

# **Social Engineering: A growing threat, with diverging directions**

J.V.Chelleth<sup>1</sup>, S.M.Furnell<sup>1</sup>, M.Papadaki<sup>2</sup>, G.Pinkney<sup>2</sup> and P.S.Dowland<sup>1</sup>

<sup>1</sup> Network Research Group, University of Plymouth, Plymouth, United Kingdom

<sup>2</sup> Symantec, Hines Meadow, St Cloud Way, Maidenhead, Berkshire, United Kingdom

e-mail: info@network-research-group.org

## **Abstract**

The age old problem of social engineering is still a threat that does not receive due attention. Due to the advancements in information technology and the explosion of the Internet, attackers have many more avenues to pursue social engineering attacks. Inadequate efforts to educate employees and staff about social engineering and password management, inappropriate usage of messaging systems, poor implementation and awareness of security policies, all lead to people being exposed to potential incidents. This paper talks about social engineering and the new avenues that it has diverged into; and how social engineering plays a part in assisting other attack schemes. The paper first introduces the concept of social engineering. It then looks at different attack methods that have proliferated due to the help obtained by social engineering schemes. The paper establishes that, in addition to being a technique in its own right, social engineering can also be used to assist other types of attack, including viruses and worms, phishing, and identity theft.

## **Keywords**

Social Engineering, Viruses, Worms, Identity theft, Phishing

## **1. Introduction**

Typically when security is spoken of in terms of information security, it is all about having secure systems and networks; anti-virus, firewalls, Intrusion Detection Systems (IDS), etc. A lot of effort is put into implementing technical security and this creates a notion that the systems/network are not susceptible to attacks and hence exploitation. However, non-technical details are often forgotten and this gives attackers a means to slip past the otherwise heavily guarded IT security systems. Keeping this in perspective, the paper talks about attacks that arise due to social engineering; a concept that has been used often to exploit computer systems and individuals alike.

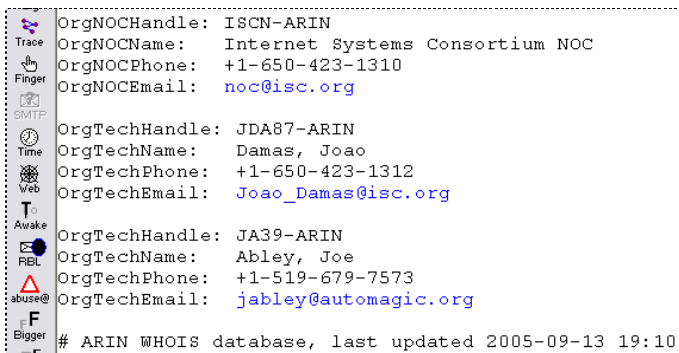
The main goals of social engineering as identified by Paradowski (2001), who calls such attackers as Cyber Cons, are fraud, network intrusion, industrial espionage, and identity theft. Of course, social engineering exploits existed long before the existence of computers - there always were individuals who deceived others into giving out valuable information. However, in the age of Information Technology, attackers found a new medium to carry out their exploits.

## 2. Setting the scene

Social engineering is an art of deceiving, to obtain information by pretending to be someone that s/he is not. Such information would not normally be provided because it may be personal or sensitive/protected. It is a human tendency to trust people without knowing much about the person. People believe what they hear and on the basis of how they hear it. If someone confidently tells a lie, it is believed much more than someone who tells the truth in an uncertain or loath manner.

Attackers make use of this human nature, to maximise their benefits by getting out information that will be useful in carrying out their exploits. A large organisation that is very concerned about security may have deployed a corporate anti-virus solution, a comprehensive firewall scheme, and even a strong intrusion detection system (IDS). If an attacker wants to penetrate this system and has the gift of the gab, then why would s/he waste time trying to overcome these security deployments? Instead there is a very good chance that s/he could get information from the employees by employing social engineering tactics.

Figure 1 shows a partial screen capture of the output from a popular tool called Sam Spade. It is a network-query tool like *nslookup*, *whois* and *traceroute*, but GUI-based. Querying a popular shopping site, and hitting a few buttons, we observe technical contact details. Attackers who use social engineering methods need to have some basic idea about the organisation to start their attack. Using such information, the attacker can query individuals and network their way into the organisation. To do so, they could pose as trusted vendors, new hires, contractors, electricians, a high level officer and so on. If an attacker is confident to pull off the personality of a higher official, it becomes very easy to get the information required. Employees often want to impress their seniors, possibly for selfish reasons and to get higher up the ladder; nevertheless this causes sensitive information to be given away rather easily to attackers.



```

Trace
Finger
SMTP
Time
Web
Awake
REL
abuse@
F
Bigger
OrgNOCHandle: ISCN-ARIN
OrgNOCName: Internet Systems Consortium NOC
OrgNOCPhone: +1-650-423-1310
OrgNOCEmail: noc@isc.org
OrgTechHandle: JDA87-ARIN
OrgTechName: Damas, Joao
OrgTechPhone: +1-650-423-1312
OrgTechEmail: Joao_Damas@isc.org
OrgTechHandle: JA39-ARIN
OrgTechName: Abley, Joe
OrgTechPhone: +1-519-679-7573
OrgTechEmail: jabley@automagic.org
# ARIN WHOIS database, last updated 2005-09-13 19:10

