SOCIAL ENGINEERING: UNDERSTANDING THE THREAT

A guide for business and security managers to help identify the threat from those who wish to extract information from employees or gain access to sites using psychological manipulation.

The guidance focuses on developing and deploying active measures for countering the threat.

December 2013

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.
Executive summary

The process of obtaining information from others under false pretences is, in essence, manipulation. Any attempt to gain entry to a site using a bogus pre-text is called penetration. Both processes are a form of what is commonly known as ‘social engineering’. They are based upon the building of an inappropriate trust relationship with individuals, and can be used against those within an organisation.

By using this information the social engineer is able to make a connection with an employee within an organisation, build on it, then move on to exploit the relationship by manipulation, taking advantage of the organisation’s lack of security procedures or even a contact’s personal vulnerabilities.

Those engaged in social engineering are diverse, for example single issue direct action groups, commercial competitors, terrorist cells or Foreign Intelligence Services seeking sensitive information from UK sources.

Social engineering attacks can be either dispersed or direct. Attackers prepare well, learning about an organisation’s structure and language in advance. Their approaches create a plausible context. They may

- exploit the willingness of employees to assist others;
- take advantage of an employee’s poor use of the internet, to introduce malware;
- use information unwittingly provided by individuals on the internet, particularly on social media;
- exploit freely-available useful information on organisational websites, such as details on security, personnel, physical access.

All employees are vulnerable to social engineering, but there are possibly more vulnerable groups such as: production workers, administrative staff, and sales and marketing people. The common factor with these individuals is that they are people who do not generally deal in especially sensitive information.

The most effective countermeasure against social engineering is education: employees should be made aware of social engineering and the value of the information they hold.

Organisations should also consider implementing policy and procedural steps such as software controls for employees’ internet access, effective filtering across internet gateways, developing internet access policy, protective marking systems for sensitive documents, employee reporting mechanisms and ensuring their website information does not offer information of use to the social engineer.

Guidance and tools to help with countermeasures are available on CPNI’s website.
Table of Contents

Executive summary .................................................................................................................. 2
Introduction – the threat ....................................................................................................... 4
The need to protect against social engineering ...................................................................... 4
Strategy .................................................................................................................................. 5
Counter-social engineering model and risk assessment .............................................................. 6
Types of attack ....................................................................................................................... 10
Vulnerabilities ....................................................................................................................... 10
How does a social engineer work? .......................................................................................... 11
Approaches ............................................................................................................................. 12
Counter-measures ................................................................................................................. 13
How to counter social engineering ....................................................................................... 13
Overview ............................................................................................................................... 13
Employee awareness .............................................................................................................. 16
Document management and accountability ............................................................................ 17
Annex A: Table of social engineering approaches .................................................................. 19
Annex B: Further guidance .................................................................................................... 23
Introduction

The threat

Those engaged in social engineering are diverse:

- Single issue, direct action groups, such as anti-vivisection activists;
- Commercial competitors, aiming to gain information on products, contracts;
- Terrorist cells, seeking information for targeting purposes;
- Foreign Intelligence Services (FIS) seeking sensitive information from UK sources to advance their own military, technological, political and economic programmes.

An academic with access to protectively marked material was cultivated in the UK by a FIS. Meetings were held at locations convenient to the academic’s home and work addresses, with meals and drinks being paid for by the FIS officer. The academic provided unclassified documents and paperwork to the officer who regularly tried to over-pay the academic for the assistance provided. The FIS officer attempted to develop a friendly relationship with the academic and gave thoughtful and personal gifts, tailored to the academic’s interests, for birthdays and Christmas.

The need to protect against social engineering

Physical security measures such as vehicle barriers, Automatic Number Plate Readers and secure fences reduce the possibility of an attack. However, they are useless if a security guard is duped into letting a person with hostile intent drive through the front gate because the driver claims that he is ‘making a delivery and has lost his paperwork and will be in trouble with his boss if he doesn’t make the drop’, but does seem to know the name of the facilities manager. A very plausible and effective story.

