Re-Floating the Titanic: Dealing with Social Engineering Attacks

David Harley
Imperial Cancer Research Fund, London

About the Author

David Harley is a Security Analyst at the Imperial Cancer Research Fund, where his career path has led through administration, network/PC/Mac support, and VMS and Unix support and development. He holds a degree from the Open University embracing technology, social sciences, and computing science. His research interests currently include virus management, network security, and education and policy issues, and has authored a number of papers and presentations in these areas. He has compiled, contributed to and/or co-maintains a number of security FAQs; is a contributing editor for the SANS Network Security Digest; and is threatening to finish co-writing a book on anti-virus measures and resources any year now.

Mailing Address: Administrative IT Unit, Imperial Cancer Research Fund, Lincoln's Inn Fields, London WC2A 3PX, United Kingdom; Phone: (44) 171-269-3114; Fax: (44) 171-269-3124; WWW URL: http://webworlds.co.uk/dharley/; E-mail: D.Harley@icrf.icnet.uk

Descriptors

human engineering, security policy, e-mail, masquerading, hoax, helpdesk management, net-abuse, spam, ethics, resource management

Re-Floating the Titanic: Dealing with Social Engineering Attacks

Abstract

"Social Engineering" as a concept has moved from the social sciences and into the armouries of cyber-vandals, who have pretty much set the agenda and, arguably, the definitions. Most of the available literature focuses on social engineering in the limited context of password stealing by psychological subversion. This paper re-examines some common assumptions about what constitutes social engineering, widening the definition of the problem to include other forms of applied psychological manipulation, so as to work towards a holistic solution to a problem that is not generally explicitly recognised as a problem. Classic social engineering techniques and countermeasures are considered, but where previous literature offers piecemeal solutions to a limited range of problems, this paper attempts to extrapolate general principles from particular examples.

It does this by attempting a comprehensive definition of what constitutes social engineering as a security threat, including taxonomies of social engineering techniques and user vulnerabilities. Having formalized the problem, it then moves on to consider how to work towards an effective solution. making use of realistic, pragmatic policies, and examines ways of implementing them effectively through education and management buy-in.

The inclusion of spam, hoaxes (especially hoax virus alerts) and distribution of some real viruses and Trojan Horses in the context of social engineering is somewhat innovative, and derives from the recognition among some security practitioners of an increase in the range of threats based on psychological manipulation. What's important here is that educational solutions to these problems not only have a bearing on solutions to other social engineering issues, but also equip computer users to make better and more appropriate use of their systems in terms of general security and safety.

Introduction

Social engineering attracts such a range of definitions, covering such a range of activities (from password stealing, to scavenging through waste for useful information, to malicious misinformation) as to be confusing at best. The question is, do accepted definitions of social engineering meet the needs of those tasked with meeting this class of threat? The term originally derives from the social sciences, but even there seems to have several shades of meaning. While it isn't my intention here to generate the definitive academic definition of social engineering as applied to IT security, I hope, nevertheless, to extract some of the elements of the various definitions below in the hope of moving towards a holistic solution to a wide-ranging practical problem. While current literature (especially the populist "Idiot's Guide" genre) tends to focus on password stealing by psychological manipulation, in so far as social engineering is examined at all (many standard works don't deal with it directly at all), cyber-vandals past and present have, in some cases, been more flexible and innovative. While most managers and general users (and not a few security practitioners) are still at the "Social engineering? What's that?" stage, the bad guys are cheerfully making use of psychological manipulation to subvert systems, and the poachers turned gamekeeper are giving considerable attention to this type of threat in conferences, training courses, and articles. They are not restricting themselves to the password stealing issue, and neither should we. What is advocated here is not uncritical acceptance of bad guys past and present as the ultimate authority on what social engineering is and what we should do about it; rather that we should recognise that there is a problem that needs to be addressed, using any useful resource available.

To this end, this paper examines several very different definitions of social engineering and offers a synthesised working definition. This definition is intentionally broad, so as to enable us to work towards controlling (not curing) the disease (psychological subversion) rather than a symptom (password stealing by psychological manipulation).
In order to advance our understanding of what the problem is, it’s necessary to examine some classic social engineering techniques and countermeasures. While some of this material has been covered by other commentators, this paper takes a somewhat innovative taxonomic approach, and includes threats which are not often considered at all in the literature, let alone considered as social engineering . This is done with the intention of avoiding the common trap of offering piecemeal solutions to a restricted set of problems. Instead, general principles are extracted from specific issues and examples. To do this, we must consider not only specific attacks and countermeasures, but the mindsets which (1) make users vulnerable to this kind of attack, and (2) make management resistant to addressing these issues. Formalizing the problem makes it easier to move on to working towards effective solutions, making use of realistic, pragmatic policies. Effective implementation of such policies, however good they are in themselves, is not possible without a considered user education programme and co-operation from management, and considerable attention is paid to the need to apply constructive ‘social engineering’ to both these groups.

The inclusion of spam, hoaxes (especially hoax virus alerts) and distribution of some real viruses and Trojan Horses in the context of social engineering is somewhat innovative and may be controversial. However, this approach derives from the increasing recognition among some security practitioners of a growth in the range and frequency of threats based on psychological manipulation. Whether such threats qualify as social engineering is an interesting topic for debat, but not the main issue. What is important here is that educational solutions to these problems not only have a bearing on solutions to issues which are certainly social engineering issues, but also equip computer users to make better and more appropriate use of their systems in terms of general security and safety.

Literature Review

The Social Sciences View

The Tokyo Institute of Technology devotes considerable resources to social engineering as an area of academic study. Hidano (Hidano, 1996) defines its purpose as to construct a theory which resolves social problems by “social recognition and measurement method, integrated theory of Psychology, Sociology and Economics, spatial and social design theory, and people’s participation and decision forum.” Jacobs uses the definition “the discipline and quantitative constraints of engineering....applied to social legislation”(Jacobs,1996), which describes rather well the basis of legislation such as laws which criminalize racial discrimination, for instance. These definitions may seem to have little to do with social engineering as security professionals usually seem to understand it: however, I intend to reclaim at least part of Jacobs' definition for security. We can't always pass laws to make people security conscious (or at least behave as if they were!), but we can attempt the same end through policy and education.

Jacobs' paper also clearly points out that legislation has proved in practice a poor environment for the application of 'real' engineering principles. "The one engineering principle most often violated is the obligation to recognize and acknowledge that the proposed process does not work, and to learn from that experience." This theme is echoed in a paper by Parish on the application of social engineering to the market place. "The problem of evaluating programmes is compounded by the tendency of governments and their agencies to attack any problem on a broad front using several policies so it is difficult to disentangle the effects of any one of them from those of the others"(Parish). In computer security, there is little enough recognition that the social engineering problem exists, far less a plethora of conflicting attempts at a solution. Nonetheless, I believe that while developing a taxonomy of threats and countermeasures, we can also learn from past mistakes in the wide world of social legislation, and attempt to deal with related problems in a holistic manner, rather than chipping away piecemeal at one problem at a time. In this way, we may hope to attenuate the effects of Rossi's brass law of evaluation: "the more social programmes that are designed to change individuals, the more likely net impact of the programme will be zero." (Rossi, 1987).

These definitions provide useful insights into ways in which we can counter psychological subversion with constructive 'social engineering', but definitions used by practising or reformed crackers place the emphasis quite differently.

