

## Social Engineering: Exploiting the Weakest Links

*Including an interview with security author,  
speaker, and consultant Kevin Mitnick*



## About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

## Contact details

For contacting ENISA or for general enquiries on information security awareness raising matters please use the following details:

E-mail: KJELL KALMELID, Expert Awareness Raising — [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2008

### Social Engineering – Exploiting the Weakest Links

---

#### **Acknowledgments**

Kjell Kalmelid, Expert Awareness Raising, ENISA and coordinator of this Whitepaper, wishes to acknowledge and warmly thank the three authors of the AR Community, who together wrote this Whitepaper. Dr. Maria Papadaki and Prof. Steven Furnell, both from the Centre for Information Security and Network Research, University of Plymouth, United Kingdom and Prof. Ronald C. Dodge JR, Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY, United States.

The authors would like to acknowledge the contributions of Taimur Bakhshi, Dr Aaron Ferguson, and Athanasios Karakasiliotis, whose research studies contributed towards the research findings presented here.

Thanks must also go to Kevin Mitnick, who kindly reviewed the whitepaper and offered comments based on his own experiences, and then gave a significant amount of his time to be interviewed on the subject.

## Table of Contents

About ENISA .....	2
Contact details .....	2
Acknowledgments .....	3
Preface.....	5
About this Whitepaper .....	5
About the AR Community.....	5
Executive Summary .....	7
Introduction .....	9
Background.....	9
Scale and sophistication.....	9
Social Engineering dissected .....	13
Perfecting a pretext.....	13
Getting the facts right .....	13
Timing is everything.....	14
Exploiting psychology .....	14
Exploiting technology .....	15
Assessing susceptibility to social engineering .....	17
Case Study 1 - Spotting the difference .....	17
Case Study 2 – Even bad bait catches something.....	20
Case Study 3 – Awareness-raising works .....	21
Recommendations .....	25
Technology-based mechanisms.....	25
Improving user awareness .....	25
Understanding the real routes .....	26
Appreciating the value of information .....	27
Performing practical assessments .....	27
Conclusions .....	28
References.....	29
Appendix:      An ENISA Awareness Raising Community interview with Kevin Mitnick ....	33

### Social Engineering – Exploiting the Weakest Links

## Preface

### About this Whitepaper

This Whitepaper is the result of a joint work of three members of the ENISA AR Community. The purpose of this Whitepaper is to explain and address the increasing problem of Social Engineering attacks. It is also the purpose to offer recommendations on how to combat this threat.

### About the AR Community

The AR Community is a subscription free community open to professionals working in the field of information security. It was launched in 2008 by ENISA in an effort to create an information security-focused community; particularly targeting professionals with an interest in security awareness raising matters.

Even though the AR Community primarily aims at attracting members in Europe, it has several members from countries outside Europe who all share the same idea; raising security awareness among people is key in order to achieve a true state of information security in any organization.



## The Authors

### **Maria Papadaki**

Dr Maria Papadaki, from Greece, is a lecturer in Network Security at University of Plymouth, UK. Prior to joining academia, she worked as a Security Analyst for Symantec EMEA Managed Security Services (MSS), UK. Her postgraduate studies include a PhD in Intrusion Classification and Automated Response, and an MSc in Integrated Services and Intelligent Networks Engineering, both awarded from University of Plymouth. Her current research interests include intrusion prevention detection and response, network security monitoring, threat management, security usability, human vulnerabilities, and security education. Dr Papadaki is a GIAC Certified Intrusion Analyst, and is a member of the British Computer Society and the IEEE. Further details can be found at [www.plymouth.ac.uk/cisnr](http://www.plymouth.ac.uk/cisnr).

### **Steven Furnell**

Prof. Steven Furnell, from the UK, is the head of the Centre for Information Security & Network Research at the University of Plymouth in the United Kingdom, and an Adjunct Professor with Edith Cowan University in Western Australia. His current areas of interest include security management, computer crime, user authentication, and security usability. Prof. Furnell is a UK representative in International Federation for Information Processing (IFIP) working groups relating to Information Security Management (of which he is the current chair) and Information Security Education. He is the author of over 190 refereed papers, as well as the books *Cybercrime: Vandalizing the Information Society* (2001) and *Computer Insecurity: Risking the System* (2005). Further details can be found at [www.plymouth.ac.uk/cisnr](http://www.plymouth.ac.uk/cisnr).

### **Ronald C. Dodge JR**

Lieutenant Colonel Ronald C Dodge, from the USA, JR, Ph.D. Academy Professor, Associate Dean for Information and Education Technology, United States Military Academy. Lt. Col. Dodge has served for over 20 years as an Aviation officer and is a member of the Army Acquisition Corps in the United States Army. Currently he is an Associate Professor permanently stationed at the United States Military Academy and the Associate Dean for Information and Education Technology. Ron received his Ph.D. from George Mason University, Fairfax, Virginia in Computer Science. His current research focuses are information warfare, network deception, security protocols, internet technologies, and performance planning and capacity management. He is a frequent speaker at national and international IA conferences and has published many papers and articles on information assurance topics.



## Executive Summary

Social engineering refers to techniques that exploit human weaknesses and manipulate people into breaking normal security procedures. From the available evidence, it is clear that the scale and sophistication of related attacks are increasing, with evermore avenues being exploited to reach users (including email, instant messaging, and social networking sites).

Successful social engineering can be seen to rely upon a number of factors, including a convincing pretext for contacting the target, potentially accompanied by a degree of background research and/or the exploitation of current events. In addition, attackers are readily able to exploit psychological factors and human behaviour, as well as users' (mis)understanding of the technology that they are required to use.

User susceptibility to social engineering is revealed by a series of email-based case studies (drawn from the authors' own research):

- From a population of 179 participants, assessing a set of 20 messages (11 bogus and 9 legitimate), users were only able to perform classification correctly in 42% of cases;
- From targeted mailings to 152 end-users within a participating organisation, 23% could be tricked into performing actions that would have rendered them susceptible to malware infection;
- From targeted mailings to successive undergraduate student populations, significant vulnerability was observed in following embedded links, divulging information and opening attachments. However, this failure rate reduced when users were exposed to training.

Recommended defences against social engineering come in several forms. In some cases (e.g. in phishing and malware contexts), it is possible to place some reliance upon technology-based mechanisms. However, the key to success ultimately lies in improving the awareness of the people who may be targeted. A checklist for users is proposed, containing a LIST of factors that they should consider when asked for information:

Legitimacy	Does the request seem legitimate and usual? For example, should you be asked for this information, and is this how you should normally provide it?
Importance	What is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused?
Source	Are you confident that the source of the request is genuine? Can you find a way to check?
Timing	Do you have to respond now? If you still have doubts, take time to make further checks or ask for help.

In addition to this, users need to understand the real routes by which information requests will legitimately occur, and to have a better appreciation of the value of the information that they may be divulging. The latter point also applies to organisations, which may

otherwise make too much information publically available, thereby aiding a would-be social engineer in making a more convincing approach. Finally, if appropriately conducted within workplace contexts, it can be both beneficial and revealing to perform practical assessments of user susceptibility; providing an insight into the vulnerabilities of both the organisation and individuals.





## Introduction

This paper provides an overview of the social engineering threat, highlighting the extent of the problem, and ultimately suggesting ways of defending against it. Section 2 provides background information on social engineering, whereas section 3 aims to illustrate the extent of the problem by presenting relevant assessment studies. The paper then presents a series of recommendations regarding the defence mechanisms that may be employed against the threat. The main discussion is supported by an Appendix containing an interview with security author, speaker, and consultant Kevin Mitnick. This considers the nature of the social engineering threat, users' susceptibility to the problem, and what can be done about it.

