

## CLICK ME: SOCIAL ENGINEERING IN MALWARE

“You could spend a fortune on technology and your network could still remain vulnerable to old-fashioned manipulation”

Kevin Mitnick (2001)

### ABSTRACT

The weakest link in the security chain and the largest unpatched vulnerability in the computer environment of any office is always the human. At the end of the day, it is up to the user to exercise responsible and secure computing principles and it's up to cyber criminals to lure the user away from them. That is where social engineering comes in. It is essentially a “con game” relying on the natural helpfulness of people as well as on their weaknesses and lack of security education.

This paper examines the how social engineering developed over time, how it is used in malware, and why it is so effective. Also described are some common tricks utilized in recent worms, viruses, Trojans and phishing and how users and administrators can recognize and resist such tactics.

## INTRODUCTION

Social engineering can be defined as *“Using deception and psychological manipulation to influence people to comply with a request; or, more generally, any trick to make a person do something they normally wouldn’t”*. For example, most people would not intentionally install a virus on their computer, but, if it poses as a love letter, very few people can stay away from clicking on it.

Initially social engineering was primarily the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. The traditional realm of social engineering has been on the phone. Kevin Mitnick mastered this tactic in the 1980s, and he explains it as “basically lying on the phone, manipulating and conning information out of people...” (Mitnick, 2002). It is all about calling up the mark, gaining his or her trust, impersonating someone in a position of power and learning some confidential information. Nowadays, similar techniques are used over the Internet. For instance, a specially crafted email message is sent, which is convincing enough to make the mark install a Trojan horse on their computer.

Social engineering works equally well online, on the phone and face-to-face, but this paper will focus on the digital form, paying close attention to the recent malware that utilized social engineering tactics to spread successfully. These tactics include creating specific subject lines or attachment names that convince a user to click - even if they think they shouldn't.

Corporate espionage, identity theft, bank fraud - all benefit from cunning social engineering attacks. Most threats that employ social engineering require user interaction to achieve their goal. They comprise **mass-mailing, IM and peer-to-peer worms, phishing attacks, spyware, mobile viruses and Trojans**. On the other hand, network worms penetrate user's systems without any user interaction as they rely on unpatched software rather than the gullible user. Also, social engineering is used heavily in SPAM and Hoaxes, but these topic is beyond the scope of this paper.

According to the analyst firm Gartner: **“Social engineering is the single greatest security risk in the decade ahead.”** And it is hard to disagree with this statement, considering that social engineering works on any platform; it continually evolves to include latest tricks and exploit recent events; and, most importantly, people cannot be quickly and easily “upgraded” to guard against it. “People, by nature, are unpredictable and susceptible to manipulation and persuasion. Studies have shown that humans have certain behavioural tendencies that can be exploited with careful manipulation.” (Mogull, 2004)

