Social Engineering

Contents

Abstract 2

1. Definition 2

2. Background 3

2.1 Evolution 3

2.2 When does a social engineer become a hacker? 3

3. Key Factors in Social Engineering Success 4

3.1 Trust 4

3.2 Emotional Responses 4

3.3 The Maxim of Perception 5

3.4 Awareness 5

4. Who is targeted? 5

5. Techniques for Attack and Defence 6

5.1 Dumpster Diving 6

5.2 Shoulder Surfing 6

5.3 Vishing 7

Conclusion 7

References 8

Abstract

You receive an automated call from your bank informing you of suspicious activity on your account. You do not recognise the last four expensive transactions. As instructed you 'press 1' to speak to an advisor to ensure that you are refunded the monies that have been fraudulently spent and, to be issued a new bank card. You suspect that your card was somehow cloned when you paid for petrol the other day – as you recall, the shop keeper did wipe your card on his t-shirt when it didn't work in the card machine.

In actual fact you have been roused into calling the very person who intends to commit identity theft and have divulged all the information he/she needs to know to access your bank account.

Welcome to social engineering.

Social Engineering (SE) is as exciting for hackers as it is dangerous for victims. The availability of digital information, coupled with an increasingly interconnected society, has become greater over the last decade to such an extent that, the opportunities for SE have proportionately grown alongside it. The mitigation and defence techniques required to prevent these attacks therefore, need to be as strong as these attacks are sophisticated.

This paper will explore SE practices and discuss preventative measures. It will indicate the direction in which SE is moving thereby implying how future mitigation and defence strategies should be formed.

1. Definition

In the context of the infiltration of systems, the terms 'social engineering' and 'hacking', the latter being more traditional form of attack, are often used synonymously. Given that SE is the deceptive practice to gain access to an IT/IS system, and hacking is the process to *"gain unauthorized access to data in a system or computer"*[1], this interchangeable usage of terminology is not entirely incorrect.

But, what separates social engineers from hackers is that they rely on human interaction in order to attack because, "s*ome online criminals find it easier to exploit human nature than to exploit holes in your software."* [2] In short, a hacker may spend hours trying to infiltrate a company's IT network to obtain an account number but a social engineer would simply ask someone for it.

Therefore, a social engineer does not need to possess the IT skills of a hacker although, being "*proficient at using computer …as well as being a skilled social engineer… can be a very lethal combination."* [3]

---

[1] Oxford Dictionaries, *Definition of Hack.* Available at: http://oxforddictionaries.com/definition/english/hack?q=hacking (accessed 20th August 2013)

[2] Microsoft, *What is Social Engineering*. Available at: www.microsoft.com/en-gb/security/resources/socialengineering-whatis.aspx (accessed 20th August 2013)

[3] Kee, J. (2008). *Social Engineering: Manipulating the Source*. Available at www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914(accessed 20th August 2013)

2. Background

Essentially SE is the practice of deception through the planned manipulation of humans. It is typically envisaged as a method of gaining access to confidential information however, an expert will gain access to information that is perceived as neither confidential nor privileged to the victim thus, classifying the attack as a 'normal' transaction.

When examining SE in a wider context it is often used by law enforcement agencies for example, undercover police officers. So although the legality of SE is questionable, its purpose is what deems it ethical or unethical.

2.1 Evolution

SE has come a long way since the 1980's 'Prestel hacks' though conceptually, hasn't developed as much as one would assume as demonstrated by the more recent 'News International' phone hacking scandal. However, the main aspect that has enabled SE's evolvement to where it is today is the wider range of access points available.

For instance, during the 2013 USENIX Security Symposium in Washington DC [4] findings from a ten month *Twitter* study was presented. Twenty seven 'merchants' were exposed to have been responsible for 'several million fraudulent accounts' "*and the criminals controlling these market places earned $127,000 to $159,000 for their efforts."*

In the early days of computing, only large organisations used technology in a way that attracted hackers. Although deception is still prevalent, the range of activities a hacker can perpetrate has increased a thousand-fold since *those* days. As the *Twittter* study demonstrates, social networking has increased the range of SE targets; where historically 'valuable' individuals and the corporate world were targeted, now the individual is within the spectrum.