### Background

Social engineering refers to techniques that exploit human weaknesses and manipulate people into breaking normal security procedures. This may involve convincing them to perform atypical actions or to divulge confidential information. Such attacks have become a long-standing problem in the security domain, and essentially recognise that it is often easier to exploit the users of a system rather than the technology itself. However, despite its longevity, it is an area in which organisations often fall down when it comes to protection. When we look at where organisations invest their money on security, it is clear that the technology aspects receive far more attention than the people. For example, in the 2007 Computer Crime and Security Survey from the Computer Security Institute, almost half of the 475 respondents (48%) reported spending less than 1% of their IT security budget on employee awareness training, with only 9% claiming to invest more than 5% of their budget in this direction (CSI, 2007). Focusing primarily upon technical aspects of security and overlooking human vulnerabilities can easily leave them with controls that are still unable to prevent incidents. Indeed, why would someone need to defeat technologies such as firewalls, authentication, intrusion prevention and encryption in order to break into a system or steal information when they can just target the weakest link; the employees? Such realisations are certainly no secret amongst the attacker community. Indeed, Kevin Mitnick, one of the most renowned hackers of the 1980s and 1990s, is on record as attributing much of his success to his ability to manipulate people rather than his technical skills as hacker. As Mitnick himself observes, it is much easier to trick somebody into revealing their password than to carry out an elaborate hack for the same purpose (Mitnick and Simon 2002).

### Scale and sophistication

Although the scale of the problem in all its forms is difficult to quantify, it is possible to cite specific evidence in certain contexts. A good example here is phishing, with statistics from the Anti-Phishing Working Group revealing that average of 27,469 unique phishing messages were reported per month in the period from January 2007 to January 2008 inclusive (APWG, 2008). Meanwhile, on a similar note, recent findings from research sponsored by McAfee reveal that despite their notoriety, 419 scams (aka 'Nigerian Letters' or 'Advance-fee frauds') are still the tenth most common category of spam email (McAfee, 2008). In wider contexts, however, social engineering is often very difficult to detect, as it

often involves unpredictable person-to-person interactions that cannot easily be seen by monitoring technologies (Koumpis *et al.* 2007).

Given the potential of social engineering, it is no surprise that the sophistication of such attacks is constantly improving. In fact, more and more avenues are being utilised to reach people; including email, instant messaging, VoIP<sup>1</sup>, and social networking sites (Microsoft, 2006). Also, there is similarly a plethora of information that is easily available at our fingertips, which can be used to make social engineering attacks more convincing. Findings from MessageLabs confirm such a trend, by reporting an increase of targeted social engineering attacks, such as whaling (a focused form of 'spear-phishing', in which attackers specifically target top-level personnel within an organisation). Specifically, they report an increase of phishing attacks that are customised with personal information for specific individual targets, to make them more convincing (MessageLabs, 2007).



<sup>1</sup> The use in this context refers to 'vishing'; social engineering scams involving Voice over IP services.



# **Social Engineering dissected**



## Social Engineering dissected

Social engineering can be used in many forms to break security; from the simple (yet often successful) approaches in phishing and malware, to the more sophisticated attempts that target individuals directly. Yet, despite the different levels of effectiveness and sophistication, two aspects that are most likely to influence the success of social engineering attacks are the pretext, and level the background research that has been conducted. Of course, the other crucial factor will be the attacker's competence in then using these factors to change the perception of the target; whether they are doing it in writing, on the telephone, or in person, the attacker must have the ability to perform in a convincing manner.

### Perfecting a pretext

The pretext is the scenario that is devised by the social engineer, in order to trick potential victims to comply with their intentions. In the case of a malware variant, this can be as varied as an invitation to download free music of famous celebrities by following a link to an infected website, as was the case with the Storm botnet (Gaudin, 2007), or a plea to help victims of highly-publicised disasters such as the Tsunami that affected South East Asia in 2005 by opening an attachment (Sophos, 2005). In a more direct context, a social engineer could call a company's support desk with the pretext of being senior staff within the company and needing some urgent help to restore important services. In fact, a similar pretext was utilised in the highly-publicised hack against Paris Hilton's phone, where a T-Mobile employee was targeted to provide crucial confidential information (Krebs, 2005). The list of potential pretexts is effectively endless, and the more convincing and well-thought they are, the more successful the attack is likely to be.

### Getting the facts right

Another contributing factor to the success of social engineering is the supporting research that aims to make the pretext more convincing. From a social engineer's perspective, background research can provide a plethora of information regarding the target that could be used in carrying out an attack. For example, Granger (2001) cites dumpster diving, suggesting that an attacker may go through the paper waste produced by an organization to gain any general and confidential information that may be useful. While investigating a social engineer's research toolkit, Nolan and Levesque (2005) suggest that global search engines such as Google can provide much useful information regarding both organizations and individuals. Social networking sites are also very rich sources of information, given their nature and the wealth of personal information that they usually contain. Background research can include an initial investigation into the security controls and type of background information that is required in order to gain the victim's trust (Mitnick, 2006). The leads generated as part of this process may inform the research stage and help the social engineer to carry out a better planned attack.

The level of background research can vary in different contexts. For example, traditional phishing attacks often contain minimal background research, usually limited to making their messages and websites look authentic by imitating the vendor's original content. More advanced attacks follow more methodical approaches that often involve extensive

planning and background research (Mitnick and Simon, 2002). Indeed, just because we are regularly confronted with blatantly obvious and indiscriminate phishing attempts (e.g. those impersonating banks, which are sent out to all and sundry regardless of whether they have an account with the bank concerned), we should not underestimate the effort that determined social engineers are willing to devote in order to obtain information, or the variety of sources available to them. In fact, this is evidenced already by the recent increase of targeted phishing attacks that utilise personal information (e.g. recipient's name and job title) as part of the messages (Messagelabs, 2007).

### Timing is everything

In some cases, however, it is not so much a question of background research as the timing of the attack. Scammers and malware writers are very adept at tuning into current events as a means of duping users into compliance. The aforementioned Tsunami incident is one such example, while a worm distributed on Christmas Eve 2007 purporting to offer a Santa Claus-themed striptease was another (Sophos, 2007a)

### Exploiting psychology

Social engineering may involve both psychological and technological ploys in order to leverage the trust of the target. From a psychological perspective, the attacker can exploit several characteristics of human behaviour in order to increase the chances of the intended victim doing what is desired. For example, Cialdini (2000) identifies six basic principles that may influence an individual to comply with a request:

- Authority – the attacker achieves the desired response from the target by making an assertion of authority.
- Commitment and consistency – targets are likely to act consistently with past behaviour, and in accordance with things they have committed to.
- Liking and similarity – the attacker exploits the fact that targets are more likely to respond to someone they like, or perceive to be similar to themselves.
- Reciprocation – the target is given something, in the hope that they will feel obliged to reciprocate by giving something in return.
- Scarcity – the target is led to believe that something they desire is in short supply or only available for a limited period. The target may consequently feel obliged to act quickly and possibly without sufficient prior thought.
- Social validation – targets may base their decision upon the behaviour of others (increasing the chances of a request being complied with by claiming that other people have already done the same thing).

While Cialdini's principles are presented in a general context, several other authors identify related factors within the IT domain. For example, Stevens (2000) refers to behavioural traits such as 'conformity' and the 'desire to be helpful', while Jordan and Goudey (2005) refer to factors of 'inexperience' and 'curiosity' that may be exploited. In the particular context of phishing attacks, these influential methods can be implemented through the technique of semantic deception (Fette *et al.* 2006) which is achieved through the language used in the text body of an email.

### Social Engineering – Exploiting the Weakest Links

#### Exploiting technology

In contexts such as phishing and malware, psychological methods are often accompanied by further ploys achieved via technical means. For example, phishing emails often involve spoofing of email addresses and masking of fraudulent URLs, and are typically accompanied by the construction of a bogus web site (potentially using markup and images stolen from the legitimate version). Once at such sites, visitors may find them to be spoofing security indicators, such as the padlock icon to denote a secure session or using faked images of VeriSign and TRUSTe seals (essentially exploiting the victim's ignorance of how the technology *should* work, in order to give a surface impression of protection). Alternatively, attackers wishing to deploy malware will often use social engineering methods to trick users into running it. This is a widely-utilised technique in the dissemination of worms and Trojan horses, with a classic example being the Love Bug worm from May 2000, which fooled users into opening a worm attachment by pretending to be a love letter. Moreover, in some cases all that social engineering is required to do is bait the user into viewing a message; direct exploitation of a vulnerability in the browser or mail client can then do the rest.