## HOW IT WORKS: EXAMPLES

*MASS-MAILING WORMS*

**Below is a chronological review indicating the evolution of social engineering used by mass-mailers:**

1999	Melissa	<b>Body:</b> Here is that document you asked for ...don't show anyone else ;-) <b>Attachment:</b> Anniv.doc
2000	LoveLetter	<b>Body:</b> kindly check the attached LOVELETTER coming from me. <b>Attachment:</b> LOVE-LETTER-FOR-YOU.TXT.vbs
2001	Kournikova	<b>Body:</b> Hi: Check This! <b>Attachment:</b> AnnaKournikova.jpg.vbs
2001	Matcher	<b>Body:</b> Want to find your love mates!!! Try this its cool... Looks and Attitude Maching to opposite sex. <b>Attachment:</b> Matcher.exe
2001	Goner	<b>Body:</b> How are you ? When I saw this screen saver, I immediately thought about you. I am in a hurry, I promise you will love it! <b>Attachment:</b> gone.scr
2002	Bugbear	<ul style="list-style-type: none"> <li>▪ Created random mail body text and random attachment filenames,</li> <li>▪ spoofed the From field,</li> <li>▪ used <u>MS01-020</u> vulnerability to execute attachment automatically</li> </ul>
2003	Sobig	<b>From:</b> <a href="mailto:support@microsoft.com">support@microsoft.com</a> <b>Body:</b> "All information is in the attached file."  <ul style="list-style-type: none"> <li>▪ Used random attachment filenames,</li> <li>▪ updated itself from the Web;</li> <li>▪ used networks of infected machines to jumpstart infection cycle</li> </ul>
2003	Mimail	<b>Body:</b> "Hello there, I would like to inform you about important information regarding your email address. This email address will be expiring. Please read attachment for details.  Best regards, Administrator" <b>Attachment:</b> message.zip
2003	Swen	Complete with Microsoft logos, links to real Microsoft resources and a very convincing text, Swen was a landmark of social engineering. <b>Body:</b> "Microsoft Client, this is the latest version of security update, Cumulative Patch update which eliminates all known security vulnerabilities affecting Internet Explorer...<more>".
2004	MyDoom	<b>Body:</b> "Dear user nick@ customer.com, Your e-mail account was used to send a huge amount of unsolicited e-mail messages during the recent week. Most likely your computer had been infected by a recent virus and now runs a hidden proxy server. Please follow our instruction in the attached file in order to keep your computer safe.  Virtually yours, The customer.com support team", <b>Attachment:</b> <random>  <ul style="list-style-type: none"> <li>▪ Very effective, users believed it came from their support team</li> <li>▪ Included username and domain to make a customized message</li> <li>▪ Added spaces in to attachment filename to hide the true extension: example: "your_password.txt .exe"</li> </ul>

2004	Mitglieder	Not truly a worm or a mass-mailer, Mitglieder was a spammed Trojan that pioneered the use of links to infected sites instead of email attachments. Users are more likely to click on an unknown link than to open unknown attachments.
2004	Bagle	Introduced propagation in password-protected compressed files: passwords were either included as text strings or as graphics. Uses fake calculator icon for its attachment. <b>Subject:</b> Hi <b>Body:</b> Test =) wpeorjfsadjffj -- Test, yep. <b>Attachment:</b> <random characters>.exe
2004	Netsky	<b>Body:</b> I've found your creditcard. Check the data! <b>Attachment:</b> visa_data.pif
2004	Zafi.D	Zafi.D spread in English, Italian, Spanish, Russian, Swedish and several other languages. The message is a simple Christmas wish. <b>Subject:</b> Merry Christmas! <b>Body:</b> Happy HollyDays!
2005	Sober.P	Sober worm pretended to be FIFA communiqué offering free tickets to the 2006 World Cup. It exploited the fact that FIFA has kicked off the second phase of ticket sales the same day the variant was discovered. Moreover, it used a clever trick of sending email messages in English or in German, depending on the recipient country-level domain.
2005	Kedebe	Pretends to be a news story: <ul style="list-style-type: none"> <li>❑ <b>Body:</b> Big day huh! What a great surprise! I just read on Arab site that Osama bin laden has been arested by US solders. It's lot to talk here. I just copied the whole text in Notepad and attached it. Nice news huh?!</li> <li>❑ <b>Body:</b> someone sent me this document which is stolen from a secret government body and deals about John Paul's death. It says he was killed by two 'doctors' who were hired by some government bodies. The text attached contains all the story behind his death and who these doctors are.</li> <li>❑ <b>Body:</b> Damn! I Heard that Michael Jackson died this morning. The news says there was an acciedent. I have attached the whole story.</li> </ul>

As seen from Kedebe's body text, social engineering is often crafted for a specific event; more examples:

- ⇒ Phishing scams related to the Katrina and Rita hurricanes and the Indian Ocean tsunami. Charity fraud emails aim to trick users into donating money on-line via spoofed websites.
- ⇒ The war in Iraq also brought a worm called Ganda that promised “ pictures taken by US spy satellites over Iraq”. This was an obvious ploy to get users to click on emails.

