

# **SOCIAL ENGINEERING AGAINST INFORMATION SYSTEMS: WHAT IS IT AND HOW DO YOU PROTECT YOURSELF?**

**BREIFING 08A/2006**

**2 JUNE 2006**

This paper was previously published by the National Infrastructure Security Co-ordination Centre (NISCC) – a predecessor organisation to the Centre for the Protection of National Infrastructure (CPNI).

Hyperlinks in this document may refer to resources that no longer exist. Please see CPNI's website ([www.cpni.gov.uk](http://www.cpni.gov.uk)) for up-to-date information.

## **Disclaimer**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

## Key Points

- Social engineering attacks are increasing in frequency and can be technical or non-technical; both manipulate staff to gain unauthorised information which can then be used to damage the organisation or for criminal purposes.
- Social engineering concentrates on exploiting the weaknesses of people, rather than IT systems or the computer security process.
- Critical National Infrastructure (CNI) companies have reported attempts by attackers using social engineering techniques to elicit internal information by means of telephone, email and face to face contact.
- Email attacks are increasingly using more sophisticated social engineering techniques to appear more credible.
- Staff targeted tend to be those who work in customer facing roles, especially IT, help desks, receptionists, security guards, cleaning and catering.
- Improving the security awareness of staff throughout the organisation is essential if the risk of successful social engineering attacks is to be reduced. This awareness training should be part of security training alongside IT and physical security training.
- Protective measures should be part of every organisation's security policy and implemented throughout the organisation.

## Introduction

1. This briefing details social engineering (SE) methodologies, the psychological triggers employed by attackers to target vulnerable staff and gives advice on protective measures.

2. The briefing considers the SE techniques deployed to gather information that breaches the organisation's security or will equip the attacker with information to mount an attack (technical or non-technical) that will breach security. The focus of the briefing is primarily on access to information systems.

3. This type of SE preys on the weaknesses of the human link in an organisation's security system. It exploits our fears or our natural tendency to trust each other and our willingness to help, in order to deceive and manipulate us to provide information.

4. The briefing has been drafted partly in response to reports from UK Critical National Infrastructure (CNI) members about recent attacks on their organisations. It highlights the need to understand the social psychology of staff members in order to improve and strengthen an organisation's security measures, its systems and networks

5. All staff need to be aware of SE approaches and techniques along with the various forms of technical attack. It is said that SE is one of 'the hardest forms of attack to defend against because simple IT hardware and software alone won't stop it'<sup>1</sup>. SE requires a focussed commitment by the organisation if it is to be prevented

6. Social engineering attacks are often closely linked to malicious activities such as:

- hacking (remote computer compromise, and possibly insider attack);
- identity theft;
- phishing (mass emails which try to gain authentication details of customers of financial organisations);
- spearphishing (targeted phishing attacks);
- pharming (phishing attacks which use technical means to direct users to malicious web sites); and
- industrial espionage and traditional espionage.

7. To explain some of these terms further:

- Phishing requires user interaction, for example following the link in an email to the malicious web site, where the user is prompted for personal information such as bank or credit card details.
- Spearphishing is a targeted attack; it focuses on a specific individual.

- Pharming refers to a class of attacks that lead to a legitimate web site address referring to an internet address operated by an attacker. Pharming can be used to lead a user to click on a legitimate web address in an email and be directed unknowingly to a malicious web site.

## Social engineering definitions

8. Social engineering has been defined in both security and psychological terms by a variety of different people and organisations; the High-Tech dictionary defines it as: “breaking an organization’s security by interactions with people”<sup>2</sup> Kevin Mitnick, once described as the FBI’s most-wanted hacker, defines SE as taking advantage of people’s naivety via influence, persuasion and manipulation to obtain vital information.<sup>3</sup> It has also been described as “the art and science of getting people to comply with your wishes”.<sup>4</sup> The Certified Information Systems Security Professionals’ study guide (CISSP) refers to SE as: “A skill by which an unknown person gains the trust of someone inside your organisation and encourages them to make changes to an IT system in order to grant them access rights”.<sup>5</sup> Yet another definition, from Wikipedia, defines SE as: “The practice of obtaining confidential information by the manipulating of legitimate users”.