This range of new opportunity makes it profitable for a hacker to farm an IT environment rather than raid it and, to exercise stealth in maintaining the deception for a longer period of time.

2.2 When does a social engineer become a hacker?

To initiate a brute force IT attack all that is needed is an IP address using which, a series of broadly unsophisticated actions can be attempted. The results can subsequently be used to form a more intelligent secondary attack until the systems behind that IP addresses have been breached. Consequently, organisations with IP based technology tend to have defence tools; the closer the attack is to a technology system, the easier it is to use an automated tool to protect it. But this is of little threat to a social engineer.

By definition SE is the use of a human being to gain access to something a social engineer has no authority to access or rights to use. A social engineer will repeat the process leading to infiltration as many times as necessary, using as many strategies as are available until, he/she has enough information to hack the target.

---

[4] Steve Ragan. (2013). *Researchers explore underground market of Twitter spam and abuse.* Available at: www.csoonline.com/article/738100/researchers-explore-underground-market-of-twitter-spam-and-abuse. (accessed 21st Aug 2013)

3. Key Factors in Social Engineering Success

The success of SE is entirely reliant on gaining valuable information as discretely as possible without leaving a traceable trail. So a good social engineer must be able to:

- Gather information outside the context of the target asset, for example, asking someone if they are at their desk in order to be able to use their already 'logged on' computer.

- Infer knowledge and, gain validation or additional information, for example, "I'm supposed to be meeting Bob, what time does he finish?"

So, whilst a hacker is likely to be an unidentified person sitting behind a remote computer, a social engineer may be a colleague, customer, or anyone with whom having interaction would not be unusual.

3.1 Trust

"Social engineering is derived because of a human characteristic to trust other people." [5]

An organisation's vulnerability to SE attacks relies on how it establishes, verifies, validates and guarantees trust. This can relate to physical, verbal/audible, visual and even emotional aspects of perception all of which are used to establish trust.

Unlike direct technology layer attacks, the human in an organisation is the target due to having the licence to 'bend' the rules for 'trusted colleagues'. As highlighted in the 2013 'Heading Off Advanced Social Engineering Attacks' report, *"attacks are duping targeted individuals into inadvertently installing malware or providing confidential information by using sophisticated social engineering techniques - often getting the victim to break security procedures or to ignore common sense."* [6]

3.2 Emotional Responses

Unlike an IT solution protecting systems against hackers, to create a sturdy shield against SE threats, one must acknowledge the emotional responses that compromise security. In a professional capacity, mostly, the responses include:

- The need for progress
- The desire to help others
- The desire to benefit oneself
- The need to prove authority

Aside from technology based strategies like *phishing*, SE tries to *"appeal to vanity or authority and other psychological triggers such as greed, fear, anger or moral duty."* [7]

---

[5] Kee, J. (2008). *Social Engineering: Manipulating the Source*. Available at www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914 (accessed 20th August 2013)

[6] Michael Cobb (2013). *Heading Off Advanced Social Engineering Attacks.* Available at: http://www.darkreading.com/vulnerability/heading-off-advanced-social-engineering/240150975 (accessed 21st Aug 2013)

[7] Michael Cobb (2013). *Heading Off Advanced Social Engineering Attacks.* Available at: http://www.darkreading.com/vulnerability/heading-off-advanced-social-engineering/240150975 (accessed 21st Aug 2013)

3.3 The Maxim of Perception

A good social engineer will have the ability to deploy strategies that appear 'normal' to the victim by engineering a scenario catered towards either the subject's obvious self-perception or, leading the victim towards a desired self-perception that will enable the attack. Albeit subtle, this error in perception is what creates the entry point for an SE attack.

An expert social engineer will give the victim a heightened sense of importance or, make a company deem their assets and relationships as being worth more than they are; all this without a trace of suspicion because an organisation is often just a stepping stone for a SE attack.