Social Engineers Define Social Engineering

In general, social engineering gets more attention from crackers, poachers turned gamekeeper, and inhabitants of the twilight zone where good guys and bad guys mingle than it does from 'legitimate' security professionals. Unsurprisingly, given that these groups tend to immerse themselves into cyberculture with more commitment than many employees and managers, much of the relevant material supplied by these groups is available on the Internet itself. It's also almost traditional for cybervandals who 'age out' to move into security in some sense, and those who may not appear to have matured sufficiently to represent a good catch for a legitimate consultancy are obviously aware of this. "One of the two hackers accused of almost starting World War III from his bedroom....announced he is now considering a career in IT security....'If I can find a job where I can get paid for doing the same sort of thing as hacking, I won't complain,' he said." (Computing, 1997)

It is typical of individuals who are further into the hacking/cracking 'scene' to use a vaguer definition of social engineering than most security books use. Indeed, the Hack FAQ (or HAQ) virtually ignores all the areas I hope to cover here to concentrate on somewhat tenuously linked issues such as squirting salt water into soda machines in the hope of being showered with change and soda (HAQ, 1994). A 'darkside' site which offers a Social Engineering FAQ and some suggestions for related attacks

(BeRnZ, 1997) suggests a mindset which has much in common not only with other documentation by practising crackers, but also with many of the available texts by virus writers: an exaggerated reverence for the abilities of the uebercracker, Social Engineer, or virus coder); a similarly extreme contempt for adults working on the other side of the blackhat/whitehat divide; a tendency to present personal prejudice as established fact, while glossing over inconsistencies. However, it would be unwise to infer from the gauche nature of such publications that their lack of substance reflects a correspondingly insubstantial threat.

A presentation at one of the Access All Areas conference (one of the conferences which attracts legitimate security, legal and law-enforcement professionals, crackers both practising and reformed, and 'legitimate' hackers) offers an interesting alternative definition. "Basically, social engineering is the art and science of getting people to comply with your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behaviour, and it is far from foolproof." (Harl, 1997) In an article for LAN Times, Al Berg quotes at length from 'experienced hacker' Susan Thunder, speaking on "Social Engineering and Psychological Subversion" at DEFCON III. "*Social engineering* is hacker jargon for getting needed information (for example a password) from a person rather than breaking into a system. *Psychological subversion* is Thunder's term for using social engineering over an extended period of time to maintain a continuing stream of information and help from unsuspecting users." (Berg, 1995).

Here, we're seeing two interconnected strands. While social engineering as synonymous with password stealing is common usage among these groups, this usage is also linked with other forms of 'psychological subversion'. The security establishment, however, has adopted the password stealing aspect without necessarily paying much attention to those other forms.

Traditional Security Definitions

Social engineering is frequently overlooked in security circles, and many classic texts don't address it at all. Stephen Cobb makes heavy use of the definition coined by SRI International: "deceptive practices to obtain information from people using social, business or technical discourse" (Cobb, 1996). The SRI definition or some variation on it is very commonly used, but somewhat limiting for our purposes. A somewhat similar definition is used in the "IT Baseline Protection Manual": *A method of "sounding" information which is not generally accessible. Often, perpetrators will pose as insiders by using pertinent keywords during conversations and thus receive information useful for other purposes*. (Bundesamt für Sicherheit in der Informationstechnik, 1997).

The trouble with such definitions is that they are easily equated with 'tricking someone into revealing their password', whereas social engineering techniques such as bluster, wheedling, and masquerading can be and are used to mount many other attacks. Psychological manipulation of individuals as a viable technique for subverting systems (in the broadest sense of the word systems) doesn't have to have anything to do with password stealing. Hoax viruses, for example, can constitute an effective denial-of-service attack, without necessarily targeting a specific individual, group of individuals or organization. If they are so targeted, they tend to spread, virus-like, far beyond the original point of entry. They still constitute social engineering as defined by the *Jargon File* (a definition much borrowed by the underground, incidentally): "**social engineering** n. Term used among crackers and samurai (hackers for hire) for techniques that rely on weaknesses in wetware (people) rather than hardware or software." (Jargon-L, 1996)

The *Jargon File* definition is almost too broad. After all, weaknesses in hardware or software are automatically less significant if people are aware of them and act accordingly. Since ignorance is a human weakness, all breaches of security could be said to constitute social engineering . While I'm happy enough to argue this position, it could make for a very long paper. Michel Kabay uses the term to cover a wider range of attacks than most, including scavenging, leftover and other threats treated later in this paper (Kabay, 1996), and parts of this paper draw heavily on his work. Nevertheless, I do intend to bring under the 'social engineering' umbrella some other attacks which aren't often considered in that context (if at all) in current literature: indeed, they aren't necessarily regarded as malicious attacks at all, but as inevitable irritations.

Extending the Definition of Social Engineering

Hoaxes (especially hoax virus alerts) are usually considered in terms of curbing their spread by unsophisticated users rather than in terms of the motivation (malicious or otherwise) of the originator. Some commentators have pointed out that hoax virus alerts are a special case of chain letter (Harley [1], 1997) and invited comparisons with the St. Jude letter [Harley [2], 1997) as analysed by Richard Dawkins (Dawkins, 1995). Others have been drawn to Dawkins' concept of the meme replicator as a unit of cultural transmission (Dawkins, 1989) in this context. Sara Gordon *et al.* refer not only to Dawkins' work and subsequent work in memetics, but cross-refer to advertising hype such as tamagotchi fever (Gordon, Ford & Wells, 1997). While these lines of thought are valuable in terms of examining the mindsets of hoax victims, as we must if we are to consider effective countermeasures, they should not distract us from the fact that the origin of many common hoaxes is not just mischievous, but malicious (Harley [1], 1997) and such hoaxes can cause significant damage. Even worse, we are beginning to see instances of chain letters and hoaxes used not only as a kind of denial-of-service attack, but as carriers of real programmatic threats such as the RedTeam virus.

It's possible (indeed, likely) that some hoaxes derive from other causes (high spirits or genuine ignorance and misunderstanding), and may not imply an (intentional) attack at all. Certainly much spam (junk-mail) seems to be generated by individuals under the misapprehension that unsolicited e-mail is an acceptable and effective marketing technique (no doubt helped along by the cynical marketing of purveyors of mass-mailing software and address lists). On the other hand, much spam is also generated by individuals selling fraudulent get-rich-quick schemes or disseminating material which can only be intended as an irritant, or black propaganda, or with out-and-out criminal intent such as the selling of pornography, pirated software, credit card numbers *etc*. There has been little consideration of these issues in security-focused literature to date, though Barrett (1996), while using a very password-stealing-oriented definition of social engineering, manages to deal effectively with a number of these issues. Electronically, much more information is available, and a subscription to the Spam-L list, while heavy on bandwidth, is a good way of checking some excellent resources and examining live examples of exactly what the everyday Internet user risks receiving in their mail.

While some proposed classification schemes (Cohen, 1997; Ekenberg, Oberoi & Orci, 1995) draw clear distinctions between threats considered here under the same banner as "social engineering", I believe this integration to be useful in terms of addressing multiple threats with broad policies. It should be emphasised, though, that a taxonomic approach to social engineering threats will be restrictive compared to other schemes in broader use in risk analysis literature.

