Social Engineering Threats and Pertinent Safekeeping Techniques

Uriri Omena, Asibor Raphael, Izebizuwa Rose

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 procedures, intrusion and attacks.

I. INTRODUCTION

As technology becomes more sophisticated and organizations more prepared for external attacks, social engineering has emerged as a low cost - high value tool for people wanting to steal your information. Social engineering requires very little technology, instead relying on the exploitation of trust, human relations and publicly available information.

As more people commit to social media as a way of living and socialising, our information and privacy becomes more vulnerable. Understanding the connection between your professional and personal information is critical Social engineering is the art of manipulating people so they give up confidential information.

Revised Version Manuscript Received on October 16, 2017.

Uriri Omena' Department of Computer Science & Information Technology, Igbinedion University, Okada, Edo State, Nigeria, E-mail: otunbaomena@gmail.com

Dr Asibor Raphael Ehikhuemhen, Department of Computer Science/Information Technology, Igbinedion University, College of Natural & Applied Sciences, Okada, Nigeria, E-mail: asibor.raphael@iuokada.edu.ng

Izebizuwa Rose' Department of Computer Science University of Benin, Benin City, Edo State, Nigeria.

The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer. Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. The term "social engineering" as an act of psychological manipulation of a human, is also associated with the social sciences, but its usage has caught-on among computer and information security professionals.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is or isn't legitimate; when to trust that the person on the phone is or isn't legitimate; when providing your information is or isn't a good idea.

Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on your doors and windows, or if have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if you trust the person at the gate who says he is the pizza delivery guy and you let him in without first checking to see if he is legitimate you are completely exposed to whatever risk he represents.

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]

II. COMMON SOCIAL ENGINEERING ATTACKS

Email from a friend. If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well.

Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

These messages may use your trust and curiosity:

- **Contain a link** that *you just have to check out*–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived.
- **Contain a download**–pictures, music, movie, document, etc., that has malicious software embedded. If you download–which you are likely to do since you think it is from your friend–you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know. And on, and on.

These messages may create a compelling story or pretext:

- **Urgently ask for your help**–your'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
- **Asks you to donate to their charitable fundraiser, or some other cause** – with instructions on how to send the money to the criminal.

Phishing attempts. Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.

These messages usually have a scenario or story:

- **The message may explain there is a problem** that requires you to "verify" of information by clicking on the displayed link and providing information in their form. The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site). Because everything looks legitimate, you trust the email and the phony site and provide whatever information the crook is asking for. These types of phishing scams often include a warning of what will happen if you fail to act soon, because criminals know that if they can get you to act before you think, you're more likely to fall for their phish.
- **The message may notify you that you're a 'winner'.** Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide *information about your bank routing* so they know how to send it to you, or give your address and phone number so they can send the prize, and you may also be asked to *prove who you are* often including your Social Security Number. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.
- **The message may ask for help**. Preying on kindness and generosity, these phishes ask for aid or support for whatever disaster, political campaign, or charity is hot at the moment.

Baiting Scenarios. These socially engineering schemes know that if you dangle something people want, many people will take the bait. These schemes are often found on Peer-to-Peer sites offering a download of something like a hot new movie, or music. But the schemes are also found on social networking sites, malicious websites you find through search results, and so on.

Or, the scheme may show up as an amazingly great deal on classified sites, auction sites, etc.. To allay your suspicion, you can see the seller has a good rating (all planned and crafted ahead of time).

People who take the bait may be infected with malicious software that can generate any number of new exploits against themselves and their contacts,

may lose their money without receiving their purchased item, and, if they were foolish enough to pay with a check, may find their bank account empty.

Response to a question you never had. Criminals may pretend to be responding to your' request for help' from a company while also offering more help.

They pick companies that millions of people use like a software company or bank. If you don't use the product or service, you will ignore the email, phone call, or message, but if you do happen to use the service, there is a good chance you will respond because you probably do want help with a problem.

For example, even though you know you didn't originally ask a question you probably a problem with your computer's operating system and you seize on this opportunity to get it fixed. For free! The moment you respond you have bought the crook's story, given them your trust and opened yourself up for exploitation.

The representative, who is actually a criminal, will need to 'authenticate you', have you log into 'their system' or, have you log into your computer and either give them remote access to your computer so they can 'fix' it for you, or tell you the commands so you can fix it yourself with their help–where some of the commands they tell you to enter will open a way for the criminal to get back into your computer later.

Creating distrust. Some social engineering, is all about creating distrust, or starting conflicts; these are often carried out by people you know and who are angry with you, but it is also done by nasty people just trying to wreak havoc, people who want to first create distrust in your mind about others so they can then step in as a hero and gain your trust, or by extortionists who want to manipulate information and then threaten you with disclosure.

This form of social engineering often begins by gaining access to an email account or other communication account on an IM client, social network, chat, forum, etc. They accomplish this either by hacking, social engineering, or simply guessing really weak passwords.

- The malicious person may then alter sensitive or private communications (including images and audio) using basic editing techniques and forwards these to other people to create drama, distrust, embarrassment, etc. They may make it look like it was accidentally sent, or appear like they are letting you know what is 'really' going on.
- Alternatively, they may use the altered material to extort money either from the person they hacked, or from the supposed recipient.

There are literally thousands of variations to social engineering attacks. The only limit to the number of ways they can socially engineer users through this kind of exploit is the criminal's imagination. And you may experience multiple forms of exploits in a single attack. Then the criminal is likely to sell your information to others so they too can run their exploits against you, your friends, your friends' friends, and so on as criminals leverage people's misplaced trust.

