Vol 8. No. 2 June, 2015

African Journal of Computing & ICT

www.ajocict.net

Social Engineering Threats and Applicable Countermeasures

A.O. Adewole
Department of Computer Science
The Polytechnic, Ibadan
Ibadan, Nigeria.
Olu_gold@yahoo.com

A.E Durosinmi
Department of Computer Engineering
Moshood Abiola Polyetchnic
Abeokuta, Ogun State. Nigeria.
cunlexie@hotmail.com

ABSTRACT

The Information and Communication Technology (ICT) security in a socio-technical world was explored and focus made in particular on the susceptibility to social engineering attacks, Social engineering is the most commonly used tactic across all levels of adversaries to gain unauthorized access into a network. While many organizations attempt to implement a policy and technical capabilities to mitigate against this threat, network intrusions through social engineering attacks are often still highly successful. A proven way to assess an organization's risk to these threats is to test the effectiveness of existing technical and organizational protections, starting with the security awareness of personnel. Most social engineering takes place via email, text message and phone. However, tactics can include simply walking in the front door behind someone possessing a valid badge, or dropping portable USB drives in the parking lot and waiting for an unsuspecting employee to plug them into their work computer. Whatever form social engineering takes, businesses and organizations are largely unprepared for how to effectively counter these attempts across their workforces. Getting employees' attention and commitment to vigilance can be difficult without proving how easy those employees can be exploited. This paper explores this social engineering attack; analyze counter measures against the attack and makes recommendations on how it can be mitigated.

Keywords - Social engineering, threats, security, intrusion and attacks.

African Journal of Computing & ICT Reference Format:
A.O. Adewole & A.E. Durosinmi (2015 Social Engineering Threats and Applicable Countermeasures.
Afr J. of Comp & ICTs. Vol 8, No. 2. Pp 177-180

1. INRODUCTION

Social engineering (SE) has been largely misunderstood, leading to many differing opinions on what social engineering is and how it works. Intruders and hackers are on the lookout for ways to gain access to valuable resources such as computer systems or corporate or personal information that can be used by them maliciously or for personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Often times, in fact more often than one can guess, they get through because of human behaviors such as trust – when people are too trusting of others, or ignorance – people who are ignorant about the consequences of being careless with information. Social Engineering uses human error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware.

The ultimate security wall is the human being, and if that person is duped, the gates are wide open for the intruder to take control [1][4]. Social engineering represents a type of confidence scheme aimed at gathering information, committing fraud, or gaining computer system access. Social engineering, almost by definition, capitalizes on human psychology, such as cognitive limitations and biases, which attackers exploit to deceive the victim. This differs from other types of UIT incidents, such as cases in which an individual inadvertently discloses sensitive information without any interaction with an outside party (e.g., posting information on public databases or losing information by discarding it without destroying it). The adversary (or adversaries) masterminding the social engineering UIT incidents may have one or more malicious objectives that correspond to the intended impact to the organization, such as financial loss, disruption, or information compromise [6][4]

Overview Of Social Engineering

There are two main categories under which all social engineering attempts could be classified – computer or technology based deception, and human based deception.

a. The technology-based approach is to deceive the user into believing that he is interacting with the 'real' computer system and get him to provide confidential information. For example, the user gets a popup window, informing him that the computer application has had a problem, and the user will need to re- authenticate in order to proceed. Once the user provides his id and password on that pop up window, the harm is done. The hacker who has created the popup now has the user's id and password and can access the network and the computer system [3].

b. The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. For example, the attacker impersonates a person with authority, He places a call to the help desk, and pretends to be a senior Manager, and says that he has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. At the very least, the individual can now access the Personnel systems as if he were the manager, and obtain the social Security numbers and other confidential/private information of several employees. He could of course do more damage to the network itself since he now has access to it [2][1] .