Another common technique used by recent worms is to build the email text by random permutation from a hard coded list. For instance, there are several different subjects, salutations, body text sections, attachment explanations and email signatures and the virus combines them at random to create a different email every time.

To summarize, most malicious email messages rely on one or more of the following:

- Address spoofing (appears to come from trusted source)
- Intriguing subject lines (who would refuse naked celebrity pictures)
- Deceptive file extensions (.pdf, .jpg, “.mp3 .exe”)
- Embedded scripts (code runs as soon as email is opened)

***INSTANT MESSAGING WORMS***

Worms spreading over IM protocols are very similar to mass-mailers, except they spread faster. They do not need to wait for the users to fetch their email, so all online contacts of an infected user are affected momentarily. The user believes that the link is from a trusted source, as the worms send their links to contacts harvested from the local contact list. This makes the user more likely to visit the site in question.

There are two groups of IM worms, those that use the IM feature of file-transfer to spread to new machines, and those that send an instant message with a link to download the worm from an infected website.

Bropia.F is representative of the first group, it sends a copy of itself to all online contacts using any of the following filenames:

- Bedroom-thongs.pif
- Hot.pif
- LMAO.pif
- LOL.scr
- Naked\_drunk.pif
- New\_webcam.pif
- ROFL.pif
- underwear.pif
- Webcam.pif

Kelvir, on the other hand sends URLs which point to infected/malicious files, accompanies by tempting messages:

- omg this is funny!
- This face, it looks like a alien
- Who does something like this..
- :D:D wow check it
- :;) haha, this is cool
- OMG :D This IS GREAT
- hahaaaa you are in the weeps picture!!
- Check me, i made this, very easy haha!
- Check this naked screensaver, wow, it's so cool!!
- Look what my dad gave me!!
- Wow, what a chick, she is so beautiful

***PEER-TO-PEER WORMS***

Relatively few pure peer-to-peer worms have been found to date. More frequently, peer-to-peer component is a part of mass-mailing worms. Quite often, the worm spreads more via e-mail, obscuring the fact that it can also spread via peer-to-peer networks.

There are no known exploits for worms to execute automatically, so convincing social engineering is a must for worms to spread via peer-to-peer networks successfully.

Such threats usually search the computer for folders used by popular file-sharing programs (Kazaa, eMule, etc.) and drop multiple renamed copies of themselves in those folders. As usual, to trick the user into downloading it, the threat pretends to be something interesting or useful to the user. The table on the right shows a subset of filenames used by Netsky.P.

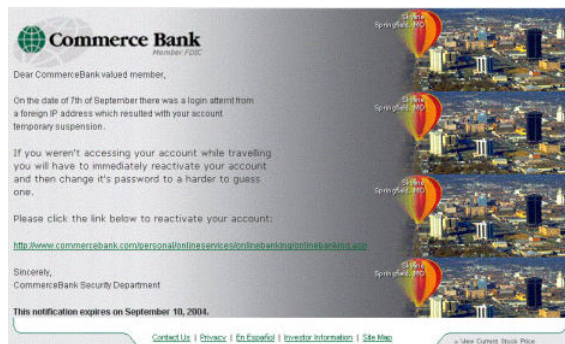
As we can see, the common themes here are free software or passwords, serial numbers or cracks, sex and nude pictures, games, photos, books, security patches or music files. Peer-to-peer networks have been a blessing for users who are fond of free music and software. But file-swappers may often be disappointed after downloading a worm or a virus instead of that coveted latest game version.

