.00%

From the CTF event we learned that pretext based attacks over the phone can be very effective method of attack used by social engineers. In the last part of this survey we asked some questions based on phone scenarios and other social engineering schemes and here table 3 illustrates them.

Table 3: Part 3 of the quiz

Question	Answer	Majority
Have you received an email, a call or letter within the past 6 months that you suspect was an attemp...	Yes	59%
When your bank call do you..	Validate their Identity	55%
How do you dispose of your sensitive letters or bills?	Shred it	74%
Do you know how the company that you work for handles sensitive material?	Shreds All Documents	38%
What do you think Social Engineering means?	The act of manipulating a person to accomplish goals	68%
Does the company that you work for have a Network Security Policy?	Yes	65%
If someone calls you asking for the type of Internet browser:	Would try to help but ask why	54%
If the phone company repair man shows up because of a broken line problem, do you answers all his qu...	Maybe	53%
If your company has information awareness training how often do you take it?	Yearly	32%

Would you consider it rude not to help someone asking for information over the phone?	No	88%
If the UPS worker comes to deliver a box, do you?	Verify if we where expecting a package	58%

In this table we have gathered what the majority of the participants mentioned about each question on the last part of the survey. From the results we get a perspective that computer users still get suspicious emails, and they are very likely to fall for a social engineering attack. Even when the majority of the participants understand what social engineering is, they also mentioned that they might give information over the phone if they feel it is necessary. Another observation if that the majority of the participants work in an environment where there are network security policies in place, and also the majority would answer questions about Internet browser if given an appropriate reason to do so. Another important aspect is that the majority of the participants mentioned that the rate of occurrence of the information awareness course is yearly. When you take the overall results and analyze them it is clear that many organizations have an information awareness course, it is clear that many people think they know how to identify when an email is suspicious but really cannot mention why, it is evident that many people are still vulnerable to social engineering. And last but not least, the majority of the people understands these threats and feels they are ready for them. Deeper investigation needs to be performed not just on regular computer users (general public) but with corporate computer users and compare the results of this survey with the one performed on a targeted audience. From the overall results increasing security awareness is needed; and targeting specific audience, would be beneficial. It is recognized that the participants where judging based on the content of the emails and no elaborated scam was performed to really test the users knowledge of the subject (like the test performed in New York). The fact of the matter is that when you take these results and compare them to the actual

pretext based attacks in the CTF in Defcon 18 it is conclusive that social engineering is still a possible attack vector and it may probably well be a very successful one too.

Recommendations

It is highly recommended that the organizations' security policy be reviewed and modified to adapt to changes. All key players on the organization should integrate and participate on the creation of this policy. This policy should not be written in stone, if there were to be any incidents, the policy should be adapted to correct those incidents. As mentioned before, it is crucial that everyone can relate to the policy, understand the consequences of not complying with this policy, and agree to them. “It is through these policies that security programs can be set up with a strong foundation and an organized method of response to security issues, as well as expectations for personnel within the organization as to who is in charge during certain kinds of incidents.” (Harris, 2009) The security program should include security awareness training, this training needs to be constantly assessed and evaluated to measure its effectiveness and prove that it is achieving its goal. “Other areas that potentially could be improved include updating policies, identifying and communicating the security awareness goals and message, repeating the security message often, and creating a security culture.” (Rotvold, 2008) To help measure the awareness training it is important to test all employees and measure their knowledge on all the covered topics.

As mentioned earlier, it is important for the organizations to make social engineering training a part of the administrative controls; it is critical that they publish the security policies, develop standards and procedures to follow them, guidelines, risk management and security awareness. It is essential that everybody in the organization understand that technology alone is not a complete solution. Also, decision makers need to consider more seriously the inclusion of social engineering in their awareness programs. A security program contains all the pieces necessary to provide overall protection to a corporation and lays out a long-term security strategy. “A security program should have security policies, procedures, standards, guidelines, baselines, security-awareness training, an incident response plan, and a compliance program”

(Harris, 2009).

There are many guidelines to providing a proper information awareness course in the organization. The National Institute of Standards and Technology (NIST), designs standards for federal computer systems, but many private industry organizations adapt these standards to their needs. In the Ernst & Young survey we learned that 56% of the respondents have an information security program because of compliance with regulations. In the case of these organizations that need to comply with regulations following NIST standards is mandatory. To establish an awareness program from ground up NIST has Special Publication 800-50 Building an Information Technology Security Awareness and Training Program. (NIST, 2003) SP800-50 provides guidelines to developing this course; there are very relevant recommendations in this publication that if followed, can very well target social engineering techniques and provide end users the tools necessary to identify this type of scans. Although this capstone project understands that the awareness training should be more technical, it will provide the perspective of the NIST as a form of comparison. The main purpose of awareness is to reach a broad audience with attractive techniques of comprehensions, making awareness an interesting procedure instead of a painful one. Here is a representation of the success route towards the implementation following SP800-50 recommendations:

1. Get support from upper management, and use their resources
2. Define key messages, audience, and delivery timeframe
3. Select appropriate communication vehicles and tailor message for audience (Here is where we would adapt to specific end users)
4. Gather required approvals
5. Deliver message to audience
6. Gather feedback

Management support is very important for end-users to take the awareness course program seriously and also to get the necessary resources to build a program. It is necessary to define a business case that supports the objectives of the organization, getting upper management supports will provide for resources and demonstrate support

that will strengthen the awareness program. Defining the key massage will determine what the user needs to know. It is important to include personnel from the respective areas so that the course is adapted to their specific needs. Have every body get involved: Help Desk, Desktop support, Managers, and end-users. Once these key players are identified then the audience needs to be defined. As we have already point out, different audience have different needs, mostly based on their role and responsibilities. Here is where this research understands that a generic course will not provide necessary outcome because all users need a key message. Selecting the best communication vehicle for the users should be next. These could be:

1. Electronic = Email, intranet, online training, podcasts, PC startup tip, screen savers, Help Desk front-end message, voice mail
2. Paper = Posters, newsletters, brochures, booklets, wallet cards, café tent cards
3. Face-to-face = Technical fairs, security road shows, booths, department/team meetings, lunch and learns, one-on-ones, focus groups
4. Other = Trinkets, "fabulous" prizes

After determining what is best for the user then it is time to get approval, mostly from people relevant to the topics being talk about: usually IT, Legal, Corporate, Human Resources, etc. The most important aspect of all and mentioned in this research in various occasions is to measure the effectiveness of the awareness course. Use metrics, help desk calls, incidents, surveys, training attendees, and above all, test the employees to see how they perform. Making awareness comprehensive and fun is the key to success. It is imperative to incorporate marketing techniques to publish this training. It is crucial to incorporate real world and business examples. Doing a pre-program survey/quiz, forms foundation and acts as baseline to post-training survey/quiz. You can measure results; even when special publication 800-50 mentions "Awareness is not training".

The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly with attention on security. Awareness presentations are intended to allow individuals to recognize IT security"(NIST, 2003) This research

believes that awareness can go further, due to the level of success of some of the social engineering attacks, users need to be enlightened with a little more technical information. Figure 9 provides a chart that represents how special publication 800-50 sees the awareness process.

Figure 13: The IT Security Learning Continuum

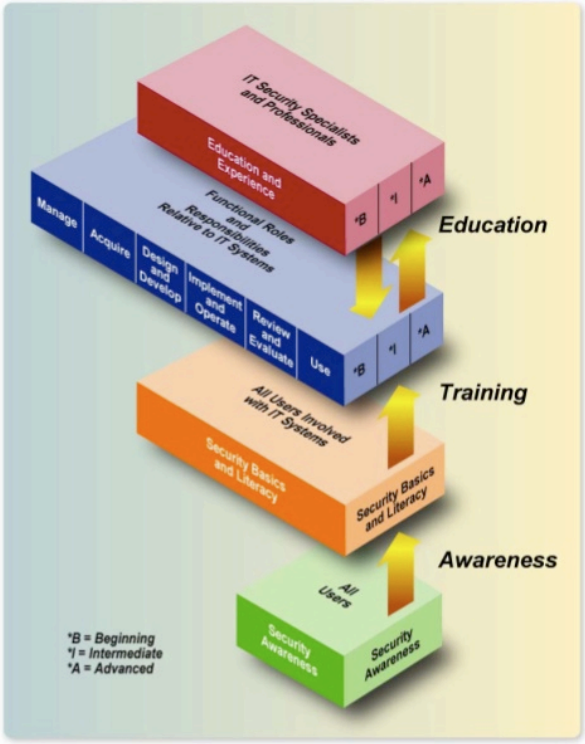


Figure 2-1: The IT Security Learning Continuum

NIST establishes learning as a continuum; it starts with awareness, builds to training, and evolves into education. Awareness should be divided into quarters and have subtopics that would make the complete process less heavy on the end-users. Here a sample plan:

1. Q1 Internet Threats and Safeguards: threats, virus, worms, spam, phishing, firewalls, Hyper Text Transfer Protocol (HTTP), HTTP Security, Secure Socket

Layer encryption

2. Q2 Information Protection: Policies, regulations, Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), the importance of the Confidentiality Integrity Availability (CIA) triad
3. Q3 Preparedness: risk management, incident response, business continuity planning
4. Q4 Defense in Depth: The human element = social engineering, physical security and an overview putting all the topics together.

Dividing the complete process into groups just like recommended by NIST will cover all the necessary topics to make the awareness program an effective one. Being that this process is a continuous one, regular updates to the topics should be performed to maintain relevance and adaptation to the new trends. This research has demonstrated that the use of generic awareness course is not being successful to social engineering attacks. A different strategy needs to be adapted to represent a better control mechanism against this growing threat.

Many security experts concur that security is an ongoing process, what seems to be working today is no longer reliable tomorrow. Chief security officers need to think like an attacker to be able to protect their organization. This is the main reason why most of them need to stay current with the events happening around them. Social engineering is a relative easy method of obtaining information from a corporation. It is generally overlooked because many CSOs feel that the "not-so-talented" attackers use this method of gathering information. The Defcon CTF proved that social engineering cannot be taken for granted and many organizations are at risk for lack of proper countermeasures to fight this growing menace. "We realized that the problem is that people are not aware that telling a stranger on the phone what version of Internet Explorer and Adobe Reader gives an attacker information they need to hack you." (Chris Hadnagy, 2010) The implementation of an effective security awareness program has been proven to work against social engineering. "The only truly effective way to mitigate the threat of social engineering is through the use of security awareness combined with security policies that set the ground rules for employees behavior, and appropriate education and training for employees." (Kevin Mitnick, 2002)

Appendix A

Survey Report

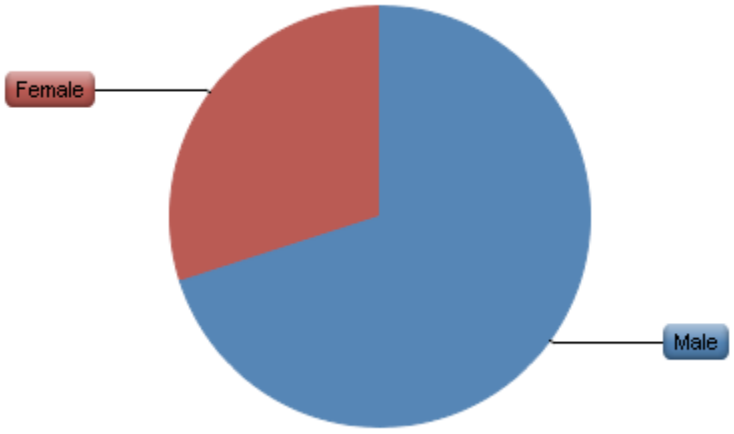
Last Modified: 11/21/2010

1. Thank You for taking part of this security survey. In the effort to better protect information and computer users from malicious attackers, it is crucial that we understand the awareness a network user posses. We will start by asking a series of questions about your computer usage and knowledge of them. Then we will administer a short test to determine your ability to spot insecurities. Your survey responses and results are kept in strict confidence and used in compliance with legal requirements. They will be anonymous; we will never use your survey questions or responses other than for the creation of a secure methodology for computer defense.

