ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Electronic Security Issues: Protecting our Electronic Life from Social Engineering Attacks

Ugochukwu Onwudebelu*
Department of Mathematics/Computer Science
And Informatics Federal University Ndufu Alike
Ikwo(FUNAI) Abakaliki, Ebonyi State, Nigeria
anelectugocy@yahoo.com

Jackson Akpojaro
Department of Mathematics and Computer Science
Western Delta University
Oghara, Delta State, Nigeria
jakpojaro@yahoo.com

Abstract: The essential need for security is apparent to organizations, government and individuals. Whether it is to secure a company's assets, abide by a law, or guard an individual's privacy, it has become evident that all are vulnerable to one form of electronic attack or another and that in order to protect sensitive information, all possible security precautions must be taken to limit any form of authorized access to electronic records or computer-related equipment. In this security-conscious era, we spend huge sums on technology to protect our computer networks and data. As IT security spending has increased so also has the number of successful attacks. This paper has been developed to highlight the fact that we all have an 'electronic life' which is been hunted by social engineers, and provides a solution on how this life can be protected. The purpose is to provide organizations and individual a simple solution for increasing security awareness against social engineering attacks towards their critical information.

Keywords: Social Engineering, Electronic Life, Human Factor, Hacking, Information Security, Security Policy, Identity Theft

I. INTRODUCTION

Man has invented many wonderful things that have changed the world and our way of life. But for every good use of technology, whether a computer, telephone, or the Internet, someone will always find a way to abuse it for his or her own purposes. For instance, the computer has unleashed countless opportunities for industrial growth, new applications, labor-saving accomplishments, improving the quality of decisions and so on. At the same time, computer technology has generated a whole new field of crime and series of problems for both designers and users of information systems [1]. Almost every day, the media reports an article detailing a case of computer fraud, corporate espionage, new computer virus, denial of service attack, or theft of credit card information. As systems became more complex and sophisticated, so also the crimes. Consequently, victims of these crimes can be left with debt, bad credit, higher interest rates, and possibly criminal charges against them until they are able to prove themselves innocent. As a result, it could take years or even a lifetime, to recover from these wrongdoings. Sufferers of identity theft for example, are always left with a big mess to clean up afterwards, while at other times, some unfortunate victims do not realize they have been defrauded until their accounts have been emptied.

The military and other stakeholders are concerned about the handling of that data considered to be sensitive, especially in this computer age where sensitive data can be obtained without having to breach technical controls. This has resulted in executives having data protection at the top of security executives' agendas. Since the World Trade Center attacks carried out on September 11, 2001, the United States government [2], along with many other governments, considers homeland security a top priority issue that must be protected. The threat of information attacks against government, corporations, and university systems is well established [2, 3]. The real threats come from sophisticated attackers with well-defined targets who are motivated by financial gain.

Security is about protecting assets as seen in the following definition: security is "protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modification" [1]. Most users have a very bad notion concerning information security with the old attitude towards Return on Security Investment (ROSI): "You don't make money on security." Security is viewed as something that should be non-interruptive to business. Prof. Edward Felton, Princeton University [4] once said, "Given the choice between dancing pigs and security, the user will choose dancing pigs every time". Users do not notice security when it works. Thus security needs to be a business enabler, not a source of pain.

Granger [5] points out that, "by merely trying to prevent infiltration on a technical level and ignoring the physical-social level, we are leaving ourselves wide open to attack." Why does technology fails? If you rely predominantly on technology to enforce security you will not be secure. Airports are sadly a great example of this. Metal detectors fail to detect non-metallic weapons. Sophisticated identity management system and firewall complex totally have been defeated by password theft. This is as a result of one security breach or the other. Those who fail to plan for a security incident are planning for failure. The weakest link in any security system is people.

People with malicious intent such as social engineers, hackers and intruders circumvent technological protection and exploit electronic vulnerabilities to gain unauthorized access to data by bypassing guards, gates, locks, walls and without making use of guns or breaking into the web server. Rather than using a wrecking bar to break in, the social engineer uses the art of deception or psychological tricks to influence the person on the other side of the door to open up for him.