# **Assessing susceptibility to social engineering**



## Assessing susceptibility to social engineering

This section examines the extent to which users are able to judge and identify social engineering attempts, drawing specifically upon three studies all taken from amongst the authors' own research activities. It should be noted that the focus is placed upon email-based attacks, on the basis that this is the context in which the majority of users are likely to come into contact with social engineering (i.e. as a result of its use in connection with threats such as phishing and malware).

### Case Study 1 - Spotting the difference

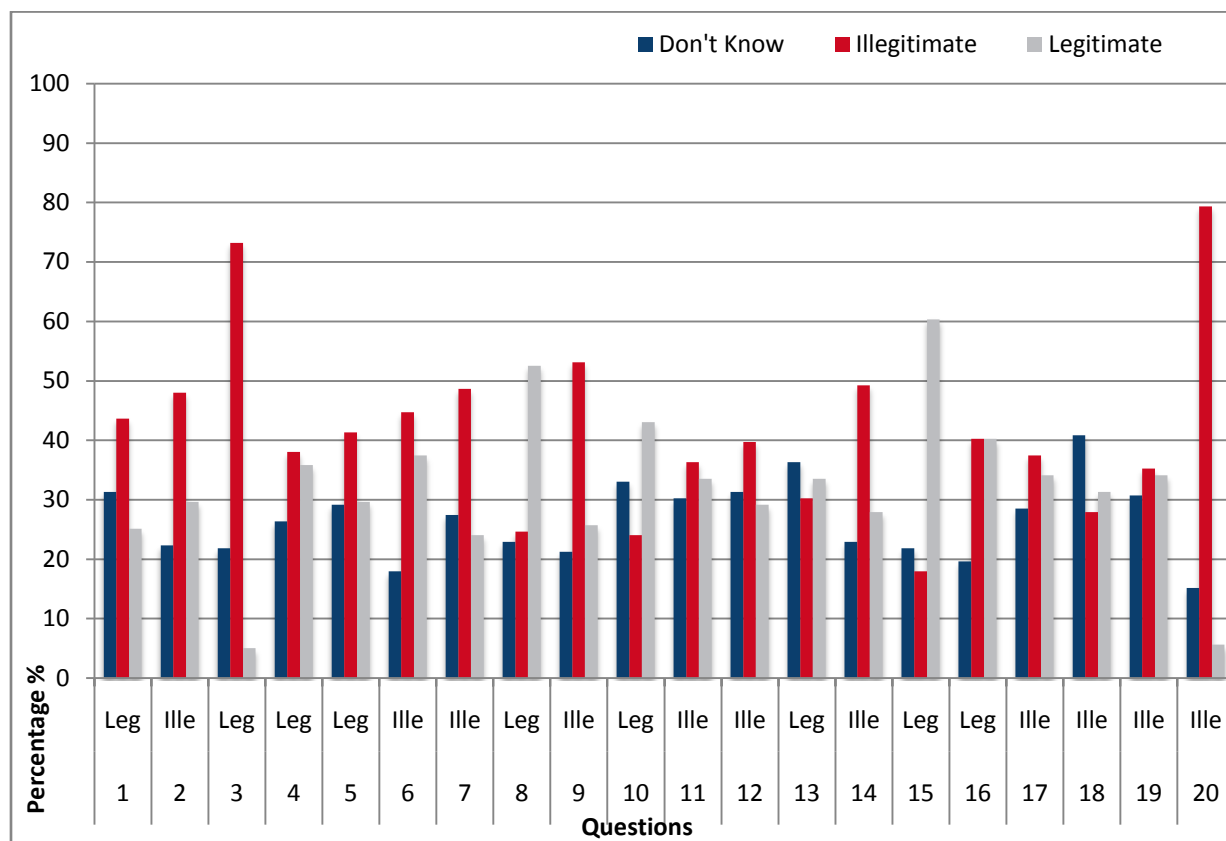
The first study concerned the ability to recognise phishing messages, and aimed to assess users' ability to differentiate between genuine messages and bogus ones on the basis of appearance alone (Karakasiliotis *et al.* 2007), with prior research from Dhamija *et al.* (2006) revealing that 25% of users look at no more than this in order to judge whether a message is legitimate. A total of 179 participants participated in an online survey, and were explicitly aware that they were being asked to identify the phishing messages.

The aim was to enable an insight into the criteria that they used in order to reach their decisions. In common with previous studies (Robila and Ragucci 2006, Dhamija *et al.* 2006) the investigation focused on the email part of the phishing attack, and a set of 20 messages (11 illegitimate and 9 legitimate) were selected for inclusion. These were gathered from a combination of websites showing phishing-related examples, as well as emails that the investigators had personally received. Collectively, the messages covered a range of legitimate



topics commonly encountered by Internet users, as well as typical ploys used by attackers. In each case, respondents could choose one of three options ('illegitimate', 'legitimate' and 'don't know', with the latter being set as the default), and could optionally complete a text box to explain their reasoning.

The overall findings are shown in Figure 1, which depicts the judgements recorded for each of the 20 messages (with the x-axis indicating which messages were legitimate (Leg) or illegitimate (Ille)). A key observation is that, in most cases, opinions were very much divided. Although there are a few instances in which a clear majority preference was established, these were not always drawing the correct conclusion (e.g. in the case of message 3, over 70% considered it illegitimate when in actual fact it was genuine). This clearly shows that many users typically face a difficult task to differentiate between a genuine email and a bogus one based upon appearance and content alone.



**Figure 1: Overall ability to judge legitimacy of email messages**

The overall level of correct classification (for example indicating 'legitimate' for genuine messages and 'illegitimate' for bogus ones) was 42%, while misclassification was 32%. This, alongside the additional 26% of 'don't know' responses, clearly illustrates the level of confusion amongst the participants (Table 1). Analysing subsets of the participants based upon the demographics we established that there were no significant differences relating to gender, age, or nationality. The results did, however, reveal that the participants were more prone to misclassifying legitimate messages, potentially suggesting that the phishing threat (and possibly the survey exercise itself) causes a heightened level of suspicion.

	Correctly classified	Incorrectly classified	Don't Know
Legitimate messages	36%	37%	27%
Illegitimate messages	45%	28%	26%
Overall	42%	32%	26%

**Table 1: Accuracy of message classification**

## Social Engineering – Exploiting the Weakest Links

Having looked at the overall results, it is interesting to consider some of the specific cases in which participants encountered difficulty. From Figure 1 it is clear that notable examples were Message 3 (a legitimate email that the vast majority considered illegitimate) and Message 18 (a bogus message that more respondents judged to be genuine). With this in mind, the messages themselves are depicted in Figure 2 (a) and (b) respectively. In the first case, it becomes apparent that respondents were suspicious of the message even though it targeted a named recipient and had an identifiable sender. From the participants' written comments it was apparent that the primary influence here was plaintext appearance, accompanied by the urgency of the language (which respondents were inclined to associate with scams rather than legitimate business). A further factor was the fact that the address listed in the message bore no obvious relationship to the company name listed in the signature. Meanwhile, the misjudgement of Figure 2(b) was led by the fact that it seemed to come from leftfield; most respondents did not recognise the context as one likely to be associated with phishing activities.