## Attack methodology

9. Often the attacker will try to convince the victim that that they are in a formal position of authority and they will trick the person to reveal sensitive information or carry out an act which is contrary to the organisation’s policies.

10. SE attackers begin by collecting readily available information about the user or the organisation. The attacker then uses this basic information to build a profile of the user, organisation, IT systems and if possible the security processes. This information is then used by the attacker to build credible stories or scenarios which will cause the victim to take physical actions, mistakenly give information, or click on a web address in an email to open a web page that may release malicious code into their computer.

11. Social engineers use several avenues of attack.

- **Via the telephone:** this is the most common form of SE approach usually to the front facing support desk staff to gain their confidence and active support.
- **Face to face:** a targeted member of staff will be approached and manipulated, tricked or coerced into giving support or information.
- **Via email:** Phishing and Pharming are the most common forms of SE attack via email. Emails are created to look like a legitimate

request from a bank or other trusted organisation with which you are happy to transact.

- **By searching through waste for personal information:** in the USA this is called “dumpster diving”<sup>6</sup> and is now also called “skimming”. It is a key activity in identity theft attacks. Skimming is now a very sophisticated form of attack and we are in the fifth generation of this activity. The searching for documents such as credit card statements and invoices was associated with the first generation of skimming attacks.
- **Web searches,** where too much detailed information about staff, departments, products, services and the organisation’s key activities is posted on web sites. This is often a very simple open source search for the SE attacker; it assists them in the target acquisition process.
- **Statutory company returns** and other public documents are used in the open source searches carried out by the attacker; it helps the attacker to focus the approach for the attacks.
- **Online, Open Information.** Online curricula vitae (CVs) are another useful source of personal information, and some web sites and news groups give details about who you are and where you work if you have posted that information.
- **Advertising,** where, once the above searches have been completed and the attacker has profiled the organisation or individuals, targeted persons in the organisation receive free hardware, storage, CDs or DVDs and other offers which will carry malicious payloads.

## Psychological triggers

12. In the social sciences of psychology and sociology there are six “basic tendencies of human nature”<sup>7</sup> said to be involved in any attempt to obtain compliance to a specific request or SE manipulation.

- (a) **Authority** – assertions or implications of authority can be highly effective, especially if used on a low-level or newly recruited member of staff. A common approach is claiming to be from the IT department, security compliance department or from a high level executive or manager, and using this perceived position of authority to telephone the help desk demanding to know why they cannot log on with their password. The attacker then intimidates the help desk into giving them a new password, by telling them there is a limited time to retrieve some information for a report to the organisation’s Chief Executive. The attacker may also

threaten to report the help desk employee to their supervisor. This approach is particularly effective in hierarchical organisations.

- (b) **Likes and similarity** – through conversation the attacker attempts to probe for a personal connection; for example, supporting the same football club, sharing hobbies or activities, or claiming to come from the same area. It is a natural tendency for human beings to associate with people who like the same things as them or who are similar to them. Once a rapport is established the victim is more likely to trust the attacker with sensitive information.
- (c) **Reciprocation** – “typical social interaction dictates that if someone gives us something then it is only right for us to return the favour”.<sup>8</sup> This is known as reverse social engineering, when an attacker sets up a situation where the victim encounters a problem, they ask the attacker for help and once the problem is solved the victim then feels obliged to give the information requested by the attacker.
- (d) **Commitment and consistency** – attackers use people’s desire to comply and be seen as committed and trustworthy in order to carry out attacks. An attacker may ask the employee to carry out a task with the implication that non-compliance could result in a reprimand or them being viewed unfavourably. An example is that of a new employee being given security policies by the attacker and then being requested to share the victim’s password to ensure they are complying with the security policy.
- (e) **Social validation** – it is human nature to want to be accepted within any community and people are much more willing to carry out tasks if they are aware that their peers have already performed a similar task. Social engineers manipulate this by “name dropping” other employees’ names within the organisation and by implying that they have willingly given their help. This makes the victim feel that it is more acceptable to help the attacker.
- (f) **Scarcity** – people have a tendency to comply when they believe that an object being sought is in short supply and that others are also competing for it, or that it will only be available for a short period of time. An attacker may send an email claiming that there are a limited number of free prizes and the winner is the person who clicks on a certain link. This can be used in Phishing attacks and in targeted email Trojan (spearphishing) attacks.