#	Answer		Response	%
	Total		0	0%

Statistic	Value
Min Value	-
Max Value	-
Mean	0.00
Variance	0.00
Standard Deviation	0.00
Total Responses	0

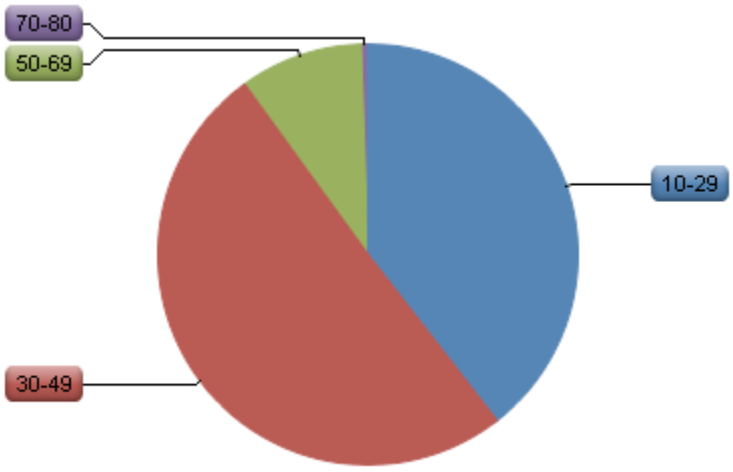
2. What is your sex?



#	Answer		Response	%
1	Male		133	70%
2	Female		57	30%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.30
Variance	0.21
Standard Deviation	0.46
Total Responses	190

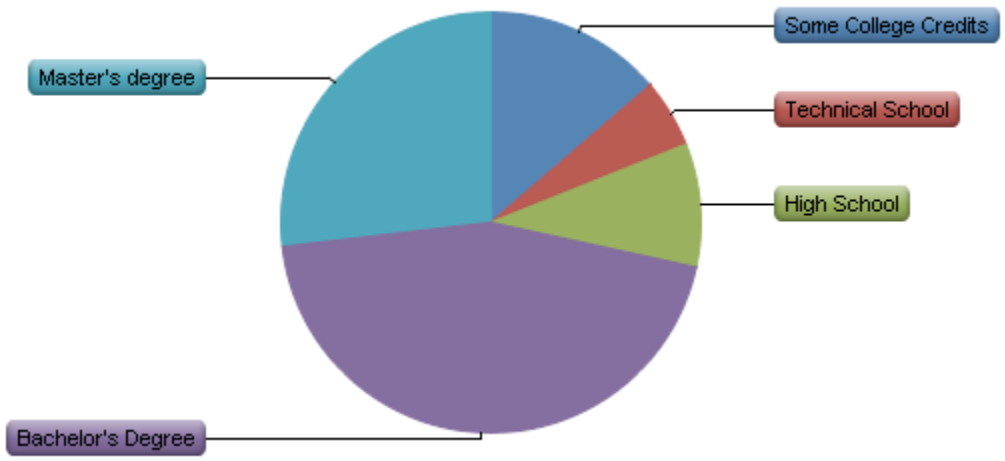
3. What is your age group?



#	Answer		Response	%
1	10-29		75	39%
2	30-49		96	51%
3	50-69		18	9%
4	70-80		1	1%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	1.71
Variance	0.43
Standard Deviation	0.65
Total Responses	190

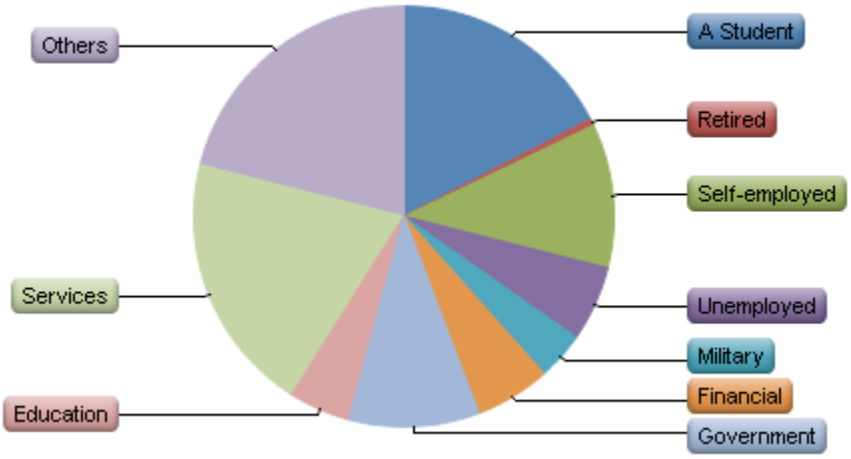
4. What is the highest degree or level of school you have completed?



#	Answer		Response	%
1	Some College Credits		26	14%
2	Technical School		10	5%
3	High School		18	9%
4	Bachelor's Degree		85	45%
5	Master's degree		51	27%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	5
Mean	3.66
Variance	1.70
Standard Deviation	1.30
Total Responses	190

5. Are you currently...?

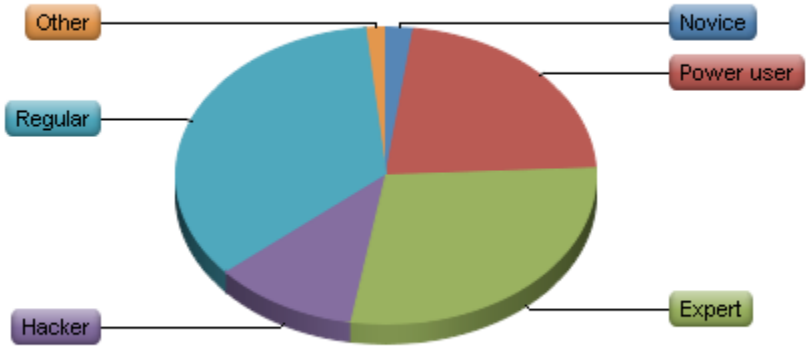


#	Answer		Response	%
1	A Student		33	17%
2	Retired		1	1%
3	Self-employed		21	11%
4	Unemployed		11	6%
5	Military		7	4%
6	Financial		11	6%
7	Government		19	10%
8	Education		9	5%
9	Services		38	20%
10	Others		40	21%
	Total		190	100%

Others
Non-profit
Employee
incapacitada
Transportation
Retail
Comp. Technician
media/communications
Banca
Research
Employed
IT Consultant
employee
Employed
Utility
Banking
Telecommunications
IT
Auditor
A prostitute
Telecommunications
Student/IT
Marketing
Design & sales
Energy
Internet
Non-profit
employed
Journalist of national newspaper
Employed
Warehouse
Associate 1
Automotive
Retired Military , emplyed commercial pilot

Statistic	Value
Min Value	1
Max Value	10
Mean	6.26
Variance	11.14
Standard Deviation	3.34
Total Responses	190

6. What type of computer user do you consider yourself?

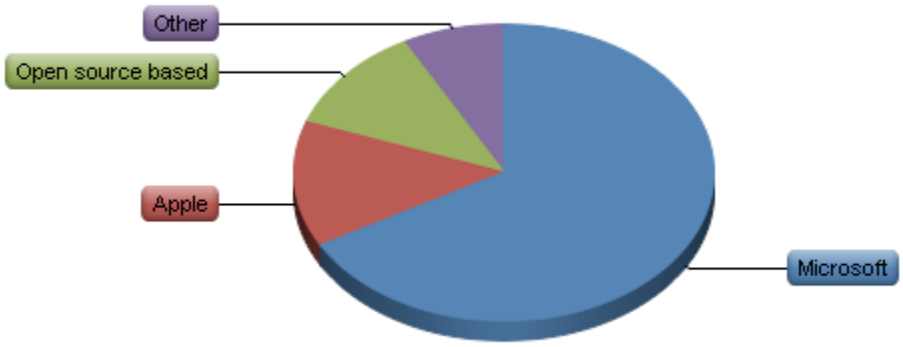


#	Answer		Response	%
1	Novice		4	2%
2	Power user		42	22%
3	Expert		54	28%
4	Hacker		21	11%
5	Regular		66	35%
6	Other		3	2%
	Total		190	100%

Other
developer
Unix Deity
Bastard

Statistic	Value
Min Value	1
Max Value	6
Mean	3.59
Variance	1.61
Standard Deviation	1.27
Total Responses	190

7. What type of Operating System do you use.

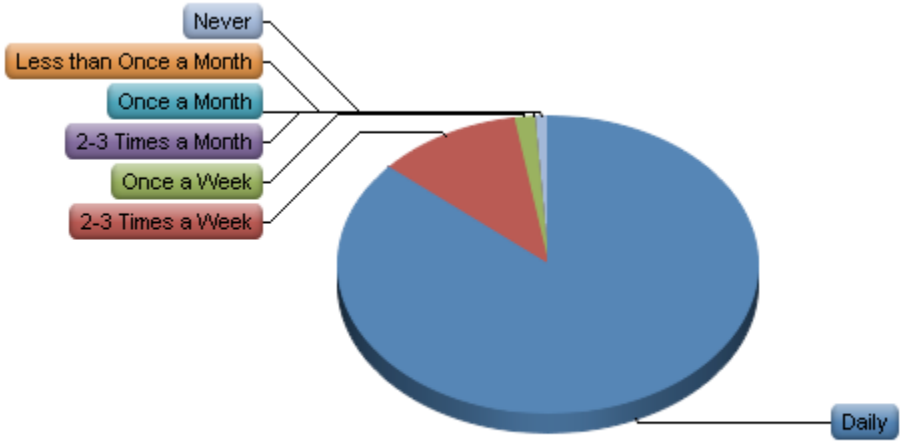


#	Answer		Response	%
1	Microsoft		127	67%
2	Apple		26	14%
3	Open source based		22	12%
4	Other		15	8%
	Total		190	100%

Other
Microsoft and Apple
microsoft/ open source
windows / linux
All of the above
All 3
The one with the thingy
Windows AND linux dual boot
All of the above
several
All above
Mix of above
PC at work, Apple at home
Everything but apple ;-)
Microsoft, Apple, and UNIX routinely used depending upon specific functions being performed

Statistic	Value
Min Value	1
Max Value	4
Mean	1.61
Variance	0.95
Standard Deviation	0.97
Total Responses	190

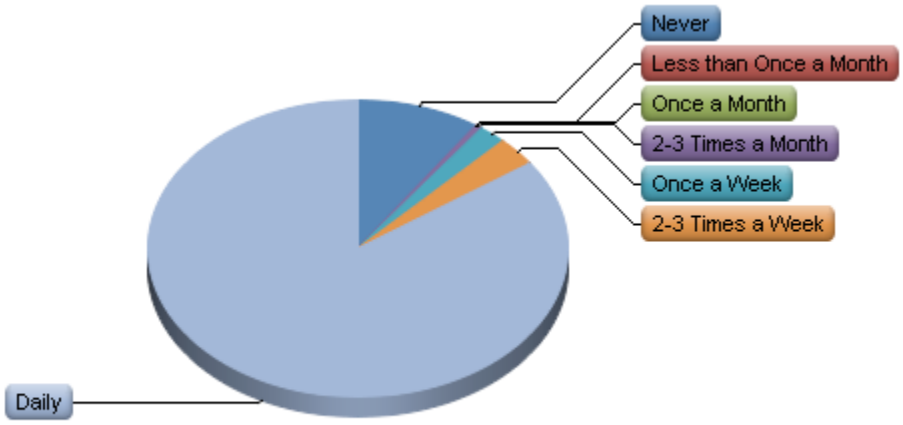
8. How frequently do you use computers at home?



