FINAL DRAFT

SOCIAL ENGINEERING AND CRIME PREVENTION IN CYBERSPACE

THE FUTURE OF HIGH TECH CRIME -SOCIAL ENGINEERING: SEMANTIC AND SYNTACTIC ATTACKS

Abstract

This chapter highlights methods of syntactic and semantic social engineering attacks (human-based and computer-based) that are currently prevalent in the cyber community. It will also present the emerging trends in high-tech crime; and, the likely future direction cyber-crime will take with respect to social engineering.

What is Social Engineering?

In this context ‘social engineering’ is the term used to describe the use of psychological tricks, the manipulation of behaviour often through deception, by cyber-criminals on unsuspecting users to gain ‘access information’. Cyber-criminals can be those people that we already ‘label’ as hackers and conmen who use social engineering in their avoidance of complex technical means to access computers in order to commit crime.

The users become the primary target associated with the cyber-criminals’ secondary target, such as the organisation’s computer system; which in turn may lead to a tertiary or main target such as a system control program, database, financial or telecommunication system. Cyber-criminals will try to gain this ‘access information’ enabling them to bypass security. This can include usernames and passwords, PIN’s (personal identification numbers), tokens and credit card information (Federal Communications Commission 2002). Once they have gained access to the system they are then able to erase, modify or copy the information to suit the needs of their attack (Guenther 2001).

Social engineering manipulates any individual’s innate desires (e.g. friendship, romance, greed) by building a trust relationship with the target; and, then exploiting that relationship to obtain the information required.

Part of the process involved in social engineering includes ID theft. In the past, this provided a means for a hacker to reach their final goal in accessing a network or system; today, ID theft alone, is becoming a major concern (Federal Trade Commission, 2005; Smith, 2006).

As ICT (information communications technologies) continue to evolve, we see an increasing use of the internet for the conduct and development of e-commerce, particularly for secure financial transactions. Tied to this development, we also see a parallel with an increase in the sophistication of ICT security utilising encryption, specialist hardware, improved application software, tokens, firewalls and other such. The problem is that whilst computer users are becoming more technically competent and computer-security literate, there has not been a comparable 'learning' or development of 'awareness' in the security aspects associated with social engineering. This applies to both within the corporate and home environments.

Corporate identity fraud (Fite 2006); the theft of an individual's identity; and, Online Auction Crime (forthcoming publication of the Australian Institute of Criminology (AIC) 2007) can all be capitalised upon using social engineering.

This aspect may become an even greater issue for ICT security in the future, as the attributes of successive generations of the population are seen to hold different values. For example, the 'baby-boomers' are now heading towards retirement age and are quite different in attributes when compared with the current 'x' and 'y' generations of today.

'Baby-boomers' attributes are perceived as having a 'belief in the government'; 'not being very computer literate'; are 'loyal and conservative'; 'reliable' and, for the most part are 'intuitive about the consequences of their actions'. The 'x' generation are seen as being 'technically competent'; 'somewhat lacking in intuitive ability'; discontent; and 'they blame the previous generation for their current situation'. The 'y' generation are considered 'highly technically competent'; 'lacking good role-models'; are 'self-centred'; 'lack consideration for others'; and, 'are only concerned with the present'. This perceptive erosion of values, based on these social attributes, may impact on security in the future through an evolution of changes in the kinds of deceptions likely to succeed. (Chantler 2006)

Motivation for Hackers

There are a variety of motivations that exist in human behaviour for the deceptions involved social engineering:

- **Technical Avoidance.** Social engineering is perceived as a much easier path to financial gain rather than become involved in trying to breach a complex and cumbersome technical pathway.

- **Self-Education.** Whilst it seems to be much more infrequent, there are still those hackers who are motivated simply by the thrill of ‘gaining knowledge’; and ‘beating the system’.

- **Financial Gain.** Motivation for financial gain information gathering can be triggered by many reasons: feeding a habit (an addiction); seen as an easy way to get money; organised crime; blackmail; etc.

- **Revenge.** Disgruntled employees use weaknesses within the ICT frameworks to ‘get back’ at the corporate entity; or, they may even target an individual within the organisation.

- **External Pressure.** Blackmail, ransom, family pressure, organized crime, moral dilemmas and extremist beliefs (orders) can be used to apply pressure to an individual to commit a cybercrime. From a psychological aspect, the social engineer will manipulate the target person’s values so that they are led to believe that they are not hurting anyone, ‘after all you are only dealing with zeroes and ones’.

