International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Social Engineering

Syed Nasir Abas, Shuvam Bhimrajkar, C. K. Raina
Computer Science Department, Adesh Institute of Technology, Chandigarh, Kharar, Punjab, India

ABSTRACT

A common thought individuals have regarding cyber attackers is that they solely use advanced hacking tools and technology to interrupt into people's computers, accounts and mobile devices. This can be merely not true. Cyber attackers have learned that one in every of the best ways in which to steal your info or hack your pc is by merely reprimand and deceptive you. During this story, we'll find out how these varieties of human attacks (called social engineering attacks) work and what you'll be able to do to safeguard yourself. Social network s area unit a number of the largest and quickest growing on line services these days. Facebook, for instance has been hierarchical because the second most visited sit e on the Internet, and has been reportage growth rates as high as third per week. One in every of the key options of social network sis the support they supply for locating new friends. For ex ample, social networks might attempt to mechanically establish that u look for currently one another so as to propose relationship recommendations. This paper presents Associate in Nursing tried survey of the present state of Social Engineering – together with the social context of the development, a quick history of notable social engineering attacks and their impact, a structured summary of social engineering attacks and customary ways, a discussion of assorted defense ways and, finally, discusses some open challenges within the topic.

Keywords: Social Engineering, Unidirectional Communication, Social Engineering Attack, Social Engineering Prevention, People Awareness.

I. INTRODUCTION

With the ever-increasing importance of and dependence on that systems in our standard of living, from good home devices to industrial management systems (ICS) and e-government, the safety of those systems is additionally rising in priority. Proof of those trends is ubiquitous – from the rise within the sophistication of attackers' ways and tools, through to the introduction of cybersecurity as a vital topic within the close at hand United States of America presidential election, wide thought of the foremost necessary and important within the democratic world . whereas awareness for cyber security problems has undeniably raised throughout recent years, efforts have typically been targeted on rising the technology aspect of the equation, whereas ignoring or, at least, not paying spare attention to the 'human factor' in cyber security. whereas several reasons for this could be cited, chief among them seems to be the understanding that since it's a technological domain, therefore should IT security (and cyber security by implication) be a technological drawback. No different development illustrates the falsehood of such implications higher than social engineering. Indeed, any try at dissecting cyber security problems, that ignores that humans are central thereto systems as their users, developers, directors and maintainers, is guaranteed to manufacture deeply imperfect results.

II. SOCIAL ENGINEERING

Social engineering may be a form of psychological attack wherever AN aggressor misleads you into doing one thing they require you to try and do. Social engineering has existed for thousands of years; the thought of scamming or conning somebody isn't new. However, cyber attackers have learned that exploitation this system on the web is very effective and might be accustomed target uncountable folks. the only thanks to perceive however social engineering works is to require a glance at a typical, real-world example. You receive a telephone call from somebody claiming to be from a pc support company, your ISP or maybe Microsoft

technical school support. The caller explains they need noticed that your pc is behaving unusually, like scanning the web or causing spam, and that they believe it's infected. they need been tasked with work the difficulty and serving to you secure your pc. They then use a range of technical terms and take you thru confusing steps to convert you that your pc is infected.

III. UNIDIRECTIONAL COMMUNICATION

Unidirectional communication happens once the conversations unidirectional only: from the wrongdoer to the target. for instance, if the wrongdoer sends a message through paper mail while not is flip address, the target cannot reply to the message. Phishing attacks are a preferred sort of attack during this class. Indirect communication is once there's no actual interaction between the target and therefore the attacker; communication happens through some third party medium. associate degree example of this sort of communication is once the wrongdoer infects a flash drive and leaves it somewhere to be found by some target. The target is curious to seek out out what's on the flash drive for private gain or, intended by moral thought, to aim to seek out the owner of the flash drive. The target inserts the flash drive into their pc, and therefore the infection on the flash drive is activated. The metaphysics model more contains many elements as mentioned within the introduction. The goal may be gain, unauthorized access or service disruption. The medium could be a means of communication like e-mail, face to face, phonephone etc . The social engineer may be either a private or a bunch of people. The target will either be a private or a company.