1001 Sex and more.rtf.exe  
3D Studio Max 6 3dsmax.exe  
Adobe Photoshop 10 crack.exe  
Altkins Diet.doc.exe  
American Idol.doc.exe  
Arnold Schwarzenegger.jpg.exe  
Best Matrix Screensaver new.scr  
Britney Spears Sexy archive.doc.exe  
Dark Angels new.pif  
Doom 3 release 2.exe  
Eminem Spears porn.jpg.exe  
Full album all.mp3.pif  
Gimp 1.8 Full with Key.exe  
Harry Potter 1-6 book.txt.exe  
Harry Potter game.exe  
How to hack new.doc.exe  
ICQ 4 Lite  
Internet Explorer 9 setup.exe  
Kazaa Lite 4.0 new.exe  
Matrix.mpg.exe  
Microsoft Office 2003 Crack best.exe  
Microsoft WinXP Crack full.exe  
MS Service Pack 6.exe  
Norton Antivirus 2005 beta.exe  
Opera 11.exe  
Partitionsmagic 10 beta.exe  
Porno Screensaver britney.scr  
Ringtones.mp3.exe  
Saddam Hussein.jpg.exe  
Serials edition.txt.exe  
Star Office 9.exe  
Teen Porn 15.jpg.pif  
The Sims 4 beta.exe  
Ulead Keygen 2004.exe  
Visual Studio Net Crack all.exe  
Winamp 5.0 (en) Crack  
Windows 2000 Sourcecode.doc.exe  
Windows 2003 crack.exe  
Windows XP crack.exe  
Win Longhorn re.exe  
WinRAR.v.3.2.and.key  
WinXP eBook newest.doc.exe  
XXX hardcore pics.jpg.exe

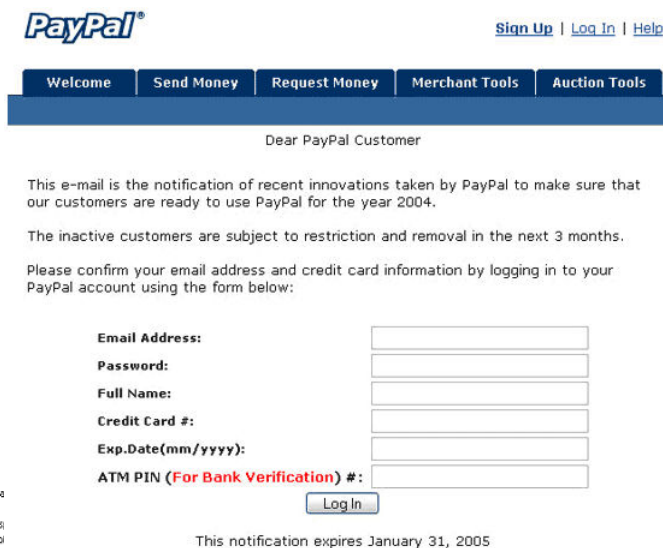
PHISHING ATTACKS

Phishing is a form of on-line fraud where the goal is to trick users into disclosing personal data. Phishers send emails purporting to be from well-known companies with links to spoofed websites. Once users go to such a site, they risk revealing their confidential information, such as banking details, to the owner of the fake site. Most social engineering used in phishing is of the "spoofing" type, where the attackers try to create a fake website and email message to mimic the spoofed company. Messages will have the company's logo and official looking text as well as a link to a web site that resembles the actual site you expect to visit, but is actually a clone of the original site. Phishing attacks can be really sophisticated. For instance, a flaw in Internet Explorer allowed hackers to display a false address while redirecting the user to an entirely different site, making it almost impossible to distinguish a phishing attack from a legitimate email. The success rate of social engineering used by a given bank-related phishing attacks, of course, depends on the number of the bank's customers that it reaches. That is why the most popular banks and online payment services are mostly phished (Citibank, USBank Washington Mutual, PayPal). By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them. Over 3 million people were lured into divulging sensitive personal information to phishers during a two-week period in December 2003 [APWG].