- **Terrorist, Political and Issue Motivated Groups.** These groups can be fanatical about their cause and will try and capitalise on weaknesses inherent in the financial and critical information infrastructure to cause shock to a target population.

- **The Wannabe ('Walter Mitty').** Often people who have psychological issues in believing that they are someone who they are not; people who want to be a 'James Bond' are only motivated to commit a criminal act, to do 'something daring', to become 'a spy' thereby satisfying their own distorted psychological needs.

The Stages in a Social Engineering Attack

There is a common pattern associated with a social engineering attack (Allan, Noakes-Fry and Mogull, 2005). Allen (2006, 5) states that 'any criminal act has a common pattern. Such a pattern is evident with social engineering, and it is both recognizable and preventable.' Allen (2005, 5) suggests that this pattern can be considered as a Cycle consisting of four stages, similar to the steps proposed by Cateledge (2005).

There are generally *four* steps in a social engineering attack (Cateledge 2005, 8-9):

1. **Information Gathering –** this involves gathering information about the person that the social engineer is targeting, or other information about the organisation or personnel that will convince the target individual to divulge the required information. A variety of techniques can be used to gather information about the targets; this information can then be used to build a relationship with either the target or someone of influence or important to the success of the attack. Typical information that may be gathered could be an internal phone directory; birth dates; organisational charts; personnel records, social activities, relationships etc.

2. **Development of Relationship** – developing a rapport with the target makes it easier to obtain the information in the next step. The social engineer will capitalise on the psychological aspect of trust. They may feely exploit the willingness of a target in order to develop an element of trust from them; often by presenting themselves as a more senior member of the organisation who will share a confidence with the target to further strengthen the element of trust.

3. **Exploitation of Relationship** – this refers to the manipulation of the target resulting in the social engineer obtaining the information e.g. username and password; or, perform an action which they may not normally do e.g. creating an account.

4. **Execution to Achieve the Objective –** having obtained the required information, the social engineer is able to use this to access the system; and the steps or stages are complete.

Whilst this example is a simplistic presentation of the stages, it must be remembered that each social engineering attack is unique; and, that it is highly likely that many phases or cycles may be involved that also incorporate traditional attack methods e.g. hacking, password cracking etc.

Psychological Triggers Behind Social Engineering

Gragg (2002) suggests that since social engineering is a social and psychological activity, it is reasonable to try and comprehend the psychology behind social engineering before considering the development of a defence system against it.

To be able to do this, it is necessary to recognise the psychological 'triggers' that are invoked during a social engineering attack. These 'triggers' are psychological principles that demonstrate a kind of power to influence, persuade or distract people in to behaving differently. Understanding these psychological triggers behind social engineering also helps to appreciate different aspects that may be used to combat the threat and enhance security. Gragg (2002, 6-9) makes particular mention of the following triggers.

Strong Affect - is a trigger that uses a heightened emotional state to enable a hacker to get away with more than what would be reasonable. If the victim is feeling a strong sense of surprise, anticipation or anger, then the victim will be less likely to think through the arguments that are being presented. *Strong affect* is introduced when the social engineer makes some statement at the outset of the interaction that triggers strong emotions. The *strong affect* includes, but is not limited to fear, excitement or panic. This could be the promise of a substantial prize worth hundreds or thousands of dollars, or the panic of having an employee's job dependent on one decision. This surge of strong emotions works as a powerful distraction and interferes with the victim's ability to evaluate, think logically or develop a counter-factual argument based on tangible facts (Rusch 1999, 4). Counterfactual thinking is a phenomena that is related directly to *strong affect*. Landman (2000, 299) explains how counterfactual thinking relies on the possibilities of anticipation and thrill that will short-circuit a person's reasonable thinking process. A typical example is to have been selected as ‘one of a few to win a fabulous prize’. The person ignores the fact that the likelihood of winning is actually very remote, but gets distracted by their own thoughts, often leading themselves to risk giving away information or access details for the possibility of a prize. It is as if the person is ‘under a spell’; or, placed into a different sense of reality which has been brought on by the sudden surprise and excitement, with a rush of other emotions.