A. What is social engineering?:

Social engineering has nothing to do with pulleys and aero dynamics. *Definition:* Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineers and malicious criminals rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. They prey on human behavior, such as the desire to be helpful, the attitude to trust people and the fear of getting in trouble. The sign of truly successful social engineers is that they receive the information without any suspicion [2]. A good social engineer does not advertise his abilities and knowledge; he ensures that his behaviors are unpredictable; he maintains a low profile and always wants people to underestimate him and not to see him as a threat (remember when you underestimate others, it can come back to bite you in the butt). As a result, the social engineer is able to take advantage of unsuspecting business and people to obtain confidential information with or without using technical hacking techniques such as sniffing, cracking, and brute forcing secured networks. This is considered social engineering because it is entirely based on successful manipulating of the victim's mind [6]. We use the equation below to show the profile of a typical social engineer (also see Figure 1):

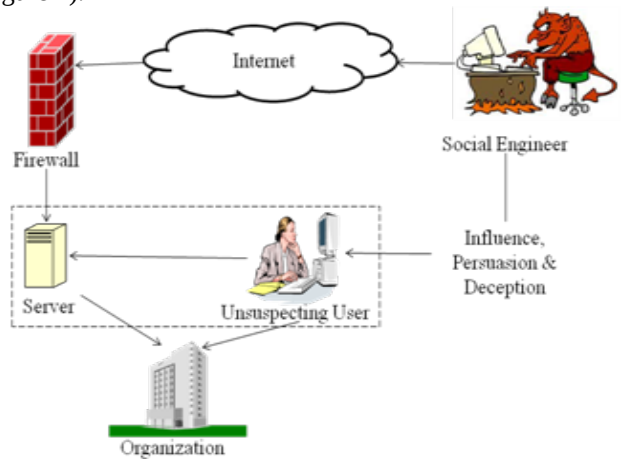

Figure 1: Social Engineering Scenario

Social Engineer = the Art of Influence and Persuasion + the Art of Deceiving People

Social engineering comes in several different forms. To think that any one particular person is not vulnerable to this manipulation is to underestimate the skill and the killer instinct of the social engineer. Often, organizations may not be aware that they were targeted or the incident was unreported because the embarrassment could potentially hurt the reputation or image of the company. Three prominent companies that were affected by social engineering are Microsoft, T-Mobile, and Hewlett-Packard [7]. A good social engineer, on the other hand, never underestimates his adversary. Impersonation [2, 8] is arguably the greatest technique used by social engineers to deceive people, such as posing as an employee of the same organization. A few examples of these tactics include phishing and dumpster diving.

B. Reverse Social Engineering:

Reverse Social Engineering (RSE) [8, 9] attack is when the social engineer acts as a person in position of authority to whom employees will turn for help, that is, attacker sets up a situation where the victim encounters a problem and contacts the attacker for help. This kind of attack is particularly juicy for the attacker, because of the seed planted in advance, when the target discovers he has a problem, he himself makes the phone call to plead for help. The attacker just sits and waits for the phone to ring. It is called reverse because the victims themselves reveal information or provide the access, without someone trying to manipulate them. Another form of RSE turns the tables on the attacker. The target recognizes the attack, and uses psychological principles of influence to draw out as much information as possible from the attacker so that the business can safeguard targeted assets.

II. RELATED WORKS

Social engineering attacks have becoming a hot topic for computer security expert and have been discussed in literature [2, 4, 5, 6, 10, 11, 12,]. Some of the methods that are used by social engineers to infiltrate security measures have been described in [2, 9, 13]. They include Impersonation, phishing, hoaxing, shoulder surfing, Keyboard logging, dumpster diving etc. The importance of security policy enforcement in organizations has been emphasized in [8, 9]. This has enabled us to be able to illustrate how it helps us to protect our electronic life. Bevis [14] recommended organizations to apply cost-effective security controls that will help combat insider security risks through education and raising awareness. Although Emekauwa [7] gave three steps in combating social engineering attacks: education, training and policy, we are of the view that technology, policy and people when properly utilized together will provide a better solution to social engineering attacks.