#	Answer		Response	%
1	Daily		164	86%
2	2-3 Times a Week		21	11%
3	Once a Week		3	2%
4	2-3 Times a Month		0	0%
5	Once a Month		0	0%
11	Less than Once a Month		0	0%
12	Never		2	1%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	12
Mean	1.26
Variance	1.39
Standard Deviation	1.18
Total Responses	190

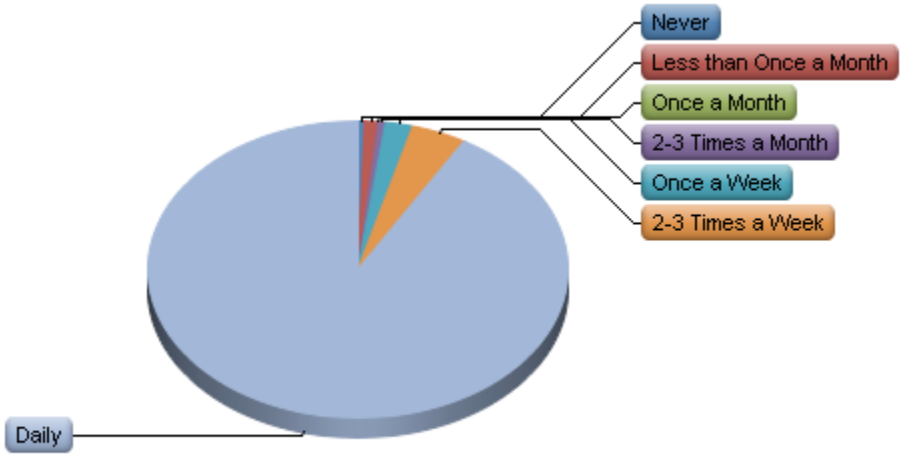
9. How frequently do you use computers at work?



#	Answer		Response	%
1	Never		18	9%
2	Less than Once a Month		0	0%
3	Once a Month		0	0%
4	2-3 Times a Month		1	1%
5	Once a Week		4	2%
6	2-3 Times a Week		6	3%
7	Daily		161	85%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	7
Mean	6.34
Variance	3.16
Standard Deviation	1.78
Total Responses	190

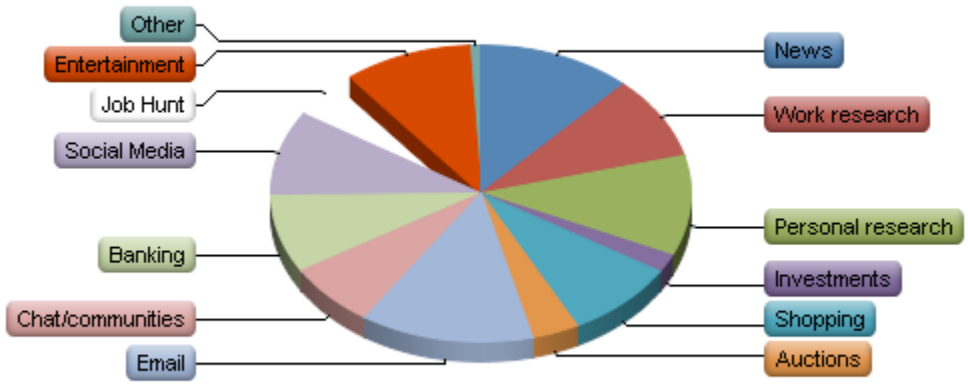
10. How frequently do you surf the web?



#	Answer		Response	%
1	Never		1	1%
2	Less than Once a Month		2	1%
3	Once a Month		0	0%
4	2-3 Times a Month		1	1%
5	Once a Week		4	2%
6	2-3 Times a Week		8	4%
7	Daily		174	92%
	Total		190	100%

Statistic	Value
Min Value	1
Max Value	7
Mean	6.82
Variance	0.60
Standard Deviation	0.77
Total Responses	190

11. What do you regularly use the web for? (check all that apply)



#	Answer		Response	%
1	News		158	83%
2	Work research		120	63%
3	Personal research		146	77%
4	Investments		26	14%
5	Shopping		115	61%
6	Auctions		48	25%
7	Email		176	93%
8	Chat/communities		93	49%
9	Banking		113	59%
10	Social Media		123	65%
11	Job Hunt		71	37%
12	Entertainment		130	68%
13	Other		12	6%

Other
facebook
job
pretty much everything :)
masturbation
pasatiempo
porn,scams
Work communication with Providers
sports
forum

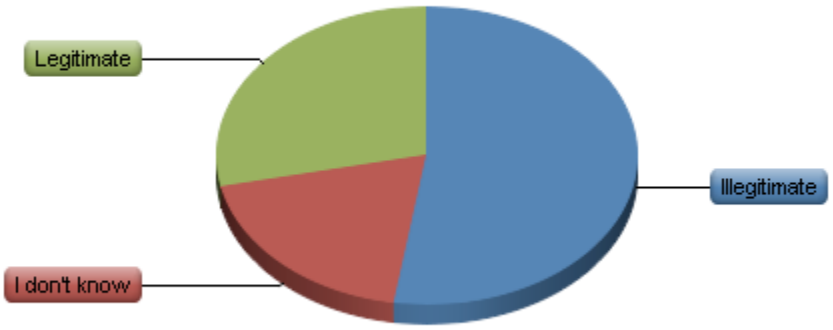
Statistic	Value
Min Value	1
Max Value	13
Total Responses	190

12. Thank You! Now for a simple Quiz

#	Answer		Response	%
	Total		0	0%

Statistic	Value
Min Value	-
Max Value	-
Mean	0.00
Variance	0.00
Standard Deviation	0.00
Total Responses	0

13. Can you recognize this email?



#	Answer		Response	%
1	Illegitimate		96	52%
2	I don't know		35	19%
3	Legitimate		52	28%
	Total		183	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.76
Variance	0.76
Standard Deviation	0.87
Total Responses	183

14. Why do you think this email is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; }

#	Answer		Response	%
1			91	100%
	Total		91	100%

Senders address, Dear Customer instead of name on account
Anytime an email ask to confirm my identity, I write it off as illegitimate.
No specific customer information. Amazon usually sends detailed data about the customer to the email. The email is also registered in the to bar.
El link me parece sospechoso
confirm your identitiy
reference to account
Among other details, because it is a general message: "Dear Customer"
because of the first bulleted item
Amazon never requested account confirmations
no es la pagina
If they ever ask me to sign into my account when I didn't plan to I believe it to be a scam
they dont ask those questions by email. someone is trying to hack your information.
Por que piden que te identifiques.
Fake
Lines around the logo do not fit properly with the lines around the text
becouse they are asking for personsl info.
Amazon subscriptions are not canceled, and several typos subtract from credibility.
Because of the square around the text
they usually request this information after you log on into the account
Legit sites generally never ask users to verify their account via email.
hunch
No tiene destinatario y el formato (background) no lo veo de ningun (mail) como yahoo, hotmail, gmail, etc.
The headers in this message are altered
Porque te esta pidiendo que confirmes tu identidad.
Is not https format
Dear customer instead of name...36 hours...if account was in danger it would be suspended right away
Link doesn't point to a secure webpage (https protocol)
Companies should not ask to log in to your account using a link in their email. Also, it does not says your name, it says "Dear customer..."
because it require your identity on line instead of asking you if you bought something from them and gave you a phone number to communicate with them
Because Amazon won't sent any message to their subscribers using a link to confirm a indentiy
No addresse in the To field
protocolo en el link debe ser https

I read about it online.
It's a sixth sense
amazon would not request me through a link to confirm my identity.
por: "sign-in.html" es muy posible que sea para obtener informacion de la cuenta del usuario de amazon.
There is no reciepient name in the TO box. The wording instills fear. Amazon would not handle a breach via email.
Not personalized and a sense of urgency
NOWHERE IN THE MAIL MY NAME IS MENTIONED, I'm addressed just as CUSTOMER.
Why would they need to confirm my identity? If my account is suspected they would just disable it.
there is no amazon's policy like that, I would prefer forward amazon this first before click any link in an email.
It says Dear Customer, not my name, it makes time limited demands, I would examine the headers and check my IDS for other signs of evil
It doesn´t have information in the field "to"
the link carries an exec in its url string
Amazon would not terminate an account within 36 hours if you didn't respond to the email.
Amazon has said they don't send announcement emails like this.
If it were legitimate then Amazon would ask you to visit their site and not provide a link. If this is legitimate then Amazon should be scolded for providing a link instead of asking the user to visit the Web site directly.
Looks too threatening and accusatory
Becauseamazon never asks for that info
I dont have an amazon account
the customer's name is not included anywhere in the email, and the link provided is HTTP, not HTTPS, and not even similar to the url for the regular amazon login page.
The name of the account holder is not included
No 'to', threatening tone, no mention of user ID, just does not look right
Live link in the email
Because it recquired additional information that I gave before.
Hi Importance, 36hour til suspension, use of "Customer", 1/20/10 4pm > 36hrs from 1/18/10 9pm
Porque amazon no manda a pedir verificación de Cuenta por Email
Amazon would never get me to click a link. They would tell me to go to the site and login.
Not Personalized. Termination of account. Gives only a link not directions how to fix if not clicking the link.
Link is HTTP not HTTPS, Also the "exec/obidos/sign-in.html" is all wrong for their page layout and format. Additionally, I think they address you by name, not "customer"
Amazon would not ask you to click a link like that (or shouldn't ask you)

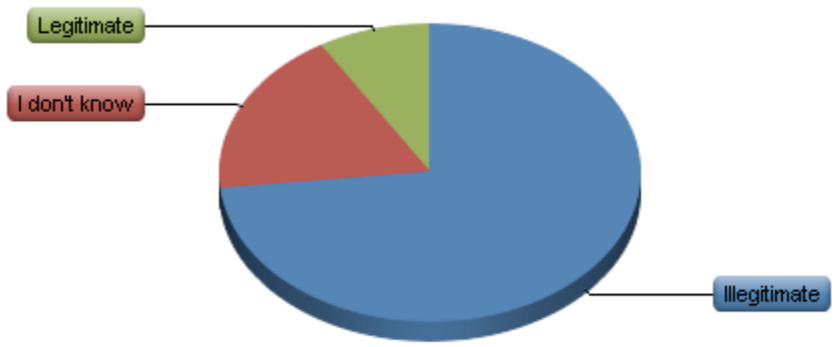
me parece bastante sopechoso de la forma que le hace saber al usuario del supuesto fraude
It looks legit, but Amazon doesn't send this type of emails.
grammatical errors; wanting to confirm my identity by clicking on a link instead of having me go directly to their site
Dont know
Address
Por que nunca preguntan código
It gives you a website to go instead of asking you to go to their website.
Amazon's business model is based on customization they would never use something as generic as "Dear Customer" also I believe they have stated in the past that they will not send links to get users to modify their information in anyway. However this does appear to be a well craft scam (assuming it is one). The e-mail address appears to be legitimate and so does the URL however it could be spoofed.
They believe that the account is compromised and they are not suspending the account. They have to suspend the account immediately
No active account will be terminated in 36 hours if it is genuine
not legitimate
Looks fake.
Misspellings. Bogus link embedded in email.
Because its looks like a picture, in the case of the letters
legitimate
no actual company asks you to clcike a link they ask you to navigate to there site then do the required steps.
It's rather threatening (all of the references to Law and account termination) and it has no personal details (usually it would be address to you, not "Customer"
The URL specified is not SSL compliant (https://). Amazon would not provide a URL which would allow the username/password to be sent in an unencrypted manner. Additionally, the To: line is blank, and the body of the email does not specify the Amazon customer to whom it is directed. The word "below" is misspelled as "bellow". Finally, Amazon would not threaten the user with account termination.
amazon never ask in a link for confirmation
I take any request for updating information as illegitimate
Nobody actually sends emails with high importance. Amazon knows uses your name when emailing. Normal extensive footers are missing. Whole concept is suspect. Would like to see where link leads to confirm whether it goes to non-amazon URL to help confirm.
Link
why should amazon want you to indentify yourself on a normal login page. Amazon wouldn't send it with high importance
It asks me to click a link as opposed to asking me to visit Amazon and sign in to my account
no es https.
I dont know

Click an "exec" link to confirm an id...doubt it

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	91

15. ---------- ---------- Citibank Notification Email Citibank is committed to maintaining a safe environment for its community of customers. To protect the security of your account, Citibank employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Citibank system for unusual activity. This is a fraud prevention measure meant to ensure that your account is not compromised. In order to secure your account we may require some specific information from you. We encourage you to log in by clicking on the link below: https://web.da-us.citibank.com/cgi-bin/citifi/portal ignoring this request for an extended period of time, may result in account limitations or in eventual account closure. Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience. ---------- ----------

---------- Can You Recognize this email?