Overloading - is a condition that is achieved by presenting mistaken premises that are unchallenged when they are heard rapidly; this is because they are presented interlaced with convincing truisms. This is a psychological trigger of *overloading*. Having to deal with a lot of information quickly affects logical functioning and can produce a ‘sensory overload.’ So that with too much information to process, people become ‘mentally passive – they absorb information rather than evaluate it’ (Burtner 1991, 2). Arguing from an unexpected perspective can also trigger overloading. The target needs time to process the new perspective but that time is not available. This leaves the target with too much information and not enough time to think it through, reducing the target’s ability to process or scrutinize the argument. The target is then more willing to accept arguments that should have been challenged (Petty, Fleming, Priester and Feinstein 2001, 2).

Reciprocation - is a psychological trigger that is often used. It is based on the premise that in social interactions if someone gives us something or promises us something, we should return the favour. This is often the case even when the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. This truth is known as reciprocation (Rusch 1999, 6).

The hacker, Kevin Mitnick, suggests that “In the corporate environment, people are unlikely to evaluate a request thoroughly, so they take a mental shortcut”. The reasoning that follows is that if someone calls and is helping with a problem, then that person is ‘one of us’ and is no threat (Farber 2002, 1). It is this ‘reverse’ social engineering that makes use of the reciprocation trigger. The hacker presents as a helper who is ready, willing and able to fix the target’s problems. Even before the problem is resolved, the target feels indebted to the hacker. This is an ideal situation for the hacker (Nelson 2001, 3).

Another way that reciprocation can be used in social engineering is demonstrated by behavioural experiments. These experiments show that when two people are in disagreement, if one will yield on some point – no matter how small – the other will feel compelled to yield as well. For a hacker this is fairly easy. They only need to make more than one request, yield in understanding on one, and then the target will feel pressure to yield on the other (Cialdini, Green and Rusch 1992, 38). Reciprocation is often seen in the corporate culture. It is an unwritten ‘bartering system’ that is considered invaluable if one wants to be successful. One employee will help out another with the expectation that, eventually, the favour will be returned.

Deceptive Relationships – are built in order to exploit the other person. One way to do this is sharing information, a belief, or a perception and discussing it as a common enemy. Mitnick (Farber 2002, 1) describes when he was conning an employee who had already become suspicious of him in a different context. This time Mitnick was establishing a relationship with the employee through email as an alias, by sharing information and technology without asking for anything in return. He also helped strengthen the relationship by talking negatively about “Kevin Mitnick” whom the employee did not realize was authoring the emails. After the relationship was established, Kevin was able to obtain all kinds of information about the target’s system. Another way one can build a quick relationship is by appearing to the target as if they are very much alike. The idea is for the victim to feel like he and the caller think alike, have the same interests or want the same things out of life. Believing that someone has characteristics identical or similar to our own provides a strong incentive to deal with that person favorably even trusting that person without legitimate motivation (Rusch 1999, 6).

Diffusion of Responsibility - Diffusion of responsibility is when the target is made to feel that they will not be held solely responsible for his or her actions. Ironically, this trigger can work very well with the use of *moral duty* as a motivation for the persuasion. Moral duty is actioned when the target feels like they are doing something to save a co-worker, to help the organisation, or, at least, to avoid feeling guilt (Nelson 2001, 4). The target is made to feel that they are making major decisions that will be the major impact between the success and failure of the company, or of the “employee” who is calling, implying that the caller may lose their job based on their decision. This can often be a very difficult decision for people to make and the target will comply more easily if they believe that they will not be held responsible for what happens.

Authority - the majority of people are conditioned to respond to authority. Rusch (1999, 6) suggests that people will do a great deal for someone they think is in authority. Consider the impact that a bogus director CEO may have on an employee who has not been prepared. This trigger is made even more powerful by the reality that it is considered a challenge to even verify the legitimacy of the authority. This lack of perspective leaves this trigger wide open for exploitation by anyone willing to misrepresent him or herself as an authoritarian figure.

Integrity and Consistency - People tend to follow-through commitments in the workplace, even though those commitments may appear to be unsound in the first place. For some it is a matter of integrity to "do what you say you are going to do", even if you are suspicious that the request may not have been 'quite legitimate'. Often this inclination is so strong that staff will even carry out their commitments so long as they can justify it to them selves in some way so that they believe the requests were made by their fellow employees. Another feature of the Integrity and Consistency trigger is that people tend to believe that others express their true feelings when they make a statement. Unless there is strong evidence to the opposite, people will believe that the person with whom they are talking is telling the truth about what they feel or need. The tendency to believe others is based primarily on their own honesty in expressing feelings (Rusch 1999, 7).