(a)

Message 3 - legitimate email that the vast majority considered illegitimate

(b)

Message 18 - bogus message that was misjudged as genuine

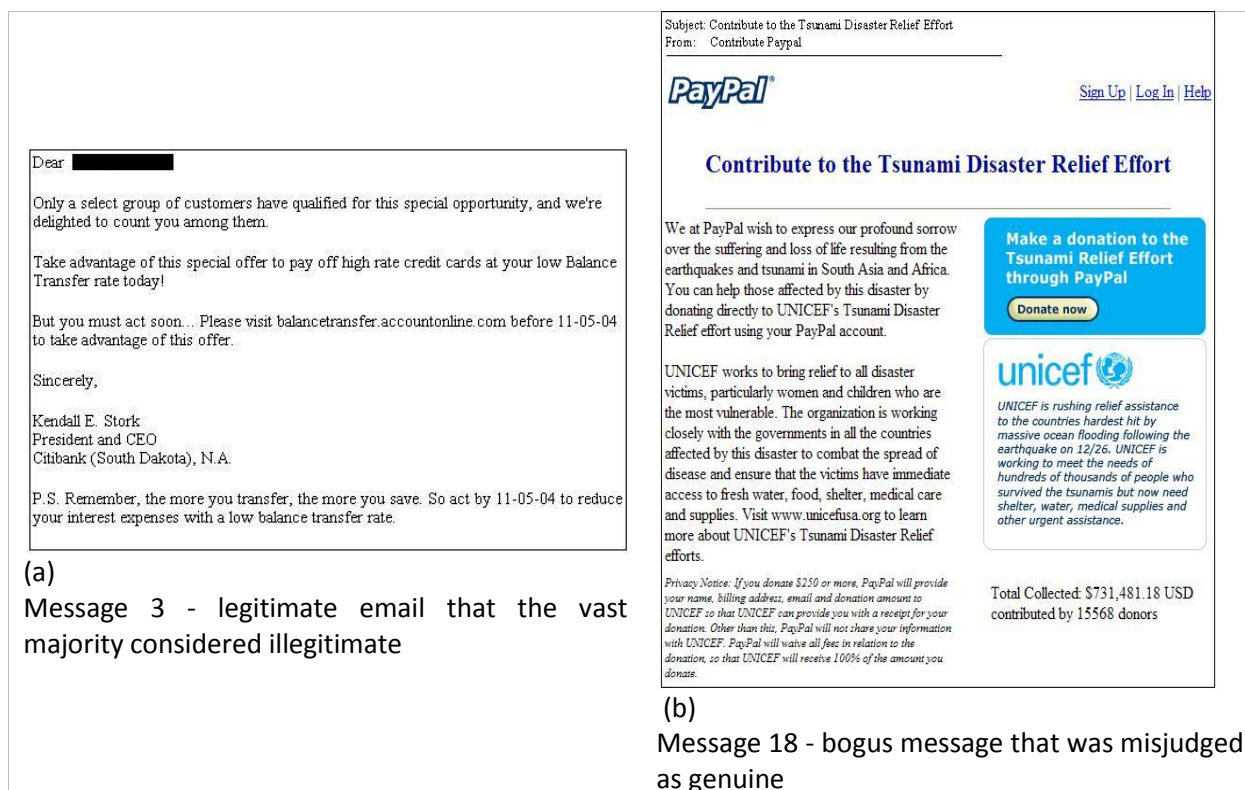


Figure 2 consists of two side-by-side screenshots of email messages. Screenshot (a) on the left shows an email from Citibank (South Dakota), N.A. addressed to 'Dear [redacted]'. The email body contains promotional text about a special opportunity to pay off high rate credit cards at a low balance transfer rate, with a deadline of 11-05-04. The signature is Kendall E. Stork, President and CEO of Citibank (South Dakota), N.A. Screenshot (b) on the right shows an email from PayPal titled 'Contribute to the Tsunami Disaster Relief Effort'. The email body expresses sorrow over the suffering and loss of life resulting from earthquakes and tsunamis in South Asia and Africa, and asks for a donation to UNICEF's Tsunami Disaster Relief effort using the PayPal account. It includes the PayPal logo, a 'Donate now' button, and a UNICEF logo with a brief description of the relief effort. The email also includes a privacy notice and a total collected amount of \$731,481.18 USD contributed by 15568 donors.

**Figure 2: Examples of messages used in the phishing recognition study**

The findings from this study can be compared to those from other experimental work. For example, Robila and Ragucci (2006) discovered that, on average, their 48 participants were able to correctly identify 60% of legitimate messages and 53% of illegitimate ones. However, it should be noted that this study used a different set of email questions, and did not include the option for participants to select a 'don't know' option. The latter was considered to be a useful inclusion in our work, as it meant that respondents were not

obliged to form an opinion one way or the other, and therefore any instances in which they did opt to select 'legitimate' or 'illegitimate' meant they felt fairly sure of the situation. A recognised limitation of both studies was that the participants were only able to judge legitimacy from the content and appearance of the messages, whereas in reality they would also be able to draw upon the context in which it was received (e.g. receiving a request to verify bank account details would obviously raise more suspicion if it came from a bank that they did not use).

However, in some cases the brand or service named in the faked message will happen to coincide with one that the recipient actually uses, or (as with the message relating to the tsunami donations) will not rely upon the recipient having a prior association with the impersonated brand). In these situations the findings demonstrate that distinguishing between genuine messages and bogus ones becomes somewhat more challenging.

### **Case Study 2 – Even bad bait catches something**

In order to conduct more realistic tests of susceptibility, the authors have utilised more direct experiments, in which genuine social engineering attempts were mounted against target user communities. One such example involved staff within a participating organisation, in which the IT department was interested to assess the extent to which its users were vulnerable to email-based attacks (Bakhshi *et al.* 2008). The premise of this experiment was a message, claiming to come from the IT department, instructing users to install a software update from an accompanying website.

This topic was specifically chosen as something that recipients would be unlikely to feel the need to share and discuss with others, particularly outside the organisation. This was considered important, in order to avoid the risk of creating an incident that could spread into the public domain; which could certainly have been the case if the premise of the study was something unspecific to the target organisation, such as a virus warning, etc. The text of the message is shown in Figure 3 (albeit with some of the content blacked out in order to conceal the name of the organisation involved and the nature of its business), and all of the information used to facilitate the 'attack' was based upon details that an external party could discover from the organisation's website.





## Social Engineering – Exploiting the Weakest Links

Sub: Important Software Upgrade

From: [REDACTED]

Sent: 7 November 2007 15:02

To: [REDACTED]

Dear staff member

The workstations within [REDACTED] are going important software upgrades. New software packages are being added to existing systems for facilitation in [REDACTED]. This is in line with [REDACTED]'s policy to provide best [REDACTED] experience for [REDACTED] staff. These upgrade packages would in due time replace legacy systems or older versions of these packages. Up-to-date knowledge regarding which new software are being added and how these may help you in your [REDACTED] experience is necessary. Since these upgraded applications would help you with your daily duties it is important that you go through the few details associated with the functionality and scope of these software applications. Please click on the following link to view specific details relating to this important software upgrade.

Secure Link: [REDACTED] [Software Upgrade](#)

Thank you for your cooperation.

Best regards

[REDACTED]

--

[REDACTED]@eml.cc

<http://www.fastmail.fm> – Access all your messages and folders wherever you are.

**Figure 3: Encouraging staff to install a software upgrade**

Although the attempt included several hallmarks of social engineering (e.g. an attention-grabbing subject, an assertion of authority, and a claimed benefit to the recipient), the email intentionally included several indications that should have raised suspicions:

- the wording of the message was grammatically dubious and therefore unprofessional;
- the 'from' email address was not a genuine address within the organisation;
- the message signature cited the IT department in general rather than a named individual;
- an external address was being used as both the source of the message and as the host of the website they were being directed to.

In addition, a further fundamental point is that staff should have been aware that the IT department did not issue or communicate with them about software upgrades in this way. In spite of these points, however, 35 of the 152 recipients (approximately 23%) proceeded to follow the link and visit the associated website in an attempt to download the suggested 'upgrade'. This demonstrates that users will often act in haste and in compliance with perceived authority.