Subsequently what someone has access to, is often more appealing to a social engineer than tapping into one's knowledge for instance, the delivery driver maybe more valuable in a secondary attack than the accountant.

3.4 Awareness

In this digital age, people have generally become savvy to mass scale and usually emailed forms of SE attacks like 'phishing'. However, social engineers are still thriving. Why? Because ultimately, we collectively still do not have enough awareness of *all* the ways in which attacks are formed.

For example, would everybody working within an organisation be aware of the company's assets? And even if they were, would they know the different asset types? Are people aware of the policies that relate to information that a social engineer may be interested in? What's more, would people even know how to report a potential SE breach?

This lack of awareness for most means that without realising it, many people are susceptible to divulging valuable information as well as revealing details about ways to gain access to information.

4. Who is targeted?

Traditionally large companies are perceived as primary targets for security based attacks. But given that they have responded with robust IT solutions, albeit that it does not guarantee immunity, it is easier for engineers to farm small/medium businesses who don't have such high levels of security, awareness, and coping mechanisms.

This does not however mean that large organisations are safer from SE attacks than their counterparts. In a 2011 study conducted by CheckPoint Software, eight hundred and fifty IT and security professionals were surveyed across the US, Canada, UK, Germany, Australia and New Zealand. The results showed *"almost half, 48 percent, had been victims of social engineering and had experienced 25 or more attacks in the past two years. Social engineering attacks cost victims an average of $25,000 - $100,000 per security incident"*[8].

So, the focus of the target has not shifted. Instead the range of focus has become wider.

[8]Joan Goodchild. (2011). *Social engineering attacks costly for business*. Available at: www.csoonline.com/article/690167/social-engineering-attacks-costly-for-business (accessed 21st Aug 2013)

Generally, larger enterprises are used to gather little pieces of information over a long time in order to build a detailed picture and plan a sophisticated attack. Small/medium organisations however, are easier to use to gain more useful information over a shorter period of time.

For these reasons, social engineers establish 'stealth relationships' whereby the subject would be unaware of their involvement in the SE relationship.

5. Techniques for Attack and Defence

Although SE techniques have seemingly formed from technological advances and increased social interconnectivity, hackers have known about ways to infiltrate high security systems without the use of technology for many years. In fact, many of the techniques *"seem to have drifted in to obscurity to the point of becoming industry folklore; the tactics of the pre-dawn information age. But make no mistake; these and other old-school tactics work with amazing effectiveness today."* [9]

The following is by no means an exhaustive list of SE techniques but, are usually used in combination with other techniques in order to be effective. For example, with 'Reverse Social Engineering', the social engineer pre-gathers information using various techniques which is then used to enforce the actual attack. This is in the form of encouraging the victim to 'legitimately' call the social engineer – someone who he/she trusts, to divulge all the information needed to access the desired data/asset.

5.1 Dumpster Diving

As the saying goes 'one man's trash is another man's treasure.' Dumpster diving is the SE technique of searching through rubbish for information that can be used to form an attack. Obvious treasures like passwords written on paper are commonly searched for but, in line with SE strategies involving gathering seemingly harmless information, even things like phone lists and calendars can be valuable.

In response, experts advise companies to establish and follow a thorough disposal policy where all paper is shredded and all storage media is erased. Knowledge is power and since misperceptions of risk make SE attacks easy to carry out, staff should also be trained on the dangers of careless disposal.

5.2 Shoulder Surfing

Shoulder surfing is the technique of using direct observation to retrieve information that can be used for attack. This can be easily carried out in public spaces for example, at an ATM or, by looking over the shoulder of someone who is working on their laptop on a train. In more 'risky' cases, observation can be carried out from a distance with the use of visual enhancing devices like, binoculars.

Again, raised awareness of this is the key to successful protection coupled with actions like covering the keypad when entering a pin code at an ATM or, using visors on computer screens that make it hard if not impossible for others to see the contents of a computer monitor.

---

[9] Johnny Long (2008). *No tech hacking a guide to social engineering, dumpster diving, and shoulder surfing*. Oxford: Syngress. Summary.