Common Traits

Whatever the motivation or technique used, there are certain common traits that usually entice the target to comply with the request(s). Allen (2006, 8) suggests that these traits include:

- The movement of responsibility away from the target, so that the target is not considered solely responsible for his/her actions.

- The perception by the target that, by conforming with the request, the target will get on the 'right side' of somebody who could award them future benefits, more commonly known as 'getting in with the boss'.

- The target's instinct to act morally in helping someone out, thus avoiding the feeling of guilt.

- Communication on a personal level, resulting in the target voluntarily complying with the request without realizing the pressure being applied.

• The target believes he/she is making a reasoned decision in exchange for a small loss of time and energy.

The likelihood of the target's compliance is further increased if:

• The aggressor is able to avoid conflict by using a consultative approach rather than an aggressive one.

• The aggressor is able to develop and build a relationship through previous dealings. The target will probably comply with a large request having previously complied with smaller one.

• The aggressor is able to appeal to the target's senses, such as sight and sound. By appealing to such senses, the aggressor will be able build a better relationship with the target by appearing 'human' rather than just a voice or email message.

• The aggressor has a quick mind and is able to compromise.

Methods of Social Engineering

Social engineering is categorised into two types: *Syntactic* and *Semantic*.

SYNTACTIC

Syntactic social engineering has often been referred to as the ‘second wave’ of network attacks. It relates to the network’s operating logic and vulnerabilities such as loop-holes in software, denial-of-service and difficulties with cryptographic algorithms (Schneier 2000, 1).

A syntactic social engineering attack is possible due to intrinsic security failings (Barrett 1997, 43). Two popular forms of syntactic attacks include the use of *malware* and *smurfing*.

Malware – refers to the group of malicious software code which is responsible for the distribution of viruses (malicious code that is downloaded onto a computer system through the use of attachments or programs, when activated by another user), worms (malicious code that once infected on a computer requires no human assistance to replicate and transmit itself to other systems) and trojan horses (responsible for creating backdoors in the infected computer system which can later be used by the hacker to access personal information).

Smurfing – a Denial of Service attack which uses ‘pings’ to test an internet host’s response. This can result in a flooding of the network therefore denying access to legitimate activity (AIC 2005a).

SEMANTIC

Semantic social engineering (or HUMINT, Human Intelligence) is considered to be the third and coming-wave of network attacks. It is used to target the security flaws in the people operating the computer rather than the machine itself and can be done using human-based or computer-based methods (Schneier 2001). As such, semantic social engineering attacks are possible due to extrinsic security failures - security measures that have been implemented ineffectively (Barrett 1997, 43).

Approaches

Direct approach. A targeted individual may be asked to complete the task on behalf of the social engineer, such as making a phone call someone inside the organization asking for their password and username.

1. **Important User** by pretending to be a senior manager with an important deadline. The social engineer could pressure the help desk operates into disclosing useful information such as: telephone numbers to remote access server, type of remote access software that's used and how to configure it and what is needed to log in to the server.

2. **Helpless User.** Social engineer pretends to be somebody who is helpless, who will capitalize on somebody's helpfulness such as secretary that takes pity on them.

3. **Technical Support Personnel** by pretending to be technical support team member social engineer could extract useful information from an unsuspecting user. Perhaps by pretending to be system engineer needing the users password to be able to ‘fix something’.

4. **Reverse Social Engineer** this technique is when the legitimate user is enticed to ask the social engineer questions to obtain information. This reverse engineering attack involves *three* parts:

sabotage of the gain access social engineer corrupts the workstation will makes it appear that been corrupted. The use of the system discovers problem tries to seek help.

marketing in order to make sure the user calls the social engineer. The social engineer must advertise, he a can do this by leaving his business cards around target's office or by placing his content number on the error message itself.

support finally, social engineer would assist with the problem, making sure that the user remains completely unaware and unsuspicious whilst he obtains the required information. (Allen 2006)

Methods

The following is a list of some of the more common methods of human-based and computer based semantic social engineering methods:

Phone – a social engineer/hacker calls up the target and presents themselves as a person of authority and uses techniques to extract the required information (Granger 2001a)

Eavesdropping – a social engineer may place themselves at a known ‘haunt’ for employees of a particular company, to be able to overhear ‘work chat’ over lunch.

Live – individuals gain access to the building of the targeted computer system in order to obtain information that may later be used to access the system. Dumpster Diving and Shoulder Surfing often form a part of this technique (Guenther 2001).