## Target acquisition

13. All of the above psychological triggers are designed to heighten a person’s emotional state, allowing the attacker to get away with more than would normally be deemed as reasonable or permissible. The surge of strong emotions from fear, surprise, excitement or panic “works as a powerful distraction and thus

interferes with the victim's ability to evaluate, think logically or develop a counterargument."<sup>9</sup> Social engineers employ these tactics in the extraction of the information they require. This paper will focus mainly on telephone and emails attacks because they are the most common method of attack and they have the lowest level of detection and arrest for the SE attacker.

14. Before any of the following SE methods are employed, it is extremely common for the attacker to carry out general research and open source searches into their target organisation, to acquire the core information they need to plan the attack, work out the attack scenarios they will use, and if possible who to use them on.

15. As mentioned, this can be done in a variety of ways, based on corporate websites, annual reports or returns, newspaper articles, searching waste bins or by simply walking into the building and reading a list of departments. These pre-attack preparations are vital; an understanding of the organisation's structure and an awareness of its internal phone numbers and employees' names (e.g. via a stolen telephony directory) are crucial to any successful attack. Familiarisation with the organisation's internal language indicates to the potential victim that the attacker is a *bona fide* member of that organisation and can therefore be trusted.

16. Attackers will try to circumvent the technical security blocks on the system (such as firewalls and anti-virus software) to install their malicious code; they could do this by using SE, getting computer users to take actions that will unwittingly allow the new code to be installed and the organisational data compromised.

## Targeting IT Help desks to gain trust

17. SE relies on the fact that human nature inclines us to help where possible. This is then reinforced by help desks, where employees are trained to help those who call requesting information or support. Examples of this have been given by Sharon Gaudin.<sup>10</sup>

### Example 1:

A woman calls an organisation's help desk and says she has forgotten her password. In a panic, she adds that if she misses the deadline on a big advertising project her boss might even fire her. The help desk worker feels sorry for her and quickly resets her password – unwittingly giving the attacker a clear entrance into the corporate network.

### Example 2:

Someone, apparently internal, calls the helpdesk claiming to be from IT security and mentions that the organisation is investigating Mr xxxx. They then state a password which they know to be wrong. The IT support person, who is often

bored, under pressure and wants promotion, is keen to be helpful, so they look up the target and respond with 'No, that is not the password, the correct one is yyyy'.

18. Although very simplistic these examples demonstrate how our desire to help, especially when driven by emotion, can lead to high level security breaches.

### **Gaining access – by asking for seemingly irrelevant information**

19. SE attackers are very conscious of the fact that they should not ask for too much information from one person during the initial stages of an attack. The information they ask for might not seem to be important, but to the attacker it might be crucial to their understanding of the organisation, its procedures, its staff, its operations, product launches, takeovers, mergers and other events. The possession of such insider knowledge adds credibility to the attacker in subsequent SE attacks.

20. The skilled hacker will try to gain information very slowly, frequently asking only for small favours or gaining information through seemingly innocent social conversation.<sup>11</sup> A recent report to NISCC detailed an incident where an attacker called claiming to be from the organisation's IT department requesting details of mouse serial numbers. This type of attack was also reported by another organisation over a year ago; it seems likely that the request for the mouse serial numbers, although seemingly irrelevant, could be used as authentication in an attack at a later date. The attacker may well call back and quote these serial numbers to the victim and ask them for confirmation. Once this is achieved the victim may think the hacker is bona fide and will be more willing to comply with any requests to divulge further, perhaps more sensitive, information.

21. SE attackers learn to sound like insiders in order to gather pieces of critical information. Information such as internal extensions, merchant ID numbers, accounts department codes, employee numbers and names of people within particular departments are all of importance. "Just like pieces of a jigsaw, each piece of information may be irrelevant by itself. However, when the pieces are all put together, a clear picture very often emerges."<sup>12</sup>

22. It can be very hard to try and defend against SE attacks as the information is often common knowledge within the organisation, but can be misused if passed to a third party.

