

A Tried and True Weapon: Social Engineering

Author: *Cristian Borghello, Technical & Educational Manager, ESET Latinoamérica*

As human beings, we are often guilty of the sin of vanity which prevents us from really seeing how easy it can be to deceive us. This sense of our own power hides the obvious fact that we know something that, for some reason, can be useful to others.

Information security is closely related to human life. In the computer world, we are usually told that *the only safe computer is the one without power.*



Considering this, if a computer can be powered off, who is the target of malware? Users are. There is no computer that does not depend on human beings. This

dependence leads to vulnerabilities that can be quite independent of the technological platform one has chosen.

Given these vulnerabilities, Social Engineering (SE) continues to be one of the most commonly used methods for propagating malware attacks because its creators take advantage from the benefits of a particular mean of communication to deceive users and lure them into a trap that often leads to some type of financial loss.

SE can be defined in general as any action or social conduct directed at obtaining information from other people and can be further described as

the art of applying social skills in acquiring information of specific interest to the attacker.

The objective of social engineering in the informational world is to deceive the user into compromising his system and revealing valuable information. The simple act of clicking a mouse or answering a telephone call can lead to the loss of confidential information—both personal and corporate. At worst, this information can fall into the hands of malicious individuals bent on obtaining some financial gain. In the words of Kevin Mitnick, one of the most recognized personalities in the world for his cybercrime activities through Social Engineering “*You can have the best technology, firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.*”¹

Every person suffers from the same weaknesses both inside and outside a computer system or professional network. In a sense, the same fraudulent tactics known around the world and practiced since the dawn of humanity only need to be adapted to the new communication technologies in order to allow malicious users to launch their attacks. The effectiveness of this procedure relies on the ability to exploit human qualities such as naiveté, innocence, curiosity, ambition, ignorance, trust, social practices and compulsiveness.

¹ Abreu, Elinor. "Kevin Mitnick Bears All." *Network World Fusion* Sep. 2000

<<http://www.networkworld.com/news/2000/0928mitnick.html>>

The individual with malicious intentions often proceeds to gain the trust of a potential victim he wishes to deceive which then tends to allow him to simply ask for the desired information and achieve his deceitful goal. In an identical trend, social engineers focus on gaining the trust of others with the intention to later deceive and manipulate them for any economic purpose. Persuasion is a key component of SE because the trick not only consists in simply asking for the desired information, but also in the manner in which the question is phrased.

The “art of deceit” can be practiced by anyone—from a seller attempting to discern his buyers needs so that he may offer them a service to malware authors who seek to cause the user to reveal passwords. Despite these similarities with some professional practices, attempts to obtain confidential information for an inappropriate use are always of highly questionable ethics.

In the world of computer security, the “art of deceit” is used for two specific purposes:

1. The user is tempted to carry out a necessary activity that will weaken or damage his computer: this occurs when the user receives a message directing him to open an attached file, open a recommended web page, or watch a video.
2. The user is led to rely on necessary information so that the attacker can propagate a fraudulent action with the acquired information. This is the case in Phishing and Scamming where the user hands over information to the perpetrator of the crime believing that

he is giving this data to a trusted party or in the belief that he will obtain some reward or prize in exchange.

Phishing and Scamming are very good examples of another primary characteristic of Social Engineering: the excellent cost-benefit ratio achieved through its use that makes it one of the most alluring techniques. Indeed, with only one telephone call, email, or text message the attacker can acquire access to valuable information from the user, business, or even a system-wide network.

Although it is possible to specify the individual peculiarities of each case, it must be understood that **no technology is capable of protecting the user from Social Engineering**. Similarly, there are no “expert users” who are safe from this form of attack and SE does not fall out of fashion as a weapon of deceit. In fact, SE only becomes more sophisticated with time and is only bound by imagination.

Nevertheless, a unique, effective method of prevention is knowledge. This knowledge does not simply consist of technical data, but rather encompasses a social awareness that permits the user to avoid becoming an easy target of these attacks. Although any attacker with experience can deceive the inexperienced user, if the latter is properly trained in recognizing the typical pitfalls and traps he will be able to avoid them. Training users can also act as an important deterrence tactic against the spread of malware.