Dumpster Diving – this refers to individuals sorting through a company’s trash in an attempt to retrieve helpful documents i.e. employee records, organisational charts that may assist a social engineering attack (Granger 2001a). Dumpster diving may also provide old computer equipment for ‘forensic analysis’ such as old hard drives, CDs, memory sticks etc.

Shoulder Surfing – literally looking over one’s shoulder to see what password an employee is typing into the computer

Bogus Surveys – surveys that are left in the mail (usually advertising a cash prize) asking subtle questions that cause the individual to unknowingly divulge personal information that may later be used by the hacker (FCC 2002)

Pop-up Windows – false windows notifying the individual that their internet connection has dropped out and are required to re-enter their user details (username and password). This information is then redirected to the hacker (Guenther 2001)

Spyware – used to record credit card information, usernames, passwords and other forms of personal information (usually through the use of a keylogger)

Phishing – hackers distribute emails presenting themselves to be from a legitimate organisation (e.g Bank). A URL is supplied (directing them to a spoof website) and the target is informed that they are required to confirm their personal information (such as username and password). This can later be used to illegally access that person's account (AIC 2005b)

Vishing – the phone version of phishing

Pharming – similar to phishing in the sense that while the user believes they are entering their personal details (username, password) into a legitimate site, they are actually using a spoofed or mimicked site which emails the user's details to the hacker for future use. Pharming however interferes with the conversion from URL to IP address by poisoning the DNS server. Therefore when an individual types in the URL of a site they are redirected to a spoof site. (De La Cuarda 2005)

Defence against Social Engineering

Most people do not realize just how much information they reveal about themselves, or the organisations that they work for, in the course of their daily discussions. Security awareness programs should include the consequences of 'loose talk'. Gragg (2002, 10) proposes a multi-layered defence against social engineering based on a conventional approach to determine what the vulnerabilities and threats are and then defend against those risks. He suggests that 'the defence must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which he or she would be stopped.'

Regardless whether these are considered as layers or levels, the basic principle of defence in depth (or layers) is that the closer you get to the target, the harder it should become.

Security Policy to Address Social Engineering

The foundation of information security is its policy. The security policy sets the standards and levels of security that can be applied to any network, system or environment. As social engineering targets people who need to know how to respond to requests. Any established policy must support end-users to feel as if they have no choice but to resist the hacker's requests. They should not be in a position where they have to question whether or not certain information can be given out. It should be well-defined beforehand by those who construct the security policy for the organisation. A security policy should address the conventional components in ICT: information access controls; setting-up accounts; access approvals; and, password changes. It should also deal with classification of documents and other media, locks, ID's, shredding policy, and the escorting of visitors; and, above all, it must be enforced (Granger 2001b, 2) A Security Policy that addresses social engineering helps staff defend against those psychological triggers presented above. Policies also have a 'balancing effect' on the authority that a person may assume when they call on the phone. A policy defines the responsibility for information or access that is given out, so that there is no question as to the employee's own risk when giving away privileged information or access.

Security Awareness Training for all users

A good social engineer will first try to set up a trusted relationship. All staff must know what kind of information a social engineer can use and the kinds of conversations that could be suspicious. They should know what confidential information is and recognise their responsibility to protect it. They also need to know that when they refuse requests they have the backing of management; this is especially important on the occasion where refusals may offend. Staff should be aware of the basic indicators present in a social engineering attack. Some of these include a refusal by the caller to give contact information, rushing, name-dropping, intimidation, misspellings, odd questions, and requesting confidential information. Employees must be willing to question the inquirer and withhold information when their challenges are met with inappropriate responses (Granger 2001b, 3). Security awareness training should follow the security policies, but there are some key points that all users should be aware of in social engineering:

1. **Determine Value –** Most people undervalue their data and access before being hacked or having hardware fail. They need to consider what they would do if they suddenly had no access to their computer.

2. **Friends and Enemies –** Friends that are made through familiarity over the phone or who, for any reason, are asking questions concerning privileged information may be enemies and not friends at all. Social engineers make friends with their victims long before they request anything. All users should be aware that just because someone seems to be a friend does not mean that they can be trusted with privileged data or access.

3. **Passwords –** Some hackers will never ask for a password. However, others will come up with very convincing reasons using social engineering as to why an employee should give their password to a complete stranger. People without security awareness often give their password away without much thought, especially when conned into providing information for a 'survey', entering into a site where they provide their password to be entered into the draw for a luxury cruise, or some other seemingly valid reason. Users will often use the same password on different systems, so a hacker that may also have obtained the victim's domain access may also gain information through Instant Messenger and chat rooms.