#	Answer		Response	%
1	Illegitimate		126	73%
2	I don't know		31	18%
3	Legitimate		15	9%
	Total		172	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.35
Variance	0.41
Standard Deviation	0.64
Total Responses	172

16. Why do you think this email is illegitimate? ---------- ---------- Citibank Notification Email Citibank is committed to maintaining a

safe environment for its community of customers. To protect the security of your account, Citibank employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Citibank system for unusual activity. This is a fraud prevention measure meant to ensure that your account is not compromised. In order to secure your account we may require some specific information from you. We encourage you to log in by clicking on the link below: https://web.da-us.citibank.com/cgi-bin/citifi/portal ignoring this request for an extended period of time, may result in account limitations or in eventual account closure. Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience. ---------- ---------- ---------- .Skin .QuestionBody .TextEntryBox { width:50em; }

#	Answer		Response	%
1			125	100%
	Total		125	100%

Because I can't validate the sender's address and the link refers to a portal, which will probably redirect me elsewhere.
"ignoring" should be capital i, not very professional
Errores ortográficos.
Any email from a bank asking for information, I consider illegitimate.
Action requirements that have consequences for the user, is not normal banking behavior.
No official heading, signature, telephone number, etc.
grammar mistake and they would never send an email to confirm this nor threaten your accts
They would never send that kind of notice via email
reference to account
Doens't look like regular Citibank emails
We should receive notifications from the company not only by email, but also, by regular mail, news, etc.
because of .....may result in account limitations or in eventual account closure. statement
It's asking for specific information from the user.
asking for specific information.
they dont ask for personal information.
Bank never sent email to request more information
Te piden que les proveas informacion cuando se supone que el banco la tenga, ademas de no tener el logo del banco
no es un e-mail original
Porque no tiene logo
Asking for my information will make me believe it is a scam
they dont ask for that kind of information by email
Por que piden información personal
you never click links of unauthorized emails
Citibank does not use this approch
there is no corporate logo. also altough the address is to a secure server, the address looks unfamiliar
No logo, no proper id.
site not related to Citibank. It should start with https://www.Citibank.com or https://www.citi.com
no tiene logo ni direccion de email
Not signed or headed by any department
the bank do not ask for info over the web
banks don't for personal information through e-mail
Doesn't look secure, besides my bank account cannot be closed due for not entering

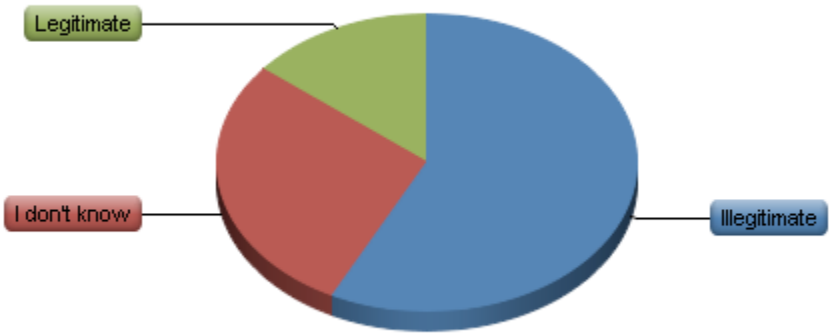
information they should already have.It's just a phishing so i enter my personal and bank information.
If it is that important they should call
not a direct Citibank website nor citibank logo.
web addres is suspicious and does not have anywhere the company logo
this sounds fishy: ignoring this request for an extended period of time, may result in account limitations or in eventual account closure.""
They inquire about this matter by phone or mail
Porque la banca no envia emails para confirmar info.
web address looks wrong
No alternative contact method, such as telephone, is provided to address the issue.
Information request
The banks do not confirm personal info through emails
If they need response from the client as soon as posible, they should require the infomation in their portal once you login.
They suppose to send you this information via current mail instead of an e-mail
No logos, URL is suspicious
Because Citibank wont use email to confirm or collect information via web. They will use correspondense and other security questions.
Asking for login, possibly poisoned/hacked website
utiliza un sbdominio
Read about it online
the url is not a citibank URL. Citibank would put a hold on my account and phone. They would not send such an email
Citibank does not send email to validate customers. When you log into your account, they will collect information you designate as proof of identity, answers to questions only you know
It is not an e-mail.
banks dont solicitate that kind of information trough e-mail.
Not personalized and a sense of urgency and bad URL
There is no logo. There is no name. Banks reccoment not to use a link in an email to answer any questions
Again. If I admionister the system I shut off a dubious account and wait fort someone to complain.
por la forma en como empiesa la direccion de donde me escriben el email
Close my account? Really?
Not specified. Too general.
looks funny
time limited demands again

The link isn´t the official site of the bank
FUBAR domain name
https://web.da-us.citibank.com
web. is an option for free domain names.
CItibank says they don'e send notification email like this. Plus, there are punctuation errors.
Your bank should never need to confirm information with you unless you are contacting them and they want to make sure you are the correct person. They should not contact you and ask you to provide information they already have.
Banks don't operate like this. At least real banks don't.
Because of the provided link
They typically include the last 4 digits of your account number and would not email customers asking for information.
a bank would not close your account with funds still in it!!! i believe your aim was me looking for https as a secure login however with html trickery that link could redirect to another site
I dont have a citibank account
no reference to your name or account numbers etc. also, the link is not on "citibank.com" it is on a sub-domain "web.da-us".citibank.com
Requesting information that they should have already
web.da-us.citibank.com?
The threat of account closure seems a bit extreme
Threatening, too much pressure to fix it now, should come by snail mail
(live) link in the email
Starts with another direction not the bank
No logo or branded images; also de URL looks fishy
page doesnt exist
Porque citibank no manda a pedir información sobre su cuenta
They failed to capitalize stuff. If this was real, it would have been proofread first.
Not personalized. Says will limit account. No other options or contact information
">
no number to call with questions. Also they normally suggest copying and pasting the URL into your browser if you can't click on it.
'ignoring' is not capitalized. Citibank wouldn't just send out a frod prevention email because it's a good thing to do.
I would suspect that the url is actually pointing to a different place. Hard to say without seeing the actual url.
no creo q un banco me envie un e-mail como este
In the URL, the domain is "da-us" and not "citibank".
wanting the person to click on a link in an email is not secure

Bad spelling
web.da-us.cit_i_bank.com
Text and address
The url "https://web.da-us.citibank.com/cgi-bin/citifi" is a spoofed site due to "web.da" added on.
Tiene un link
They do not ask for this info via e-mail.
I can't see the email address.
A bank would not (or at least should not) "encourage you to log in by clicking on the link below"
Requirering specific info.

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	125

17. Can you identify a URL? http://paypalsecurity.co.uk/security/protectyourdata.asp



#	Answer		Response	%
1	Illegitimate		97	57%
2	I don't know		48	28%
3	Legitimate		24	14%
	Total		169	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.57
Variance	0.53
Standard Deviation	0.73
Total Responses	169

18. Why do you think this URL is illegitimate? http://paypalsecurity.co.uk/security/protectyourdata.asp

#	Answer		Response	%
1			96	100%
	Total		96	100%

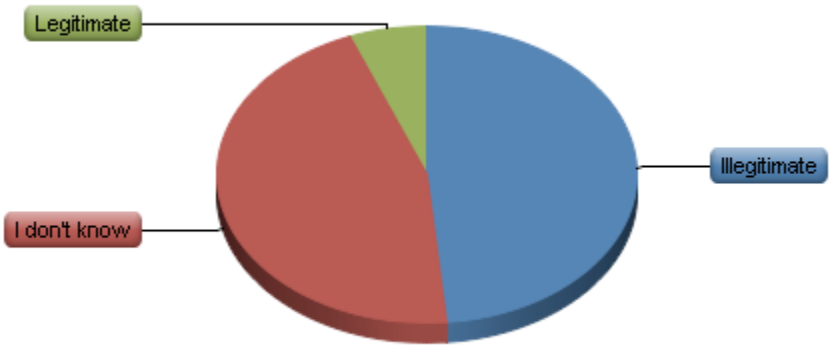
I expect any security link to be https
over emphasis on security
Paypal uses a secure server
Falta de SSL en el URL.
the name seems illegitimate due to naming conventions for paypal which would be under the paypal url
.uk and says paypalsecurity
It ends on .asp
no https...
Should be https
paypal uses https on everything
el dominio no existe
por ser de pay pal
Entre y no existe
the s is missing from http
Piden verificar tus datos de seguridad
https://
Only www.paypal.com is real
its from the uk and the asp
identity of website has not been verified. Website does not exist.
porque deberia decir https:// y debe no dice .com como deberia
Does not exist
the .uk
ends in .asp
it should be something like paypal.com/security
improperly structured domain
This is a forgery of a Paypal account
It's not paypal.com
Esa no es la direccion de Paypal.
Pretends to be from Paypal.com but is from co.uk
Is not https
just looks fishy
protocol must be https
Paypal always use their domain: paypal.com for everything. This is also a .uk domain
Paypal URL does not contain .co.uk
Not the official paypal uk website

not a secure site using https
falta parotocolo y dominio sospechoso
I'm not sure.
Just simply Iknow
there is not such domain name
It is not a paypal URL
it's not https and it suggests it's used for data protection
it's not paypal.com
it is a good url.
It is not an HTTPS
UK????
no termina en .com
Not Working
.co.uk?
Its not a secure site
after dot not convincing
httpS:// the web page displayed is not secure
it is not paypal
The link doesn´t seem official
If I were in the UK, maybe I would know better, but since I'm in the US I wouldn't click it.
https
Paypalsecurity.co-uk, not a subdomain of paypal.com
paypal have a section for security on their own domain.
paypal is a us base company and the domain name is not using the stadard paypal.com TLD
not a paypal domain
That is not propoerty of paypal
not the official paypal.co.uk domain if it was a subdomain of the URL i'd be tempted
Its parents were not married
paypalsecurity.co.uk is not owned by paypal, and the link is a script, which is not protected by SSL....HTTPS
paypalsecurity.co.uk? really?
it doesn't point to anything related to paypal
.co not .com
paypalsecurity? BS!
La url no corresponde
Not in form of paypal.*/*
security in the first part of the name. Would expect paypal.co.uk/security or security.paypal.co.uk

non-https. Also running off paypaysecurity.co.uk (not paypal.co.uk).
not https, not the official paypal.com
Paypal would use a subdomain for "security" (i.e. security.paypal.com) instead of a new domain. The URL says "security" twice (kind of overselling the idea). The ".co.uk" doesn't help it seem por legitimate either.
https
Not in correct sequence
".co" is suppose to be ".com"
Por debe decir US y Uk
www. is missing
No https://
Paypalsecurity is not a subdomain of paypal.com
Doman Whois results say the site is owned by John Rattigan from NJ
dont have security (HTTPS)
Lack of "HTTPS"
.co.uk gives it away and the paypal "security" is a good one to....
No usa https
it's not from paypal.com
It's not SSL encrypted (https://) and contains a .co.uk, instead of .com
Should be https
unknown address
It isn't https://paypal.com so it not affiliated with Paypal
There's no such thing as "paypalsecurity".co.uk
PayPal's domain is paypal.com and not paypalsecurity
Not a secure link and paypalsecurity does not exist
no

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	96

19. Can you identify a URL? http://203.144.234.138/us/safedata/index.html



#	Answer		Response	%
1	Illegitimate		81	49%
2	I don't know		76	46%
3	Legitimate		10	6%
	Total		167	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.57
Variance	0.37
Standard Deviation	0.61
Total Responses	167

20. Why do you think this URL is illegitimate? http://203.144.234.138/us/safedata/index.html .Skin .QuestionBody .TextEntryBox { width:30em; }