Furthermore, an organisation can have all the latest information security, such as robust firewalls and highly secure passwords, but again these are redundant if a receptionist is talked into telling someone claiming to be an ‘IT support’ person key information needed to get into the system. The human element is often the weak point; this guidance looks at this aspect rather than the nature of the technical threat and corresponding countermeasures.
Strategy

The first step is to decide on a strategy for the counter social engineering approach; this strategy should allow the organisation to concentrate on the key vulnerabilities. To do this, answer three key questions:

- What to protect?
- How to protect it?
- How long to protect it?

Providing focus in this way means that the response to the threat should be proportionate and sustainable.

What to protect?

The first step is to decide what really needs protecting; this could be a physical location or information but the emphasis should be on what is critical to business continuity. It is impossible to protect everything, so the emphasis should be on what is critical.

Social Engineers are unlikely to be looking to answer the million dollar question with one direct question (‘what is the code for the server room?’); instead, they will attempt to piece together the information like a jigsaw, picking up little pieces, different cues and signals given by staff who do not know value of these little snippets.

For example: If someone asked you straight out for the password to your computer at work, you wouldn’t tell them. However, you might, if the enquirer has a good reason for asking (such as an IT magazine doing a survey), admit that to remember it you use a memorable word. Then in a separate conversation you might admit to someone else (perhaps a harassed IT support person) to using the name of the road you live in, but not tell them what it is. Then finally, in a totally separate conversation with someone else, you might happily tell them the name of the road. The result of all this circuitous manoeuvring? Access to your password. The key here then is not to fall into the trap of giving out pieces of supposedly unrelated information, which allows the social engineer to put them together to form a complete picture.

How to protect it?

The next question to answer is what approaches and techniques should be used to address the threat. There are various methods available to counter social engineering. The choice of approach will be partly driven by the nature of the threat; it should also be partly driven by a consideration of what will fit with the security culture of the organisation. What will be the reaction of employees to any new procedures put in place? Does this mean that the organisation does not trust its employees? Will the new rules just be seen as unnecessary bureaucracy that gets in the way? Without the buy-in of employees, the new procedures will not work (see CPNI’s Security Culture Review and Evaluation (SeCuRE) tool).

How often should you review effectiveness of countermeasures?

The final question to answer is how long the measures should be in place. Countermeasures may need to be reviewed on a 12 or even 6 monthly cycle. This ensures that they remain effective and proportionate depending on the nature or duration of the threat.
Counter-social engineering model and risk assessment

It is important to take a structured and planned approach to the problem of countering the social engineering threat. The approach should also be:

- Threat led
- Evidence-based
- Effective
- Tested
- Proportionate
- Practical

One way to ensure that the approach adopted meets all of these criteria is to follow the Counter Social Engineering Model outlined below.

Figure 1: Counter Social Engineering Model

The model is cyclical in nature and should be seen as a constant process; the different elements are outlined below.
1. Define protection requirements

The first step is to identify the specific requirement, physical location or information set that needs protection. It is important to resist the temptation to say ‘everything’. A simple approach to address this issue is to ask the question: ‘What keeps you awake at night?’ and then identify one or two key issues.

2. Assess the threat

A more formal approach is to conduct a full risk assessment exercise. The key issues here are to identify the factors that are key to business continuity of the organisation. These factors will generally be information or physical infrastructure, or both. A useful way to prioritise these factors is along two dimensions, impact and likelihood:

- **Impact** – what would be the adverse effects on the organisation if a successful ‘attack’ was made on that asset (i.e. information lost or physical site damaged)? The impact on the organisation can range from small (data is easily recoverable, the information is not sensitive, or there is a backup physical site) all the way up to critical (data is lost totally, information is highly sensitive or there are no contingency plans in place to remove to another site).

- **Likelihood** – what is the probability that the attack will take place?

Using these two considerations can help to focus protection efforts with emphasis given to the high impact/high likelihood combination first. This analysis should produce a clear set of principal protection requirements where the counter social engineering effort should be focused.