Towards a Working Definition

A company offering training in countermeasures and diagnosis of social engineering attacks include on their web page a number of examples and the following, more cynical definition: "The skillfull [*sic*] manipulation of a governed population by misinformation to produce a desired change." (Keytel, 1997)

This gives us more idea of where the vandals are coming from than an out-and-out Social Sciences definition. I particularly like the vagueness of 'desired change', because it's broad enough to cover all the issues we worry about in security. (Of course, it would be nice if we could assume that good guys do it with information rather than misinformation......) In fact, if we ignore the legislative implications of the term 'governed population', this definition rather neatly ties together into a single definition the social sciences concept of social engineering, and the concept of psychological subversion as I intend to explore it here, and the following definition, the one from which I intend to work in this paper, is similar, but incorporates elements from previously considered definitions.

"Psychological manipulation, skilled or otherwise, of an individual or set of individuals to produce a desired effect on their behaviour."

It's a very broad one, and it applies to techniques not unique to computer vandals. It's no coincidence that helpdesk staff are so often targeted by Social Engineers: legitimate users often employ the same manipulative techniques. On the other hand, this definition also covers the approach I intend to advocate here of countering malicious social engineering with constructive social engineering through education. Whereas the Social Engineer will want to exploit the victim's behaviour without necessarily modifying it, the aware security professional will be more concerned with the behaviour modification involved in the education of the security-unaware user.

Social Engineering and Information Protection

Let's begin by considering the classic information protection model in terms of social engineering attacks.

Privacy

This is what we usually associate with social engineering , especially in the context of password stealing by masquerading. Of course, once unauthorised access has been gained, attacks on integrity or availability are as possible as the simple theft of information.

Integrity

social engineering is usually seen as a means of accessing the technology which enables integrity to be compromised. However, it's perfectly possible to use social engineering as a means of directly compromising integrity.

"This is the computer centre. We've just discovered a major bug, and I'm going to have to ask you to make some temporary modifications."

Availability

A masquerader can, in principle, launch a denial-of-service attack through misinformation delivered over the phone or in person. This isn't the only route, though. Hoax virus alerts employ exactly the same technique: a warning attributed to the FCC, or IBM, or AOL can and does result in panicking users refusing to use services to which they're entitled out of fear of the consequences.

These hypothetical examples indicate that psychological subversion has possibilities and implications for security professionals beyond the traditional definitions of social engineering as password stealing. To appreciate the full risk potential it embodies, we need to examine more closely the varieties of threat we're faced with, and define them more formally.

A taxonomy of Social Engineering and Related Threats

Masquerading

Using a false identity in order to perpetrate an attack is often associated with password stealing, but may be used as a vehicle for many other types of attack. It's also often thought of as something that's done on the telephone, but it doesn't have to be. In fact, while it's easy to masquerade as "a user" or "an administrator" over the telephone, it may be easier to masquerade as a specific person by forging e-mail or even faxes. It may be very easy to extract sensitive information from someone who has been misled as to the identity of the person they're communicating with. There's also a possibility here for a man-in-the-middle attack where an attacker taps into an existing connection between two parties who have already authenticated each other, so that the attacker doesn't need to be authenticated.

It's possible to masquerade as a program, too (though this may stretch the definition a bit), given the chance to plant a fake login or other program which requires a password, for instance. This doesn't have to involve an outsider planting a Trojan horse into your files by gaining root access. Shared/common user accounts could be perfect for this. In an environment where users are not discouraged from borrowing accounts, a malicious insider might plant such a Trojan into his own account.

Password stealing

This is often associated with masquerading. One such (common) attack is to impersonate an infrequent user on the telephone who's forgotten his or her password (finding infrequent users on poorly-protected systems is a classic use for the *finger* utility). Another is to masquerade as a systems administrator, operator, credit bureau *etc*. and ask for a password for testing, diagnosis etc. This particular form of impersonation may be by telephone, person-to-person, or via e-mail (or even facsimile).

A common alternative attack is stealing password files, often for decryption with utilities such as crack. While this does not in itself constitute a social engineering attack, its effectiveness may be increased by the use of social engineering techniques such as gaining temporary access to someone else's account by (for example) shoulder-surfing, accessing a terminal still logged in to someone else's account, or by gleaning personal information that might assist in guessing passwords.

Dumpster diving

Dumpster diving, also referred to as scavenging/trashing**,** is sometimes regarded as social engineering , sometimes as a separate threat. Either way, it's often a seriously effective attack, and has to be addressed. Trawling through corporate trash can uncover all sorts of useful material: discarded paperwork, classified and unclassified: drafts of sensitive reports and memos, internal phone directories, inventories. Discarded media: material ranging from odd floppy disks and tapes through obsolete hard disks to whole systems is sometimes fished out of skips. Trashing may therefore be a precursor to a whole range of attacks: social engineering , phreaking (Computer Underground Digest, 1997) unauthorised access to inadequately disposed of data, and password cracking based on personal information are a few examples which come to mind. Dealing adequately with this class of threat may require a whole range of policies and techniques, probably graded according to the sensitivity of particular systems.

Leftover

Electronic garbage can also be a rich source of information to the vandal who contrives to be in the right place at the right time. Terminals and terminal emulators may keep recent transactions in buffer memory so as to allow the operator to scroll back, at need. A terminal left temporarily unguarded may be a source of leakage or unauthorised access. File buffers, print buffers and other temporary files may get left on disk by an uncompleted process. On PCs, such files are frequently mislaid by the operating system as a byproduct of system crashes: disk utilities may identify these as lost clusters and revive them on demand.

Material which is deleted during an editing session is not always irretrievable afterwards. Some word-processing software (especially where multiple levels of undelete are offered as a facility) may retain all deleted material. Database management systems often offer a compaction function which removes this material, but such a function is less common in word-processors. Systems with a "trashcan" directory or folder don't usually render deleted material immediately inaccessible. Even the plain DOS DEL command doesn't actually overwrite a deleted file immediately, but simply tweaks the File Allocation Table.

Hoax Virus Alerts and other Chain Letters

Hoax virus alerts can have more impact than real viruses, on a well-secured site. These attacks are not normally associated with breaches of integrity or privacy so much as availability. These have a startling resemblance to the traditional chain letter, such as the St. Jude letter, and I prefer to categorize them as a special case of chain letter (Harley [1], 1997). To all intents and purposes, however, they constitute a denial-of-service attack, and at the point of origin usually demonstrate a malicious, mischievous, or at best extraordinarily naive mindset. They exploit technically inexpert users by playing on their gullibility and altruistic urge to help, by encouraging them to spread a message whose usual effect is damaging.

The user is unable to make proper use of the facilities available to him/her because of fear of an imaginary attack, and if not carefully handled, finishes up feeling stupid and exploited, and may be reluctant to act appropriately in the future for fear of being made to look stupid again.

Helpdesk staff, system administrators etc. are tied up responding to panicking users, validating reports which are not obviously hoaxes, and keeping users and other IT staff informed and educated. Network bandwidth, mailboxes *etc*. are clogged with junk.