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

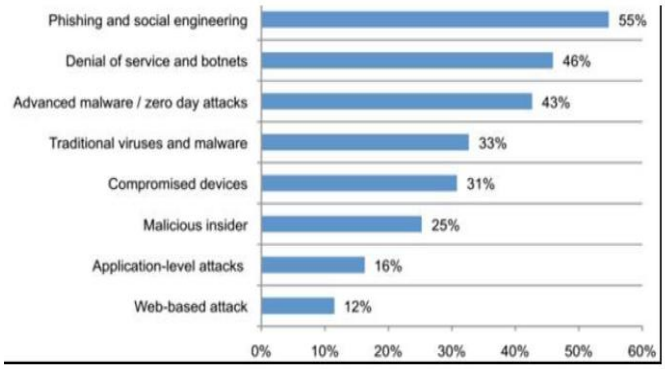
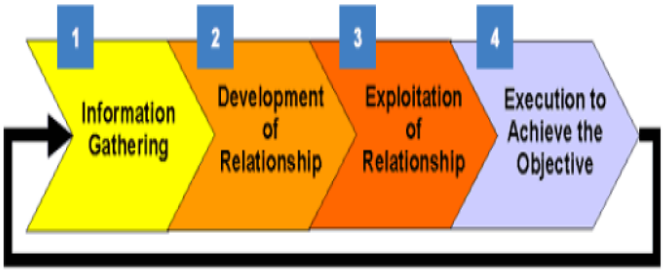


Fig 1: Frequency of social engineering when compared to other security Attacks.

Source:
http://securitywize.com/the-risk-of-an-uncertain-security-strategy/1430xxxx



Social Engineering Progression

Don't become a victim

- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency,
  or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it's a scam.
- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations *on your own* to avoid falling for a scam.
- **Don't let a link in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

Curiosity leads to careless clicking–if you don't know what the email is about, clicking links is a poor choice. Similarly, never use phone numbers from the email; it is easy for a scammer to pretend you're talking to a bank teller.

- **Email hijacking is rampant**. Hackers, spammers, and social engineerers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control someone's email account they prey on the trust of all the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.
- **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.
- **Foreign offers are fake**. If you receive email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
- **Set your spam filters to high.** Every email program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase 'spam filters'.
- **Secure your computing devices.**
  Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks

Potential 'red flags' Be cautious of: • Emails and phone calls from people asking questions about your finances or computer, employees, or security procedures. • External third-party software/USBs given as gifts - always have these checked with your ICT Service Desk before use. • Phishing - emails that appear to originate from a trusted and legitimate source, like your bank or a fellow employee. These often contain hidden links (shown when hovering), spelling errors and unexpected attachments. Never give out your username and password to anyone.

How secure is your information? Our society is now experiencing a hyper-information age. As an individual, the choices you make every day in relation to your information can have a great impact on your safety and your privacy. Some things to think about: • It's not just corporate information criminals are after, it's your personal details too. If enough of your personal information is available in public, or you give this to someone who deceives you, they may be able to access your bank accounts and impersonate you. • Ensure your privacy settings are switched to high for all social media - work or personal - and check this regularly. • Only accept social media requests from people you know and trust. • Avoid uploading your CV or including details on your profiles that could reveal security information about your work or home. • Ensure you change your passwords regularly, and choose passwords that are difficult to guess Knowing how to prevent and respond to social engineering can protect you and your workplace.

What you can do:

• Ensure you understand the value of the information you hold. It may seem arbitrary in isolation, but pieces of information drawn from different sources can allow someone to form a picture of your identity or your organisation's security.

• If you receive a suspicious phone call or email, note down as much detail as you can about the incident: • What kind of information was the person trying to obtain?

•What area of your organisation was targeted?

•Where were you targeted, for example at home, at work or travelling for business?

•Is this just one incident or is there a pattern/frequency?

•What damage has been caused?

• Report suspicious emails to your ICT Service Desk.

• Report other suspicious contacts to your Agency Security Advisor or other Security Personnel.

III. 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 Scenarios 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. 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.

IV. JUSTIFYING SOCIAL ENGINEERING

What follows are specific measures through which users and organizations can militate 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

V.CONCLUDING REMARKS

In this paper, we investigated 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 ights.
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 : bhttp://doi.org/10.1109/SCC.2014.108
6. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. Available at: http://www.ieeesecurity.org/TC/SPW2014/papers/5103a236.PDF

Mr. Omena Uriri holds a Bachelor of Science degree and a Masters of Science degree in Computer Science both from the prestigious University of Benin, Benin City, Nigeria. He is doing his Ph.D at the University of Portharcourt. His research area includes software engineering, software matrix, web services/service engineering. He currently works as a lecturer in the Department of Computer Science and Information Technology, Igbinedion University, Okada Edo State, Nigeria

Dr. Asibor Raphael Ehikhuemhen, hails from Uromi in Esan-North East area of Edo State, Nigeria. Holds a Ph.D in Mathematics (Computational Fluid Dynamics). Has his Master's degree from Olabisi Onabanjo University, Ago-Iwoye Ogun State. And a Doctor of Philosophy in Mathematics from Ambrose Alli University, Ekpoma, Edo State, Nigeria. A researcher in Combustion, Electro-osmotic flow, Medical Physics. Haematology, A member of IAENG, NAMP, MAN etc. Currently the Chairman, Igbinedion University Data Committee, Sub-Dean and a member of the institution's Admission committee.

Izebizuwa Rose' Department of Computer Science University of Benin, Benin City, Edo State, Nigeria.