III. ELECTRONIC LIFE INDICATORS (PARAMETERS)

In today's environment, almost everything employees do involves the handling of information. Therefore, everybody must understand what constitutes innocuous and critical information and that it is not just the bosses and executives who have the information that an attacker might be after. Workers at every level, even those who do not use a computer such as sanitation crew, are liable to be targeted because they might be a stepping stone to the attacker's ultimate goal, that is, they might be manipulated into revealing seemingly innocuous information that the attacker uses to advance one step closer to obtaining more sensitive company information. Remember, the social engineer's modus operandi: Gather as much information about the target as possible, and use that information to gain trust as an insider.

When money or good is stone, somebody will notice it has vanished. But, when information is stolen, most of the time no one will notice because the information is still in their

possession. In most cases, companies and individuals never know when a social engineer has "stolen" information; so many attacks go unnoticed and unreported as mentioned above. In this paper, we introduce the term “electronic life” (e-life) to refer to all personal sensitive information which if obtained by an unauthorized user can be used to cause substantial harm electronically. Our electronic life is equivalent to our physical life, except for the fact that it is in an electronic form (computer files, database files, email) and not flesh and blood.

A social engineer will target an employee /user who has little understanding of how valuable the information being sought is, so the target is more likely to grant the stranger's request. One of the fundamental tactics of social engineering is gaining access to information treated as innocuous, when it is not. Apart from password other critical information include: caller ID, security code, customer information, user profiles, health records, health-related benefit information, customer list, account usernames, employee numbers, social security numbers, birth dates, billing address, salary history, financial records including direct deposit information, mother's maiden name, credit card numbers, account numbers or names, employee medical history, or any other personal identifying information.

The most common information that a social engineer wants from an employee, regardless of his ultimate goal, is the target's authentication credentials [15]. With an account name and password in hand from a single employee in the right area of the company for example, an attacker has what he needs to get inside and locate whatever information he is after. Having this information is like finding the keys to the kingdom, with them in his hand; he can move freely around the corporate landscape and find the treasure he seeks. There are two key components in cyberspace that hackers are often interested in targeting: the user computer and the server computer (see Figure 1 above, the dotted lines). The reason is that both sides of the Internet connection hold personal and business information that lure hackers.

A. Security’s Weakest Link: Human Factor:

The "weakest link" philosophy has demonstrated that 100% protection is unattainable. The security of a system is only ever as strong as its weakest link. The weakest link in any security system is people. There is no point investing ₦XXX in technology that can be readily bypassed by social engineering attacks. An adversary will find the weakest link and exploit it. Since every security measure involves some sort of human intervention and social engineering by definition involves some kind of human interaction, an attacker will very frequently use a variety of communication methods and technologies in attempting to achieve his or her goal. Just look at our airports today. Security has become paramount, yet we are alarmed by media reports of travelers who have been able to circumvent security and carry potential weapons past checkpoints. A most recent classical example is the failed 2009 Christmas Day bombing by Farouk Abdulmuttallab. How was this possible during a time when airports are on such a state of alert? Are the metal detectors failing? No. The problem is not the machines. The problem is the human factor. The newly hired representative in the customer service group may be just the weakest link that a social engineer breaks to achieve his objective [16].

Many information technology (IT) professionals hold to the misconception that they have made their companies largely immune to attack because they have deployed standard security products - firewalls, intrusion detection systems, intrusion prevention systems or stronger authentication devices such as time-based tokens or biometric smart cards. As noted security consultant Bruce Schneier [17] puts it, "Security is not a product, it's a process." Moreover, security is not a technology problem – it is a people and management problem. It is human nature to trust a fellow man, especially when the request meets the test of being reasonable.