Considering that 14,135 cases of phishing were reported in July 2005 [data from the Anti-Phishing Working Group], and that only a third of U.S. cyber-crime cases are reported [according to FBI], we can clearly see that phishing is thriving and continuing to evolve. Here are some related screenshots:



Dear valued Charter One member,  
Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.  
It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and so could please take 5-10 minutes out of your online experience and renew your records you will not run into any future probi service. However, failure to confirm your records may result in your account suspension.  
Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.  
To confirm your bank account records please [click here](#).  
Thank you for your time,  
Charter One Billing Department.

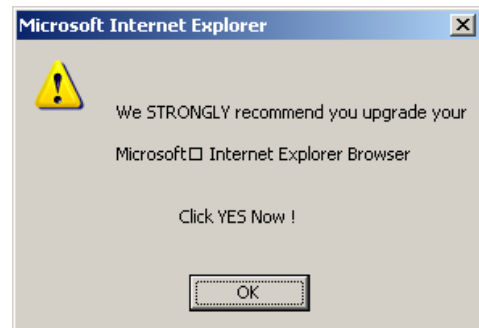


***SPYWARE***

Most spyware nowadays does not need to interact with the user or get their permission to install. Often spyware is dropped by worms or botnets, which also lower the Internet Security settings, so that pop-up advertisement served by the spyware would not be blocked. In fact, it is one of the primary sources of income of virus writers today, because the spyware companies pay between 5 and 25 cents per installed program. The alleged Zotob worm creator admitted that he does not care if people remove the worm because “it’s the spyware stuff that he installs that’s making him the money”. (Krebs, 2005)

Spyware also gets installed behind the scenes while the user is browsing the web (so-called “drive-by downloads”). Yet another way for spyware to be installed is through DNS cache poisoning, whereas the user is redirected to malicious websites when typing a legal website URL by a corrupted DNS server cache. Creating Spyware and infecting users with it is a profitable business as adware (the least evil category of spyware) alone generates \$2 billion annually from pop-up ads, hijacking home pages, and redirecting searches (Keizer, 2005)

However, a sizable portion of spyware is still installed when an unsuspecting user clicks on a popup when browsing the Internet. This is where social engineering is used to create appealing banners for users to click on. These banners suggest playing games (scoring a hockey goal, hitting a baseball with a bat, or punching the monkey), present quizzes in popups or just suggest, “Click HERE to close this window”. Examples of some popups that cause spyware to be downloaded are displayed below:



***MOBILE PHONE THREATS***

The first proof-of-concept virus for smartphones running Symbian OS appeared in June 2004. By October 2005, mobile viruses have been found in 30 countries. Operators have had to block multimedia messaging traffic, and 3.5% of MMS traffic is already 'malware'.

Currently most threats that run on a cell phone platform are either Trojans, worms with Bluetooth vector, or worms with MMS vector.

The user typically downloads Trojans because they masquerade as pirated games or cracked programs for the mobile phone. They use the technique of spoofing a real application the user wants, which is also used by peer-to-peer worms.

Bluetooth worms require the proximity of the source and destination phones for a successful infection. Also, the user is prompted to “OK” the new installation. This fact was used for a while to downplay the threat of cell phone virus infections, as it was believed users would not allow unknown programs to run on their phone. This was a mistake, as we now know. Curiosity leads users to click in most situations even when they know they should not.

MMS worms send messages similar to mass-mailers, with appealing subjects, sparking the victim’s interest to make them run the attached virus. [Commwarrior.A](#) uses the following MMS messages:

<p><b>Subject:</b> Norton AntiVirus <b>Message:</b> Released now for mobile, install it!</p> <p><b>Subject:</b> 3DGame <b>Message:</b> 3DGame from me. It is FREE !</p> <p><b>Subject:</b> Display driver <b>Message:</b> Real True Color mobile display driver!</p> <p><b>Subject:</b> Dr.Web <b>Message:</b> New Dr.Web antivirus for Symbian OS. Try it!</p> <p><b>Subject:</b> Free SEX! <b>Message:</b> Free *SEX* software for you!</p> <p><b>Subject:</b> Happy Birthday! <b>Message:</b> Happy Birthday! It is present for you!</p> <p><b>Subject:</b> Internet Cracker <b>Message:</b> It is *EASY* to *CRACK* provider accounts!</p>	<p><b>Subject:</b> MS-DOS <b>Message:</b> MS-DOS emulator for SymbianOS. Nokia series 60 only. Try it!</p> <p><b>Subject:</b> Nokia ringtuner <b>Message:</b> Nokia RingtoneManager for all models.</p> <p><b>Subject:</b> Security update #12 <b>Message:</b> Significant security update. See <a href="http://www.symbian.com">www.symbian.com</a></p> <p><b>Subject:</b> SymbianOS update <b>Message:</b> OS service pack #1 from Symbian inc.</p> <p><b>Subject:</b> Virtual SEX <b>Message:</b> Virtual SEX mobile engine from Russian hackers!</p> <p><b>Subject:</b> WWW Cracker <b>Message:</b> Helps to *CRACK* WWW sites like hotmail.com</p>
--	---

***TARGETED TROJANS***

In June 2005 alerts were issued by UK National Infrastructure Security Coordination Center about government departments and businesses being targeted by a continuing series of e-mail attacks designed to covertly gather sensitive and economically valuable information. These attacks were going after specific individuals who have access to commercially or economically privileged information. Shortly after, alerts were issued by US-CERT about similar attacks targeting US Critical Infrastructure networks.

The attacks involved the use of e-mails containing so-called Trojan horse programs or links to Web sites containing Trojan horse files. These emails used a spoofed sender address, pretending to come from trusted contacts, news agencies or Government departments. The attackers made use of distribution lists to target large numbers of recipients with similar interests and information relevant to the recipient's job or interests to entice them into opening attachments. Once installed on a user machine, Trojans obtained passwords, scanned networks, exfiltrated information, and launched further attacks.

A targeted attack has significantly higher probability of success, because it is unique and handcrafted for the individual it is targeting. For example, if you have received an email from a co-worker referencing their feedback about the memo you have sent previously, would there be any reason to be suspicious? Targeted Trojans often use rootkit-like techniques to remain below the radar of the infected user, which, combined with their hugely malicious intent (stolen proprietary secrets are more damaging than lost employee productivity or computer time), make them a big concern to enterprises today, especially the military and governmental organizations. They are also much more difficult to identify and fight from an antivirus standpoint, because, unlike worm outbreaks, few or no customers at all are reporting infections and forwarding samples.

Such targeted Trojans rely on **Manipulated Situation type of social engineering trick discussed later in this paper.**

## WHY IT WORKS: THEORY

Here are the primary reasons social engineering works:

1. People tend to trust others, and they are compassionate.
2. People are curious.
3. People are unaware of the threat.
4. People just do not care about security.

Social engineering relies on the perception that humans are trustworthy. So when an employee receives an email, he or she assumes it is from another human, and so it can be trusted. In reality, the employee could be wrong on both accounts – the mail might actually have been sent by an untrustworthy human (hacker) or a computer program (virus). This tendency to trust that is inherent to all humans can be exploited in a myriad of possible ways, and it is this tendency that is the hardest to eradicate. Several ways to fight it are discussed later in this paper.

**The goal of social engineering in malware is always “to get the mark to install the malware”.**

The methods used to achieve this goal vary greatly, but include some of the following:

1. The attacker will try to relieve the mark from responsibility, and make them believe they are not responsible for their actions.
2. Conversely, the attacker will exploit the mark’s fear and threaten/warn the mark that he or she will be held responsible if he does not comply with the request promptly.
3. The attacker might lead the mark to believe the action has some potential benefit for the mark, so the mark will comply because of the possibility of self-gain.
4. Also, the attacker will likely use “appeal to authority”, pretending to be a figure of importance or someone in charge.
5. The attacker will try to persuade the mark that the action is trivial and has been done by all other employees, thus using social pressure of conformity.