4. **Uniforms and Badges –** It is easy to make fake badges and get uniforms to pretend that an intruder has a legitimate reason to be on site.

5. **Key Personnel Resistance -** Key personnel include IT help desk personnel, customer service, business assistants, secretaries and receptionists and system administrators and engineers. Good resistance training will help prevent employees from being persuaded to give information away that the hacker might need. Several resistance-training techniques can be used from the field of social psychology to help adequately prepare employees to resist the persuasion techniques of a social engineer.

Innoculation – employees are given weakened arguments that will be used by the social engineer. It works on the same principle as preventing the spread of a disease by giving an innoculation. Employees would be exposed to the arguments that a social engineer might use along with strong refutation argument that could be used by the employee. Studies indicate that this is an effective and long-lasting resistance technique. The concern is that the trainer must be able to anticipate the all the arguments of the social engineer (Sagarin; Cialdini; Rice; Serna; 2002, 527).

Forewarning – relates to the content of an incoming message and the persuasive intent of an incoming message. Forewarning of the content causes greater resistance to a social engineering attack than the forewarning of persuasive intent. The practical aspect of this training is to warn that not only will the social engineer attempt to persuade the target, but more importantly, that the arguments they use will be manipulative, deceptive, and insincere. Staff must be told that the hacker's intent is criminal and that they are intent on stealing from them. This 'black and white' definition of terminology is necessary if forewarning is to be effective (Sagarin et al; 2002, 527).

Reality check – It is important to let staff realize that they are vulnerable. Often people tend to be unrealistic about their own vulnerability believing that nobody could ever fool them. This perception leads many of them to ignore legitimate risks and fail to take measures to address those risks. However, once they have this aspect demonstrated to them, that they are vulnerable, the training outcome is much more effective (Sagarin et al; 2002, 536).

There are *three* stages of perceived susceptibility to risk:

1. Awareness – knowing a risk exists;
2. General Vulnerability – a belief in the likelihood of the risk for others; and
3. Personal Vulnerability – acknowledgement of one's own personal susceptibility.

Security awareness and resistance training has limited value if it is limited to only *awareness* (Sagarin et al; 2002, 540).

Memory Jogging – one exposure to security awareness training in social engineering will only be effective for a short period. Regular memory joggers or reminders are necessary to keep people aware of the dangers that may be approaching. This can be done through the use of regular reports of incidents and even no incidents; perhaps as an adjunct to a weekly business report, or a regular dedicated security newsletter.

Social Engineering Traps - are set up in the system to actually expose and stop an attack. A trap will alert the potential victim and security that an attack is in progress. Gragg (2005) presents several suggestions for trapping the social engineer.

The Justified Know-it-all – A bold social engineer will not hesitate to walk right into an organisation and start exploring. It is imperative that all personnel be briefed on the security risks of the physical presence of a social engineer; and, they should have the power to do something quickly to deal with this un-escorted visitor. This trap is useful even if badges are used, as hackers will often make a fake badge and not expect to be confronted. In large organisations a nominated staff member can be assigned to act as a the 'designated sheep dog' to 'round-up' intruders found wandering on their floor.

Centralized Security Logs – must be monitored by information security personnel to prevent an effective attack. These are not just the access logs onto a network or system; they also include Help Desk and Customer Service requests. In fact, there should be a communications channel where a record is kept each time staffs are asked to provide sensitive information; or if they are suspicious. For the central log to be an effective the log must be examined on a regular basis.

Phone-Back Policy – a simple procedure that seems to be often forgotten, makes an effective trap to block the approach from a social engineer in having a password reset. Calling back must be supported by a persons ID with secondary and even tertiary confirmation information, only known by the company and the true identity. Again an entry in the security log should also be generated. (Farber; 2001, 1)

Three other enhancements can be used to enhance the phone-back policy, or used in 'stand-alone' mode:

The Three Questions - provides a list of questions and answers that the Help Desk personnel can use to verify identity. These questions would have been arranged earlier with the employee. The questions should be obvious for the employee but not for others.

Bogus Questions - are questions that imply false information and give the caller a chance to correct or build upon the false information. An example of this type of question would be to ask 'How is your new car?' If the caller says, 'I don't have a new car' then the caller has passed a single test. At this point the employee would apologize and explain that they must be mistaken. However, if the caller starts talking about the new car, or lets the target talk about the new car, then the hacker has been hooked. The person receiving the call target should immediately notify security.