We are all human. Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call and involves minimal risk. Despite the efforts of security professionals, information everywhere remains vulnerable and will continue to be seen as a ripe target by attackers with social engineering skills, until the weakest link in the security chain, the human link, has been strengthened. Deploying more technology is not going to solve the human security problem. This is because an attacker is not going to spend time attempting to compromise a computer system or network when the weakest link in the chain might be physically unprotected. Despite our intellect, we humans - you, me, and everyone else - remain the most severe threat to each other's security.

B. Natural Aspects of Human Behavior Exploited by Social Engineering Attackers:

Social engineers can wear many hats and many faces. Just as the criminal mind cannot resist temptation, the social engineer’s mind is driven to find ways around powerful security technology safeguards. And in many cases, they do that by targeting the people who use the technology. Albert Einstein is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering [18] attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. The social engineer anticipates suspicion and resistance, and he is always prepared to turn distrust into trust. A good social engineer plans his attack like a chess game, anticipating the questions his target might ask so he can be ready with the proper answers. Skilled social engineers are very adept at developing a ruse that stimulates emotions, such as fear, excitement, or guilt. Based on this positive impulse, the attacker can play on a person's sympathy, make his victim feel guilty, or use intimidation as a weapon.

To summarize the natural aspects of human behavior exploited by social engineering to drive the target towards becoming a victim in the attack we would list the facets as Thapar [9] did. The following are some of the natural facets: appeal to authority, appeal to ego, attitude to trust, desire to be helpful, fear of losing, incurring loss, laziness or ignorance, enthusiasm to get free rewards, and low perceived cost of information

IV. DISCUSSION

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. That company may still be totally vulnerable [8]. In like manner, Individuals may follow every best-security practice recommended by the experts, submissively install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches. Those individuals may still be completely vulnerable. This is because as developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers (hackers, intruders, social engineers) will turn more and more into exploiting the natural facets of human element. This attack can be minimized if not stopped by applying our complete or active security culture rather than partial or passive security culture in their companies or lives (see Figure 2 below).

W = Policy + People [Partial Security Culture] (1)
X = Policy + Technology [Partial Security Culture] (2)
Y = People + Technology [Partial Security Culture] (3)
Z = Policy + People + Technology [Complete Security Culture] (4)

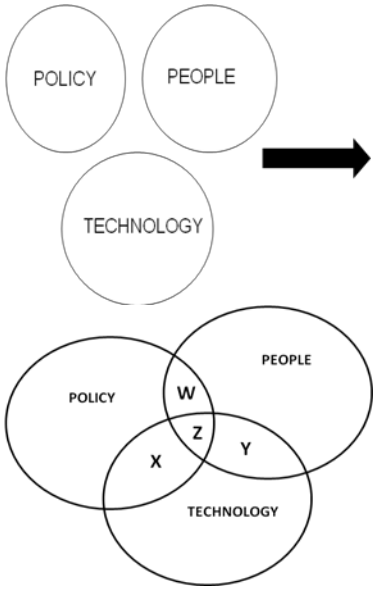

Figure 2: Effective combination of Policy, People and Technology

A. Partial Security Culture:

The social engineering will exploit the vulnerabilities in W, X, or Y to carry out a successful attack on the company or individual. Any company that has W, X, or Y in place is prone to social engineering attacks. When W, X, or Y is in place then we say that the firm is implementing a partial or passive security culture. In W, X, or Y environment information security is not given priority since either policy, people or technology is missing in their implementation steps. With the variety of different forms of threats looming in the environment, even a small lapse in security can bring down the electronic life of an organization or individual. The risk of deploying partial security cultures (W, X, Y) to prevent social engineering attacks cannot be underestimated. The financial cost could be punitive to both the organization and individual. In the event of a compromise resulting from W, X, or Y implementation, only the organization's data classification policy and the value of the data lost will determine the extent of the damage.