#	Answer		Response	%
1			81	100%
	Total		81	100%

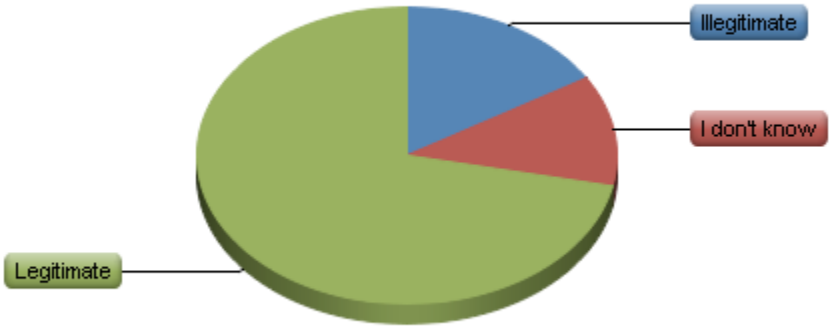
use of ip address directly as the url is not standard industry practice. would suggest a direct address to a static ip address, usually an attacking computer
using IP address as url seems shady.
Por los numeros
no https and no branding
IP instead of DNS name
no hostmane
no esta disponible
Ip is shown not the name of the company
No existe
No company name or data
Pq ni tiene una pag para dirigirse
Piden entrar tus datos de seguridad
it seems like an IP address ..
So many numbers in the #
It seems to be a mobile/unnamed domain name
because it starts with numbers
yes, it's providing IP address on the URL.
it looks like an ip address
no creo que un URL comienza con numeros
Internet address doesn't show the IP address on their links
It's an IP address. Could be anything
Highly suspicious due to the use of IP instead of domain and no HTTPS
protocol and ip
Web pages using ip addresses in their address doesn't inspire trust. Regular users can't recognize if it is safe.
For my point of view if the site is not from the US I will not acces the site. Also I check the site first in Whois prior to gain access to it.
IP
No DNS name for site
el dominio no esta registrado es un ip
Phishing pages often have numerical web addresses
Destination host unreachable
it is an IP Address
It is not https. I would not respond to a direct address..
el ip en el URL.
IP address used instead of domain name

Does not have a Domain Name Registered for the IP Address used.
There is not ..com and I was not able yo ping the address.
I don't know where the IP is going
Starts with an IP address
no lo reconsosco el monton la direccion de ip
Not Working
nslookup 203.144.234.138 returns this 203-144-234-138.static.asianet.co.th
there was an ip displayed on the web direction
can't tell what/where it is or what it is supposed to be I would not go for it
carries a ip address which is not known for sure could be a redirect
A straight IP address? Pass.
http://203.144.234.138/us/safedata/index.html
Likely illegitimate, no domain name, http connection to "safe data"
IP based domains are asking to phishing sites.
Because it has an ip
it's not likely a company would provide their IP address instead of a domain name.
unless it was a friends site or something informal i.e. forum. why would they give IP rather than domain
Im just guessing now
they use an IP rather than regular URL. they must be hiding the site name for a reason.
no obvious identification
Isn't 203 a class D address, whereas most businesses will get a Class A?
IP address (as opposed to domain name)
Request TImedout, also "safedata" is a pretty let me infect you type shit
No especifica nada la URL
IP address
ip address only. Not company domain name.
non https, don't trust IP's.
Should use a domain name!
If someone is coercing me to click this link, I would be weary of the IP instead of a hostname.
should have a name after the //
IP instead of name
Numbers
IP from Thain, maybe an chinese proxy
don't like it, can't identify
Usually reputable websites won't have an IP number in the URL
Who uses direct IP addresses for legitimate purposes?

IP traces to Thailand which may not make it illegitimate, but its listed as a possible phishing site.
Number string at beginning of address is suspicious.
No utiliza un hostname
it connects to an IP instead of a URL. Highly likely its a phishing attempt.
A DNS lookup of the URL shows it registered to Thailand. Though there are no specific blacklists against the URL, the associated name servers are suspect, since they have no apparent relation to the "safedata" listed in the full URL above. Thusly, it must be treated as illegitimate.
unknown address
DNS exists for a reason! Using the IP address rather than a domain name just obscures the target website and credible sites would go out of their way to do the opposite.
this could be any machine in the web without a domain name
No domain name, could lead anywhere
no

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	81

21. Can you identify a URL? https://paypal.com



#	Answer		Response	%
1	Illegitimate		27	16%
2	I don't know		20	12%
3	Legitimate		119	72%
	Total		166	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.55
Variance	0.58
Standard Deviation	0.76
Total Responses	166

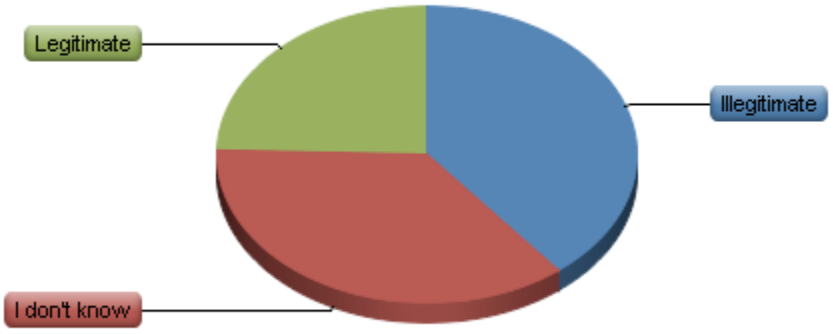
22. Why do you think this URL is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; } https://paypal.com

#	Answer		Response	%
1			26	100%
	Total		26	100%

html
Falta www
i think they're not https
por que no tiene el www
https is not right, it should be http
http://www.paypal.com
http prefix does not contain s in the url
It should read "http://www.paypal.com"
its http://
https and not www
no www
hay blancos entre los slashes y asi no sale ninguna direccion
Incomplete address
Because the legitimate Paypal contain www.
no esta firmado www
missing www
I would expect paypal to be www.paypal.com
no www in address
WHERE IS THE WWW?
url not owned by paypal, and there is no WWW... which is definately present in the legitimate site.
falta www
Esta mal escrita
'S' after 'http'.
Because its refers to a secure site without login address
it's not a official wed address
I refuse to talk to unknown addresses

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	26

23. Can you recognize this email?



#	Answer		Response	%
1	Illegitimate		64	39%
2	I don't know		59	36%
3	Legitimate		40	25%
	Total		163	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.85
Variance	0.62
Standard Deviation	0.79
Total Responses	163

24. Why do you think this email is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; }

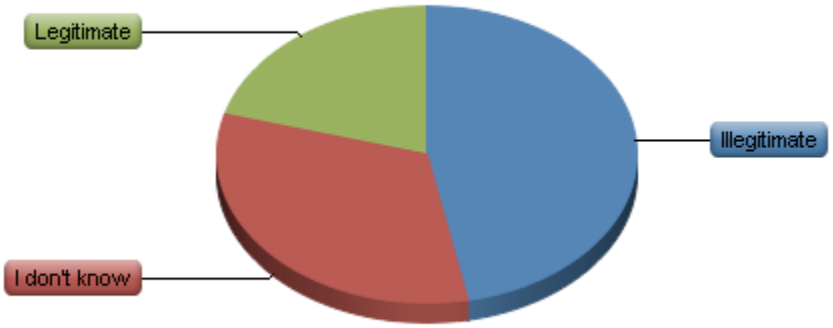
#	Answer		Response	%
1			61	100%
	Total		61	100%

Because it has too many grammar errors to be from a nonprofit organization.
grammar
I consider illegitimate, anyone asking for money who doesn't make sure their letter has no misspellings.
formatting, and incorrect use of 's in email
Ort Errors
asking for money
Donations
The address is not shown
Look like a spam e-mail.
Linking to a bunch of sites does not make it legitimate, anyone can make an e-mail like this
Muy probable nunca le has dado tu email personal a Wyclef Jean
Wycliff and friends looks auapicious
There are grammar mistakes in this email that makes me suspicious.
Grammar errors
Typos make it less credible
Too generic, source not specified
badly broken english
It has many grammar errors
Poorly written
How they get your email? Once you click on those links, you can be redirected to a phishing website where they compromise your information while you think you are "really helping"
Spelling errors
Because the message is sent out in a mass-mailing list to hundred and thousands of individuals and is not personalized the message.
Terrible English, and Wyclef Jean himself is an unscrupulous bastard
Horrible grammar and syntax
I just know from the news
El como esta organizado la carta y las palabras me hacen pensar que se trata de algun fraude.
email format, wording, gammar errors, use of celebrity name. no personalized greeting
Bad written, not even a spellcheck was done.
many spells errors
So many reasons... We'll go with terrible spelling/grammar
Poor grammer, no flow to the information, random capitalization errors.
Many grammar, spelling, and punctuation errors.
Too many typos

Because they don ask for money that way
that many typos typically means spam
bad grammar. doesn't look pretty enough for them to be asking for my money. charities make profit why list any charities outside of the same holding company?
obvious grammar and spelling mistakes throughout
too many errors and lack of traceable information
does spam count as illegitimate?
Poorly written email
Bad spelling, grammar
Live links in the email, grammatical errors
Legit or Not, it's learned not learnt, and i wouldnt mess with an illiterate person's email haha
Porque son otras organizaciones
' Trying SQL injection
Poor formatting and spelling
If it came to me, in my inbox it seems suspect only because I've never had correspondence with Wyclef outside of my headphones. Otherwise, it seems legitimate.
List
This uses similar tactics to the “Nigerian Prince” scam. It is unlikely that this type of campaign would include e-mail unless a user has subscribed to a mailing list.
Por que estan pidiendo dinero
spam
Bad structure and grammar.
because not recognize
I actualy ogt that e-mail scam in my inbox. they point you to "communityites you know" giving you a sense of safty... most cases the e-mails i got the URL were facts as well.
No es ilegítimo
The email sender is likely fraudulent, since a legitimate organization wouldn't solicit charitable donations via generic email. Additionally, there are many spelling and formatting errors, which indicate that it is fraudulent.
To many errors in the text , I would donate through known entities
Formatting and spelling is terrible. Looks like spam more than something more malicious but it's getting deleted either way.
Hatai scam...clasic

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	61

25. Can you identify a URL? https://security.ebay.passwordreset.com/



#	Answer		Response	%
1	Illegitimate		75	47%
2	I don't know		52	33%
3	Legitimate		33	21%
	Total		160	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.74
Variance	0.61
Standard Deviation	0.78
Total Responses	160

26. Why do you think this URL is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; } https://security.ebay.passwordreset.com/

#	Answer		Response	%
1			75	100%
	Total		75	100%

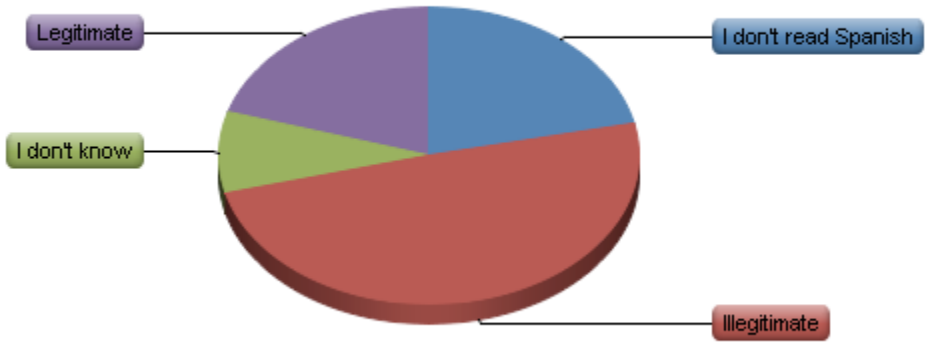
Intenta hacerse pasar por otra web.
not standard use of url for ebay password reset
https:
Doesn't look like Ebay's security URL
not valid domain name for ebay very suspicious (security.ebay.PASSWORDRESET.com)
la pagina no existe
ebay.passwordreset.com?
No existe
Por que una vez creas una cuenta ellos no te piden nuevamente que verifiqueso resetees
Only www.ebay.com is real
When resetting a passqord the address (url) is different
the s
website does not exist
Does not exist
It should read "http://..."
not the correct page for password reset
https
por lo mismo de orita los slashes separados
Because of the passwordreset in the URL
Pretends to be from ebay.com but is from passwordreset.com
looks fishy
Domain adresses should be read from right to left. The primary domain here is passwordreset.com, fake
ebay does not have a site to reset password. The way it work is that ebay send you a message with a temporary password to reset your password.
Not ebay
passwordreset.com is not a secure way to reset a password
falta firma www
I don't trust
it is not under "ebay.com" domain. passwordreset.com it's an illegitimate domain name
i would expect ebay to be www,
Again - Domain name not ebay.com instead it's passwordreset.com.
It's not ebay.com
no www in address and password reset would not be in the url name
Not working
straight to password reset?
nslookup return unknown