Spam

This is a surprisingly complex issue. One classic social engineering aspect lies in the way that those who advertise in this way are conned by those who sell mailing lists and spamming software into believing that they're buying in to a real marketing opportunity. Then there are the fraudulent pyramid schemes, Ponzi schemes *etc*. which are promoted in this way (Barrett, 1996). Some of the potential risks include:

- Flaming and consequent intimidatory responses (flame wars, mailbombing, other forms of harassment).
- Some people find spam threatening in itself (how does this person know where to find me?).
- Replying with REMOVE or CANCEL to non-existent mailboxes, resulting in nuisance bounces to the wrong person.
- Opting out by sending one's address to a list which is actually harvested by spammers as a source of addresses. Many who sell lists on, or in some case buy them, are not concerned with the fact that someone who opts out from lists is unlikely to be a source of profit.
- Losing mail, causing looping/bouncing through inapt and inept mail filtering. For instance, discarding mail unread because of poor configuration, or selection criteria which may exclude legitimate and even important mail.

Direct Psychological Manipulation

This blanket term covers a number of possibilities: seduction and bribery, intimidation (especially when combined with impersonation of one of the target's superiors, for example), extortion and blackmail. Many of the threats classified by Ekenberg (Ekenberg, 1995) under the category crimes may come under this heading: *e.g.* malicious mischief, bomb threats, faked communications). social engineering is a little like covert channel exploits: knowing of the possibility isn't necessarily helpful because the sheer range of potential attacks is so difficult to address. However, it's unnecessary to throw up our hands in horror and give up altogether. A little judicious policy and education can go a long way towards addressing the problem. Security is, in the end, always a people problem, but social engineering intensifies the need to address human weakness as a problem requiring solutions.

Seven Deadly Vices: a taxonomy of user vulnerabilities

We could be positive and call this section the Seven Deadly Virtues, substituting trust for gullibility, modesty for diffidence, enlightened self-interest for greed, *etc*. Either way, it's clear that a trusting nature is not altogether a positive trait in a security-conscious environment.

Attacks directed against software are never an insoluble problem. Loopholes tend to be found one at a time. (In fact, in the case of recent versions of Microsoft Word, there is one main loophole, their vulnerability to malicious macros, but it's a particularly major loophole.)

It can generally be predicted and proved that a particular problem exists with a particular version under particular conditions. For instance, any version of Word which supports WordBasic is potentially vulnerable to macro viruses or Trojans. Word 6 or is potentially vulnerable to a given number of known threats according to the platform on which it's run. That number is modifiable according to the counter-measures applied. Even if a program can't be upgraded, downgraded or patched, it can be replaced or discarded.

People (wetware, liveware, meatware, humanware) on the other hand, are not susceptible to the same degree of control. As the sour and venerable MIS joke goes, "It'd be a great job if the users didn't keep getting in the way." You can't replace a malfunctioning person with an uncorrupted instance of the same version number. If you plug in a more generally competent person, it may still take time for them to learn that job.

Many useful operations can't be performed under controlled circumstances. People are generally not susceptible to implanting with hard-coded responses, being good at heuristic analysis and extrapolation, but apt to forget programmed responses under pressure.

They can and do make arbitrary choices and decisions, depending on the phases of the moon and the prevailing wind. At 0900, a porter demands accreditation from everyone who comes in, including the CEO and Bill Gates. At 1430, after a particularly good lunch and a beer or two, he waves through a stranger with an armful of cable and a toolbag.

Gullibility

In 'real' life, people tend to take others at face value until they're made aware of a reason not to. Individuals who are not particularly computer literate are particularly at risk in this respect. Outside our own area of expertise, we may have difficulty in evaluating the not only the benevolence but also the expertise of those who appear to know more than we do. What we're really talking about here is ignorance. Unfortunately, people who have quite different jobs can't be expected to become security experts as well. All we can do is to draw attention as forcibly and clearly as possible to particular danger areas. Much as the accountants will hate it, we're talking policy and education.

Curiosity

Naive and uninformed curiosity has been causing problems since the Garden of Eden and Alice's Adventures in Wonderland. Hostile applets with a nice big button to click on; Trojan Horse programs that promise interesting cultural experiences - like expensive and unnoticed phonecalls to Moldavia. There's an element of social engineering in every Trojan Horse. Pornographic images are a frequent carrier for viruses and Trojans in some newsgroups. It's frequently said (often by me) that viruses identifiable by subject headers such as Good Times or Join The Crew are sheer fantasy, but the ShareFun macro virus almost fits this description - it sends mail with the header "You MUST read this!" and an infected Word document as an attachment. This is, of course, a nice piece of psychological manipulation more recently emulated by the RedTeam virus. In this case, an infected program is sent as an attachment to a message which is basically a classic virus hoax alert. However, the attachment is claimed to be a cure for the hoax virus. Subversion of real anti-virus software by using it as a carrier for real viruses has been seen many times in the past.

Courtesy

There should be more of it, but a certain amount of discrimination is called for. A classic way to gain unauthorised entry is to get to a secure door with an armful of boxes at the same time as someone with legitimate access. It goes against the grain for many people not to hold the door open for the next person through. The less awkward it is for an authorized person to get in, the less awkward others will feel about letting them gain access themselves. When using a turnstile, though, each aspiring entrant authenticates his or her self, either by using an authentication device or by identifying themselves to reception staff. Using trained reception staff to administer a choke point is much more practical than educating the whole organization.

Greed

Which we might define as susceptibility to some form of bribery or seduction. Well, you can't change human nature, or pay the janitor the same rate as the MD. (Not an entirely random example: the magazine 2600 once published an article on getting into a targeted organization by obtaining a job as a janitor.)You can do a little human engineering of your own, though.

Diffidence

People are reluctant to ask a stranger for ID, or ask them to look away while entering their password, or refuse to give their password.

Thoughtlessness

This might be defined as an insufficiency of paranoia. You can’t expect the average user to think like a security specialist, but you can raise awareness through education and enforcing realistic policies.

Apathy

Q: Which is the most useful to a social engineer? Ignorance or apathy?
A: I don’t know and I don’t care

Apathy is, in the end, a resource management problem. Either personnel selection procedures are lacking, or maintaining morale is seen as a low priority. In fact, maintaining morale needn’t always be resource-intensive, though.

Towards a Solution

Management Attitudes

Managers frequently display a degree of paralysis when urged to consider security issues, especially in a field as lightly documented as social engineering. Don’t get hung up on worrying about the costs.. Consider a pilot project: task an individual or a working group with information-gathering and making recommendations. If you have the resources and can find a consultant with demonstrable expertise in this area, then buy in that expertise. It can be (and usually is) expensive to engage outsiders for long enough to do a realistic assessment of the needs of your organization: if you opt for in-house research, you’re probably trading knowledge of the organization off against lack of experience in an area that even security professionals are not often well aware of -- and in many organizations, security administration is not allocated to security professionals. If you go this route, you must ensure that the individual(s) tasked with this mission have motivation, time and resources to learn as they go along, and are not required to become experts in social engineering in their coffee breaks.

Don’t get too bogged down worrying about about panicking your users by drawing their attention to the fragility of what they may perceive as secure technologies, either. Users are apt to attacks of vertigo when they find that their assumptions about the privacy of their e-mail or the efficacy of the firewall at countering all sorts of threats are unfounded. However, a little user paranoia is a healthy corrective to corporate complacency. Better to acclimatise to paranoia pre-emptively than to acquire it reactively after a major security breach.