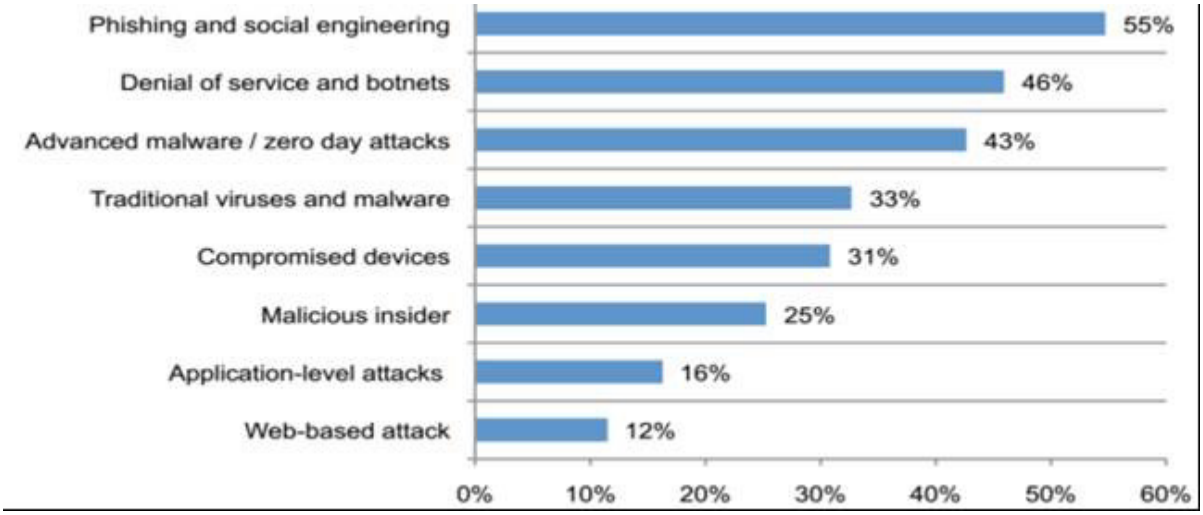

Fig 2: Frequency of social engineering when compared to other security Attacks.
Source: http://securitywize.com/the-risk-of-an-uncertain-security-strategy/1430

2. STEPS IN SOCIAL ENGINEERING ATTACKS

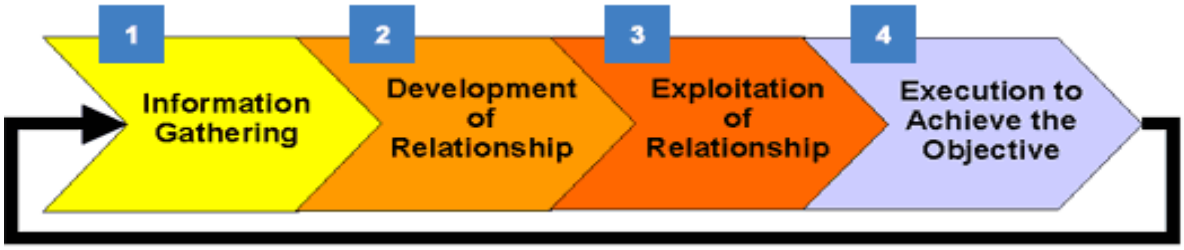

Fig.1: Social Engineering Progression

In the first phase, information gathering, an attacker uses various techniques to track down detailed information that can be used to gain the trust of an individual connected to the targeted organization. The attacker will then use this information to develop a relationship with the individual in phase 2 of the attack cycle. This can take one phone call or it can happen over a period of weeks or even months. After the relationship is established, the attacker will exploit the relationship (phase 3) to get the target to reveal information or perform an action that would not otherwise take place. Phase 3 either accomplishes the attacker's objective or opens the door to achieving the final objective in phase 4.

2.1 Guarding Against Social Engineering

Social engineering attacks are elusive and underhanded. However, they are not impossible to combat, organizations need to implement processes that undermine the effects of social engineering and, beyond that, establish a culture of security and accountability within the company (Defense, Awareness, & Company, n.d.). One way to test the current security culture of an organization is to do a simple self-quiz. Think about how the employees in an organization would react if an unfamiliar person who looked out of place sat down in a cubicle and started working on a computer. The following questions should be asked:

i. Would one of the employees become suspicious about this event?
ii. Would any employee choose to report it?
iii. Would any employee know how to report it and who to report it to?

If an organization do not feel confident that employees would be able to intervene in this potential security breach, there is a need to take several concrete actions to improve organization's security culture. Assuming a well-conceived security policy is in place, the first and most important action is to educate users about your company's security policy, or at least the parts of it that potentially affect them.

3. HOW SOCIAL ENGINEERING WORK

Social engineering is defined as a "non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures."

3.1 Common Social Engineering Scenarious Include:

Employee Information: Documents that contain information about employee's names, departments etc. are very important as they can be used during the physical penetration test as information which is valid. Knowing already information from inside will allow you to establish more easily the trust as you will appear as someone valid.

- **Employee Information:** Documents that contain information about employee's names, departments etc. are very important as they can be used during the physical penetration test as information which is valid. Knowing already information from inside will allow you to establish more easily the trust as you will appear as someone valid.
- **Emails:** Obviously you can find corporate emails and from other sources like LinkedIn, official website etc. but also papers containing some email address is always a good finding as you will be able to discover internal information and also the structure of the emails accounts inside the company.
- **Headed Papers**: these kinds of papers can help penetration testers to create forgeries of the documents. This is essential for any social engineering engagement as you can cheat the employees to perform the action that you want.