```

**Figure 1: Partial screen capture from Sam Spade tool**

That is one way to use social engineering by gathering information and then exploiting the relationship. The possibilities are endless and depend on how innovative the attacker is. If information can be easily obtained by simply querying, then why would an attacker go through the trouble of surpassing firewalls? This also

indicates that an attacker need not be highly proficient programmer and s/he does not need great technical skills; a flare to talk and confidence can do equal or more damage, at times much quicker and with far less at stake.

### **3. Combination of attacks**

Social engineering methods will not always be used in isolation. Often, a combination of two or more attack methods is used to exploit the target, as shall be seen in this section which relates different attack methods to social engineering tactics.

#### **3.1 Obtaining passwords**

People are rightly considered as the weakest link in IT security. Even after an organisation has taken every step towards a great IT security deployment, if the system administrator gives away a password, it jeopardises the entire organisation and it falls prey to social engineering attacks; the entire security infrastructure will fail. Even employees sharing their passwords and login details cause vulnerabilities to arise in the security system. Colleagues in an organisation come to trust each other and often lend their passwords to each other for different reasons (many of which may be legitimate) but it can never be predicted when an individual might misuse the login details at his /her disposal. Additionally, when an employee gets to know more about another employee, at times it becomes easy to guess the kind of passwords that the latter would use.

It should be noted that in any organisation, there are so many systems that have to be maintained by an administrator, that it becomes very cumbersome to remember different and complicated passwords; and hence there exists a trend to use simple dictionary words, birthdates and family names, equipment names, model numbers or even keep the default passwords. It is common to find passwords like ‘cisco’ and ‘intel’.

#### **3.2 Viruses and worms**

Social engineering tactics have frequently been used as part of virus and worm attacks, as shown in Table 1. Users have been tricked into opening and running harming messages that claim to be legitimate programs or applications. The human mind is inquisitive and can get tricked into responding to such incentives, which cause their systems/network to be exploited successfully.

The success and possible damage of an unsolicited mail with a harmful payload can be judged by its rapid spread and also by the number of machines compromised. Social engineering comes to the rescue and helps to increase the levels of curiosity and want. Clearly, most individuals would have been thrilled to see a ‘*Love letter*’ in their rather boring inbox and would be interested to open it; and a good proportion of users would have clicked away without checking and thus infected their systems.

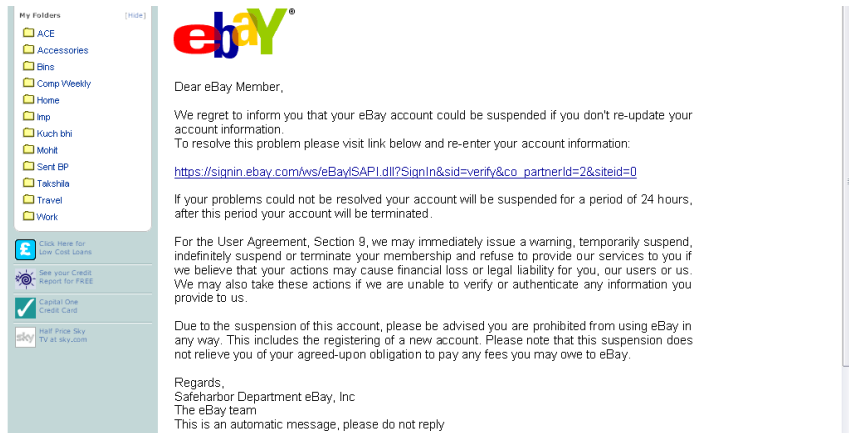
Name	Appearance	Background tasks
<i>Christma Exec</i> , 1987 (Virus)	Promises to draw a Christmas tree, and does draw it.	Sends out copies of itself in the users' name.
<i>Happy99/Ska</i> , 1999 (Worm /Trojan)	Displays fireworks on the screen.	Modified the WSOCK32.DLL file. Caused a 2nd mail to be sent with the worm to the same recipient.
<i>Melissa</i> , 1999 (Virus)	Promised account names and passwords of erotic sites.	Affected the document template in Microsoft Word and ran a macro that opened Outlook and sent mails to 50 recipients.
<i>PrettyPark</i> , 1999 (Worm)	Bears an icon of a character from a television show, South Park.	Modifies system registry. Emails itself to addresses in the Windows address book. Mails private system data and passwords to IRC Servers.
<i>Love Letter</i> , 2000 (Worm)	Appeared to have a Love letter text file attached to it, which was actually a VBS script.	Infected Windows and system directories. Sent out emails to addresses in Outlook and also tried to spread through IRC channels.
<i>Anna Kournikova</i> , 2001 (Worm)	Pretended to carry a JPEG picture of the tennis star.	If executed, it emailed copies of itself to all addresses in Outlook.
<i>Gibe</i> , 2002 (Worm)	Disguised as a Microsoft security bulletin and patch.	Secretly installs a backdoor onto the system.