23. Targeting more junior members of staff such as IT help desk operators, secretaries and customer facing staff (who are trained to be helpful to those people requesting information) is a common approach used by the social engineer. Secretaries are a very useful aid to attackers if they are unaware of the value of specific organisation information or how that information might be used to benefit the attacker and damage the organisation. They may also be more susceptible to an SE attacker who uses an approach such as

- A caller who invokes authority for information their manager handles.
- A person who seems friendly and likeable.
- A person who appears to know people in the organisation who are known to the victim or their manager.
- A request that the attacker claims is urgent and that their manager might be in trouble for not have carried out some action.
- The inference that the victim will gain some kind of favour or recognition.

24. The secretary or personal assistant is often the first person the sales person targets in an organisation, because they know that this is a key person for access to managers and their information. A social engineer may claim that there is a virus or worm in the organisation's computer system, that "this is really urgent" and "I don't want this to reflect badly on you". These types of claims are frequently employed to try and manipulate the victims into carrying out the attacker's SE requests by heightening the victim's emotional state.

25. Phishing emails frequently use these SE techniques - "there has been a security breach, please update your identification details". This is to induce a user to click a web link that takes them to a system where they are prompted to give personal information such as PIN numbers or bank details.

### **Pretending to be a colleague or a new employee**

26. As we have seen many social engineers will pose as colleagues or as new entrants to the organisation. They will then call the support desk asking for password information or for a password to be reset because they have forgotten the password due to the mass of information given to them on their induction. The victim in the IT department may feel compelled to be helpful. Everyone was once a new employee and everyone will have memories of starting a new job, so social engineers play on this in the hope of invoking these memories and thus gaining a sympathetic response from the victim. People want to be receptive and helpful to those within their own organisation. 'Social engineers know how to exploit people's natural desire to help and be a team player.'<sup>13</sup>

### **Posing as a delivery person, workman or executive**

27. "A man dressed in a suit with a rather harried expression on his face walks into a room full of workers. He says he just started working for the organisation but he's forgotten the password to the finance database, asks if anyone can remind him? Chances are that at least one person will tell him."<sup>14</sup>

28. This example illustrates a further tactic used by SE attackers, that of dressing for the part they are playing to create an illusion for the person they are trying to deceive or influence.

29. Delivery personnel can easily be impersonated by buying the right type of clothing and using the right equipment. “If you dress in brown and stack a whole bunch of boxes in a cart, people will hold the door open for you because they think you’re a delivery guy.”<sup>15</sup>

30. This again highlights the problem with trusting people more because they are dressed appropriately, and expecting certain things from a given situation; so external contractors, telecommunications staff and post office workers are all very useful guises to adopt.

31. Kevin Mitnick when working as a programmer at GTE California soon discovered that if he came in one day with no badge and dressed in casual clothes he would be stopped and questioned about who he was and where his ID was. One day he arrived with no badge but in a business suit, and simply latched onto a crowd of people heading for the entrance and walked in with them. Even if the guards had noticed his missing badge they would not stop him as he had management appearance and was with people who were wearing their badges. This predictability from the security guards was based on the fact “they were making judgements based on appearances – a serious vulnerability that social engineers learn to take advantage of.”<sup>16</sup>

32. One test set out to reach the office of a chief executive. An employee working for a competitor posed as a contractor who was installing antiglare/heat screens on glass windows. He picked a hot day to do this. He made up a believable pass and letter of introduction and found staff sweltering in offices all wanting their rooms measured up for the estimate to have the antiglare screen. He was frequently escorted from room to room by volunteers wanting to make sure their office was included and being made tea. By use of playing on peoples good nature he easily reached his target.

33. An interesting social engineering attack carried out on behalf of an organisation by their penetration testing team sent CDs and USB sticks to 100 randomly chosen members of staff, along with a letter addressed to each individual inviting them to inspect the contents. More than half of the recipients connected them to their work clients, even though they had no reason to assume that the contents were malware-free.

34. At UK military bases in the 1990s the security guards had to be told to stop all military staff who were running into the establishment and check their passes. Previously, the runners were permitted to run into the base without being checked: the assumption was that if they were in running gear and with a military tee-shirt and carrying a small rucksack, then they were clearly military personnel.