Compliance principles seek advice from the explanations why a target complies with the attacker's request, and techniques embrace those accustomed perform social engineering attacks. samples of techniques embrace phishing, pretexting, molestation and quid professional quo. samples of compliance principles include: friendly relationship or liking: individuals area unit a lot of willing to suits requests from friends or individuals they like. Commitment or consistency: Once committed to some- issue, individuals area unit a lot of willing to suits requests according to this position.

Scarcity: individual's area unit a lot of willing to follow to requests that area unit scarce or decreasing in accessibility.

Reciprocity: Individual's area unit a lot of willing to suits an invitation if the requester has treated them favorably within the past.

Social Validation: individual's area unit a lot of willing to follow to an invitation if it's seen because the socially correct issue to try and do.

Authority: individuals follow simply to requests given by individuals with a lot of authority than they need.

Once the compliance principles, techniques and medium are selected, the attack vector are often set-up and therefore the social engineer will still the particular offensive part. Following section introduces the planned social engineering attack framework.

IV. SOCIAL ENGINEERING ATTACKS

The simplest thanks to defend against social engineering attacks is to use wisdom. If one thing appears suspicious or doesn't feel right, it should be Associate in nursing attack. Some common indicators of a social engineering attack include:

- ✓ Somebody making an amazing sense of urgency. If area unit feeling you're feeling} such as you are harassed to form a really fast call, be suspicious.
- ✓ Somebody inquiring for data ought to them must not have access to or should already grasp.
- ✓ One thing too sensible to be true. a typical example is you're notified you won the lottery, even supposing you ne'er even entered it.

If you think somebody is attempting to form you the victim of a social engineering attack, don't communicate with the person to any extent further. If it's somebody career you on the phone, hang up. If it's somebody chatting with you on-line, terminate the affiliation. If it's Associate in nursing email you are doing not trust, delete it. If the attack is work-related, make certain to report it to your facilitate table or data security team quickly. We have become only too acquainted with the kind of offender WHO leverages their technical experience to infiltrate protected laptop systems and compromise sensitive information. We have a tendency to hear concerning this breed of hacker within the news all the time, and that we area unit driven to counter their exploits by finance in new

technologies which will bolster our network defenses. However, there's another form of offender WHO will use their ways to skirt our tools and solutions. They're the social engineers, hackers WHO exploit the one weakness that's found in every and each organization: human science. Employing a type of media, together with phone calls and social media, these attackers trick folks into providing them access to sensitive data.

Social engineering may be a term that encompasses a broad spectrum of malicious activity.

1. Phishing

Phishing scams could be the foremost common forms of social engineering attacks used these days. Most phishing scams demonstrate the subsequent characteristics:

- ✓ Seek to get personal info, like names, addresses and social insurance numbers.
- ✓ Use link shorteners or introduce links that send users to suspicious websites in URLs that seem legitimate.
- ✓ Incorporates threats, concern and a way of urgency in an endeavor to control the user into acting promptly.

Some phishing emails ar a lot of poorly crafted than alternatives to the extent that their messages frequently exhibit writing system and synchronic linguistics errors however these emails are not any less centered on directive victims to a pretend web site or type wherever they'll steal user login credentials and other personal info.

A recent scam sent phishing emails to users when they put in cracked APK files from Google Play Books that were pre-loaded with malware. This specific phishing campaign demonstrates however attackers unremarkably try malware with phishing attacks in a shot to steal users' info.

2. Pretexting

Pretexting is another type of social engineering wherever attackers target making a decent pretext, or a unreal state of affairs, that they will use to do and steal their victims' personal info. These forms of attacks normally take the shape of a trickster United Nations agency pretends that they have bound bits of data from their target so as to substantiate their identity.