B. Complete Security Culture:

The most effective way to mitigate the threat of social engineering is through the application of complete or active security culture (Z), that is, combining the use of security *technologies*, security *policies* that set ground rules for employee behavior, and appropriate education and training for the *people*.

C. Technologies:

Imagine a scenario in which a social engineer has been given the assignment of obtaining the plans to one's hot new product due for release in four months and one has have been working on it for two years. What is going to stop him? The following will not stop him: your firewall, strong authentication devices, intrusion prevention/detection systems, encryption, limited access to phone numbers for dial-up modems, code names for servers, Anti-spyware software or access control lists. The truth is that there is no technology in the world that can prevent a social engineering attack. Often when information security is discussed, the technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programs, and encryption are the only areas addressed as security was considered the job of the operating system conventionally. However, an important layer of information security defense that is not given the attention that it deserves is the weakest link - human layer [7].

Conference rooms, training rooms, and similar areas need to have their network ports secured and protected with firewalls or routers. Allowing a stranger into an area where he can plug a laptop/notebook into the corporate network increases the risk of a security incident. Sensitive files can be protected by installing proper access controls so that only authorized people can open them. Some operating systems have audit controls that can be configured to maintain a log of certain events, such as each person who attempts to access a protected file, regardless of whether or not the attempt succeeds. Obviously things can go wrong with hardware and software.

D. Policies:

Policies eliminate ambiguity and important decisions or actions from being made by judgment calls. The value of a company data can be made known to the employee by security policies that have a well defined classification of data. The data should be classified in terms of its importance to the company. A data classification policy will help individuals to implement proper controls with respect to disclosing information. Security policies should not tend to overlook people like receptionists, help desk personnel, secretaries, administrative assistants, telephone operators and security guards who do not handle sensitive corporate information and yet can act as human firewall to prevent unauthorized

disclosure of information. In addition, they need to have special security training so that they can be alert to the types of tricks associated with a social engineering attacks.

Naturally, the policies [8] must be realistic, not calling on employees to carry out steps so burdensome that they are likely to be ignored. However, it is important to note that security policies, even if religiously followed by all employees, are not guaranteed to prevent every social engineering attack alone. As business needs change, as new security technologies come to market, and as security vulnerabilities evolve, the policies need to be modified or supplemented. A process for regular review and updating should be put into place. A well thought-out information security policy combined with proper education and training, will dramatically increase employee awareness about the proper handling of corporate business information. This will help to mitigate the risk to an acceptable level.

E. People:

The social engineer identifies and exploits the weakest link, that is, the threat least costly to the attacker – the people. The only viable solution to protecting against these threats is by generating overall people awareness in conjunction with technologies and reasonable policies. Once people are aware of the critical data that they possess, the crucial need to protect it, along with the strong possibility of exploitation, subsequently, a strong defense will be built and social engineering attacks will decline [11]. Employees must be educated about what information needs to be protected, and how to protect it. Security awareness also means educating everyone in the company on it security policies and operations. Training may show biggest ROSI in security as users are train to spot the signals and know how to respond.

Awareness would also allow people to be more heedful of what they throw away in the trash. When people are cognizant of the value of the information they possess, they will be more careful of how they handle it and will take the appropriate precautions of disposing of the trash properly. This should include using a shredder to do away with confidential information and being attentive to those who handle trash removal.

The following affects our 'electronic life' profoundly: dumpsters diving, site name displayed in the address bar, discarding of electronic media and warning message. The individual at home is just as vulnerable to dumpster diving as an organization. Naturally, employee/user decisions are largely based on subjective factors, rather than on the sensitivity, criticality, and value of information. Information is also released because employees are ignorant of the possibility that in responding to a request for the information, they may be putting it into the hands of an attacker. Dumpsters are usually not locked in protected areas in most companies and homes. As a result, this makes them very attractive to hackers, intruders and social engineers.