ebay is not a subdomain of passwordreset
It´s strange the option to reset a password.
sorry i would say secure ad its https
passwordreset.com
It's all a subdomain of passwordreset.com, not ebay.
Ebay have their own password reset name.
It didn't work when I tried it. Plus, it would most likely end with ebay.com.
if it were a legitimate ebay url it should read something like https://security.passwordreset.ebay.com
passwordreset.com is not an ebay domain
the domain is passwordreset.com not ebay
it's possible it's a legitimate URL for passwordreset.com but not eBay
TLD.
security.ebay is a subdomain of "passwordreset.com" in this case...this would not be ebay,
domain of passwordreset.com?
TLD IS INCORRECT
several levels of subdomain, passwordreset.com looks suspicious
The domain passwordreset.com seems fishy
passwordreset.com....
passwordreset.com?
passwordreset in the domain name
passwordreset.com? really?
Ebay's not going to use a third party domain to reset their passwords.
passwordreset.com is the domain which could be totally separate from ebay.com
Domain is "passwordreset.com" and not "ebay".
Due to the page "security.ebay" being on the "paswordreset.com" domain. It should be the other way around. They usually send a password reset email or supply a password reset link an email.
eBay tiene su propia seguridad
The domain is passwordreset.com not ebay.com
domain registered to someone other than ebay.com, and the ebay password reset page is scgi.ebay.com
I would have to see the page that lead to this link. I wouldn't trust it directly.
I tried it out. It's fake.
almost had me on that onse.... the domain "passwordrest" e-bay does not own it.
Nombre de dominio
security.ebay is just a subdomain of "Passwordreset.com" which doesn't belong to ebay.
This URL may be legitimate, but if eBay were to send such an email, a genuine link would

redirect the user to the standard https://ebay.com login screen. To err on the side of caution, it should be treated as illegitimate. A separate browser session should be initiated and the URL should be manually typed into the address bar (https://ebay.com).
Why keep asking the same question????
TLD is passwordreset.com not ebay.com
passwordreset.com....good luck

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	75

27. Can you recognize an email?



#	Answer		Response	%
1	I don't read Spanish		34	22%
2	Illegitimate		78	49%
3	I don't know		14	9%
4	Legitimate		32	20%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.28
Variance	1.04
Standard Deviation	1.02
Total Responses	158

28. Why do you think this email is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; }

#	Answer		Response	%
1			78	100%
	Total		78	100%

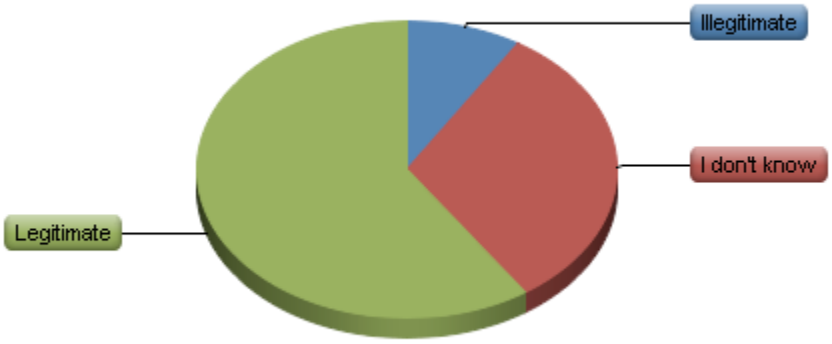
Cause of the sender's address. Bppr is not .es (Spain)
Direccion de correo electronico erronea.
Any email asking for information about a bank, I consider illegitimate.
the url source is incorrect
they would never do it online, they would tell you to call
Banks dont ask for that kind of information
email is not the right venue
info@bancopopulars.es not real
The notification should not include the link and an inmediate action. Just the notice.
invalid email endind with S. info@bancopupularS.es and theres a time limit plus the real bank may required a telephone call to customer services to verify your identity or a trip to the bank
porque el dominio es bancopopular.es en vez de popular.com
Banco popular never sent email. They call
The email address is populars.es is misspelled and is from Spain
I have been in this situation and there is no way to reactivate other than waiting 24 hours
Banco Popular will cancel the transaction automatically. You will have to call them probably
En este email, creo que es por la dirección que termina en .es y si es aqui en Puerto Rico deberia terminar en .com
.es no hoy banco popular aya
the email address doesn't match Banco Popular emails sent in the past.
you call the bank to make a change
email address Not related to "Banco Popular"
porque por lo regular el banco solicita que llame por telefono
Contradictory; it says the account's been temporarily suspended, but threatens to suspend it after 24 hours.
For important things they ask you to call
for reset of the account, they ask you to call to customer service
not banco popular email domain sand ends in .es
email .es
not the usual way their email look
On this matter, they call you by phone This is a fake e-mail
It's from @bancopopulars.es, not bppr
Por el enlace
Email was sent from a domain different from the one use by Banco Popular
Nobody can force you to change your password just by email.

Email address looks suspicious and the pressure is atypical
Email is asking for verification vía a specific link and within certain timeframe
the email sender is from spain and banco popular is in Puerto Rico
It is good to check the source email. Bancopopulars.es is not the official domain. Once again, using a link in emails to login to your account it's not safe
Because Banco Popular does not have a .es site.
Banco Popular doesn't send out such emails
direccion del sender tiene origen en espana y el banco es de puerto rico
The authors email address is incorrect
I jave block my account wit hthis bank and I have never received an e-mail
the domain name "bancopopulars.es" is illegitimate. is has a "s" in the end.
Usualmente cuando este tipo de cosas pasa uno debe comunicarse con un representante de servicio.
There'd be no reason fo me to receive a spanish email, There is no name in the TO box.
Populars
banks dont solicitate that information trough e-mail.
Don't know spanish but I do know that this is email has a sense of urgency
They are asking to use a link inside the email.
por la forma del aviso importante
*.es
Because the pressure to do it quickly.
Because of the email address.
bancopolulars.es doesnt exist
I don't bank there and I am not Spanish, nor can I read Spanish or ask for my banking in Spanish
Usually the bank doesn´t desactivate a count.
Again, they won't terminate your account for not clicking on an email.
bancopopularS
Banks don ask for that
reactivate an account electronically is not a regular request of banks, the urgency to respond (within 24 hours) is always suspect
.es
Because BPPR notifies its corumers by other manner
Porque un Banco no te manda a pedir la información de la cuenta
not in native language
no siempre voy a utilizar el mismo IP si uso diferentes computadoras
Porque el mail es "@bancopopulars.es" y no "@bancopopular.es". Hay que prestar atención a los detalles ;-)

asking to act on a link instead of going to bancopopular.com
The .es
Yes
I don't read spanish but when I looked up "Banco Popular" it returned an actuall bank with that name but the domain was "popular.com", not "bancopopulars.es"
El banco popular tiene seguridad y lo q puede hacer es frisar la página.
N\A
Por la dirección de email y porque es ilógico que suspendan mi servicio del banco por eso
The main tip-off here is that the return address is bancopopulars.es. Additionally, the bank would likely contact the customer via telephone if such a suspicious act were detected. Finally, they would not suspend your account or require reactivation, before notifying the customer via telephone.
they asking to go to an alternate ip address to go to.
Same answer I would call them or even visit a Brach office

Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	78

29. Can you identify a URL? http://cars.com



#	Answer		Response	%
1	Illegitimate		14	9%
2	I don't know		50	32%
3	Legitimate		94	59%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.51
Variance	0.43
Standard Deviation	0.66
Total Responses	158

30. Why do you think this URL is illegitimate? .Skin .QuestionBody .TextEntryBox { width:50em; } http://cars.com

#	Answer		Response	%
1			14	100%
	Total		14	100%

Falta www
isnt it www?
no esta completa la direccion
To vague no www
no
its missing the s
no www
The correct site is www.cars.com
falta www
sorry it's legitimate
I'm not able to access the site or ping it.
I think is legitimate. Just press the wrong buttom. Sorry
Porque no esta completa
missing www. before cars

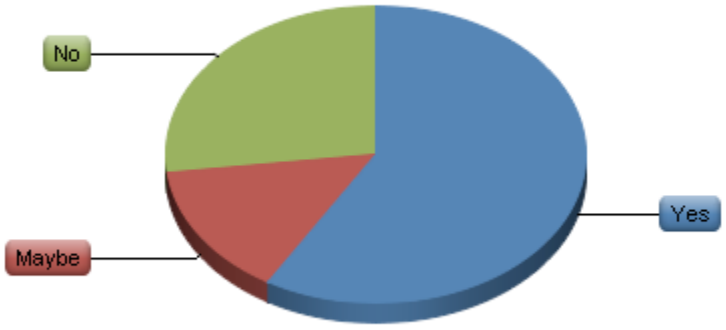
Statistic	Value
Min Value	1
Max Value	1
Mean	1.00
Variance	0.00
Standard Deviation	0.00
Total Responses	14

31. Thank You !! Just a few more questions and we are done. We thank you for your time.

#	Answer		Response	%
	Total		0	0%

Statistic	Value
Min Value	-
Max Value	-
Mean	0.00
Variance	0.00
Standard Deviation	0.00
Total Responses	0

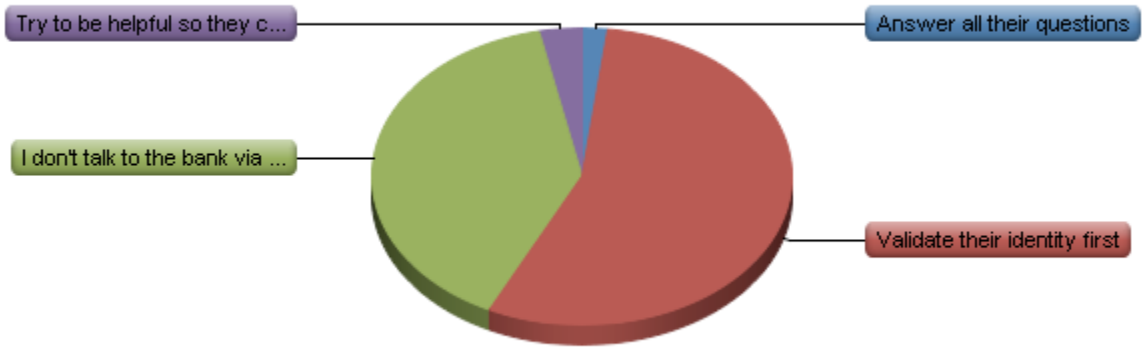
32. Have you received an email, a call or letter within the past 6 months that you suspect was an attempt to get your personal details for fraudulent purpose?



#	Answer		Response	%
1	Yes		89	59%
2	Maybe		22	14%
3	No		41	27%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.68
Variance	0.76
Standard Deviation	0.87
Total Responses	152

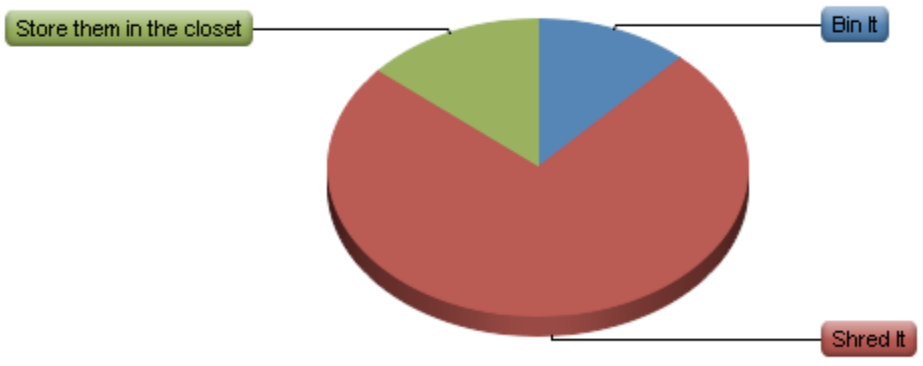
33. When your bank or utility supplier calls do you:



#	Answer		Response	%
1	Answer all their questions		3	2%
2	Validate their identity first		84	55%
3	I don't talk to the bank via a phone		60	39%
4	Try to be helpful so they can help me		5	3%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.44
Variance	0.35
Standard Deviation	0.60
Total Responses	152

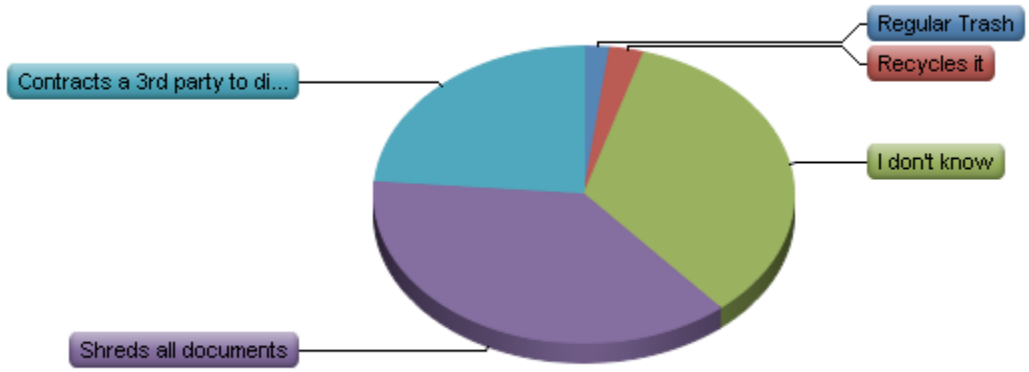
34. How do you dispose of your sensitive letters or bills?