More advanced attacks also will attempt tod} manipulate their targets into playing an action that permits them to take advantage of the structural weaknesses of a corporation or company. a decent example of this might be associate assailant United Nations agency impersonates associate external IT services auditor and manipulates a company's physical staff into lease them into the building.Unlike phishing emails, that use worry and urgency to their advantage, pretexting attacks have faith in building a false sense of trust with the victim. this needs the assailant to create a reputable story that leaves very little area for doubt on the a part of their target. Pretexting attacks ar normally accustomed gain each sensitive and non-sensitive info. Back in October, for example, a gaggle of scammers exhibit as representatives from modeling agencies and escort services, made-up faux background stories and interview queries so as to possess ladies, together with young ladies, send them nude footage of themselves.

3. Baiting

Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads, if they surrender their login credentials to a certain site.

Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media.

One such attack was documented by Steve Stasiukonis, VP and founder of Secure Network Technologies, Inc., back in 2006. To assess the security of a financial client, Steve and his team infected dozens of USBs with a Trojan virus and dispersed them around the organization's parking lot. Curious, many of the client's employees picked up the USBs and plugged them into their computers, which activated a keylogger and gave Steve access to a number of employees' login credentials.

4. Quid Pro Quo

Similarly, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find. These attackers offer IT assistance to each and every one of their victims. The fraudsters will promise a quick fix in exchange for the employee disabling their AV program and for installing malware on their computers that assumes the guise of software updates.

It is important to note, however, that attackers can use much less sophisticated quid pro quo offers than IT fixes. As real world examples have shown, office workers are more than willing to give away their passwords for a cheap pen or even a bar of chocolate.

5. Tailgating

Another social engineering attack type is known as tailgating or "piggybacking." These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.

In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens their door, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company.

Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk.

In fact, Colin Greenless, a security consultant at Siemens Enterprise Communications, used these same tactics to gain access to several different floors, as well as the data room at an FTSE-listed financial firm. He was even able to base himself in a third floor meeting room, out of which he worked for several days.

V. SOCIAL ENGINEERING PREVENTION

Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about. Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm.

Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.

- **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Incapsula Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.
- **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

VI. PEOPLE AWARENESS

- Make the information in training programs as relevant and engaging as possible. This will keep training programs - and, more importantly, the information covered by the training - fresh in the minds of the attendees.
- Teach employees basic social engineering techniques. When employees understand how social engineering schemes work, they will be in a better position to recognize these types of attacks and protect against them.

- Teach employees that almost any data could be valuable to a social engineer – not just what might normally be considered "sensitive" or protected as NPI. The social engineer's goal is to get at your firm's sensitive data and they are willing to take many less conspicuous steps to attain their end game
- Teach employees that it is okay to say "No". A very effective and often used tactic of social engineers is veiled threats that if the employee doesn't assist them, their boss/manager will hear about it and be angry. As a matter of procedure, employees should not be penalized for being reluctant to share sensitive information over the phone or through email.
- Evaluate the effectiveness of your training programs and threat awareness through "social" and "physical" penetration testing. Penetration tests are mock social engineering attacks orchestrated by professionals trained in imitating realistic attackers. Such exercises will demonstrate to employees how easily one can be duped. Being the target of a successful social engineering exercise defines the reality of the threat for your staff as well as allows the firm to understand how vulnerable they are to these risks.

In addition to the items mentioned above, here are some other techniques to follow:

- Establish security protocols, policies, and procedures for handling sensitive information. Make sure ALL employees are made aware of them. Regularly reiterate their importance.
- Train employees in security protocols relevant to their position.
- Identify information that is considered sensitive and evaluate its overall exposure to social engineering risk. Specify to trained personnel when, where and how this information should be securely handled and stored.
- Identify information categories that may not be considered sensitive but could still be targeted by social engineers for the purpose of advancing their attacks.
- Implement effective physical security controls such as visitor logs, escort requirements, and background checks for new employees or temporary workers.
- Establish a system where sensitive documents and media are securely disposed of and not simply thrown out with the regular office trash. If not already in place, insist on the use of dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff.
- Consider banning the use of non-corporate storage media such as flash drives.
- Institute the use of a web content filtering system that allows you to block employee access to questionable and potentially malicious web sites that can lead to system compromise. The items listed are not intended to be all-inclusive nor specific to the state (or states) in which your firm conducts business. Rather, they are intended to serve as a starting point for a detailed discussion on safeguards that should be implemented in order to protect your firm from social engineering and data security breaches.