People must be made to know that malicious attackers do look through trash to obtain information that may benefit them. Individuals interested in trash cans include: Intelligence agencies, phone phreaks, hackers [19], head-hunters, private investigators, information thieves, police departments, and a parade of people from mafia. Corporations play the dumpster-diving game, also, and use it for corporate espionage. Dumpster diving is not enjoyable, but the payoff is extraordinary. Just like pieces of a jigsaw puzzle, each piece of information obtained from dumpsters or gather from different sources may be irrelevant by itself. However, when the pieces are put together, a clear picture emerges and turned out to have more than a childish reward to the attacker. In dumpsters, no malicious scripts are needed, no ports are scanned and no computer is used. He can get enough information to guide his assault against the target company, including trade secrets, passwords, network infrastructure layouts, memos, meeting agendas, travel schedules, letters and the like that reveal names, departments, titles, phone numbers, and project assignments. All those details might seem trivial to insiders, yet they may be highly valuable information to an attacker.

The way present day sophistication of electronic security threats is moving demands that users pay attention to the site name displayed in the address bar to verify whether it is in fact the correct address of the site they are trying to access. Attackers create fake website to lure users. Take a look at the following web addresses: eBay.com, eBey.com, eBsy.com or PayPal, Paypai. If a user should look carefully to these addresses, at first sight they seem to be the same thing. However, at a close glance they are different. Take for instance, the eBay.com, an attacker would pay the price of creating web sites, eBey.com, eBsy.com, the letters 'e' and 's' which replaces letter 'a' in the originally spelling eBay.com. Attackers then assume that the users might make a mistake in spelling or typing errors. If you look critically at your keyboard the letter 'a' is followed by letter 's', any spelling or typing errors, will definitely lead the individual to a fake web site - eBey.com, eBsy.com. This same method is used in duping users in similar web sites that attracts huge audiences. Any private information - such as e-mail address, password, or anything else considered private - submitted to such sites will be detrimental to the user and organization. Therefore, users should look at the address bar for verification purpose before inserting their personal details.

Another issue to look at is the issue of deleting file from the system and discarding removable media. Most users are ignorant of the fact that deleting files does not actually remove them; they can still be recovered — as Enron executives and many others have learned to their dismay. Before discarding any electronic media that ever contained sensitive company information, even if that information has been deleted, the item shall be thoroughly demagnetized or damaged beyond recovery using the procedures approved by security experts. Computer attackers attempt to recover any data stored on discarded e-media such as hard-disk drive. Workers may presume that by just deleting files it can never be recovered. This presumption is absolutely incorrect and can cause confidential business and personal information to fall into the wrong hands.

Finally, another security issue, mostly ignored, appears as a warning message that says something like "This site is not secure or the security certificate has expired. Do you want to go to the site anyway?" Many Internet users do not understand

the message, and when it appears, they simply click 'Okay' or 'Yes' and go on with their work, unaware that they may be on quicksand.

V. CONCLUSION

With the abundance of confidential information that organizations must protect, and with consumer fraud and information theft at an all time high, security has never been as important as it is today for businesses and individuals alike. The threat of a break-in that violates our 'electronic life' may not seem real until it happens. To avoid such a costly dose of reality, we all need to become aware, educated, vigilant, and aggressively protective of our information assets, our own personal information, and our nation's critical infrastructures.

A company has a responsibility to make employees aware of how a serious mistake can occur from mishandling non public information. Individuals should ask the following questions, "If I gave this information to my worst enemy, could it be used to injure me or my company?" and "How careful am I in making sure sensitive information isn't posted where it's accessible to audiences I meant to protect it from?" Valuable information must be protected no matter what form it takes or where it is located. Policies should be put in place to address key areas such as e-mail use, telephones, internet access, building entry and waste disposal. Employees must come to appreciate and accept that the threat of social engineering attacks is real [20], and that a serious loss of sensitive corporate information could endanger the company as well as their own personal information and jobs. As the old saying goes, prevention is better than cure. Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate.