Policies Count

Security policies are often regarded as a time- and paper-consuming waste of space, or, alternatively, as an alternative to action. In the real world, the truth lies somewhere in between. You can’t necessarily (reasonably) discipline a user for not conforming with an unpublished policy, but you can start to exert some leverage. This may be particularly so where individuals in the higher echelons are responsible for poor practice and may resent being brought to account for it. Management non-intervention while the resident expert beavers away is not enough if someone higher up the tree decides to stamp on his fingers. Covering your back shouldn’t be the main concern in a healthy corporate environment, but there’s no need to paint a bulls-eye on it. If you are concerned enough about the sort of threats examined here to task someone with establishing countermeasures, don’t expect them to do it wearing manacles.

“Spaf’s first principle of security administration: if you have responsibility for security, but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong.” (Garfinkel & Spafford, 1996)

Without positive management support, the best you can hope for is (probably part-time) strictly reactive application of Band-Aids.

Implementing Conceptual Firewalls

Start off with a little risk analysis. If the problems can’t be demonstrated, there will be an understandable reluctance to allocate resources and alarm the users. A well-written preliminary conceptual report may be sufficient to encourage the freeing of funds for a serious risk analysis project. At the very least, it should be possible at this stage to task a suitable person or persons to carry the project forward. Take time to consider: do they have the expertise, or are resources available to them to acquire expertise? Do or will they also have authority, resources and time to implement defences? This isn’t a job for the office boy, and it isn’t particularly a technical job, though technical knowledge is rarely a drawback.

Now, draft a policy. Draft as many policies as you need, not to mention guidelines and procedures. A policy is not necessarily an acceptable substitute for action (it’s often a delaying tactic, coming somewhere between the working party, steering committee, and management approval), but it may be a very useful first step. At this point, it needn’t (and probably can’t) be comprehensive. At least it demonstrates that a problem has been identified and that the will exists to address it. Securing higher management approval is the vital first step in securing an organization. Once you have an acceptable draft policy, you have some authority, even before detailed planning and implementation. Here are some policy areas which need to be addressed in most organizations.

Well-Founded Policy

Acceptable Use Policies

Most organizations have no clear policy as regards the use of the Internet (including electronic mail, the World Wide Web, newsgroups etc.). It is a mistake to leave the novice cybernaut without direction. Most computer users today haven’t served their time on the ‘Net and don’t have the technical or historical background that security professionals usually do. It isn’t necessary to teach them TCP/IP or the history of ARPANET, but it might be good practice to let them know

- that e-mail is not necessarily private, but may be read by authorised or unauthorised persons.
- that mail doesn’t always come from the source it seems to originate from.
- that quoting or forwarding mail without permission may be not only a breach of netiquette, but have copyright implications.

- that other legislation applicable to the printed word may also apply to e-mail or postings to newsgroups.
- that putting material onto the World Wide Web doesn't mean it's in the public domain.
- what degree of recreational browsing or internet social interaction is acceptable.
- to what degree it's acceptable to use work resources for extra-curricular (especially commercial) activities. This one is likely to find a place in Desktop Acceptable Use Policies, too.

The user of a desktop machine should understand clearly (when applicable) that the desktop belongs to the organization, not the user, and that there are expectations which must be met regarding use of authorized and legitimate software and peripherals (especially modems, which may breach firewall security), conformance with company guidelines on issues such as virus management and other security issues such as the use and the effectiveness or otherwise of CMOS passwords, screensaver passwords, and other access control measures. A frequently overlooked issue is that mail-agent software on the desktop is rarely as secure as it is on a multi-user system, and can often be made very insecure indeed. It will probably also be necessary to address issues specific to the use of laptop computers and other portable equipments, either here or in a separate AUP.

Users of multi-user systems frequently need guidance about the need for authentication through passwords, about the dangers of sharing passwords, even with apparently authorized personnel (and that real systems administrators hardly ever need to ask for a user's password). A frequent bugbear is the need to enforce secure passwords. In these circumstances, it may be helpful to keep the aggravation down to a minimum. Enforcing the use of multiple unmemorizable passwords and over-frequent changes of password often does as much harm as allowing short dictionary words and no password ageing, especially in terms of morale. Where system sensitivity requires it, explaining the associated problems may help in enforcing a stricter regime.

All such policies should make plain a users rights and responsibilities. You may also need to cover privacy issues such as the following, though a general Information Protection Policy would also be applicable here.

- shared accounts/passwords
- digital signatures
- acceptable use of encryption
- respect for others' work and accounts
- who can disclose what, to whom and when?
- acceptable authentication
- need to know
- mandatory use of secure channels

Staff are often diffident about challenging apparent breaches of good practice.
. Reassure them that it is not only acceptable, but desirable or even mandatory for them to ask strangers for their ID, or to ask others to look away while entering passwords.

. Ask them to respond without hostility if someone confronts them in this way.
. Quietly remind them that conformance with guidelines is expected, and with policies is mandatory.
. Empower them to verify identity.
. Indicate what level of verification is acceptable. Making the initial challenge but accepting a vague response may give the challenger a self-satisfied glow, but doesn't noticeably improve security, even in terms of coming across someone in the corridor, let alone giving away passwords.
. Lay down guidelines. Don't expect individuals to be word-perfect on policies and guidelines, but do prioritize raising awareness of their existence and making them accessible.

Good policies are an essential weapon in the fight against psychological subversion. However, effective implementation entails not only raising the awareness level among general users, but special attention to a number of critical support issues.

Administering the HelpDesk Function

Users frequently make a point of emphasizing the importance of their role or that of their superior, or exaggerating the time the length of time a trouble ticket has been outstanding or the gravity and/or urgency of the problem, or bypassing normal channels, in order to get quicker, more senior or more expert service. Bear in mind that social engineers use the same techniques:

- Subtle intimidation
- Bluster
- Pulling rank
- Exploiting guilt
- Pleading for special treatment
- Exploiting a natural desire to be helpful
- Appealing to an underling's subversive streak

Helpdesk staff need a sensible framework to work within. First and foremost, they need a superior who is willing, authorized, and knowledgeable enough to make sensible decisions about when, if ever, to bend the rules, and who won't throw a thorny problem back at them. They need a good understanding of what the rules actually are, what their responsibilities are, and what recourse they have in the event of a grievance. They also need to know that when they have a run-in with a difficult user, that they will have the backing of management, as long as they conform to policy.

Other IT Support Staff

IT staff in general both pose and are vulnerable to special risks. They're often assumed to have a wider range of knowledge than is really appropriate. Even worse, they're under pressure to reinforce that view of themselves, not only to bolster their own self-image, but to reflect well on the unit of which they're part. They may have privileged access to particular systems (but not expert knowledge of those systems, necessarily). They are often encouraged to experiment, and are usually expected to teach themselves as much as possible. It's no coincidence that IT staff constitute a classic virus vector, either: in the absence of proper controls, they are apt to flit from user to user without taking elementary precautions. Training in security issues for staff in general is virtually ignored in many organisations, not altogether surprisingly, given the cost and administrative overheads of enforcing training in areas which are not often seen as relevant to the average user. However, organisations which withhold training in these areas from IT support teams take serious risks: team members make tempting targets for social engineering attacks.

IT Security and other Units

Physical and IT security personnel often have an uneasy and distant relationship, even in institutions where they share a common node of the management tree.