**Table 1: Social engineering methods used by viruses and worms (Chen, 2003)**

### 3.3 Phishing

Phishing, which has now become a very serious threat, also employs clever social engineering methods. Emails are shown to be sent by banks and other financial organisations, and they get people to divulge personal information like bank account numbers, passwords, etc. The success of such an attack depends on the number of individuals who actually are duped by clicking the links within the emails. Hence, phishing mails are sent out in huge numbers to have at least a small percentage of users clicking away to their doom.

As seen in Figure 2, the user is made to believe that the email has been sent by eBay. This kind of mail is among the sophisticated phish mails, which has developed over time and has been designed to look genuine. Many users will actually click on the link given and be taken to a site that looks like ebay.com, but actually is a illegitimate site that will ask for the user's personal details. Depending on the level of complexity, malicious code could also be run on the users' machine when they are directed to the fake site.



**Figure 2: A phishing email, supposedly from eBay**

Although, the email is cleverly disguised, such damage can easily be avoided if the mail is scrutinised a little; in this particular case the following observations can be made:

- the email comes from a spoofed id: support\_num\_100737@ebay.com;
- it is not a personalised email, mentions ‘Dear eBay member’;
- there is no sender name, and comes from a so called ‘Safeharbor Department’.

However, the attempt may still be sufficient to fool casual or naïve users. As such, it is useful for potential victims to be educated about safe surfing habits and social engineering tactics.

### 3.4 Identify theft and fraud

Identity thefts are again an area that can make use of social engineering methods for fraud to maximise the attackers’ benefits. Identity thieves existed long before the information technology age, but now the Internet has made it so much easier to masquerade as someone else. Anonymity on the Internet gives rise to many more attacks, because it is very difficult to track down individuals who can use various means to conceal their true identity. Different attacks methods combined with social engineering give many new avenues to commit *efraud* by stealing another individuals’ identity.

Trojans slipped into an individuals’ machine by means of viruses or worms can collect personal information that might be later used to steal money, or impersonate the individual. User account information gathered by simply asking, or by guessing, or using tools - can be used to log into different systems and exploit them, or log into an online shopping site and benefit the free purchases. Phishing attacks can grab personal information, and the attacker can steal from the victim without being caught until they have fled. Attackers can penetrate into an organisation and cause a variety

of damages from physical destruction of equipment to stealing valuable proprietary information.

To commit a successful e-fraud, the attacker must employ different levels of social engineering to gain knowledge about the target. The more information that is gained, the easier it is to crack the target. Similarly for an Identity theft, the attacker must know as much information about the individual he is impersonating; failing which his/her cover will be blown and s/he could be caught. Thus we see that social engineering is the basis for successful e-fraud.

## 4. Conclusion

To quote Kevin Mitnick: "Why do hackers use social engineering? It is easier than exploiting technology vulnerability. You can not go and download a Windows update for stupidity... or gullibility" (Gedda, 2005). It is a perfect explanation given by a former hacker and famous social engineering expert. Many attackers would rather just ask information from an unsuspecting employee using social engineering skills or by combining social engineering tactics along with other attack patterns.

The onus lies in the hands of the organisation to educate their employees about social engineering tactics. All factors that contribute to social engineering exploits should be considered and the employees must be made aware of such patterns. Security policies should be devised and there should be specific clauses addressing the problem of social engineering. These policies should be promoted from time to time and employees should be trained on best practices. This has to be a continuous process, as the only way to combat a non-technical issue, is to cultivate non-technical safeguards too, along with maintaining the technical levels of protection.

## 5. References

Chen, T. (2003), "Trends in viruses and worms", *Internet Protocol Journal*, vol. 6, September 2003, 23-33

Ernst & Young (2004), "*Global Information Security Survey*", [http://www.ey.com/global/download.nsf/International/2004\\_Global\\_Information\\_Security\\_Survey/\\$file/2004\\_Global\\_Information\\_Security\\_Survey\\_2004.pdf](http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf), (Accessed: November 07, 2004)

Gedda, R. (2005), "*Hacker Mitnick preaches social engineering awareness*", <http://www.computerworld.com.au/index.php/id;1016567243;fp;16;fpid;0>, (Accessed: August 28, 2005)

Paradowski, C. (2001), "*The Cyber Con Game - Social Engineering*", [http://www.giac.org/certified\\_professionals/practicals/gsec/0971.php](http://www.giac.org/certified_professionals/practicals/gsec/0971.php), (Accessed: September 02, 2005)