Finally, to implement an effective information security strategy to protect our e-life, a complete security culture defense model should be used. Any error emanating from the human area will be arrested and stopped by both the technical controls and policies aspect. Although, social engineering attacks are one of the hardest threats to defend against because they involve the human factor as well as its attacks may be inevitable for the reason that humans are such easy targets, nevertheless, that does not mean that they are unpreventable. It is possible for organizations and individuals to protect themselves by applying complete security culture. Our concluding statement is a warning: users should never reveal any personal information carelessly to any individual (attacker) otherwise they might find their lives electronically destroyed.

VI. RECOMMENDATIONS

In summary, we present the following measures that would enhance and protect our 'electronic life' in the cyberspace environment. The list is by no means complete.

a. A company's security policy needs to be distributed enterprise-wide, regardless of position. This will help employees to take solid decision concerning divulging information rather than making judgments based on appearances and perceptions.
b. Learning tends to fade unless reinforced periodically. The threat is constant; the reminders must be constant as well.
c. People must be made aware of the consequences of failing to abide by information security policies, whether through carelessness or resistance.
d. User awareness is an essential part of mitigating the security threats cause by social engineers. An awareness program needs to be ongoing and never-ending.

VII. ACKNOWLEDGMENT

We would like to take the opportunity to pay our gratitude to Prof. B. A. Oluwade for his time, effort and contributions during the process of writing this paper.

VIII. REFERENCES

[1]. P. S. Browne, "Computer Security - A Survey" Proceedings tf the **1976**. NCC, **1976**, pp. 53 – 63

[2]. Rhodes, C. Safeguarding Against Social Engineering, East Carolina University, 2006.

[3]. "Insiders Pose The Biggest Threat to Data Security" CSO Focus. http://www.cio.com/sponsors/100105_vontu.pdf, 2006 Vol.2 No.1,

[4]. D. M. Lewkovitz,. "Social Engineering or: The Gentle art of having others hurt themselves for your amusement." SecureLink, Infotech, Ruxcon, Sydney 2004.

[5]. S. Granger, "Social Engineering Reloaded." SecurityFocus. http://www.securityfocus.com/print/infocus, 2006.

[6]. W. Munyaneza, Rwanda: Social Engineering. http://allafrica.com/stories/201005240946.html The New Times, 23 May 2010,

[7]. U. Emekauwa, "The Human Layer of Information Security Defense"www.**infosecwriters.com**/text_resources/pdf/UEmekauwa, 2008.

[8]. K. D Mitnick, and W. L. Simon, The art of deception: controlling the human element of security. Indianapolis, Wiley Publishing, Inc. 2002.

[9]. A. Thapar, Social Engineering: An Attack Vector most Intricate to Tackle, www.infosecwriters.com, 2007.

[10]. C. Byrd, Positive Thinking Strategy for Information Security, 2005.

[11]. J. Littman "The Invisible Digital Man" pp 65-66, 2007.

[12]. A. A. Noureddine,. And M. Damodaran, "Security in WEB 2.0 Application Development", Proceedings of iiWAS2008, ACM, pp: 681-685, 2008.

[13]. B. Cialdini, Robert "The Science of Persuasion." Scientific American, Vol 2, page 284, 2001.

[14]. J. Bevis, "Extreme Social Engineering: Combating the Insider Security Threat - A Security Awareness Exercise." CSO Focus Vol.2 No.1 October 2007.

[15]. C. Li, and C. Pahl, Security in the Web Services Framework, 2003. pp: 681-686.

[16]. SOFOCU. "Special Report on the shift to data Security Stop the Insider Threat," VONTU, INC. 2005, vol. 2 no: 1

[17]. http://www.schneier.com/blog/

[18]. R. Ravne, and M. Hermansson, "Fighting Social Engineering," Stockholm March 2005.

[19]. P. Hollows, Hackers are Real-Time. Are You? Sarbanes-Oxley Compliance Journal, http://www.sox.com/, 2005

[20]. J. Rusch, Jonathon the "Social Engineering" of Internet Fraud. INET '99 Proceedings. http://www.isoc.org/inet99/proceedings/, 1999