- IT personnel should at least understand the need for physical controls and have some involvement in the physical securing of IT equipment, especially when sophisticated technical controls such as handheld authentication devices are employed.
- Non-IT security people need at least a basic understanding of how IT hardware hangs together in order to appreciate where the weakness are: not only in terms of sabotage, theft and espionage, but even in terms of accidental damage. In many cases, they'll be the first line of defence against breaches of the physical perimeter.

It's not only people formally employed in security who need to be involved. Liaison with personnel departments is critical. Staff with access to critical systems or data should be subject to special contractual and other controls, and temporary/contract staff should not be overlooked. Staff leaving or changing jobs within an organization may entail changes to access controls in a number of contexts, and it's essential that access privileges reflect the current status of the individual. Staff working in personnel departments are themselves tempting targets for social engineering attacks, since they have privileged access to all kinds of interesting and saleable information.

General Education

General users should not be expected to become security experts. Indeed, it's unrealistic to expect them to be particularly IT-literate beyond the requirements of their work. This makes the quality of the educational and other resources available to them particularly important, not only in terms of accuracy and pertinence, but also accessibility. Training and first-line documentation should be as brief and clear as possible, but more detailed resources should be available and <u>known</u> to be available. In particular, such documentation should make as few assumptions as possible about the technical knowledge of the reader: unfortunately, this is not always consistent with the equally pressing requirement that it should be as <u>short</u> as possible.

Make it clear what is forbidden, and what the penalties are - leave as few "I didn't think it mattered just doing such-and-such..." loopholes as possible. Why should lower grades take security more seriously than management? The likelier it is that contraventions will be detected and punished, the less susceptible the average employee will be to bribery or independent felonious action.

Set a good example, too. Managers who are ‘too important’ to be inconvenienced by security precautions are excellent targets for the social engineer.

The Draconian model is not the only possibility, though. Employees who feel that their job function is taken seriously and that their contributions are valued have more incentive to be loyal than those who don’t. Cultivate loyalty, but don’t rely on it....

Heads of department require particular cultivation. It is necessary that they have a sufficient understanding of the technological and other risks to which their staff may be vulnerable to take whatever measures are appropriate, including encouraging subordinates to take advantage of educational opportunities and conform with guidelines.

Consider training in computer ethics. This not only raises awareness of what the Evil Hacker may be up to, but also of the responsibilities of the individual in terms of countering social engineering attacks by better awareness of the problem and the techniques involved. It also gives them an appreciation of what is acceptable in their own computing activities. It is received wisdom that most targeted attacks are still directed from inside rather than outside. The majority of staff won’t have the knowledge or desire to hack into prohibited, secured areas, but may be seriously careless about using other people’s systems, software, or data files without authorization. Indeed, they may be tempted by a small act of rebellion, not realising that an apparently small indiscretion may create enormous breaches. Train them to think about the grey areas, and they’re less likely to be pulled across the line that separates more-or-less legitimate corner-cutting from breaches of policy or even illegal acts.

Discussion and Conclusion

Recommendations for Managers and Other Decision-Makers

1) Risk Analysis

I hope I’ve convinced you that social engineering is a significant threat. However, it’s seriously under-documented, and committing major resources to deal with a threat many people have never heard of or considered is not always easy. This paper gives some background, but useful statistics are scarce: I can’t point you to a survey which tells you how much a year social engineering costs the ‘average’ organization. Statistics on security breaches in general are easier to come by, but they don’t tell you how much use individual intruders made of social engineering, so you have to approach it from the other end: gathering information on how vulnerable you are to this threat, and what measures are available to counter it.

2) Security Policies and Insurance Policies

Security is a cost centre. Like fire insurance, it’s a large expense set against the risk of an attack which may never come, though with social engineering it’s probably truer to say that such attacks are frequent, but not necessarily recognised as such. Security policies aren’t popular: they take time to put together properly and are of no practical use without a realistic educational program to back them up. In other words, they cost.

However, your policies represent your recognition of the problems you face, your assessment of your vulnerabilities, your degree of commitment towards the level of protection you need to implement, and the foundations of that implementation. Without positive management support for the establishment and implementation of policies, the best you can hope for is purely reactive containment of security breaches without fully understanding their causes so as to lessen the impact of similar future incidents.

3) General Education

If you don’t take the social engineering threat seriously, you can’t expect your staff to. You have to allocate resources to assessing the risks, defining policies, and making sure your users know what is expected of them. You can’t achieve the last of these without a realistic user awareness programme. You don’t have to turn everyone into a security expert, but you do have to ensure that everyone has a minimum of training to raise awareness of the issues and, most importantly, to ensure that they know where to go for information and guidance if they have to. You also have to set a good example by conforming to good practice personally.

4) Graduated Training

Different job functions require different levels of training. IT staff generally need a deeper knowledge of security than most users, and a realistic appreciation of what is required of them. Non-IT security staff need a passing acquaintance with technology even if they never use a computer themselves, if they’re to handle physical security effectively. Units which are particularly tempting targets to the social engineer, such as Personnel/Human Resources departments, may need special consideration, too.

5) Positive Management

An individual is likelier to take pride in doing their job properly if they see that management:

- values the job function - nothing is more dispiriting than feeling that no-one cares whether your job gets done or not
- values the contribution of the individual performing that function
- considers it important that the job is done well

People often respond well to being given a more impressive job title or more formal responsibility, enhancements which may cost little or nothing. Of course, bigger paychecks help, too. On the other hand, inappropriate use of such incentives can be seriously unconstructive. There is such a thing as an over-enhanced sense of one’s own worth.

Recommendations for Researchers

This paper makes a number of assumptions about good practice, based on personal experience and review of some of the available literature. The sad fact is that trustworthy hard data in security is hard to come by, and just about all the data regarding real-life social engineering attacks is anecdotal (and likely to remain that way, given the shyness of most corporates when it comes to publicizing attacks of any sort that have been made on them, successfully or otherwise).

1) Statistics are often quoted ‘proving’ that insider attacks are much more common than attacks by outsiders. I’d like to see more research on classification of such attacks in order to recognise insider ‘attacks’ which are, in fact, user error of some sort with no overt malicious motive, or the result of psychological subversion by outsiders.

2) BS7799, the British Code of Practice for Information Security Management, is an interesting example of a document which attempts to provide “a comprehensive set of security controls comprising the best information security practices in current use”. (BSI, 1995). It is based on a collaboration between the Department of Trade and Industry, the British Standards Institution, and a number of large corporates. To what extent are we justified in assuming that what the big corporates do is really ‘best practice’? How can we measure their effectiveness?

Practical Implications

Social engineering is not a single threat. It’s a whole class of problems, with no single one-fits-all solution. Social engineers prey on human weaknesses, the vices and virtues discussed previously. In “Howard’s End” Forster said something like “The confidence trick is the work of men, but the no-confidence trick is the work of the Devil” - good morality, perhaps, but poor security. In attempting to counter social engineering attacks, we ask users to rise above not only their own ignorance, but in some respects their own better natures.

It doesn’t come naturally to most people to challenge strangers in the workplace, or not to hold a door open for someone: in fact, it may be harder to overcome these socialized ‘failings’ than it is to overcome mere technical inexpertise.