3. Estimate vulnerabilities

The next step is to assess the actual vulnerabilities the organisation has to these threats. For example, which members of staff are vulnerable to a social engineering attack? For example:

- **Outward facing roles** (sales & marketing/customer service/ receptionists)
- **At a lower level** (those who may not appreciate the importance/sensitivity of the information or site)
These roles may be targeted to by a social engineer but **anyone in the organisation is at risk**. In addition, the social engineer will also look for individual characteristics about the staff members; characteristics that may make them vulnerable to exploitation:

- **Sexual behaviour**
- **Addictions** (alcohol/drugs/gambling)
- **Debt**
- **Personal interests** (charities / hobbies)
- **Vulnerable work role** (external contacts / extensive travel)

A staff member with any of these characteristics may be vulnerable to manipulation. Many of these can be easily identified, especially with the increase in popularity of social networking media.

The prospective social engineer will therefore conduct a lot of preliminary research on the organisation and its staff members before engaging in an attack. Any threat assessment should look at the organisation’s external signature and identify where vulnerabilities might lie:

- **Online research** (organisation websites/social media/user sites, blogs/public reports)
- **External events** (conferences/seminars/workshops/forums)
- **Social activities** (pubs/bars/restaurants)

The key question to address is what potentially valuable information is available to a social engineer through these means that can be used to plan an attack?

### 4. Employ countermeasures

Having defined the protection requirements, assessed the threat to these, and identified where the vulnerabilities lie, the next step is to develop and deploy the appropriate countermeasures that are consistent with:

- **Vulnerability profile** – do they address the threat?
- **Organisational culture** – will they be acceptable?
- **Operational considerations** – will they be practical?

The answer to all these questions needs to be ‘yes’ for the countermeasures to be effective. The range of possible countermeasures includes:

- **Employee awareness**
- **Document management and accountability**
- **Counter-elicitation training**
- **Counter-surveillance**

This is only a brief list and these are covered in more detail later.
5. Measure effectiveness

Once the countermeasures are in place, it is important to test the effectiveness of the new approaches to see if they are actually reducing the organisation’s vulnerabilities.

6. Dissemination

To complete the cycle, it is vital to report back on the effectiveness of the programme, especially to senior management. This is key, especially because these countermeasures are expensive and there is often no tangible return. It is also important to broaden out the reporting to other groups or parts of the organisation including strategic partners who might also be vulnerable to the threat.

Further advice on carrying out a risk assessment in your organisation can be found in the CPNI guidance *Personnel Security Risk Assessment*.

Types of attack

Vulnerabilities

All employees are vulnerable to social engineering, but there are possibly more vulnerable groups such as: production workers, administrative staff, and sales & marketing people. The common factor with these individuals is that they are people who don’t generally deal in especially sensitive information; furthermore, employers don’t spend very much time encouraging them to be discreet about what they know. Essentially, employers or the employees themselves underestimate the value of the information they deal with. Additionally, employees such as receptionists, personal assistants, and customer service representatives, who have been specifically trained to be helpful to those requesting information, are more vulnerable to these kinds of attacks.

The social engineer seeks to take advantage of natural tendencies that make individuals more vulnerable to manipulation:

- desire to be helpful
- need for recognition or a tendency towards self-effacement
- need to correct others or prove someone else wrong
- a tendency to discuss things that are not of direct concern, a natural tendency to gossip
- satisfaction of talking to a sympathetic listener
- interest in sharing confidences with or show off expertise to another professional
- indiscretion when not in control of one’s emotions

Finally and perhaps most obviously, people are generally unable to keep secrets.
How does a social engineer work?

The process of acquiring information to establish a relationship can take many forms, for example:

- by exploiting willingness of employees to assist others;
- taking advantage of an employee’s poor use of the internet, to introduce malware;
- using information unwittingly provided by individuals on the internet, particularly on social media;
- exploiting freely-available useful information on organisational websites, such as details on security, personnel, physical access.

By using this information the social engineer is able to make a connection with an employee within an organisation and build upon it. The social engineer is then in a position to exploit the relationship by manipulation, taking advantage of the organisation’s lack of security procedures or even a contact’s personal vulnerabilities.

A full list of approaches countermeasures can be found at Annex A.
Approaches

Social engineering attacks are either dispersed or direct. Dispersed attacks – also known as ‘mosaic’ attacks – are where one or more people pose as a co-worker, new employee, delivery person or workman, for example, and attempt to collect information from different sources over an extended period of time. They may ask employees in the target organisation for small favours or apparently insignificant pieces of information, or gather information through seemingly innocent conversation. Although each piece of information may not be useful in isolation, it can still be highly valuable to the social engineer when pieced together.