Call Hold – any suspicious call or any call asking for a password reset or privileged information should be put on hold. People are more easily persuaded to do something questionable when there is pressure, surprise, or overloading. The key is to take a minute and process the information that is being given, to determine if it is legitimate, needs further verification or should be denied.

Incident Response - is critical so that the security network is not just waiting for the social engineer to find someone in the organisation that does not know or care about security. A well-defined process must exist so that any employee can immediately report an incident as soon as they suspect something is wrong. This process should actively follow the hacker and proactively inform other potential victims.

Current Trends

There has been a reported massive increase in the use of bot-nets (zombies) within the last year. Symantec reported that on average in excess of 10,000 bots were discovered every day in the first six months of 2005. This figure is double the number identified during the same period in 2004. The use of phishing as a form of social engineering (1.04 billion detected incidences) has also been reported to have nearly doubled from the first half of 2004 to the first half of 2005 (Computer Crime Research Centre (CCRC) 2006a, 5). However between the periods of 2005-2006 the number of reported phishing incidences has remained relatively the same. This may be due to computer user's increased awareness of cyber crime and also the development of the new technique called pharming (De La Cuarda 2005).

Vishing (the phone version of phishing) may also replace some phishing activity. Vishing is used to extract essential credit card information (e.g. account number, expiry date, security code) by informing the target that there has been fraudulent activity on their credit account and instructing them to call a "help line" where they are further instructed to enter their details for confirmation (CCRC 2006b, 1).

These figures seem to support the view that there has been a shift from nuisance hacker assaults, to profit-motivated attacks. Attacks are becoming smaller with a more focused objective. Keyloggers (programs designed to capture a computer user's keystrokes) are also becoming a more prevalent form of spyware with 93% of companies involved in an IT security survey claiming that they had been infected (CCRC 2006c, 4).

Future Trends

The use of bots is expected to increase in the near future. The community of Bot computers are expected to become involved in "more sophisticated, targeted attacks" (CCRC 2006c, 1). This reflects a general trend toward more focused attacks in all areas of hacker assaults. While syntactic attacks such as worms and viruses were previously spread to cause disruption and inconvenience, the use semantic social engineering methods such as bots and pharming are used to steal personal information that may be used to access bank accounts. Therefore organised crime is expected to utilise this form of criminal activity and take a more active role in future high tech crime. Furthermore, there is expected to be a target shift from desktop computers to smart devices i.e. cellular phones, Blackberry's and other such internet-linked organisers, due to user's inclination to store confidential information such as bank pins on such devices. These are expected to become the next prime target for largely semantic attacks.

The introduction of commercial appliances being linked to the internet (e.g. vending machines, gas pumps, ATM's) and the increased usage of mobiles to pay for such products suggests that this will be the target area of virus's in the future. Other non-PC devices will also be targeted. This includes routers, switches and backup devices. Furthermore, real-time programs such as IM (Instant Messaging) are likely to be increasingly targeted in the near future with a 1,700% year over year increase (CCRC 2006c, 3). There appears to be a trend towards a greater emphasis on the development of semantic/human intelligence methods rather than the previously used syntactic measures. This is due to semantic methods placing value on particular information (i.e credit card information) rather than the use of syntactic methods to release viruses and denial-of-service attacks. Human based social engineering is able to obtain information in many cases that technological methods are unable to. This further illustrates the changing trend towards profit-motivated attacks.

REFERENCES

Allan A., Noakes-Fry K. and Mogull R. (2005) 'Management Update: How Businesses Can Defend against Social Engineering Attacks'; March 16, 2005; Gartner.

Allen M. (2006) 'Social Engineering – A Means to Violate a Computer System'; June 2006; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Australian Institute of Criminology (AIC) (2007) (Publication Forthcoming) 'Online Auction Crime'. AIC High Tech Crime Brief, AHTCC; Canberra.

Australian Institute of Criminology (AIC) (2005a) 'Concepts & Terms' - High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb001.html) accessed 20 Dec 2006

Australian Institute of Criminology (AIC) (2005b) 'Phishing' - High Tech Crime Brief (http://www.aic.gov.au/publications/htcb/htcb009.html) accessed 20 Dec 2006

Barrett N. (1997) *Digital Crime: Policing the Cybernation*. Dover, NH, London: Kogan Page, UK.