## **Payload**

35. Gaining physical access either by posing as a colleague or as a delivery person opens up numerous possibilities to the attacker to gather a great deal of

information. Once inside the intruder can shoulder-surf passwords, gather password or sensitive documents left carelessly on workstations or gain access to the corporate network through unguarded network ports,<sup>17</sup> through the use of hardware devices such as keystroke loggers attached to workstations or through network traffic monitoring equipment.

## **Email attacks and malware (malicious software)**

36. Email borne worms and targeted attacks frequently employ SE techniques to persuade the victim to open their email, click on a web link or open an attachment with a malicious payload; an example of this was the Kournikova worm which promised an image of Anna Kournikova as an attachment. Trojan Horse programs<sup>18</sup> are delivered in either email attachments or through links in an email to a malicious website; the victim has to be encouraged or enticed to ignore the organisation's security rules not to open these links. Emails will employ SE methods, including the use of spoofed sender address or information relevant to the recipient's job or interests, thus inducing them into opening the documents. This was the approach used in some of the email attacks documented in the NISCC Briefing of June 2005.<sup>19</sup> After the 7th July 2005 terrorist attacks on London, NISCC saw emails using this event as a subject line to persuade recipients to open the email. In one attack the details from a document posted on the web were reused within two hours to send an email to the same group of interested parties – with a malicious software attachment. Another email purported to contain information on the recipient's interests.

37. An SE attack exercise was carried out in the spring of 2004 at the US Military Academy, West Point.<sup>20</sup> The exercise was designed as a spearphishing and email attack with embedded malicious software, and was targeted against over 3000 students. These students are a sophisticated user base; they receive two four-hour lectures on information assurance and network security during their training. The results of this exercise were

- 29.3 % of the users opened the embedded email.
- 47.9% of malicious attachment emails were opened.

38. In this exercise the email seemed to be genuine, from a senior person and relevant to their key interest (their course grades). The recipients were successfully manipulated to:

- open an attachment;
- click on a link contained in the email taking them to an internet web site; and
- reply providing personal details.

39. Information on the techniques SE attackers use to install Trojan Horse programs through email are widely available on the Internet and frequently include forging sender identification, using deceptive subject lines and

embedding malicious code in attachments. The majority of users click on embedded hyperlinks and open attachments in emails received from individuals they do not know, or more insidiously from supposed insiders.

40. Sophisticated SE attacks have also been reported in Canada (June 2005) and the USA (the TITAN RAIN attack 2005)<sup>21</sup> where specific individuals were targeted (as opposed to the large random distributions which are usually associated with Trojan attacks, such as phishing attacks).

41. Trojan email attacks targeting specific individuals have increased substantially over the last year. Fake email will often claim to come from a colleague, the personnel department or the help desk and it will refer to familiar information to gain the user's trust and to encourage them to click the icon which then downloads the malicious software. The "From" address of the email may be spoofed, making it appear to come from a colleague or reliable third party organisation; the subject line and text of the email may be made to appear relevant to the recipient's work, or may be copied from a previous legitimate email and the attachment name and type appear relevant to the text and to the recipient's work.<sup>22</sup>

42. In May 2005 Israeli Police announced the conclusion of an 18 month investigation into industrial espionage. Some of the country's leading companies had been targeted by social engineers. In one case an identified employee received an email containing what appeared to be a legitimate business proposal from a known partner organisation. On opening the proposal, malicious software installed a sophisticated key logger which captured and stored all keystrokes on the user's workstation. The software then seems to have propagated itself throughout the organisation's network to offices in Germany and the USA.<sup>23</sup>

43. February 2005 saw a SE attack by another variant of the MyDoom worm (a mass email worm that sends infected messages with various subject lines and body messages). One subject line was "hello, mail system error – returned mail, message could not be delivered, error and delivery failure". Once the email is opened there is a further attachment with a plausible name. Recipients who opened the attachment were likely to compromise their own computer.

44. An attempted attack was recently reported to NISCC where an email arrived from an alleged employee of the Institute of IT Security Auditors asking if the organisation would like to receive a copy of their annual report. In addition the email requested the contact details of people in the IT security department. It appears from further investigation that the email was fraudulent and was an attempt to gain information about security personnel.

45. It is apparent from these examples that there are a variety of ways to launch an attack using technical means combined with SE techniques. Although IT security departments can do much to prevent these varied attacks getting through firewalls and anti-virus software, it is very difficult to stop them all by technical means. Raising staff awareness and educating staff is crucial. User

must therefore be made aware of the possibility of these attacks and how best to defend against them.