A directed attack is generally aimed at a specific individual within an organisation who has access to valuable information. The social engineer will pose as a business contact at a conference, for example, and may spend some time building a close relationship with the targeted individual before using the trust established to access information. This is likely to begin with requests for easily obtainable, non-sensitive information, gradually moving on to demands – sometimes accompanied by a degree of coercion – for more confidential data. The dispersed and directed forms of social engineering may be employed simultaneously, or the dispersed attack may be used to gather the information required to mount a more directed attack later.

Regardless of approach, the skilled social engineer will not simply ‘grill’ one individual for a long period of time in a very direct manner. The approach will be much more opaque and dispersed across different times and different targets. Specifically, a skilled manipulator will:

- attempt to gather information piecemeal
- conduct enquiries over an extended period of time
- ask for small favours
- gain information through seemingly innocent conversation

Social engineering attackers prepare well, learning about an organisation’s structure and language in advance. They then use methods such as posing as a co-worker or a new employee, posing as a delivery person or workman, pretending on the telephone to have lost their computer password, or simply appearing to befriend a colleague to conduct the attack. These approaches create a plausible context in which the social engineer can strike up a seemingly innocent conversation with the target or ask for help in an apparently legitimate fashion.

CPNI has produced a film entitled Piece of Cake, which dramatizes how individuals can access information by using data collected from an organisation to facilitate an approach on a specific employee (www.youtube.com/user/UKCPNI).

The approach may take one of a number of different forms, each designed to persuade the employee to comply. The approaches seek to draw on established principles of persuasion, themes and styles that have been shown to have real influence on people.

- See Annex A for a comprehensive list of approaches, examples and countermeasures.
Counter-measures

How to counter social engineering

To counter social engineering, an organisation should:

- undertake a comprehensive risk assessment of its critical operations which may be targeted by a social engineer (see CPNI’s guidance on Personnel Security Risk Assessment);
- make employees more security aware (see CPNI’s SeCuRE tool);
- make employees fully aware of the threat from social engineers and what measures they can take to protect themselves and the organisation (see below, page 14);
- employ software controls to ensure that only reputable websites can be accessed, reducing the risk of malware being introduced onto systems;
- ensure information on the organisation’s website is sufficient to inform the public, without offering information that helps the social engineer (see CPNI’s Security-minded communications);
- teach employees to recognise the signs of social engineering and how to deal with it confidently.

The above guidance and tools can be found on CPNI’s website.

Overview

A typical reaction to a successful test, or indeed a real attack, is to tighten up on the physical or information security: more policies, stronger locks, more guards, tighter password controls. This will have no effect if the human dimension is not addressed. The two biggest issues to address are:

- the lack of employee awareness of the threat;
- the lack of employee participation with the procedures and policies in place.

Social engineering targets individuals rather than IT systems or buildings. The most effective countermeasure is education: employees should be made aware of social engineering and the value of the information they hold.

A programme of social engineering awareness should include an overview of the wide range of possible social engineering attacks that employees might face and give practical advice for countering them, including:

- Be selective when posting personal or employment information on social networking sites;
- Avoid talking about sensitive work issues in social situations;
- Do not open emails from unknown or suspicious senders;
- Treat all email attachments with caution.
The following counter-measures can be incorporated into an organisation’s internet access policy (and which technically competent employees might also consider taking in their home computing environments):

- Use software controls that ensure only reputable websites can be accessed, reducing the risk of malicious software being installed on the system.
- Where it exists, turn off the option to automatically download attachments to emails.
- Implement effective filtering across internet gateways (e.g. spam blockers, firewall and antivirus software)
- Make sure that the latest updates to these and the operating system are promptly installed.