Nevertheless, technical inexpertise presents its own distinctive problems. A reactive response to a user’s report of an E-mail virus is relatively simple. You could simply say “No, there is no Good Times virus - it’s a hoax.”, which may be enough if your user is considerate enough to ring the helpdesk and say “I’ve just received a message about a virus called Good Times”. A more attractive approach might be to say to enhance your user’s technical grasp by demonstrating the absurdity of the alert they’ve received. “You can’t burn out a CPU by making it perform the operations it was built to perform, and anyway there’s no such thing as an Nth complexity binary loop.” Let’s suppose that your user rings back and says “I know Good Times is a hoax, but apparently there’s a Trojan Horse Virus which......” You could continue to raise your user’s technical awareness: “Trojan Horses and viruses aren’t the same thing [so what are the differences? Isn’t a virus a special case of Trojan Horse? Isn’t a virus dropper a Trojan Horse?]. Software can’t physically damage hardware.[Not ever? Couldn’t you overdrive an antique monitor? Couldn’t you reprogram a modem or a flash BIOS?]”.
It seems that the more you explain, the more questions you have to answer. The logical end to this road is the point at which your user has become a security expert - good if your business is creating security experts, but that’s a market which is easily saturated.

Alternatively, you could focus on technical issues which relate specifically to hoaxes, rather than to computing and computers in general. “Here are some of the features of the E-mail you’ve received which imply that its a hoax. It’s all in capitals. It has far too many exclamation marks. It asks you to forward it to everyone you know.” This is much better. It equips a receptive user with a heuristic algorithm which will trap any chain letter and most hoaxes (most of which are special cases of chain letter). This is actually as far as most of the current literature on the hoax virus phenomenon goes.

But let’s consider a warning which says “There’s a new virus which [insert the usual improbable characteristics here]. Don’t panic, I’ve enclosed a program as an attachment which cures it.” This is a very rough approximation of what the RedTeam virus does. The virus it describes doesn’t exist, but the attachment is virus-infected. The virus description in this case would be trapped by the previous heuristic [“P.S. Make sure you warn all your friends of this new threat!”], but that’s no guarantee that the real virus wouldn’t get its place in the sun. The world is full of people who haven’t caught up with this heuristic. Those who have are not safe. “It does sound like a hoax, but just to be on the safe side....”

Let’s hypothesise a little. How should we react to a virus alert which acknowledges all the heuristics which might be deployed against all known hoax viruses, but claims to be a special case, or misrepresents a standard instance of social engineering as an exception, and bypasses such crass symptoms as capitalization and multiple exclamation marks? We could, of course, continue to attempt to raise the level of technical awareness of our users. Or we could go back to first principles. “If it doesn’t say quack, it doesn’t waddle, says it hates water, but has an orange beak, maybe it’s a duck after all.” RedTeam still says quack. Our hypothetical alert doesn’t. It might bypass all our anti-hoax heuristics: however, it would still have to persuade its intended victim to execute it. In a well-founded environment, such an alert would still fall foul of the Prime Directive: “Thou shalt not run unauthenticated programs”.

You can’t make realistic rules to cover every potential future threat. If you did, no-one would read all the way through the manual. Keep the rules few, simple and general, but concentrate on helping your users to extrapolate from a broad principle to a specific instance. That’s where education can counter social engineering.

Research Implications

Documented research into social engineering hasn’t kept pace with dialogue between practitioners, let alone with real-world threats. Of course password stealing is important, but it’s important not to think of social engineering as being concerned exclusively with ways of saying “Open, sesame.....” Even within this very limited area, there is scope for mistrusting received wisdom. No-one doubts the importance of secure passwords in most computing environments, though the efficacy of passwording as a long-term solution to user authentication could be the basis of a lively discussion. Still, that’s what most systems rely on. It’s accepted that frequent password changes make it harder for an intruder to guess a given user’s password. However, they also make it harder for the user to remember his/her password. He/she is thus encouraged to attempt subversive strategies such as:

- changing a password by some easily guessed technique such as adding 1, 2, 3 etc. to the password they had before the latest enforced change.
- changing a password several times in succession so that the password history expires, allowing them to revert to a previously held password.
- using the same password on several systems and changing them all at the same time so as to cut down on the number of passwords they need to remember.
- aides-memoire such as PostIts, notes in the purse, wallet or personal organizer, biro on the back of the wrist.....

How much data is there which ‘validates’ ‘known truths’ like “frequent password changes make it harder for an intruder to guess a given user’s password”? Do we need to examine such ‘received wisdom’ more closely?

Issues for the 21st Century

It’s too late. Social engineering as a means of subversion predates Babbage by many millenia, and is only going to go away when the human race does. The shipwreck is resting on the seabed, and many commentators haven’t yet noticed this particular means of letting water into the hull. What can we do to refloat the Titanic?

- Research and document the issues.
- Read some of those ‘hacker’ websites.
- Acknowledge the need for comprehensive policies as a management tool .
- Acknowledge that policies are the end of the beginning of dealing with the problem, not the beginning of the end. Without effective implementation, they are only the means by which management convince themselves that they’re taking action. (“Meetings: the practical alternative to work.....”)
- Acknowledge that there is no effective implementation of policy which doesn’t include a degree of education.
- Be realistic. Education doesn’t mean teaching EveryUser all they need to become a security expert. It means teaching them all they need to know to use computers safely.
- Do it or don’t do it, but make an informed decision, and don’t wait for the 21st century.....

REFERENCES

Daniel J. Barrett 1996 Bandits on the information superhighway” - (O’Reilly)

Berg, Al 1995 Cracking a social engineer. LAN Times, Nov. 6, 1995, pp 140-142

BeRnZ 1997: http://www.aracnet.com/~gen2600/socfaq.html, http://members.tripod.com/~bernz/ (November 1997)

British Standard Institution 1995 BS7799 British Standard Code of Practice for Information Security Management.

IT Baseline Protection Manual. Bundesamt für Sicherheit in der Informationstechnik, Bonn.

Stephen Cobb The NCSA Guide to PC and LAN Security. (McGraw-Hill) Page 230

Frederick B. Cohen (1997). Information System Attacks: A Preliminary Classification Scheme. Computers and Security 16(1): 29-46.

Notes from the Underground: 2 interviews with Se7en: Computer Underground Digest Vol 9:Issue 49

“Hacker turns to vendors as IT PI”: Computing, 4th December 1997, page 32.

Richard Dawkins 1995 River Out of Eden” - (Phoenix) pp170-174

Richard Dawkins 1989 The Selfish Gene OUP 1989 Paperback Edition page 192

Love Ekenberg, Subhash Oberoi, and Istvan Orci. 1995. A cost model for managing information security hazards. Computers & Security (14,8) pp707-717.

Simson Garfinkel & Gene Spafford 1996 Practical Unix and Internet Security. (O’Reilly) pp 39-40.

Sarah Gordon, Richard Ford, Joe Wells. 1997 Hoaxes and Hypes. Virus Bulletin Conference Proceedings, October 1997.

The HAQ (The Hack FAQ) Edition 2.07, 11th June 1994. (November 1997)

[People Hacking: the Psychology of Social Engineering - Text of Harl’s Talk at Access All Areas III, 05/07/97 - http://www.abel.net.uk/~dms/archive/aaatalk.html]. (November 1997)

David Harley 1997[1]. “Dealing with Internet Hoaxes/Alerts”. EICAR News 3;2 pp10-11 (also at http://webworlds.co.uk/dharley/)

David Harley 1997[2]. “Dealing with Social Engineering Attacks.” SANS Network Security ‘97 Technical Conference Proceedings.