Below are some more common social engineering tricks used (Mitnick, 2002):

- Posing as a Microsoft security patch. (Swen.A, Sober.D, Dumaru, MyDoom.AD and Pandem.B, Xombe, Zapchast.F)
- Offering help if a problem occurs (MyTob)
- Posing as an authority figure (MyDoom, Sobig)
- Capturing victim keystrokes (Trojans)
- Using false pop-up window asking for log-in (spyware, Trojans)
- Using insider lingo to gain trust (targeted Trojans)
- Offering a prize for registering web site with username and password (spyware)

Most of the attacks fall in these two categories:

**Direct Request** (worms)

The simplest possible way to get the user to do something is just ask them. It is straightforward, because instead of using force or threatening the user, it just gently suggests the idea of “clicking” and hopes the user complies. Based on prior experience, most people will comply (we learn from our past experiences that helping others is beneficial), and it keeps us in control – it is my own decision to help. Most people will comply to avoid confrontation.

**Manipulated Situation** (targeted Trojans).

These are techniques that require prior research and reconnaissance about the mark and tailoring the message specifically to their interests or creating a situation where the mark will likely comply with the request. Scouting, eavesdropping on conversations, contacting the person anonymously, and, of course, searching the internet can give the attacker more than enough information to make a very convincing request for a specific user or a group of users. The more factors the target must consider in addition to the basic request, the more likely the target is to be persuaded. (Harl, 1997)

Worms exploiting user vulnerabilities tend to be more successful when inducing an instinctual response instead of a rational logic assessment. (Myles, 2005)

Different methods work for different targets. Technical users base their judgment on the strength and validity of the argument presented by the email. Weak arguments made to highly involved persons produce counter arguments and lessen the likelihood of compliance. Conversely, non-technical users are likely to grant the request based on the urgency of the matter, the number of reasons given for needing the information, or the status of the person making the request (Siltrow, 2001).

**COUNTERMEASURES**

There are no technical solutions to the problem of social engineering, as it manipulates common email user activity and popular interests. However, there are several non-technical solutions that together should minimize its effect.

A large part of social engineering success is due to people's inability to keep up with a culture that relies heavily on information technology. Often people are not aware of the value of the information they possess and are careless about protecting it. Case in point: nine in ten (90%) office workers at London's Waterloo Station gave away their computer password for a cheap pen! (Leyden, 2003) This is why education is the number one weapon against social engineering.

Most importantly, we have to stress to the users: "don't click it":

- "If you weren't expecting a file attachment then don't click it.
- If you don't recognize the sender or haven't directly solicited the email then don't click it.
- If you think there is anything strange about the email at all, be very wary." (Sturgeon, 2004).
- NEVER follow URLs embedded in ANY emails, type them into the browser directly.

To foil a social engineering attack, it helps to be able to recognize it. Specific user security training is necessary for this. For instance, users should know that any of the following in an email should raise a red flag and make the users highly suspicious:

- Requests out-of-ordinary information
- Claims to be from a person of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Has minor errors (misspellings, grammar errors)

Re-iterate to the users again and again to not follow any instructions sent in an email, but always verify by phone. After all, the best defense against social engineering is an individual who has had sufficient training on how this type of hacking is accomplished. In addition to following the company's security policies, employees should always be aware of threats and should regularly practice secure behaviors while at work. (Dubin, 2002)

Security is often regarded as the IT department's responsibility, but it is important to shift this responsibility to the end user. Each employee plays a key role in the security of their organization.

In addition to the user education and training, organizations also can:

- Update their incident-handling procedures to include social engineering attacks.
- Update their security policy to address social engineering attacks.
- Feature the threat of social engineering on the intranet and online newsletters.

**Defense in depth:** each one of the techniques above might have a weakness, but combining them and using them in a layered fashion should protect the users from a large portion of the threats discussed.