An organisation should also consider implementing the following procedural steps:

- Develop and communicate an internet access policy that clearly defines acceptable use of the internet.
- A system of protective marking for sensitive documents with associated handling procedures.
- Provide a mechanism by which employees can report suspected social engineering attacks.
- Provide a review process to identify any trends or repeated attempts to acquire certain pieces of information, so that other employees can be made aware;
- Ensure that the information posted on the organisation’s website(s) is sufficient to inform the public, and conforms to regulatory requirements without offering superfluous details that help the preparation of social engineering attacks;
- Implement a policy of shredding paper before disposal if it contains sensitive information;

- Require employees to declare gifts over a certain value. Review the list frequently so that unusual trends or inappropriate gifts can be spotted;
- Maintain a clear desk policy and a culture where information is handled on a ‘need to know’ basis;
- Include counter-social engineering training as a standard element in induction and regular ongoing security programmes. Articles in company newsletters and on the organisation’s intranet sites can also help to reinforce the message.
Some employees may be particularly vulnerable to social engineering attacks, e.g. those in customer facing roles, or those with access to important assets such as IT administrators or security guards. Consider additional training in countering manipulation for these groups as follows:

- Reminders of the control procedures that apply to their roles, especially those governing how/when an enquirer’s credentials should be checked before providing information.
- Being wary of unusual behaviours, e.g. a caller’s refusal to provide contact details, and the use of the common social engineering techniques of authority, conformity, empathy, reciprocity and consistency.
- Being assertive so that they can terminate a line of questioning they consider to be suspicious.
- Given support by line management when challenging those are believed to be social engineers.

A customer-facing employee who terminates a call or refuses to provide information on the grounds of a suspected social engineering attack must be confident that they will have the support of their line management. It is therefore important to ensure that the subject of social engineering is adequately addressed in the procedures governing that role. Similarly, assertiveness training can also be used to great effect to develop an individual’s ability to simply say ‘no’ to another person. This is a skill that a lot of people struggle with and is something that can be quickly developed through practical training.
Employee awareness

The best defence for all staff, but especially vulnerable employees, is to be alert to the different types of elicitation approaches and techniques.

Focus and priority should be given to the most vulnerable employees: customer-facing and possibly those not in positions identified as posing a key risk. Employee awareness programmes, using seminars and workshops to highlight the various manipulative attempts to extract information are an effective method for training staff; being forewarned of the possible types of approaches is the best counter measure for guarding against manipulation.

It is important to get employee buy-in or else any changes will not be effective. Often, a clear dissemination of the findings of a threat survey or penetration test can highlight the threat to employees as well as give them an appreciation of how to recognise approaches that might be suspicious. Most attacks can be prevented if the target:

- Verifies the identity of the person making a request
- Verifies the person making the request is authorised to do so?

A good awareness workshop should cover the following issues:

- Description of the approaches social engineers use
- Description of specific techniques used by social engineers
- How to recognise a possible attack
- Procedure for handling a suspicious request
- Where to report suspected attacks – who needs to know i.e. line management, security managers etc; with the confidence that it will be acted upon
- Importance of challenging anyone who makes a suspicious request regardless of their claimed position or importance
- Importance of not implicitly trusting anyone without proper verification, even though it is natural to give them the benefit of the doubt
- Importance of verifying the identity and authority of anyone making a request for information
- Procedures for protecting sensitive information

This last point is very important when information is the key protection requirement. A good awareness programme should therefore provide a summary of the key security policies; such as:

- Computer and voicemail passwords
- Procedure for disclosing sensitive information
- Email usage
- Physical requirement such as wearing an identification badge
- How to determine the classification of information
- Proper disposal of sensitive information
- Obligation of employees to comply with these procedures
To make awareness programmes as engaging as possible, consider role plays or videos.

On-going awareness can also be achieved through:

- **Reminders on the organisation intranet**
- **Including items in organisation newsletters**
- **Posters in communal areas**
- **Email reminders**
- **Phone stickers**

Security awareness can also be included in annual appraisals and reporting.

**Document management and accountability**

Information can be elicited from documents as well as individuals; a lot of successful penetration attacks occur because information is too available. This is because protocols are not sufficient for storing, controlling, accounting or destroying information properly. Also, information is often distributed too widely within an organisation to employees who ‘do not need to know’; and employees are not made sufficiently aware of the sensitivity of information. Some simple protective marking and handling restrictions can address these issues.