## **Defence strategies and mitigation**

46. “Anyone who thinks that security products alone offer true security is settling for the illusion of security”.<sup>24</sup>

47. Training and Awareness programmes can reduce the chances of a successful SE attack. Employees need to be trained to be aware of the value of the information to which they have access and the type of SE attacks that could be carried out to gain access to it. Organisations train their people to be helpful, but they rarely train them to be part of the security process.<sup>25</sup> The implementation of a multi-layered security strategy is critical to the organisation’s depth of defence.

## **Training and awareness**

48. SE attackers primarily target perimeter or outward-facing staff such as receptionists, help desks, security guards and cleaners. These employees may “have little to no technical knowledge and they may be less aware of security, especially when they feel that the information they are working with may not be highly confidential or sensitive.”<sup>26</sup>

49. All employees must be given a sense of responsibility and ownership for the organisation’s security process; they must be included in the process from their first day of employment. Staff should be given the confidence to challenge others for identification credentials. Part of the training should include staff being “attacked” by internal security experts as a means of developing experience and awareness on the types of phishing, pharming and spearphishing attacks they are likely to experience from real SE attackers.

50. All staff should be aware of their role within the organisation’s security plans; they should be aware of common approaches and signs of abnormal interest, for example the “refusal by the caller to give contact details, rushing their request, name-dropping, intimidation, misspellings, odd questions, and requesting forbidden information.”<sup>27</sup> These are all intrusion and information acquisition approaches used by social engineers.

51. The training programme for employees should include presentations on SE stories from current attacks and incidents to demonstrate the process itself and show how the SE attacker goes about extracting information. “Telling authentic stories of what happened to the ‘other poor guy’ increases resistance to these exploits in a non-threatening way, inoculating the employee against a vulnerability to SE.”<sup>28</sup>

## Verification

52. The requirement to verify credentials needs to be ingrained into employees and should apply to anyone about whom they may have doubts regardless of the position they claim within the organisation, how they are dressed, how urgent they claim the request is or what claims they make concerning lost data or damaged systems.

Verification has 3 stages:

- verification of identity;
- verification of employment status; and
- verification of the need to know.

## Examples of verification processes

- Ring the caller back to check the number and verify who they are – if possible use the number already listed in the organisation directory rather than one they give you.
- If possible get a trusted person to vouch for the caller.
- Telephone the employee's immediate supervisor and request verification of identity.
- Put the caller on hold and seek advice from your supervisor – this also allows valuable thinking time and prevents the attacker extracting information via emotional manipulation.
- If they are missing their ID badges, call and verify who they are; similarly for any contractors claiming to have an appointment.
- Check the staff employee directory, which must be kept up to date, for employment status.
- Call the employee's manager or their workgroup for verification of employment.
- Have a set procedure in place for when an employee needs any kind of authentication information and ensure the procedure is followed.
- Establish need to know by job title, workgroup and responsibilities.

53. This verification strategy will only be effective as part of an information security policy backed by senior management. Because social engineers will use the cover of someone in authority as a regular method of attack, it is imperative that if an employee challenges a senior manager, the person asking for verification will not be reprimanded for it but rather praised for ensuring proper implementation of the security policy. If an employee feels they will be viewed unfavourably they will be reluctant to challenge anyone who claims to be of a high status or seniority. Training should therefore include the best methods to challenge in a customer-friendly way someone who purports to be in authority.

## **Passwords and authentication information**

54. “The most common information that a SE attacker wants from an employee, regardless of his ultimate goal is the victim’s authentication credentials.”<sup>29</sup>

55. Once an attacker has an employee’s user name and password they can gain access and cause disruption and damage within the organisation. Password policy is simple: “passwords should not be disclosed over the telephone at any time, more appropriately, passwords should not be disclosed at all.”<sup>30</sup>

56. Employees need to be fully aware of the importance of their password as “without training, people tend to give their passwords away without much thought.”<sup>31</sup>

57. Training should include comparisons with the PIN number for your bank account and clearly establish that any request for your password over the phone should be treated as highly suspicious and reported to the security team. If the attacker is trying to pose as an employee then verification procedures should be implemented.