#	Answer		Response	%
1	Bin It		18	12%
2	Shred It		113	74%
3	Store them in the closet		21	14%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.02
Variance	0.26
Standard Deviation	0.51
Total Responses	152

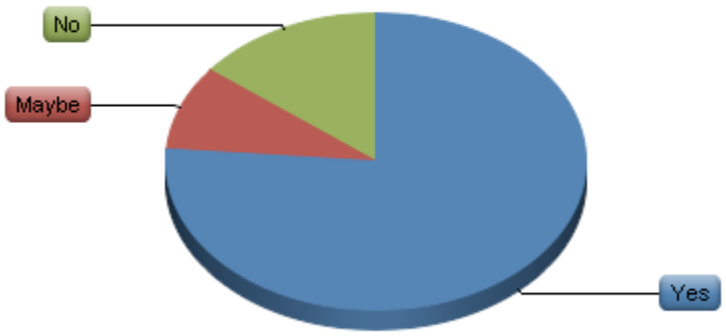
35. Do you know how the company that you work for handles sensitive material?



#	Answer		Response	%
1	Regular Trash		3	2%
2	Recycles it		4	3%
3	I don't know		52	34%
4	Shreds all documents		57	38%
5	Contracts a 3rd party to dispose		36	24%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	5
Mean	3.78
Variance	0.82
Standard Deviation	0.91
Total Responses	152

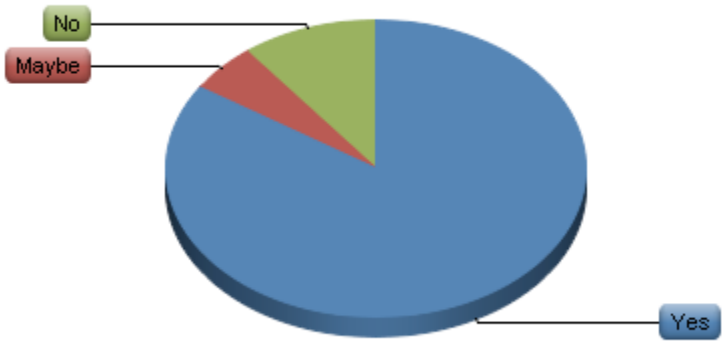
36. Do you know what a network security policy is?



#	Answer		Response	%
1	Yes		116	76%
2	Maybe		14	9%
3	No		22	14%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.38
Variance	0.53
Standard Deviation	0.73
Total Responses	152

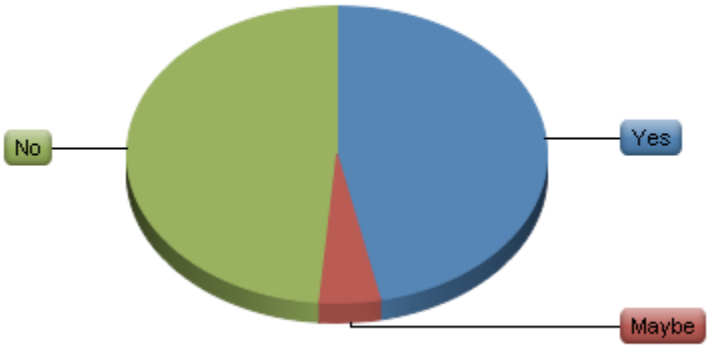
37. Have you heard the term “phishing” before?



#	Answer		Response	%
1	Yes		128	84%
2	Maybe		8	5%
3	No		16	11%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.26
Variance	0.41
Standard Deviation	0.64
Total Responses	152

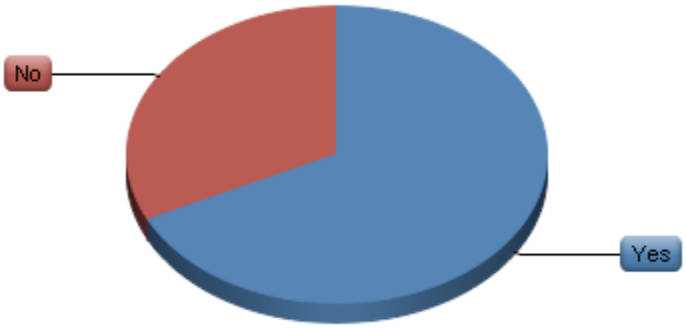
38. Have you ever taken an information awareness course?



#	Answer		Response	%
1	Yes		71	47%
2	Maybe		7	5%
3	No		74	49%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.02
Variance	0.96
Standard Deviation	0.98
Total Responses	152

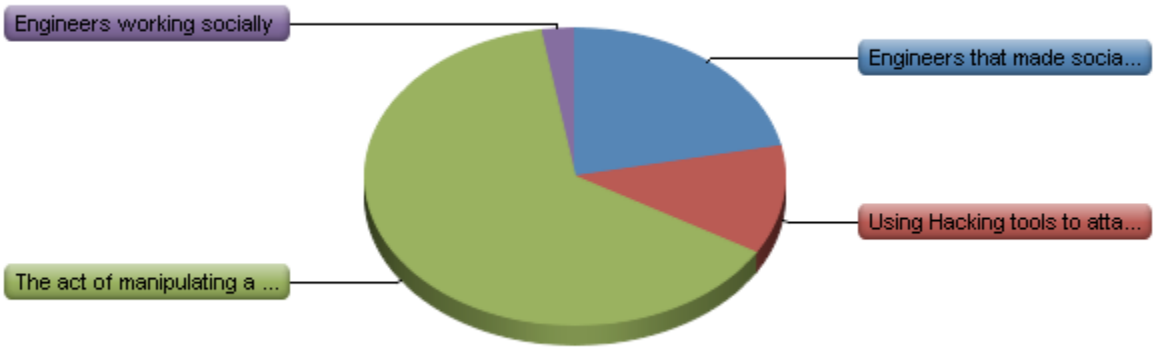
39. Have you heard the term "Social Engineering" before?



#	Answer		Response	%
1	Yes		103	68%
2	No		49	32%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.32
Variance	0.22
Standard Deviation	0.47
Total Responses	152

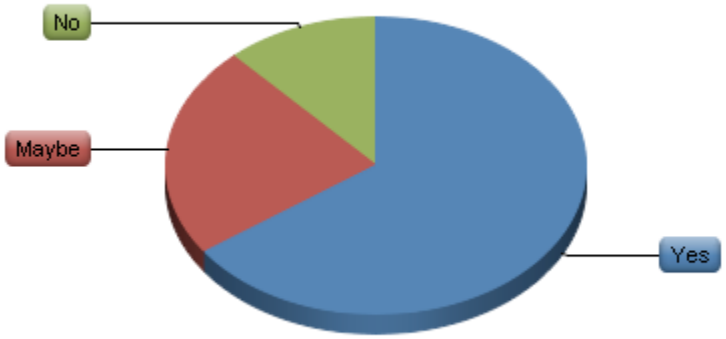
40. What do you think Social Engineering means?



#	Answer		Response	%
1	Engineers that made social media networks possible		33	22%
2	Using Hacking tools to attack social media networks		18	12%
3	The act of manipulating a person to accomplish goals		97	64%
4	Engineers working socially		4	3%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.47
Variance	0.74
Standard Deviation	0.86
Total Responses	152

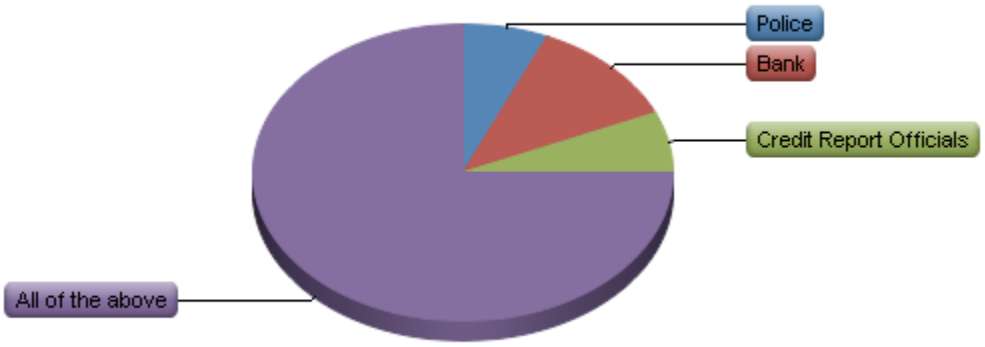
41. Does the company that you work for have a Network Security Policy?



#	Answer		Response	%
1	Yes		99	65%
2	Maybe		35	23%
3	No		18	12%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.47
Variance	0.49
Standard Deviation	0.70
Total Responses	152

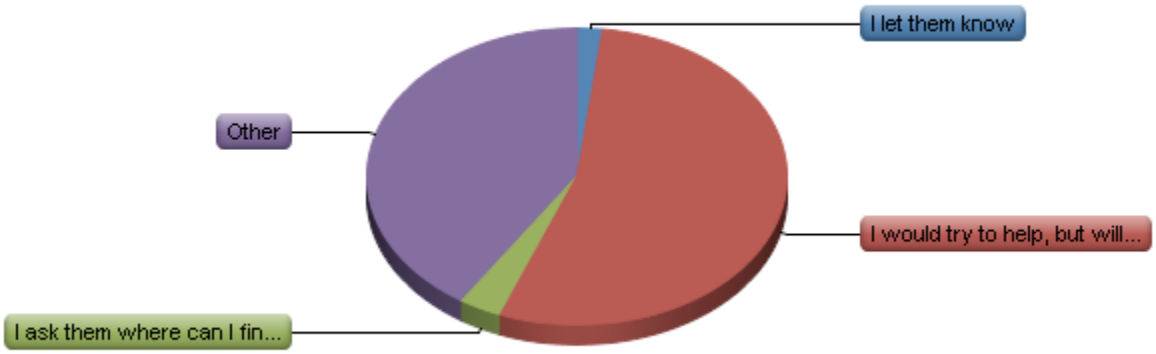
42. If you suspect you have become a victim of identity theft, who will you contact first?