- **Protective marking**

Implement a simple system of marking material. The specific system used is dependent on the actual sensitivity of the information along with the culture of the organisation and its day-to-day operations. The main consideration is simplicity of the marking scheme. To this end, there should only be two or three levels. The scheme should clearly delineate what material should be protected and the handling restrictions associated with the different levels of marking. The marking should reflect the nature of the damage that would occur if this information should fall into the wrong hands. Another classification to consider in conjunction with this protective marking is information that is for internal use only and that which can be released externally.

Alongside this marking scheme should be a system of programme code names; information associated with any given project should be restricted only to those involved in the project. This is known as a ‘knowledgeability’ list (or a ‘Need to Know’ policy) and helps to track those employees who have access to the information. At worst, it provides a good starting point for an investigation if a compromise should occur.

For especially sensitive material, numbered copies of documents can be made (e.g. copy x of xx) and printed on coloured paper to indicate whether the document has been photocopied. For extra security, these documents could also have a unique identifier that is issued by a central registry or designated project coordinator.

Instigate a clear desk policy and make it a stipulation that protectively marked material be kept in a locked container (e.g. a security cabinet with a combination lock). In this way, any opportunity for opportunistic removal of documents, perhaps by cleaning staff, can be prevented. These procedures can be enforced with random bag searches on exit and entry as well as guards patrolling offices at night; especially before cleaning staff enter the premises.
Finally, consider a shredding policy for sensitive material. This should be a 100% policy and include such items as post-it notes with names and numbers on them.

- **Information sharing protocols**

Not all information held in the company will be sensitive and project related, but most will be of interest and useful to a social engineer. The handling of requests for information both externally and those seemingly internal can be addressed with sensible protocols.

- **Behavioural detection**

This capability involves members of a guard force who are specially trained in behavioural detection actively looking for signs of suspicious behaviour. Although these signs of suspicious behaviour encompass hostile reconnaissance, behavioural detection can be effective in picking out a range of other behaviours which social engineers may display. A feature of a robust behavioural detection programme is effective engagement with and challenging of suspicious individuals. Good questioning can un-nerve a potential social engineer. CPNI’s Personnel Security team have developed a highly effective behavioural detection programme called Passenger Assessment Screening System (PASS), which analyses possible suspicious behaviour of passengers in areas such as airports or train stations; speak to the CPNI Personnel Security team for further details.

- **Influence Activity (IA)**

Influence Activity is the co-ordinated use of media, guard force presence, posters etc. to create desired effect. The effect is to harden the prospective target by making it look more secure.

The Personnel Security team at CPNI have developed a highly effective programme of Influence Activity for protecting key sites. Speak to CPNI for details on the *Deterrence Communications Toolkit*. 
### Annex A: Table of social engineering approaches