VII. CONCLUSION

Social engineering poses a significant threat to firms of all sizes. Nearly every month regulators report that individuals and firms are fined due to divulging client NPI or, worse yet, wiring their client funds to unrelated third parties after receiving fraudulent phone calls or e-mails. Organizations must address these threats as part of an overall risk-management strategy. Firms need to be mindful that social engineering techniques change, and there are always new and different schemes to be employed. Employees may not realize the information they deal with every day is a valuable commodity to a social engineer and that they need to protect it. A strong defense strategy against these threats is to generating overall awareness through training and testing. Ongoing training will provide employees with the information and skills they need to recognize and respond to new or evolving social engineering threats. Having these proper tools at your disposal can improve the safety of your data and help protect against abuse. Testing will actively keep your employees' awareness piqued while giving management a "health check" on how well their staff is equipped to stop these threats

VIII. REFERENCES

[1]. Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems

(2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6.Chapter 2, page 17

[2]. Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.

[3]. Anderson, D., Reimers, K. and Barretto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge.publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)

[4]. Schlienger, Thomas; Teufel, Stephanie (2003). "Information security culture-from analysis to change". South African Computer Journal. 31: 46-52.

[5]. Jaco, K: "CSEPS Course Workbook" (2004), unit 3, Jaco Security Publishing.

[6]. The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011). "HP Pretexting Scandal by Faraz Davani". Scribd. Retrieved 15 August2011.

[7]. "Pretexting: Your Personal Information Revealed", Federal Trade Commission

[8]. Fagone, Jason. "The Serial Swatter". New York Times. Retrieved 25 November 2015.

[9]. "Train For Life". Web.archive.org. 5 January 2010. Archived from the original on 5 January 2010. Retrieved 9 August 2012.

[10]. "The Real Dangers of Spear-Phishing Attacks". FireEye. 2016. Retrieved 9 October2016.

[11]. "Chinese Espionage Campaign Compromises Forbes.com to Target US Defense, Financial Services Companies in Watering Hole Style Attack". invincea.com. 10 February 2015. Retrieved 23 February 2017.

[12]. "Social Engineering, the USB Way". Light Reading Inc. 7 June 2006. Archived from the original on 13 July 2006. Retrieved 23 April 2014.

[13]. "Archived copy" (PDF). Archived from the original (PDF) on 11 October 2007. Retrieved 2 March 2012.

[14]. Conklin, Wm. Arthur; White, Greg; Cothren, Chuck; Davis, Roger; Williams, Dwayne (2015). Principles of Computer Security, Fourth Edition (Official Comptia Guide). New York: McGraw-Hill Education. pp. 193-194. ISBN 978-0071835978.

[15]. Raywood, Dan (4 Aug 2016). " BHUSA Dropped USB Experiment Detailed". info security. Retrieved 28 July 2017.

[16]. Leyden, John (18 April 2003). "Office workers give away passwords". Theregister.co.uk. Retrieved 11 April 2012.

[17]. "Passwords revealed by sweet deal". BBC News. 20 April 2004. Retrieved 11 April2012.

[18]. Treglia, J., & Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, June 3-4.

[19]. Mitnick, K., & Simon, W. (2005). "The Art Of Intrusion". Indianapolis, IN: Wiley Publishing.

[20]. Allsopp, William. Unauthorised access: Physical penetration testing for it security teams. Hoboken, NJ: Wiley, 2009. 240-241.