Fig. 1: Social Engineering Awareness Poster
Source: https://commons.lbl.gov/display/cpp/Social+Engineering

- **Invoices:** Invoices unveil information about the company's clients and partners. This can prove very handy as the penetration tester can use this information in order to masquerade himself as an employee of the company that the target is doing business which in this scenario will give him an easy access to the target premises.
- **Usernames and Passwords:** It is quite common for many company employees to keep their usernames and passwords in sticky notes. This piece of information can be often found in the garbage as administrators are enforcing passwords to be change every 2 or 3 months. Such a discovery will unveil how usernames and passwords are constructed and with a bit of luck some of them can be valid.
- **Electronic Media**: USB sticks, CD and DVD disks even hard drives can be found in the garbage. These can be collected and analyzed later off-site. Usually nobody would bother to delete the data from a USB stick or to destroy properly a DVD disk before he throws it to the

trash so such a discovery means wealth amount of corporate information.

- **Handbooks, Manuals And Operating Procedures**: Manuals and handbooks are often found in company's trash. This is because these documents are get updated often and the older versions are no longer needed. Usually in these documents there is plenty of information regarding internal processes and systems which can have their own role in the engagement.
- **Signatures:** Papers that contain signatures especially from authorized people like CEO's, Head of departments and Account Managers are also important as the signature can be easily copied and used in a variety of scenarios as a valid authorization document.

4. MITIGATING SOCIAL ENGINEERING

What follows are specific measures through which users and organizations can mitigate against social engineering attacks.

1. **Skepticism is Healthy**: No information without verification! Do not provide any personal or confidential information over phone, text, or internet to anyone unless you can verify who that person is and that person actually has a legitimate need for the said information. Employees are often scammed into revealing sensitive information by social engineers who pretend to IT professionals from the same company. Dispose of any sensitive documents with shredders, keep your computer protected with anti-virus programs, and most importantly of all, don't be gullible and thus get tricked into sharing confidential information. Remember that skepticism is a good thing.
2. **Check your Status:** There are plenty of security agencies that companies and individual contract just to protect them against the threat of social engineering. These agencies can gauge how vulnerable your network or organization is to social engineering attack. This can often be a wake-up call for many companies as well as individuals.
3. **No 'Phishy' business**: 'Phishing' is a very popular method of social engineering. E-mails requesting personal information is sent to people from seemingly legitimate sources (banks, financial organizations etc.) To inspire confidence and create a sense of false security. Sometimes these e-mails redirect people to fake websites that closely resemble the original and then proceed to extract personal data. 'Pharming' is another such method that redirects people to fake websites nearly identical to the legitimate one they are trying to access. There are several security software programs that combat Phishing and pharming. But make sure your network's employees are security conscious and aware of such scams because there is no substitute for being plain vigilant.
4. **Use the right software:** Firewalls and anti-virus programs are very important for any network to use for obvious reasons. But these days content filtering systems and programs are becoming increasingly popular. They increase online security by blocking malicious websites and prevent users to becoming prey to phishing and pharming. In addition to this, you should never forget to keep your system software up to date. Patches and updates often fix security loopholes.
5. **Security Awareness**: A culture of security awareness can go a long way and it is of the utmost importance in any organization or company or network. Most people do not fall prey to such attacks intentionally. Both executives and employees should be educated on basic security training to enable them to protect confidential data. In fact, executives are more vulnerable because they have a relative lax attitude towards security protocols. Implement basic security measures to protect confidential data like classification of sensitive information and two-factor authentication for sensitive data. This can help make your network nearly impermeable

5. CONCLUDING REMARKS

In this paper, we x-rayed social Engineering in its many guises. Using concrete examples, we showed how social engineering scams can be used to defraud unsuspecting users. We also revealed that social engineering scams can occur via email, websites, text messages, and sometimes phone calls. We embellished the social engineering scenario in order to provide some understanding to electronic mailing systems and online consumers that can serve as bases for empowering users and organization in their quest to mitigate social engineering attacks.

REFERENCES

[1] Defense, T. U., Awareness, S., & Company, Y. (n.d.). InfoSec Reading Room The Ultimate Defense of Depth : Security Awareness In tu ll r igh ts.

[2] Ghari, W. (2012). Cyber Threats In Social Networking Websites. International Journal of Distributed and Parallel Systems, 3(1), 119–126. http://doi.org/10.5121/ijdps.2012.3109

[3] Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. 2014 IEEE Security and Privacy Workshops, 236–250. http://doi.org/10.1109/SPW.2014.39

[4] Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. The Art of Human Hacking, 408. http://doi.org/10.1093/cid/cir583

[5] Model, A. (2013). Social Engineering in Social Networking Sites : http://doi.org/10.1109/SCC.2014.108

[6] Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. Available at: http://www.ieee-security.org/TC/SPW2014/papers/5103a236.PDF