<table>
<thead>
<tr>
<th>Social Engineer may use:</th>
<th>Explanation:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>Emphasis on his/her seniority or professional credibility in order to capitalise on a tendency to respond to requests from those in power.</td>
<td>An attacker pretends to be from the IT department or a senior manager in the organisation or indeed from another organisation in order to intimidate the employee. In January 2013 a former business relationship manager at a communications company tried to persuade his former colleagues to allow him access to company premises and IT systems. The ex-employee, who had left the company the previous year due to redundancy, told staff he was now working as a contractor for the company, and was awaiting his new pass and laptop. He also persuaded an employee to facilitate his access to the company IT systems using his own login. When confronted by a senior member of staff at the company, the ex-employee stated he wanted to maintain personal relationships with company staff as he had known all of them prior to leaving the company. The ex-employee was then escorted off the premises. The company then spoke to the individual’s current employer (a vendor of the company’s services) to remind them of their responsibilities. The ex-employee was dismissed by his new employer following an investigation.</td>
</tr>
<tr>
<td>Conformity</td>
<td>Stating that other colleagues have provided the information or allowed access, thus legitimising the request as other people have complied previously.</td>
<td>The social engineer claims he/she is conducting a survey and names a number of people in the organisation who have already taken part. The target feels that if these other people have answered the questions then it must be alright to do so.</td>
</tr>
<tr>
<td>Liking</td>
<td>Focusing on shared interests in order to establish a friendship, capitalising on the target’s tendency to be more likely to assist someone he/she likes.</td>
<td>Through conversation, the social engineer makes a personal connection with the target; this could be a seemingly shared hobby or interest, or perhaps a shared background.</td>
</tr>
<tr>
<td>Consistency</td>
<td>Highlighting that the target (or someone similar) has complied in the past, hoping that the individual will do so again in order to be consistent with his/her previous actions.</td>
<td>The social engineer contacts a new employee and highlights certain security policy issues and gets the target to agree with these. He/she then introduces the subject of passwords and states a certain convention for constructing a password and then asks the target to make a new password using this convention.</td>
</tr>
<tr>
<td>Scarcity</td>
<td>Stating that the object being offered is in short supply or available for a limited time.</td>
<td>The social engineer contacts the target and states that they are conducting a survey and the first 500 people to participate will be entered into a draw for a prize.</td>
</tr>
</tbody>
</table>
| **Pretexting** | Adopting a pretext or plausible reason for making the request, for either information or gaining entry. It gives the target a justifiable reason for complying. A good pretext:  
- Is well researched but simple;  
- Will stay as close to the social engineer’s own self as possible;  
- Appears spontaneous;  
- Uses props;  
- Provides a logical conclusion or follow through.  
The social engineer needs to find out as much as possible about the target organisation or individual before mounting an attack. | A social engineer poses as a delivery man, dressing in the correct uniform, driving in a car using the same livery as a legitimate company, being aware of standard delivery practices etc.  
In September 2013 a man posing as a BT engineer entered a bank in south London, where he may have attempted to install a device that would have allowed hackers to access its network from outside. |
| **Dumpster diving** | Gathering information from an organisation’s or employee’s waste which will help in mounting an attack. | A social engineer rumbles through paper waste from an organisation, which has not been properly destroyed, either by shredding or pulping. |
| **Phishing / Pharming** | The social engineer will masquerade as a trustworthy third party to acquire sensitive information, usually by email. Pharming will redirect internet users to bogus websites. | An email from the user’s bank asks them for access information to their account; such as passwords, account numbers. |
| **Trojan Horse / Gimmes** | Email attachments take advantage of the victim’s curiosity or greed to affect the introduction of malicious software (malware) to an organisation’s IT systems. The consequences might range from simply causing occasional annoyance to users, to allowing computers to be remotely controlled by a third party. | An email arrives, seemingly from a legitimate source, asking the victim to open up the attachment as it will be to their advantage. |
| **‘Road apple’** | A CD ROM or USB flash drive which contains malware and left in a location where it is sure to be found, such as a desk or in a lift. It will appear genuine and possibly bears the organisation logo. Once inserted into a CD ROM drive or USB port, it infects the computer. | A USB flash drive is left by the front door of an organisation, bearing the company logo and the words ‘not to be removed from building’. A conscientious member of staff will hand the USB into reception, who may then send it to the organisation’s IT department for further investigation. CPNI’s DVD *The Full Picture* highlights what can happen when such a USB device is introduced into an organisation’s system ([www.youtube.com/userUKCPNI](http://www.youtube.com/userUKCPNI)) |
| **Social networking websites** | A social networking website is a forum that allows people who share interests, friendships or activities to interact online. There is a tendency to share personal details, information about their employing organisation, as well as photographs of themselves and others. Research shows that even individuals who are aware of the risk of identity theft and concerned about privacy will engage enthusiastically with such sites, which have varying levels of security. | An employee will place a photograph of themselves and their colleagues on a social network site, identifying each in the picture and where they work. |
| **Organisation websites** | Some organisations in the interests of transparency and customer engagement, publish biographies and personal contact details and even office floor plans on their internet sites. Posting unnecessarily detailed information on the organisational website can be invaluable to a social engineer, greatly reducing the research effort required in advance of an attack. Further advice is available from CPNI’s Security Minded Communications guidance. | An organisation posts its Employee of the Month on its website, identifying the individual, what they are working on and personal particulars in some detail. This information can be used by the social engineer in preparation for an attack. |
| **External business events coverage** | Employees regularly attend external events such as conferences, seminars, exhibitions etc. These are fertile hunting grounds for social engineers. | At a basic level a social engineer may just collect business cards and information packs containing employee names, company logos, job titles etc. At the other end of the scale a more aggressive social engineer may actually attempt to elicit information out of unsuspecting targets. |
| **Hostile Reconnaissance** | Any penetration attack will require good information about the target; this can be obtained through close target reconnaissance. This can range from general ‘pattern of life’ information to provide an attacker with information on the normal routine at the site, through to specific information for targeting purposes. | A social engineer can work from static positions such as cafes, bus stops and other seemingly innocent positions, where they can view organisational activity. They can also pretend to be an actor or street vendor to gain information. Further information on HR can be found in CPNI’s guidance Understanding Hostile Reconnaissance. |
| **Mock surveys** | Social engineers take on the guise of a survey researcher; this provides an excellent pretext for gathering basic information on employees. | A social engineer knows an organisation has several sites across the UK. By conducting a survey with one site, establishing facts about the organisation or names of employees, a social engineer can use this detail, putting subsequent contacts at other sites at ease with their extensive knowledge. |
| Mistaken phone calls | A social engineer can call a random telephone number in an organisation and engage in a conversation as if the call was legitimate. | To learn the name and contact number of the organisation’s Accounts Manager, they may adopt the following approach:  
Social Engineer (SE): Hello Bill, this is Jon from Acme Supplies, I wanted to talk to you about our last invoice.  
Target: Sorry, I’m not Bill.  
SE: Oh, could I speak to Bill Williams, the accounts manager please?  
Target: Actually the accounts manager here is Joan Smith.  
SE: Of course it is, my memory is shocking. Would you mind giving me her number please.  
Target: Certainly, it is...... |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ruse interviews</td>
<td>In some extreme cases, the social engineer may exploit the desire of employees to sell themselves during a bogus or ruse interview.</td>
<td>A social engineer establishes a bogus social network profile, claiming to be a specific industry recruiter. He connects with a number of individuals who are from that particular industry. He can send them fake job vacancies and ask for interviews, where they will be happy to discuss their current work.</td>
</tr>
</tbody>
</table>
| Restaurant/bar coverage | A social engineer may simply regularly visit the known social haunts of employees and just sit and listen to the ‘shop talk’ of being discussed. | A social engineer can identify specific restaurants, bars, sandwich shops, coffee shops which are frequented by employees at key points of day, e.g. the morning coffee run, at lunch or on a Friday night.  
A more aggressive social engineer may even strike up a seemingly innocuous conversation and befriend an individual or colleague. |
Annex B: Further guidance