Social Engineering and Malware

SE is widely used by malware creators and cybercriminals due to its high level of efficiency. Malware authors begin to apply the concepts of SE during the planning phase of an attack. The more legitimate and trustworthy a message or source appears and the more gullible the user is, the greater the chances are of the attacker successfully accomplishing the propagation of the malware are.

1. Natural Disasters

The flood of email exchanges regarding the period of devastating storms in Europe in 2007 evidences the effectiveness of SE. In this case, a new family of malware known as Nuwar (or Storm Worm) used people's naive curiosity to spread one of the greatest malware epidemics in recent years. For approximately two years, Storm Worm proceeded to send hundreds of different messages addressing a variety of topics to create an enormous Botnet with millions of infected victims.

In many similar instances, malware authors have consistently incorporated current regional or world events into malware to accomplish their goals. Previously, email worms used to be sent as message attachments claiming to contain pictures or video of natural disasters, terrorist attacks, wars, and cyber wars between Russia and Estonia (2007) and Georgia (2008).

Throughout the years, computer-related fraud tactics have relied on the good will of users to perpetrate a wide variety of scams. In each of the

situations described above, there have always been examples of email scams in which a person who is interested in making a charitable donation to victims finds himself giving money to the unethical perpetrator of the fraud.

2. Celebrities

Malware programmers also use famous figures and politicians to ensure that their creations will spread by deceiving the unsuspecting and overly curious users.

In many instances throughout the history of malware, messages have been sent mentioning Michael Jackson, Britney Spears, Jennifer Lopez, Anna Kournikova and other world-famous figures.

Many malicious software programs do no more than achieving some notoriety in the press as in the case of infections based on news about Lady Di, Britney Spears or the continuing Kamasutra (VB.NEI worm). In these cases the degree of media attention to the malware incursion far outweighed the actual rate of infection. Nevertheless, in other cases worms have been able to reproduce themselves exponentially through email, instant messaging, and P2P. Social networking sites have also become increasingly relevant because they are used to send messages offering videos or news about famous people that often result in the downloading of malware.

3. Brands and Popular Events

One of the most common practices is the exploitation of a user's trust in a specific company or recognized brand. The use of company names or

organizations does not just occur with email attachments but can also arise through the use of Trojans and Phishing techniques. One highly frequent practice in spreading malicious code entails forwarding messages that appear as if they came from a well-known software company announcing a supposed vulnerability while assuring the recipient that the attached message or link is a critical security patch.

To lend greater credibility to the message, malware authors include a legend at the end of the email declaring that the attachment has been scanned by a well-known antivirus application and that it is free from malware. In addition, there are other cases in which the message includes references to famous events like the World Cup or the Super Bowl.

The lists of names and likenesses of famous business as well as current events are updated constantly in an attempt to continue the rates of malware incursion by constantly generating new trustworthiness in the authenticity of the messages. Through these updates, malware authors continue to use SE to exploit both the ignorance and curiosity that contribute to the user's vulnerability.

Many of these email messages are sent on a massive scale and often are equipped with HTML or rich text including the logos and typical formatting information of the company or business entity sponsoring the event. In the cases of scamming and phishing, the methods employed are similar and differ only in that they often include attached files. The messages created for phishing tend to use names of companies related to the business

world, easily recognizable internet sites, and telephone companies.

Since the majority of businesses and organizations have policies explaining that they will in no instance send emails with attachments, users should always disregard these messages.

Conclusions

SE cases are as diverse as they are endless and this article only attempts to inform you, as a potential victim, about some of the most frequent methods with which infections occur and it is important that computer users continue to both inform and educate themselves about potential risks.

While many computer users are aware that many items on the Internet lack trustworthiness, there is an especially high likelihood that malware is at the root of any unsolicited attempt to provide the user with information. Nevertheless, human vanity often does not allow us to see that we are the most permanent and susceptible fixture of any computer or network.

The user is both the target and the means of access to the actual computer environment which makes training extremely important in helping users understand that they constitute a vital link in the chain of online security.