#	Answer		Response	%
1	Police		10	7%
2	Bank		18	12%
3	Credit Report Officials		10	7%
4	All of the above		114	75%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	3.50
Variance	0.89
Standard Deviation	0.94
Total Responses	152

43. If someone calls you asking for the type of Internet browser:



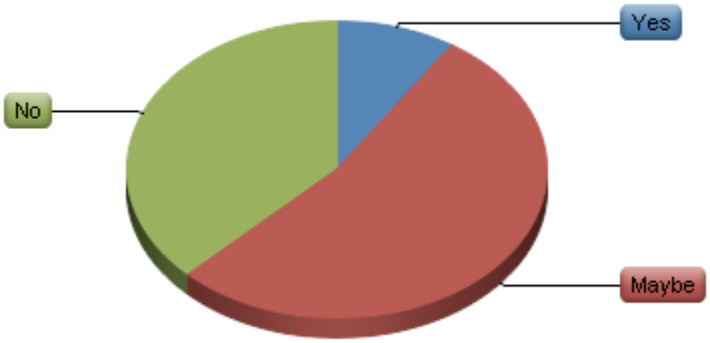
#	Answer		Response	%
1	I let them know		3	2%
2	I would try to help, but will ask why		82	54%
3	I ask them where can I find that information to tell them		5	3%
4	Other		62	41%
	Total		152	100%

Other
If its at work, I'd refer them to the IT dept.
I don't think I understand this question
no
No
i wont let them know.
No doy información
I will ask them why do they want that information.
I won't say
not tell
hang up
Dont answer
Would ask the purpose and then determine if I should answer any questions
No
If is at work I support them if is at home I do not answer the question.
no digo nada
I would not tell them
hang up the phone
identify them - knowledge of browser type exposes vulnerabilitie of the browser.
Haria las pregntas necesarias de contestar cualquier tipo de pregunta
No need for anybody to know this
No one needs that information unless I initiated a help call
dont tell
Who is someone?
don't answer
I tell them one that I don't have.
I dont anwer
find out who they are and why they are calling and validate all of it
never. why should the person know this information?
Tell them Netscape Navigator 1.0
What's yours ?
Ask them as to the reason they need this information.
Why do they need to know?
I don't tell them.
I tell them i use Lynx
i would not share
I'd ask them it's relevency. how they got my number. Who gave it to them.

probably...remove my number im signed up with TPS
tell them to fuck off
unless i knew exactly who was calling and why, i'd hang up as they may be trying to exploit my browser
I don't answer any surveys
Not going to tell them unless I can verify who they are and that they have a need for the information
I dont answer
I lie
Depends who asks.
I hang up
Ask how the DefCon competitions are going.
Want to know why and probably not tell them
Tell them to take their new exploit and shove it!
I would try to play dumb and see how much info I can get out of THEM.
I will say: I use IE 6 lol
wouldn't answer
Isn't yours working...? Do you need a suggestion for an alternative...? LOL..!!
I would mess with them
Lie to them.
give no info unless I am convinced of their identity
I can't imagine why they'd want it.
hang-up the phone.
No contestaría
say "I Don't Speak English" then hang up.
I would validate their identity and the reason the information is necessary.
not to answer
Try somebody else...

Statistic	Value
Min Value	1
Max Value	4
Mean	2.83
Variance	1.00
Standard Deviation	1.00
Total Responses	152

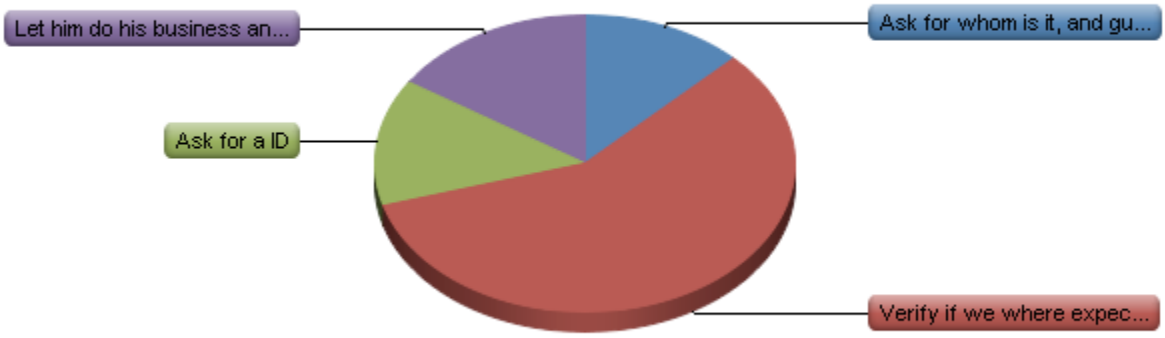
44. If the phone company repair man shows up because of a broken line problem, do you answers all his questions?



#	Answer		Response	%
1	Yes		14	9%
2	Maybe		81	53%
3	No		57	38%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.28
Variance	0.39
Standard Deviation	0.62
Total Responses	152

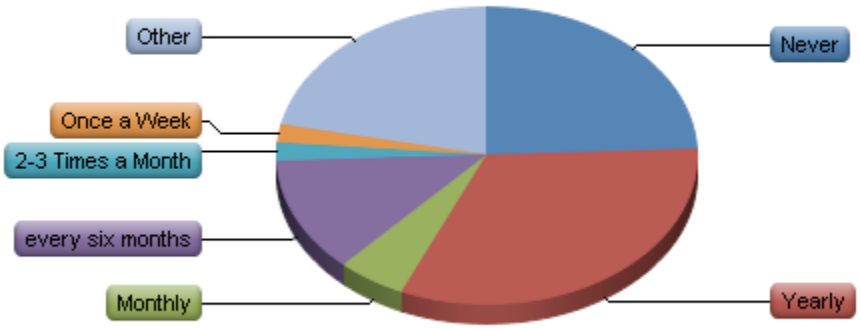
45. If the UPS worker comes to deliver a box, do you?



#	Answer		Response	%
1	Ask for whom is it, and guide him to recipients seats		19	13%
2	Verify if we where expecting a package		88	58%
3	Ask for a ID		21	14%
4	Let him do his business and I do mine		24	16%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.33
Variance	0.79
Standard Deviation	0.89
Total Responses	152

46. If your company has information awareness training how often do you take it?



#	Answer		Response	%
1	Never		37	24%
2	Yearly		49	32%
3	Monthly		8	5%
4	every six months		19	13%
5	2-3 Times a Month		3	2%
6	Once a Week		3	2%
7	Other		33	22%
	Total		152	100%

Other
no training that i know of
Every other year
no training provided
No trabajo
Cuando lo pidan
They dont have awareness training.
No information awareness training. My university only offers brochures
i dont know if they have one
dont have
we don't
no hay
Current employer doesnt have info awareness
quarterly
N/A
They don't
Do not have awareness training
once (i'm a student) its on the syllabus though
my uni course means i have to veryaware of what information i give out at all times anyway
Don't know
Not applicable
Dont have it
we dont
Never has been offered to me.
i am retired
none
one time
We don't have info awareness training
Haven't a training yet.
Don't have one but I research all threat vectors via web.
once in 5 years since hired.
n/a
N/A

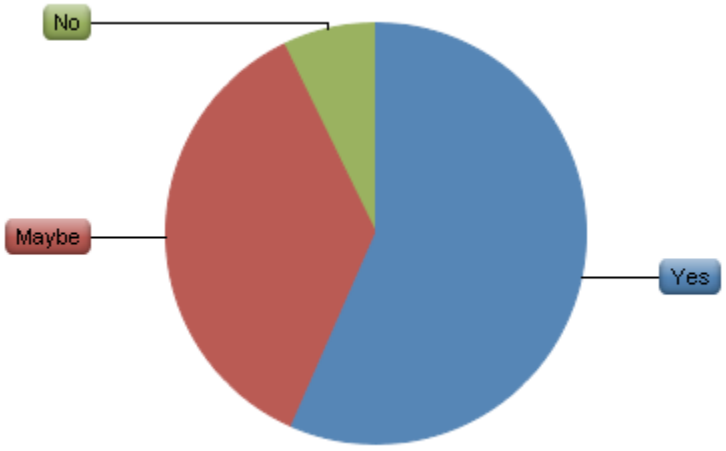
Statistic	Value
Min Value	1
Max Value	7
Mean	3.28
Variance	5.10
Standard Deviation	2.26
Total Responses	152

47. Would you consider it rude not to help someone asking for information over the phone?

#	Answer		Response	%
1	Yes		19	13%
2	No		133	88%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.88
Variance	0.11
Standard Deviation	0.33
Total Responses	152

48. Do you feel capable of identifying a phishing scam?



#	Answer		Response	%
1	Yes		86	57%
2	Maybe		55	36%
3	No		11	7%
	Total		152	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.51
Variance	0.40
Standard Deviation	0.63
Total Responses	152

49. Thank You for participating on this survey, here is an example of what to look for on a email

#	Answer		Response	%
	Total		0	0%

Statistic	Value
Min Value	-
Max Value	-
Mean	0.00
Variance	0.00
Standard Deviation	0.00
Total Responses	0

References

APWG, (2010). *Anti-Phishing Work Group 2010 Report.* Retrieved October 20, 2010, from http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf

CNET, (2002). *Are Mac users smarter?* Retrieved October 22, 2010, from http://news.cnet.com/2100-1040-943519.html

comScore, (2010, January). *Facebook and Twitter via mobile browsers grows by triple in the past year.* Retrieved October 20, 2010, from http://www.comscore.com/Press_Events/Press_Releases/2010/3/Facebook_and_Twitter_Access_via_Mobile_Browser_Grows_by_Triple-Digits

Dang, H. (2008). *The Origins of Social Engineering.* Retrieved October 20, 2010, from https://www.mcafee.com/us/local.../msj_origins_of_social_engineering.pdf

Ernst & Young (2010). *Borderless security: Ernst and Young's Global Information Security Survey.* Retrieved October 20,2010, from *http://www.ey.com/US/en/Newsroom/News-releases/Emerging-technology-trends-increase-risks-of-protecting-corporate-information*

Grasz, J. (2010, August). *More than one third of employers use social media to promote their organizations.* . Retrieved October 20,2010, from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr583&sd=8/18/2010&ed=08/18/2010

Hadnagy, C. (2010, September). *Social Engineering Capture the Flag Results Defcon 18.* Retrieved October 30, 2010, from http://social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf

Haber, L (20009, April). *NewYork State raises the bar for end user security training.* Retrieved November 4, 2010 from http://www.networkworld.com/news/2009/042709-user-security-phishing.html

Harris, S (2007). *CISSP All in One Exam Guide*, Columbus McGraw-Hil

Hansche, S. (2010). Official ICS2 Guide to CISSP. Auerbach Publications Inc.

Hansson, B. (2008). *Job Realted Traning and Benefits for Individuals.* Retrieved November 22, 2010 from http://www.oecd-ilibrary.org/education/job-related-training-and-benefits-for-individuals_237755412637

Hasan, Prajapati, & Vohara, (2010, June). *Case Study on Social Engineering Techniques For Persuasion.* Retrieved October 21, 2010 from http://airccse.org/journal/graphhoc/papers/0610jgraph2.pdf

Hulme, G. (2010, February). *Anatomy of a Modern Hack.* Retrieved November 20, 2010 from http://www.informationweek.com/blog/main/archives/2010/02/anatomy_of_the.html

Karakasiliotis, A. (2006). Assessing end-user awareness of social engineering and phishing. *Australian Information Warfare and Security Conference* Paper 12

Mitnick, K. D. (2002). *The Art of Deception.* Indiana: Wiley Publishing,Inc

Navetta, D. (2010, February). *The Curious Case of EMI v. Comerica: A Bellwether on the Issue of "Resonable Security"?* Retrieved October 20, 2010, from http://www.infolawgroup.com/2010/02/articles/reasonable-security/the-curious-case-of-emi-v-comerica-a-bellwether-on-the-issue-of-reasonable-security/

Nielsen, W. (2010, February). *Global Audience Spends Two More a Month on social network.* Retrieved October 30, 2010, from http://blog.nielsen.com/nielsenwire/global/global-audience-spends-two-hours-more-a-month-on-social-networks-than-last-year/

NIST, (2003). *Building an Information Technology Security Awareness and Training Program.* Retrieved October 30, 2010, from http:// csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

PriceWaterHouseCoopers(PCW) (2011). *Global State of Information Security Survey.* Retrieved November 4, 2010 from *http://www.pwc.com/gx/en/information-security-survey/index.jhtml*

Rotvold, G. (2006). How to create a security culture in your organization. *Information Management Journa,l 42.6 32, Computer Database.*

Schneier, B. (2008, January). *Social Engineering Bank Robbery.* Retrieved October 20, 2010, from http://www.schneier.com/blog/archives/2008/01/socialengineeri.html

Symantec, (2010, January). *Expect These Security Trends to Dominate in 2010. .* Retrieved November 15, 2010, from http://www.symantec.com/connect/blogs/expect-these-security-trends-dominate-2010

US-CERT (2009, October). *Avoiding Social Engineering and Phishing Attacks.* Retrieved October 20, 2010, from http://www.us-cert.gov/cas/tips/ST04-014.html