- **Holistic Management of Employee Risk (HoMER)**
  Guidance to managing the risk of employees’ counterproductive behaviour, whether inadvertent, negligent or malicious.

- **SeCuRE2**
  This can be used to shape the direction of security policies. It also provides a snapshot picture of how employees view security in the organisation. Results are presented in graphical format to make them easy to interpret, and suggested actions are provided about improvements that could be made.

- **Personnel security risk assessment**
  Focuses on individuals (be they permanent employees, contractors, agency staff etc), their access to an organisation’s assets, the risks they pose to the organisation and the sufficiency of any countermeasures implemented.

- **Ongoing personnel security**
  This guide brings together advice from Government departments and private organisations in a single document focusing on the key elements of an effective security culture.

- **Online social networking**
  This joint CESG/CPNI guide details the risks associated with the use of online social networks and gives advice on how they can be used safely.

- **Guard force motivation**
  This guide is intended to support those responsible for managing security personnel, in order to provide practical advice on workforce motivation, to improve security effectiveness and efficiency.

- **Security-minded communications**
  This guidance shows communication professionals how to audit their internet profile. It provides ideas about how to publish information in a customer-focused way that doesn’t give away too much detail.

- **Deterrence Security Toolkit**
  Materials designed to assist with Security Minded Communications.

- **Communicating personnel security messages**
  A range of animations and films designed to convey effective personnel security messages – all of which are available on the CPNI YouTube site.

- **Understanding hostile reconnaissance**
  This guidance aims to inform security managers about hostile reconnaissance, to explain the research that has gone into analysing past hostile reconnaissance incidents and to outline how appropriate advice and techniques can be applied.