In the end, the virus success is a measure of its social engineering effectiveness. Gone are the days where most phishing or virus attacks could be identified by just poor spelling. And it is likely that malware authors will continue improving their tricks and devising new ones. We will have to wait and see. "The nature of social engineering is that it's only obvious if you know it's a trick - and too often people are finding out the hard way." (Sturgeon, 2004)

## REFERENCES

1. Dubin, Lawrence: "The Enemy Within: A System Administrator's Look at Network Security", <http://www.sans.org/rr/papers/download.php?id=530&c=b9e3d8c9c46b46872d3a14de785f4fd7>
2. Gordon, Sarah: "Social Engineering: Techniques and Prevention". Computer Security, 1995
3. Granger, Sarah: "Social Engineering Fundamentals", <http://www.securityfocus.com/infocus/1527>, <http://www.securityfocus.com/infocus/1533>
4. Harl: "People Hacking: The Psychology of Social Engineering" Text of Harl's Talk at Access All Areas III, March 7, 1997.
5. Hurley, Edward: "No Cone of silence for this malware" Mar 25, 2004 [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci956740,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci956740,00.html)
6. Keizer, Gregg: "Worst Spyware Down, Infected Sites Up" <http://www.techweb.com/wire/security/162100621>
7. Krebs, Brian: "Conversation With a Worm Author", Washington Post Security Fix Blog [http://blogs.washingtonpost.com/securityfix/2005/08/a\\_couple\\_of\\_wee.html](http://blogs.washingtonpost.com/securityfix/2005/08/a_couple_of_wee.html)
8. Leyden, John: "Office workers give away passwords for a cheap pen", April 18, 2003 [http://www.theregister.co.uk/2003/04/18/office\\_workers\\_give\\_away\\_passwords/](http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/)
9. McKay, Dave: "Social Engineering Fundamentals, Or: How I Learned to Stop Worrying and Hack the People", Speech at the Bellua Cyber Security Asia 2005 conference.
12. Mitnick, Kevin. & Simon W.L. (2002). The Art of Deception: Controlling the Human Element of Security. New York: John Wiley & Sons.
13. Mitnick, Kevin: "My first RSA Conference", (2001) <http://www.securityfocus.com/news/199>
14. Mogull, Rich quoted by Kotadia, Munir: "What's the greatest security risk?" Nov 1, 2004 <http://software.silicon.com/malware/0,3800003104,39125457,00.htm>
15. Myles, Jordan and Goudey, Heather (2005). The signs, signifiers and semiotics of the successful semantic attack *14th Annual EICAR Conference 2005* 14, St.Julians/Valletta, Malta. <http://papers.weburb.dk/frame.php?loc=archive/00000135/>
16. Siltrow, John et al: "Social Engineering, Part 1" ITAudit, Vol4, 2001 <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=339>
17. Sturgeon, Will: "Cheat Sheet: Social engineering", November 15, 2004 <http://software.silicon.com/security/0,39024655,39125919,00.htm>

### **About the author:**

Nick Bilogorskiy is a researcher with Fortinet Technologies, based in Vancouver, Canada. Nick is a member of the Anti-virus Information Exchange Network (AVIEN) and the WildList reporter for Fortinet. Since he joined the company, he moved through different positions, including QA Engineer for AV Signatures, QA Manager for AV Engine, and now he is working as Escalation Manager within the security research team, committed to protecting the end-users from virus outbreaks and promoting cooperation with other vendors. Prior to joining Fortinet, Nick worked at Microsoft, Art In Motion and NCompass Labs.

### **Author contact info:**

Nick Bilogorskiy  
Escalation Manager – Fortinet Inc.

Suite 1200, 4710 Kingsway  
Burnaby, BC V5H 4M2  
Canada

[nbilogorskiy@fortinet.com](mailto:nbilogorskiy@fortinet.com) – email

604-430-1297 ext 320 – office