Burtner W. K. (1991) "Hidden Pressures." Notre Dame Magazine, Winter 1991- 92 p29-32.

Cateledge B. (2005) 'Social Engineering Overview'; University of South Carolina, Colombia, USA. (http://www.chem.sc.edu/support/publicSocialEngineering.pdf) accessed 20 Dec 2006

Chantler A.N. (2006) 'Intelligence Futures: Brace Yourself, Be Prepared to Accept the Unacceptable'; Presentation at the Annual Conference of AIPIO (Australian Institute of Professional Intelligence Officers) October 2006; Brisbane, Australia.

Cialdini R. B., Green B. L. and Rusch, A. J. (1992) "When Tactical Pronouncements of Change Become Real Change: The Case of Reciprocal Persuasion" Journal of Personality and Social Psychology: Vol. 62(1), 1992, 30-40.

Computer Crime Research Centre (CCRC) (2006a) ‘Hackers Replaced by Phish Con Artists’; Date: January 03, 2006 (http://www.crime-research.org/analytics/pure-hackers-replaced-by-phish-con-artists/) – accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006b) ‘Telephone Version of Phishing’; Date: July 13, 2006 (http://www.crime-research.org/news/13.07.2006/2116/) accessed 20 Dec 2006

Computer Crime Research Centre (CCRC) (2006c) ‘Hackers Shift Targets in 2006’; Date: March 06, 2006 **(http://www.crime-research.org/analytics/1862/**) accessed 20 Dec 2006

De La Cuarda, F. (2005) ‘Pharming – a new technique for Internet fraud’ Computer Crime Research Centre. (www.crime-research.org/news/07.03.2005/1015) accessed 1 Dec 2006

Farber, D. (2002) “Mitnick on Mitnick: ‘Why I’m going legit’ (Part Two) Interview with Dan Farber.” ZDNet. October 8, 2002. http://www.silicon.com/public/door?6004REQEVENT=&REQINT=55863&REQSTRI1

Federal Communications Commission (2002) ‘Computer Security Notice: Social Engineering’; Computer Security Week; Federal Communications Commission, USA. (http://csrc.nist.gov/fasp/FASPDocs/security-ate/December-2002-2.pdf) accessed 18 Dec 2006

Federal Trade Commission (2005) ‘Take Charge: Fighting back against Identity Theft’; Federal Trade Commission, Washington D.C. USA. (http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf) accessed 20 Dec 2006

Fite B.K. (2006) ‘Corporate Identity Theft’; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Gragg D. (2002) ‘A multi-Level Defense Against Social Engineering’; SANS Institute, San Diego, California, USA. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006

Granger S. (2002a) “Social Engineering Fundamental, Part I: Hacker Tactics.” Security Focus Online. (http://online.securityfocus.com/infocus/1527) accessed 20 Dec 2006

Granger S. (2002b) “Social Engineering Fundamental, Part II: Combat Strategies.” Security Focus Online. (http://online.securityfocus.com/infocus/1533) accessed 20 Dec 2006

Guenther M. (2001) ‘Social Engineering – Security Awareness Series’; Information Warfare Site U.K. (http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf) accessed 20 Dec 2006

Landman, J. and Petty, R. (2000) “It Could Have Been You: How States Exploit Counterfactual Thought to Market Lotteries,” Psychology & Marketing Special Issue: Counterfactual thinking. Vol. 17(4), April 2000, 299-321

Nelson, R. (2001) “Methods of Hacking: Social Engineering.” Institute for Systems research, University of Maryland, http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html) accessed 30 Feb 2006

Petty R. E., Fleming M A., Priester J. R. and Feinstein A. H. (2001) “Individual versus group interest violation: Surprise as a determinant of argument scrutiny and persuasion.” Social Cognition: Vol. 19(4), Aug 2001, 418- 442.

Rusch J. (1999) ‘The Social Engineering of Internet Fraud’; United States Justice Department – Proceedings of the 1999 Internet Society Conference, USA. (http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm) accessed 20 Dec 2006

Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B. (2002) “Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion.” The Journal of Personality & Social Psychology: Vol. 83(3), Sept 2002, 526-541.

Schneier B. (2000) ‘Semantic Attacks: The Third Wave of Network Attacks’ (http://www.schneier.com/crypto-gram-0010.html#1) accessed 20 Dec 2006.

Smith R.G. (2006) ‘Preventing Identity-related Crime: 100 points, biometrics or identity cards’; AIC Trends & Issues No 324, August 2006; Canberra.