Professor Noboru Hidano.“Social Engineering”. http://www.soc.titech.ac.jp/hidano-lab/socialengineering.html. (May 1997)

Dr. Joseph J. Jacobs “Why ‘Social Engineering’ is an Oxymoron”. http://www.pff.org/pff/jaco0125.html. (May 1997)

The Jargon File (Jargon-L) 1996- HTTP://www.fwi.uva.nl/~mes/jargon/ (May 1997)

Michel E. Kabay 1996 The NCSA Guide to Enterprise Security - Protecting Information Assets. (McGraw -Hill) pp308-310.

Keytel 1997. HTTP://www.keytel.com/socl.htm/ (November 1997)

Professor Ross Parish“Social Engineering in the Market Place”.

Peter Rossi“The Iron Law of Evaluation and Other Metallic Rules”. Research in Social Problems & Public Policy Vol 4 (1987) 3-20.

Additional Resources

Social Engineering: Anything by Ira S. Winkler (“Case Study: Social Engineers Wreak Havoc” [www.ncsa.com]; “Who are the Hackers?” [www.infowar.com]

Policy Issues: Building Internet Firewalls. D. Brent Chapman & Elizabeth Zwicky (O’Reilly).
Information Security Policies Made Easy. Charles Cresson Wood (Baseline Software)
RFC 1244 “Site Security Handbook”
Frederick B. Cohen Protection and Security on the Information Superhighway. (1995)(Wiley).

Hoaxes, chain letters etc.: ftp://usit.net/pub/lesjones/good-times-virus-hoax-faq.txt
Les Jones’ Good Times FAQ
http://ciac.llnl.gov/ciac/ (CIAC has a hoaxes/false alerts page)
http://www.soci.niu.edu/~crypt/ (Crypt newsletter)
http://www.av.ibm.com/current/FrontPage (Anti-Virus Online - includes hype alerts and a good article by Joe Wells)
http://www.urbanlegends.com/
http://www.kumite.com/myths/
http://www.drsolomon.com/
http://www.datafellows.com/
http://www.symantec.com/

Spam, UCE etc.: http://webworlds.co.uk/dharley/security/spam.txt (resources list)
http://www.informatik.uni-kiel.de/%7Eca/email/english.html
http://www.sendmail.org/antispam.html   [both sendmail orientated]
http://spam.abuse.net/spam/faq.html
http://www-fofa.concordia.ca/spam/ (good links)
http://www-fofa.concordia.ca/spam/FAQs.html
mailto:listserv@peach.ease.lsoft.com with text:
SUBSCRIBE SPAM-L firstname lastname
http://peach.ease.lsoft.com/archives/SPAM-L.html
http://www.cybernothing.org/faqs/net-abuse-faq.html
http://members.aol.com/emailfaq/emailfaq.html
http://ddi.digital.net/~gandalf/trollfaq.html
http://www.cauce.org/ [Coalition Against Unsolicited Commercial Email]

Ethics: RFC 1087: “Ethics and the Internet”
Association for Computing Machinery Code of Ethics and Professional Conduct 1992
British Computer Society Code of Conduct 1992
Practical Computer Ethics - Duncan Langford, McGraw-Hill 1995
Computer Ethics - Tom Forester & Perry Morrison, MIT Press 1995
Computer Ethics Institute - 10 Commandments of Computer Ethics
(1st annual Conference on Computer Ethics, 1991).

High Noon on the Electronic Frontier - Ed. Peter Ludlow, MIT Press 1996
Ethics Pages - http://www.ncsa.com/
Urs E. Gattiker & Helen Kelley: “Techno-crime and terror against tomorrow’s organization: What about cyberpunks?” http://www.ncsa.com/

Appendix

Glossary

AUP (Acceptable Use Policy)	Guidelines for users on what constitutes acceptable usage of a system, network services *etc*.
Availability	One of the three basic principles of information protection/security. Data should be available whenever it's needed. See also **privacy**, **integrity**.
Chain Letter	Originally a letter promising good luck if you pass it on to others or misfortune if you don't, thus breaking the chain. Hoax virus alerts are a special case of electronic chain mail: the recipient is urged to pass on the warning to everyone he knows.
CMOS Password	Most PCs can be configured so that the bootup sequence is suspended until a password is entered, so that in theory only the owner/authorised user of the system can access data.
Covert Channel Attacks	A term applied to using an unusual communications channel to transmit information illicitly.
Cracker	Someone who breaks into computer and telecommunications system. Doesn't have the ambiguity of 'hacker', though the press and many security people use the terms interchangeably.
Denial of Service Attack	An attack which compromises the availability of system services and therefore data.
Dumpster Diving (Scavenging, Trashing)	Searching waste for useful information (especially discarded paperwork, electronic media *etc*.).
Electronic Garbage, Leftover	Data, passwords etc. left in memory or on disk where a knowledgeable intruder might be able to access them.
Ethics	Moral philosophy, dealing with human conduct and character. In the context of practical computer ethics, we are mostly concerned with 'normative ethics', the establishment of a code of values based upon accepted social norms, but applied specifically to the use of computers.
FAT (File Allocation Table)	The means by which some operating systems keep track of the physical location on a disk of the components of a file.
finger	A utility which allows a network or internetwork user to find out (1) account names on a remote server (2) whether the holder of a known account name is logged onto the system. This can enable someone who doesn't have an account on a given system to match an account name to a real person, and determine various data including the last time they logged in.
Hacker	Originally, someone with a strong (often

	experimental) interest and knowledge of computers and software. Commonly used as if synonymous with ‘cracker’ (a term coined in an attempt to distance computer intrusion from ‘legitimate’ hacking.
Integrity	One of the three basic principles of information protection/security. Data should be protected from accidental or deliberate corruption, deletion *etc*. See also **privacy**, **availability**.
Phreaking	Using electronics to make free phone calls or make them at the expense of others, access phone company computers *etc*.
Ponzi Schemes	A fraudulent scheme by which the victim is persuaded to ‘invest’ money. As the number of participants increases, the fraudster uses money sent by later investors to pay off early investors and build up numbers and confidence in the scheme, until he chooses to disappear with the money. The Internet offers virtually cost-less administration of such schemes.
Privacy	One of the three basic principles of information protection/security. Data should be accessible only to people who are entitled to access it. See also **availability**, **integrity**.
Programmatic Threats	Malicious code (malware) such as viruses and Trojan Horses
Pyramid Schemes	An alleged money-making scheme by which one person sends money to a number of people who send money to a number of people *ad infinitum*. A particularly common variation is to disguise this (generally illegal) scheme as a ‘legitimate’ scheme to buy and sell mailing lists, software, t-shirts....
Samurai	‘Hackers for Hire’: hackers or crackers who sell their skills.
Shoulder-Surfing	Looking over someone’s shoulder to ascertain their password or PIN.
Social Engineering	A term applied to a variety of attacks which rely on exploiting human weakness rather than technological loopholes. Often specifically applied to password stealing, but applied in this paper to any attack involving psychological manipulation.
Spam	Unsolicited electronic mail, especially commercial/junk e-mail. Also applied to the practice of posting large numbers of identical messages to multiple newsgroups.
Wetware (Meatware, Liveware, Humanware)	Slang term for people, especially computer users.