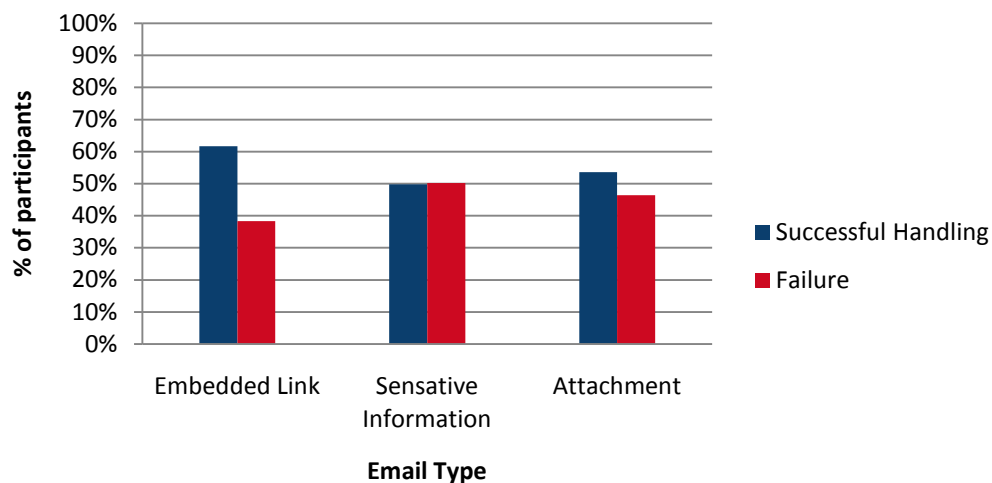
### Case Study 3 – Awareness-raising works

A further study, completed over the span of three years at an undergraduate college, indicated that students were initially highly susceptible to spear phishing attacks, but that training and awareness programmes greatly reduced the rate at which they fell victim to

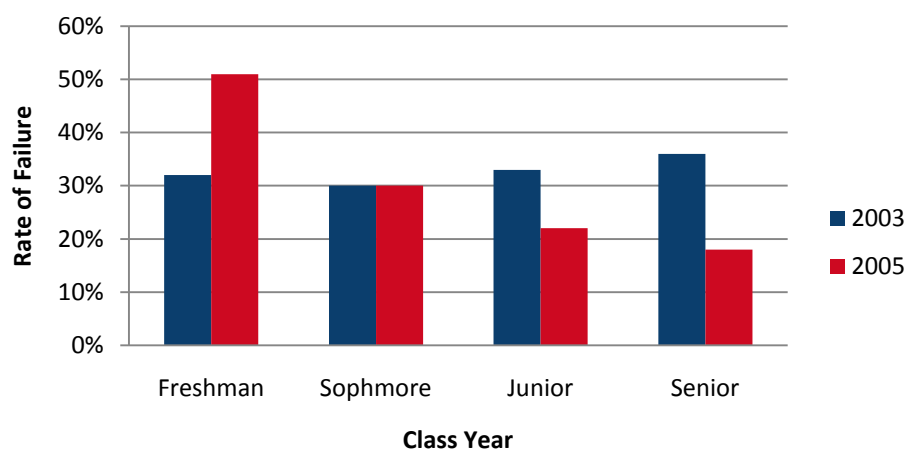
fraudulent emails (Dodge et al. 2007). In this study a collection of students were sampled from each class year to evaluate the response rate to three attack vectors:

1. following an embedded URL;
2. entering sensitive data in an online form; and
3. opening an attachment.

Case one and case two both relied on the student following the embedded URL within the received message. In case two, the data was analyzed to obtain the rate at which students entered sensitive data in the online form. The aggregated results for all cases are shown in Figure 4 and 5.



**Figure 4 Aggregate Email Phishing Results by Email Type over Three Years**



**Figure 5: Aggregated Phishing Email Results Over Three Years**



### Social Engineering – Exploiting the Weakest Links

The execution of the exercise was accompanied by a training and awareness programme, designed with the intent of reducing the vulnerability of students to fall victim to the spear phishing attacks. As can be hypothesised from the results in Figure 5, the rate of failure for a population of users did decrease the more they were exposed to the training and awareness training.

For anyone considering similar assessments, it should be stressed that neither these experiments nor those from Case Study 2 were undertaken lightly, and were carefully planned in advance within the organisations concerned. Ethics approval for the experiments was sought and obtained, including recognition of the need to deceive participants, who would not know in advance that they were participating. Approval was granted on the basis that the underlying intention of the study was awareness-raising, and therefore to the benefit of the organisation and the user community, rather than just using them as guinea pigs to make a point.



# Recommendations



## Recommendations

Having identified the problems and presented some specific evidence of the difficulties involved, this section proceeds to consider how social engineering threats might be tackled.

### Technology-based mechanisms

As observed at the start of the paper, technical safeguards represent the most common response to security issues. Indeed, technology can provide assistance in some social engineering contexts; most notably scenarios such as phishing and malware, where the attempt arrives via electronic means.

A variety of measures can limit the effectiveness of phishing. For example, enabling phishing filter functionality within web browsers can shield end-users from known phishing sites and suspicious characteristics. If service providers are able to take a more active stance, then the incorporation of intelligent tokens or mobile devices into the authentication process will undermine the ability for phishers to acquire the necessary user credentials through social engineering methods. Similarly, effective and up-to-date antivirus protection should enable the identification and restriction of malware regardless of well-crafted solicitations to the user to open it.

Unfortunately, although it may provide some help, it must be recognised that technology will not be a complete solution and can only deliver viable protection in a sub-set of the possible scenarios in which users will be at risk. It will not, for example, be able to safeguard against attempts that occur in person or over the phone. Equally, it will not prevent more extreme forms malware-based attack (e.g. using social engineering alongside a custom Trojan for which the antivirus protection could not be expected to have a signature). As such, it must be recognised that, because social engineering targets people, the threat can only be fully addressed by people-based mechanisms.

### Improving user awareness

User education must certainly have a part to play. However, as the evidence shows, it is unlikely that users can be explicitly trained on how to identify social engineering and phishing in all their guises. It is certainly true that they can be trained up to a point; for example, today's widespread awareness of the dangers with unsolicited email attachments demonstrates that users *can* exercise caution with things that they have been told to be wary of. This hypothesis is supported by the results obtained by Dodge and Ferguson (2006). However, expecting to provide specific advice for all contexts is unrealistic, and we cannot rely upon users to keep themselves up-to-date or to adequately generalise their knowledge in one scenario to suit others. In addition, it is recognised that the effectiveness of training will attenuate over time, and so the less that users are required to explicitly remember the better it will be. Therefore, in order to aid the situation, we propose a simple list of questions that users ought to ask themselves when confronted with information requests that they are in any way unsure of. Indeed, users should only need to remember that there is a LIST of issues (namely Legitimacy, Importance, Source and Timing) in order to help to remember the questions concerned:

Legitimacy	Does the request seem legitimate and usual? For example, should you be asked for this information, and is this how you should normally provide it?
Importance	What is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused?
Source	Are you confident that the source of the request is genuine? Can you find a way to check?
Timing	Do you have to respond now? If you still have doubts, take time to make further checks or ask for help.

**Figure 6: LIST of issues and questions**

The above checks should be applied in both workplace and personal scenarios, and should provide a useful basis for assessing a request before responding to it. Of course, they are not foolproof and there may still be judgements that are not clear-cut. For example, a surface impression of 'legitimacy' may be easily achieved (after all, if something seemed clearly illegitimate then that would be point enough to stop) and this question requires people to give a deeper level of consideration in order to answer it properly. Similarly, some users may have difficulty judging a factor such as 'importance' unless they are being asked to provide overtly sensitive information such as a password. Nonetheless, if users are confident having run through the LIST, then one can still be assured that they have applied some key criteria, and also that they have taken time to consider the situation rather than just providing an immediate and instinctive response.

### Understanding the real routes

In addition to getting them to spot the hallmarks of problems, another useful awareness strategy is to emphasise the ways in which activities will *legitimately* occur. For example, no matter how convincing the messages may look, the fact that many banks now directly tell their customers that they will *not* contact them by email should effectively pull the rug out from under phishing attempts via this route. The reason that such attempts continue to be successful reflects the fact that users are not sufficiently aware of how things are *meant* to happen. Thus, ensuring an understanding of policies and correct routes will help to prevent them from being caught out. Having said this, users also need to be aware of the contexts in which risks will remain. For example, Soghoian *et al*'s (2008) assessment of political phishing recognises that despite the risks of fraudsters exploiting in this context, the legitimate politicians still *want* to continue to make contact and solicit donations by email, because they actively benefit from the immediacy of the medium (i.e. the fact that recipients may respond on instinct rather than being required to go through several steps to make a donation; which may reduce their likelihood of seeing the process through). Meanwhile, the context itself provides a rich opportunity for phishers; given that legitimate donation requests arrive by email and users who respond expect little more than an acknowledgement that they have made a donation, someone duped into 'donating' in response to a bogus message is unlikely to be any the wiser.