58. Passwords need to be changed on a frequent basis, and password discipline enforced by senior managers and security staff. Consider the use of extra factors of authentication (such as smartcard tokens) to access critical systems or to gain remote access. However, this is still not infallible; a common SE attack is to attempt to get a Secure ID PIN reset, once the attacker has gained the token via a lost or stolen laptop.

## **Data classifications, protective marking and procedural advice**

59. A clear data and information classification and procedural policy should be set out and implemented providing all employees with security guidelines to follow in a difficult access or verification situation, instead of devolving the decision on the release of information to the support staff. This policy must explicitly provide for verification of identity.

60. Within the UK, there is no standard system for marking sensitive material that originates outside of central government. However, some companies already have a protective marking system to safeguard their key information. Depending on the protective marking, certain people may be given access to different levels of information, but again the main issue is to verify that the person is who they say they are and that they have a need to know.

61. Procedures must be created to be followed for situations including: reporting suspicious calls; showing ID and challenging those without ID; shredding sensitive documents; releasing organisational chart information; releasing private details about employees; disclosing internal directories; opening attachments; participating in phone surveys and disclosing passwords. Help desks must have

procedures to follow for resetting passwords, changing access privileges, setting up a new account and disabling accounts. “Increasing employee confidence by laying out clear policies decreases the chance that the persuader will have undue influence on an employee.”<sup>32</sup>

## **Risk mitigation and best practice**

62. The following protective measures are recommended.

- Put in place verification procedures for identification of claimed employment status including contractors.
- Set up a data classification system with guidelines for the release of each level of information.
- Training on security issues for all staff. This should include either working examples of social engineering or real life examples to prove that everyone is at risk and the ease with which it can be carried out. It should also include the importance of your password and user name and the dangers of having a password that a third party knows.
- Key personnel should be given resistance training to SE attacks. These key personnel should include help desk assistants, customer service staff, secretaries, receptionists and system administrators.
- Carry out frequent penetration testing and information assurance exercises to develop awareness, and provide the users with immediate feedback. The goal of any such exercise should be to produce a culture of security within the organisation.
- Frequently and randomly carry out social engineering exercises, to “inoculate” all staff in this style of attack.
- All staff should be made aware that they are a vital part of the security system and have a responsibility for it.
- All staff should remain vigilant to SE attack and manipulation. You should always use your judgement when opening emails. If it does not look right do not open it.
- All non-technical information system users need to have spoofed emails and Trojan horses explained to them along with their security implications. Users need to be taught that if a Trojan horse program is installed the intruder can gain full control of the user’s computer and access usernames and passwords, download more sophisticated Trojans, collect system information and upload documents and data. They also need to be

aware that Trojan horses can be in various file types including databases, documents, executables, help files and compressed files.

- All information system users need to be taught how to run anti-virus software and how to install updates. They should be educated not to open attachments or follow links until they have been through anti-virus scanning and the email is consistent with previous communications by the sender.
- Staff need to be trained how to challenge people who are in authority in a customer friendly way. This will ensure that attackers and genuine senior staff alike will be challenged.
- Awareness needs to be kept at a constant high level via refresher courses and by posting recent examples of SE attacks on the organisation's intranet. Employees need to be aware of the value of the data on the system even if given out in seemingly innocent portions.
- Depth of defence within all systems is an important component in overall security; this helps to reduce multiple attacks and social engineering exploitation. Use double or triple ID checking for verification and multi-factor authentication for access to information systems.
- Carry out regular audits and test the security procedures with your staff. This should include inspections to check for unauthorised hardware devices attached to information systems.
- Understand the threat from the insider attack, the control of contractors, vetting and the knowledge staff take with them when they leave your organisation. See the NSAC briefing paper on this and consider additional authentication.

63. As a key part of the security plan there should be handling instructions for treating suspicious media (such as CD-ROMs) and emails.