5.3 Vishing

'Vishing' is formed from 'phishing' and 'voice'; it is the SE technique whereby an engineer will telephone their subject, usually using an automated message - similar to how banks inform people that they may have been a victim of fraud. The aim is to encourage the victim to divulge personal information that can be used for identity theft.

Some specific techniques and technologies used that are classified as 'vishing' are:

- *Wardialing* where an automated message poses as a bank asking for card and PIN numbers
- *VoIP,* an internet-based phone system like 'Skype', that can be used to work in tandem with other technologies often used to exploit databases
- *Caller ID Spoofing;* using readily available tools to display a false name on the recipient's caller ID typically using labels like, 'bank'

As financial institutions repeatedly state, they would never ask a customer for a PIN number. Keeping this at the forefront of one's mind is certainly a useful form of protection as is, not responding to telephone calls or emailed requests for personal and/or financial information.

Conclusion

Due to the ominous nature of SE and sheer scope of evolving techniques, it is easy for the education of it to include an element of scare mongering. It is however, important to consider that at some point or another, we have all potentially handed over pieces of information that could be used to form an attack for example, showing an ID badge.

SE is incredibly transparent when the technique used has been uncovered but, its sophistication lies in its ability to go undetected during the attack phase. This is beautifully demonstrated in a 'test' carried out by Chris Hadnagy, author of 'SE: The Art of Human Hacking'. He shows a powerful CEO being manipulated by a charity scam by social engineers who discovered, through his 'Facebook' page, that he had a family member suffering from cancer. Another illustration involves a family visiting a theme park but having forgotten to print their emailed coupon at home, they request access to their email using the theme park's computer. In doing so, the seemingly harmless family infiltrate the theme park's IT systems - by opening a harmful file on their computer.

SE is rife amongst organisations and individuals alike and chances are, its presence will never be completely extinguished. However, with increased awareness and robust response, cases of successful SE can certainly be reduced.

References

Joan Goodchild. (2011). *Social engineering attacks costly for business.* Available at: www.csoonline.com/article/690167/social-engineering-attacks-costly-for-business (accessed 21st Aug 2013)

Joan Goodchild (2010). *Social engineering techniques: 4 ways criminal outsiders get inside.* Available at: www.csoonline.com/article/596512/social-engineering-techniques-4-ways-criminal-outsiders-get-inside?page=3 (accessed 22nd August 2013)

Johnny Long (2008). *No tech hacking a guide to social engineering, dumpster diving, and shoulder surfing*. Oxford: Syngress. Summary.

Kee, J. (2008). *Social Engineering: Manipulating the Source*. Available at www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914 (accessed 20th August 2013)

Margaret Rouse (2005). *Dumpster Diving.* Available at: http://searchsecurity.techtarget.com/definition/dumpster-diving (accessed 20th August 2013)

Michael Cobb (2013). *Heading Off Advanced Social Engineering Attacks.* Available at: http://www.darkreading.com/vulnerability/heading-off-advanced-social-engineering/240150975 (accessed 21st Aug 2013)

Microsoft, *What is Social Engineering*. Available at: www.microsoft.com/en-gb/security/resources/socialengineering-whatis.aspx accessed 20th August 2013)

Neil DuPaul (2013). *Hacking the Mind: How & Why Social Engineering Works.* Available at: www.veracode.com/blog/2013/03/hacking-the-mind-how-why-social-engineering-works (accessed 18th August 2013)

Oxford Dictionaries, *Definition of Hack.* Available at: http://oxforddictionaries.com/definition/english/hack?q=hacking (accessed 20th August 2013)

Robert Siciliano (2010). *Top 5 Vishing Techniques.* Available at: www.finextra.com/community/fullblog.aspx?id=4791 (accessed 20th August 2013)

Steve Ragan. (2013). *Researchers explore underground market of Twitter spam and abuse.* Available at: www.csoonline.com/article/738100/researchers-explore-underground-market-of-twitter-spam-and-abuse. (accessed 21st Aug 2013)