### **Appreciating the value of information**

Users also need to be more aware of their own data and why it is sensitive. For example, there is significant potential for data-scraping from social networking sites such as Facebook and MySpace, with attackers lifting information that users themselves have placed there with little regard for who could see it and how it could be misused. User pages on the aforementioned sites are often littered with details such as dates of birth, addresses, personal interests, family background and employment details, with many users exercising no caution in how widely they share it (Sophos, 2007b). This can work against the individual in both personal and workplace scenarios, with the consequence that they could end up being convinced that someone knows enough about them to be trusted purely by virtue of the details that they themselves have made publically available online.

From a similar perspective, organisations need to consider what they do with information – including what they dispose of and what they put on public display. To what extent are they rendering their own staff more susceptible to social engineering by making details available that someone else could use in an attempt to deceive them? For example, listing things like staff names and roles on a website gives a would-be attacker an immediate insight into who can be contacted for what, and whose name could be dropped in to add legitimacy (“Is that Mr Jones in the Finance Department? Your IT Director, Mr Smith, asked me to call you to discuss your experience with the accounting software we’ve provided ...”).

### **Performing practical assessments**

Finally, taking a more active stance, practical testing and demonstration of users’ vulnerability can have value, if conducted in an ethically-sensitive manner. Findings from the authors’ ‘software upgrade’ study demonstrated that many users were actually appreciative of being alerted in this way rather than falling victim to a genuine incident, and the following quotes are examples of comments received by email once users were made aware that the test had been conducted:

*“You got me! And that is a bit of a wake-up call for me, as I like to believe that I know what I am doing, in terms of not opening emails that look suspicious, and looking at where links take me before I click them. It just goes to show....”*

*“Very nifty, one always looks out for phishing using the identity of banks and other large corporations, but one never expects [the IT department] to be misused for these purposes. I almost fired off an email to [the IT department] to complain about their unprofessionalism. Well done!”*

Equally, however, there is a clear potential for such tests to generate problems. Indeed, prior to the comments above, a number of users had contacted the IT department to complain about the original message, either because they perceived it to be genuine (and therefore considered the IT department to be unprofessional for having sent it) or because they actually suspected it to be bogus and wanted the IT department to warn others. As a consequence the IT department became nervous about continuing the experiment, and study was terminated early in case such responses were poised to become the beginning of an onslaught of criticism. The inherent difficulties perhaps explain why such approaches are not used very extensively; for example, only 13% of the 475 respondents in the CSI’s



2007 Computer Crime & Security Survey indicated that they tested the effectiveness of their security training by seeing whether employees could spot internally-generated social engineering attacks (CSI, 2007).

## Conclusions

In conclusion, with deception, fraud and confidence tricks all predating the appearance of IT, it is clear that social engineering is a problem that is not about to disappear. The fact that IT provides a variety of channels through which it can be conducted, and the fact that it is proving itself to have utility in a variety of contexts – from hacking and malware through to identity theft and other fraud – clearly means that the threat is more likely to grow than to diminish. With this in mind, if we cannot eradicate it then we need to manage and control it, reducing our risk and exposure in the same way that we handle many other types of security threat. This requires action that addresses users as individuals, in both their personal and workplace contexts (indeed, boosting their awareness in one context is very likely to have a beneficial effect in the other). None of it will necessarily provide a safeguard against the most determined and devious attackers, but the effective removal of the low-hanging fruit would at least make the pickings for the rest a lot less rewarding.



## References

- APWG. 2008. *Phishing Activity Trends - Report for the Month of January, 2008*. Anti-Phishing Working Group. [http://www.apwg.org/reports/apwg\\_report\\_jan\\_2008.pdf](http://www.apwg.org/reports/apwg_report_jan_2008.pdf) (accessed 26 July 2008).
- Bakhshi, T., Papadaki, M. and Furnell, S.M. 2008. "A Practical Assessment of Social Engineering Vulnerabilities", in *Proceedings of the Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008)*, Plymouth, UK, 8-9 July 2008, pp12-23.
- Cialdini, R.B. 2000. *Influence: Science and Practice (4th edition)*, Allyn & Bacon.
- CSI. 2007. *CSI Survey 2007 - The 12th Annual Computer Crime and Security Survey*. Computer Security Institute. GoCSI.com.
- Dhamija, R., Tygar, J.D. and Hearst, M. 2006. "Why Phishing Works", in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, Montréal, Québec, Canada: 581-590.
- Dodge, R.C., Carver, C. and Ferguson, A.J. 2007. "Phishing for User Security Awareness", *Computers & Security*, vol. 26, no. 1, pp73-80.
- Fette, I., Sadeh, N. and Cranor, L. 2006. "Web Security Requirements: A Phishing Perspective", W3C Workshop on Transparency and Usability of Web Authentication New York City, USA, 15-16 March 2006. <http://www.w3.org/2005/Security/usability-ws/papers/13-cmu-requirements/> (accessed 26 July 2008).
- Gaudin, S. 2007. "After Short Break, Storm Worm Fires Back Up With New Tricks", *InformationWeek Magazine*, 4 September 2007. <http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201803920> (accessed 26 July 2008).
- Granger, S. 2001. "Social Engineering Fundamentals, Part I: Hacker Tactics", *SecurityFocus*, 18 December 2001. <http://www.securityfocus.com/infocus/1527> (accessed 26 July 2008).
- Jordan, M. and Gouday, H. 2005. "The Signs, Signifiers and Semiotics of the Successful Semantic Attack", *Proceedings of 14th Annual EICAR Conference*, St.Julians/Valletta, Malta, 30 April – 2 May 2005, pp344-364.
- Karakasiliotis, A., Furnell, S.M. and Papadaki, M. 2007. "An assessment of end-user vulnerability to phishing attacks", *Journal of Information Warfare*, vol. 6, no. 1, pp.17-28.
- Koumpis, C., Farrell, G., May, A., Mailley, J., Maguire, M. and Sdralia, V. 2007. "To Err is Human, to Design-Out Divine: Reducing Human Error as a Cause of Cyber Security



Breaches”, Human Factors Working Group - Complimentary White Paper, Cyber Security Knowledge Transfer Network, United Kingdom.

Krebs, B. 2005. “Paris Hilton Hack Started with Old-Fashioned Con”, *The Washington Post*, 19 May 2005. <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711.html> (accessed 26 July 2008).

Nolan, J. and Levesque, M. 2005. “Hacking human: data-archaeology and surveillance in social networks”, *ACM SIGGROUP Bulletin*, vol. 25, no. 2, pp33-37.

McAfee. 2008. “McAfee, Inc. Experiment Reveals the Growing Psychological Nature of Spam”, Press Release, McAfee, Inc. 1 July 2008.  
[http://www.mcafee.com/us/about/press/corporate/2008/20080701\\_181015\\_c.html](http://www.mcafee.com/us/about/press/corporate/2008/20080701_181015_c.html) (accessed 26 July 2008).

MessageLabs. 2007. *MessageLabs Intelligence: 2007 Annual Security Report*, MessageLabs Intelligence Reports, December 2007.  
[http://www.messagelabs.com/mlireport/MLI\\_2007\\_Annual\\_Security\\_Report.pdf](http://www.messagelabs.com/mlireport/MLI_2007_Annual_Security_Report.pdf) (accessed 26 July 2008).

Microsoft. 2006. “Midsize Business Security Guidance: How to Protect Insiders from Social Engineering Threats”, Microsoft TechNet, August 2006.  
<http://www.microsoft.com/technet/security/midsizebusiness/default.mspx> (accessed 26 July 2008).

Mitnick, K.D. and Simon, W.L. 2002, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley publishing, Inc.

Mitnick, K. 2006. “The Art of Deception”, Presentation at CSC Executive Exchange, 5-8 November 2006. <http://www.kevinmitnick.com/media/CSC-Testimonial.pdf> (accessed 26 July 2008).

Robila, S.A. and Ragucci, J.W. 2006. “Don’t be a Phish: Steps in User Education”, *ACM SIGCSE Bulletin*, vol. 38, no. 3, pp237-241.

Soghoian, C., Friedrichs, O. and Jakobsson, M. 2008. “The Threat of Political Phishing”, in *Proceedings of the Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008)*, Plymouth, UK, 8-9 July 2008, pp126-143.