## Endnotes

---

- <sup>1</sup> Jones, Chris “Social Engineering: Understanding and Auditing” 3 March 2004, <http://www.sans.org/rr/whitepapers/engineering/1332.php>
- <sup>2</sup> <http://www.computeruser.com/resources/dictionary/definition.html?lookup=8057>
- <sup>3</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>4</sup> Bernz . “The Complete Social Engineering FAQ!” 14 Jan 1997, <http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt>
- <sup>5</sup> Neil Barrett, “Digital Evidence”, Elsevier Ltd, March 2003
- <sup>6</sup> This is the process of going through an organisation’s rubbish to find information that has value in itself or can be used as a tool for a further SE attack.
- <sup>7</sup> Robert B. Cialdini. “Scientific American” February 2001
- <sup>8</sup> Jones, Chris “Social Engineering: Understanding and Auditing” 3 March 2004, <http://www.sans.org/rr/whitepapers/engineering/1332.php>
- <sup>9</sup> Rusch, Jonathon J. “The ‘Social Engineering’ of Internet Fraud.” United States Department of Justice 1999, [http://www.isoc.org/inet99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/inet99/proceedings/3g/3g_2.htm)
- <sup>10</sup> Gaudin, Sharon. “ Social Engineering: The Human Side of Hacking” 10 May 2002, <http://www.crime-research.org/library/Sharon2.htm>
- <sup>11</sup> Gragg, David “ A Multi-Level Defence Against Social Engineering” 13 March 2003, <http://www.sans.org/rr/whitepapers/engineering/920.php>
- <sup>12</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>13</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>14</sup> SANS Institute 2001
- <sup>15</sup> Gaudin, Sharon “Social Engineering: The Human Side of Hacking” 10 May 2002, <http://www.crime-research.org/library/Sharon2.htm>
- <sup>16</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Chapter 10, 2002
- <sup>17</sup> Jones, Chris “Social Engineering: Understanding and Auditing” 4 Nov 2003
- <sup>18</sup> A Trojan Horse (“Trojan”) is an attack method in which malicious or harmful code is contained inside apparently harmless files.
- <sup>19</sup> <http://www.niscc.gov.uk/niscc/docs/ttea.pdf>
- <sup>20</sup> Aaron J Ferguson “Fostering Email Security Awareness: the West Point Carronade. Educause Quarterly, 2005, <http://www.educause.edu/ir/library/pdf/eqm0517.pdf>
- <sup>21</sup> [http://en.wikipedia.org/wiki/Titan\\_Rain](http://en.wikipedia.org/wiki/Titan_Rain)
- <sup>22</sup> [http://ww3.psepc-sppcc.gc.ca/opsprods/info\\_notes/IN05-001\\_e.asp](http://ww3.psepc-sppcc.gc.ca/opsprods/info_notes/IN05-001_e.asp)
- <sup>23</sup> Wall Street Journal 2005
- <sup>24</sup> Mitnic, Kevin & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>25</sup> Gaudin, Sarah “ Social Engineering: The Human Side of Hacking” 10 May 2002 <http://www.crime-research.org/library/Sharon2.htm>
- <sup>26</sup> Jones, Chris “Social Engineering: Understanding and Auditing” 3 March 2004, <http://www.sans.org/rr/whitepapers/engineering/1332.php>
- <sup>27</sup> Gragg, David “ A Multi-Level Defence Against Social Engineering” 13 March 2003, <http://www.sans.org/rr/whitepapers/engineering/920.php>
- <sup>28</sup> Wendy Arthurs “A Proactive Defence to Social Engineering” 2 August 2001, <http://www.sans.org/rr/whitepapers/engineering/511.php>
- <sup>29</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>30</sup> Mitnick, Kevin D. & Simon, William L. “The Art of Deception” Hungry Mind Inc., 2002
- <sup>31</sup> Gragg, David “ A Multi-Level Defence Against Social Engineering” 13 March 2003, <http://www.sans.org/rr/whitepapers/engineering/920.php>
- <sup>32</sup> Gragg, David “ A Multi-Level Defence Against Social Engineering” 13 March 2003, <http://www.sans.org/rr/whitepapers/engineering/920.php>

---

**National Infrastructure  
Security Co-Ordination Centre**  
PO Box 832  
London  
SW1P 1BG

Tel: 0870 487 0748  
Fax: 0870 487 0749  
Email: [enquiries@nisc.gov.uk](mailto:enquiries@nisc.gov.uk)  
Web: [www.nisc.gov.uk](http://www.nisc.gov.uk)