Sophos. 2005 “Tsunami disaster donation plea is really a virus, Sophos reports”, Press Release, Sophos, 17 January 2005.  
[http://www.sophos.com/pressoffice/news/articles/2005/01/va\\_vbsuna.html](http://www.sophos.com/pressoffice/news/articles/2005/01/va_vbsuna.html) (accessed 26 July 2008).

Sophos. 2007a. “Santa’s virus striptease goes down a Storm, warns Sophos”, Press Release, Sophos, 24 December 2007.  
<http://www.sophos.com/pressoffice/news/articles/2007/12/santa-storm.html> (accessed 26 July 2008).

### Social Engineering – Exploiting the Weakest Links

---

Sophos. 2007b. "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves", Press Release, Sophos, 14 August 2007.  
<http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html> (accessed 26 July 2008).

Stevens, G. 2002. "Enhancing Defenses Against Social Engineering", SANS Institute, GIAC,  
[http://www.giac.org/certified\\_professionals/practicals/GSEC/570.php](http://www.giac.org/certified_professionals/practicals/GSEC/570.php) (accessed 26 July 2008).

## **Interview with Kevin Mitnick**



## Appendix: An ENISA Awareness Raising Community interview with Kevin Mitnick

Supporting the Whitepaper, the authors spoke to security author, speaker, and consultant Kevin Mitnick about users' susceptibility to the threat and what can be done about it.

**Authors:** Given that social engineering has been recognised for many years, how has the threat evolved, and do you think it is properly understood by potential victims?

**Kevin Mitnick:** I think social engineering has become more prevalent because you have the security technologies that make it more difficult to exploit technical vulnerabilities, and fraud is like a bubble; when you press down on it in one place it pops up somewhere else. So, the more technologies and processes are out there to mitigate the technical hacking, the more you are going to have people that will resort to social engineering. Social engineering is often easier, and I think the threat has grown because software manufacturers have become more concerned about putting out the patches and about fixing technical holes, because of the negative press. So again, what will the attackers resort to? Social engineering! Then you might have attackers that are not so technically astute, who might use social engineering in any event.

It is understood by *some* potential victims, but only the people who are already aware that social engineering exists and the types of approaches that social engineers will make. The majority of people out there are *not* aware of what social engineering is, because a lot of companies don't train people on this type of attack.

**Do you think people have become any more aware of the problem?**

Only the people who have been trained or that have seen it played out in the press. I think more people are aware of it now than they were in the 1990s because of the companies adopting security awareness programs, and high profile attacks like my own, which would have been played out in the press. I don't know if people equate social engineering with the Nigerian fraud scams, but I don't think so. I think people put them in different buckets. When someone is trying to scam me out of money or property by conning me I think that's in a different bucket than somebody trying to trick me into visiting a website that will exploit a browser vulnerability, that will plant malware into my machine, or that will have access to the internal network of the company. I don't think people connect those two.

**What is the most important message to put across to people?**

There a lot of messages, like the different attack strategies, when attackers are trying to trick somebody into planting malware into a machine, that will reveal confidential

information, that will do some sort of action that will appear to be innocuous, that allows the attacker to be successful. I think the most important message is that social engineering exists and there are people out there that will try to con and manipulate you to target corporate resources and your own personal information. I think that if there's a way of putting it in the context where the potential victim has some sort of self-interest, where it could negatively affect them, I think they'll be more motivated to pay attention to the message. More people are concerned about their self-interest than an attacker possibly getting information from their company.

**Are there any awareness raising strategies that are particularly successful at conveying this message?**

Yes, when I do my social engineering workshops, I put the audience into particular situations, in kind of role play, to see how they'll pan out. So, in other words you set up an interactive game or an interactive role playing exercise that will test the delegate's response to how they would respond to a particular request. And then if that person makes a mistake then we're able to correct it, or if they respond to it properly you give them their attaboys. So, I think actually the role playing and the interactive games, where the victim is put into the types of situations that social engineers normally will try to exploit, are usually more effective.

You could tell somebody "Oh, this person got scammed by the Nigerians and sent out 2 million dollars of the company's money because they were going to get a return of 30 million"; That's all nice. Or "Social engineers will call you up for your password"; I think there are many different companies that put a warning they will never call you for your password, but that really isn't effective. They really need to make the training interactive and put the trainee into the situation, into a role playing exercise and to determine how that trainee will react. You could then correct any incorrect responses, or just to see how they would actually respond.

It's still kind of difficult though because in a training class people are much more aware. When they're at work, trying to get their jobs done and they're on time pressure and there's other circumstances going on, it's much easier to convince the target to take a mental shortcut to just comply. So there's a difference between classroom environment and an attacker doing it in real time. But this is all we have to work with at the moment. For example, when I do my social engineering workshops, and I have all the delegates gathered into a hotel, I kind of burn them the night before, where someone will call their hotel room pretending to be the front desk, to say that their credit card credential didn't go through or they were declined. Later on they get a call from their credit card company claiming 'you need to come down and straighten this out', but it's late at night and the delegate is usually in bed. What will happen is the hotel will offer to send up an employee with a form that they will have to fill out. It might have just a *little* bit of personal information that they will have to fill out, and then they can handle the rest of it in the morning. We found by doing this exercise that most of the delegates will go ahead and fill out the form because the person that actually knocks on their doors is wearing the hotel uniform. And then we will hand out those forms in class to show how we were able to burn them the night before, because they were unaware of the attack.

---

#### **Which technique presents the most critical threat, and which one do you believe is the highest volume threat?**

Well, the highest volume would be a technique used in a worm, because then you're going to have a high volume problem. That's usually tricking the target to follow a hyperlink that goes to a site that hosts malicious software that exploits a browser vulnerability or even an email client vulnerability. You're going to target more people, more victims.

As for critical threats, I would say that two types of attacks are quite interesting. The USB attack, where the attacker plants doctored USB drives and they trick the user into plugging that in a home computer or a corporate machine, which executes malware. This is usually effective, even in corporate environments, because they leave autorun on. But also the new types of vishing attacks where the attacker is able to be the man in the middle. That's pretty critical because it's really difficult to detect, especially if an attacker doesn't rely on the victim calling a number that belongs to the attacker, but they're able to access the telephone switch and actually redirect the calls to go to the attacker's equipment and then route to the victim's equipment. So the attacker is truly the man in the middle and the caller is unaware. That's pretty critical.

As far as the *most* critical threat, it's where the attacker uses a social engineering attack that infects many people with malware. I think it goes to the critical and for the highest volume threat.

#### **What do you believe is the greatest opportunity for short term success on combating social engineering?**

Using technology whenever possible to remove the decision making process of potential targets. In my experience, it's not feasible to think that in the short term we could immediately remediate that threat. The greatest opportunity for short term success is using technology whenever we can and to immediately have a security awareness training programme that educates people about these threats and the typical methodologies that are being used by social engineers. I go around the world speaking about social engineering all the time and a lot of people out there in these audiences have no idea about what caller id spoofing is. And this is such an old form of hacking that's been around for years in the hacking community, or the phone phreaking community, yet the average person on the street does not know it exists. So I think the greatest opportunity is education and training, and using technology whenever possible to remove the decision making process.

The truth of the matter is most of the successful attacks are hybrid: you combine social engineering with exploiting technical vulnerabilities. And that's where it gets really difficult to remediate, because the attackers are using social engineering when it's expedient and in other cases when they can do it through purely technical means, they'll do that. Like for example, if an attacker breaks into a company that has hundreds of servers, and the attacker is targeting a particular piece of information. They may use a technical vulnerability to breach the network and use social engineering to find out what server on the network has the information that they want to steal. So, because the attacker is

already on the network their requests may seem innocuous to an employee: “So what if I give out the name of the server that contains our marketing materials to someone who I think is an employee, because they sound like an employee, they come with an employee extension on my caller ID?”. How do you remediate that? It’s really difficult, because if an attacker spends the time and resources to do it right, they’re going to really look like internal. When I used to do these attacks, I used to set up my own phone extension in the corporate environment. I would phone the telephone department, using social engineering again because they would never expect it, and I would have my own telephone extension in the corporation, in their electronic telephone directory. So when I called somebody, that’d be coming from a legitimate extension within the corporation and they could call me back and leave messages on voicemail. That is such a believable scenario, how do you train somebody, or how do you create such a paranoia level that changes the corporate culture to be so paranoid to even be questioning people that appear to be so legitimate. So, it’s really hard to balance the problem.

So, what we’re talking about here is helping organisations and maybe some citizens not to become the low hanging fruit for the average social engineer. In that respect, it’s a lot easier problem to conquer, but what I’m thinking about is somebody sophisticated that sets up their own extension within the organisation, is listed in the electronic records of the directory in the internal website... what do you do? That’s tough. How do you verify employees? Is it always a static way where you always ask the same questions, or the same process of calling them back? In my own experience with the telephone companies, each phone company has a division called the Non-Pub Bureau, at least this is how it used to be with the Baby Bells and knowing that their process of authenticating a caller was always to call them back at a number listed in the company directory . So the way to exploit their process was simply to setup a telephone number in the corporate directory, or to actually use the call forwarding feature on somebody who already existed and anytime you can be called back, there’s no other questions asked, you’re legit. So, once the attacker is able to map out the processes used by an organisation to verify the identity of a caller, they’re able to manipulate it and then all bets are off. And because organisations often set up a process and never change it, it’s always constant, so this gives the attacker plenty of time to figure out how to manipulate that process.

**Do you feel that enough is done to make people aware of the threat both in the workplace and amongst the general public, and who ought to be responsible for this awareness raising?**

No, I don’t think enough is done, obviously, because we still have the problem, and one of the key mitigation factors to social engineering is awareness training, especially in the general public. Within some organisations their security awareness training programmes cover social engineering, and in others they don’t. The organisation ought to be responsible as they’re trying to protect their resources. From a consumer’s viewpoint, and who’s responsible for training the consumer not to leak their personal identifying information, I don’t know who’s responsible for that. I guess you’d think that ‘buyer beware!’.

In Japan there was a very interesting social engineering attack, what they called the mumbling attack. Somebody would call the elderly people in Japan and mumble and when



## Social Engineering – Exploiting the Weakest Links

the person thought this was a family member or friend they would say there's a dire emergency, I need you to wire money, there's a big problem, maybe a medical emergency or something like that, and the elderly person would be duped into thinking that this person was a relative or friend and they would wire money. And you'd think that this would work only on a handful of people but it literally was so successful in Japan that thousands of people were victimised, and how they corrected the problem was that the ministry of justice had a public service announcement in television in Japan to educate people that these criminals are out there, they're doing this type of social engineering attack to steal money from you. So, I guess it takes cases like this before government bodies become involved. I don't know what government bodies in America would be responsible for this, but I can't imagine the Department of Homeland Security doing it, but it would be nice to have public service announcements to the general public at prime time, educating people about cons, swindles and social engineering, so they can protect themselves in the organisation and in their personal lives. That would be nice.

### **What do you think the role for an organisation like ENISA could be at a European level for fighting social engineering?**

It would be nice to help get the message out in a public social announcements way, like we discussed, and maybe raise awareness of these organisations that social engineering is a real threat, that there's real consequences, real possibilities of suffering a loss, and convincing organisations that they have to consider social engineering in an overall risk management programme. And maybe even helping these companies develop or to include some curriculum on security awareness programmes. And then also from the consumer perspective, because don't forget, identity thieves – I don't know if you have a problem in Europe but we do in America with identity theft – is helping the consumer be more resistant against social engineering attacks where someone is trying to sweet talk them out of their personal details, which could be used to steal their identity. I think that's an easier sell maybe to the BBC, and other television organisations. But ENISA could actually take some steps to help the public and the organisations to mitigate the threat. Of course there's no magic bullet, they won't eliminate it in its entirety, but they could help some people along the way.

### **Given the virtually limitless guises in which social engineering can crop up, is it really realistic to think we can educate people to be sufficiently safe?**

I think we can do our best, but there are influence techniques, like reciprocity, where the attacker will do a favour for the victim, and the victim will reciprocate, by complying with the attacker's request. You know, it's hard! But I think we have to try, we have to educate people into the different types of influence tactics that attackers will use. So hopefully the person could use some critical thinking and possibly recognise an unethical approach. And if you're educated to use some of the Cialdini principles in your white paper, the reciprocity approach, the authority approach, the scarcity approach – the scarcity in the sense that unless you comply with the request, you're going to lose something. So, it's not about realising a gain, it's about avoiding a loss, and a lot of attackers will frame their social engineering attack, that unless the victim complies, they're going to suffer a loss. So, if people understand how these approaches work, they'll be able to raise the bar; if people are paying attention and are interested.

---

**To what extent do you think it's possible to engineer out the dependency on people – for example by using biometrics rather than basing authentication upon secrets that users can be tricked into revealing?**

Two-factor authentication is good - biometrics is good but it's expensive. So, I find that in most cases organisations will look at the potential loss and then the potential cost of using biometrics or two factor authentication, and all usually revert back to using static passwords. But in my own personal experience, Motorola used two factor authentication to allow people that were outside the campus and accessing the corporate network; and despite them using this technology I was able to convince one of the IT managers in the computer operations department to give me the PIN of the SecureID token used in the operations department (which was shared through the people in that department), and any time I needed access to the corporate network they would simply read off the token code, over the telephone. And for like a whole week I got complete remote access to Motorola's computing resources! How hard is that going to be to do if someone called up a user that's gullible, claiming they're from the IT department, saying they're trying to synchronise the token, that they're trying to resolve a problem, and would you please read off your information? I think there's a high majority of people that will do it, if they really believe that the caller is legitimate and if they have some level of gullibility.

In another case, the attacker couldn't care less about getting access to the corporate network; they simply want the customer list. So they basically con that employee with the SecureID token or the fingerprint biometric to get the customer list for them and then email it, fax it or whatever. So, it does raise the bar, though in getting access to the corporate network, but in these other situations I've just brought up it's just not effective.

**Should organisations take a proactive stance and test their employees' resilience in this fashion?**

I believe so. In my company, 30% of our revenue is from doing pen testing, and I have to tell you I think that I've only done social engineering assessments in the whole lifetime of my company, because companies don't pay attention to the social aspect, the human factor. I think there's a misunderstanding that the threat is technology. And what they'll do is test their technology and they'll look for a technical security penetration test, and that's it. So I really think that by influencing these organisations to consider also social engineering security assessment would really help to raise the bar because again, the hacker is going to look at the weakest link in the security chain, and if they see that's your technology, they'll exploit it there, if they see it's your people – if you don't educate your people about social engineering and they're easy targets – then that's where the attacker is going to attack. It's really common sense!

But there's also an ethical issue here, because the organisation is licensing an outside company, probably they're outsourcing it to a security firm and effectively saying "you could go ahead and deceive our employees". And deception can reduce employee morale. People could become really annoyed about being intentionally deceived by the company in a test. So I think it's important to put employees on notice that the company either outsources, or they do these tests internally from time to time in an effort to raise the

### Social Engineering – Exploiting the Weakest Links

security of the organisation, and have employees sign a paper that they understand that they might be subject to these types of tests. And when they do happen in the future, they have a choice – they could sign the paper and accept it, or they can just not join the company or they can quit. So that way they're put on notice and there can be no complaints.

#### **Given the sophistication and popularity of social engineering attacks, how do you think it's likely to evolve in the future?**

I think social engineering is going to continue. Social engineering has been around long before we were born, so that's going to continue. The attackers are going to map out the processes, how people are authenticated, and ways to manipulate people's perceptions in what's really going on, and they're going to come up with more sophisticated pretexts. It's just like how social engineering has evolved 5 years ago, with caller ID spoofing; before that just wasn't around. There will be different methodologies for building trust and confidence, so there's a higher likelihood that these attacks will work. I think that they're going to continue and as we deploy new technologies, like smart mobile devices, that will also be an attack medium for social engineering. For example, being able to maybe send the message to a mobile device, where the message being a social engineering message, but the exploit is technical. Again, combining social engineering with technical exploitation, gives a kind of a hybrid to advance the attacker's objectives. But I think it's going to be a problem that's going to continue, despite of all the efforts of raising awareness.



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280  
[www.enisa.europa.eu](http://www.enisa.europa.eu)