CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Bulletin - Volume 1, Number 5, March/2016

Social engineering and cybercrimes

Marvin Ferreira

With the access to the Internet made popular by the constant use of the broad band and mobile devices and the consequent growth of social networks, it has become easier and easier to share personal information, such as, photos, videos, and texts. And together with this easy individual exposure, the risks of having these data misused, including by digital criminals, also known as cyber criminals, have increased.

The uncontrolled sharing of personal data in social networks exposes privacy intrusion, making people more vulnerable to the techniques of the so-called Social Engineering.

Social Engineering can be understood, within the information safety context, as the manipulations of individuals to induce them to share private and secret information with hidden criminals and fraudsters.

A tendency observed in the current applications and social networks indicates that the funnier they are, the more private information they will require from the users in exchange.

These private data when obtained by malicious people can be used for frauds, accessing systems, or cybercrimes, based on digital information.

The Social Engineering Techniques try to lead people to irrationalities. Thus, cybercriminals gain the individual’s confidence to obtain, for example, their bank password or other private and secret information.

The additional actions of the virtual criminals involve the investigation of the victim’s habits, hobbies, and preferences, elements that are easily obtained in the social networks.

Some of the Social Engineering techniques are:

Pretexting – By creating a scenario, ambient, or situation to involve the victim, the criminals search for private information or stimulate some action that allows, for example, the access to a computer or system. In these cases, the victim is induced to believe in a false identity, a corporate support technician, for example, and, then, ends up giving away the employee’s or client’s data, believing in the false system maintenance.

Diversion Theft – It consists in making delivery companies or the mail company deviate their vans from their route and deliver the mail to other addresses, that is, the criminals’.

Phishing – One of the oldest techniques and an electronic scam still very practiced. It occurs by sending an apparently legitimate email of a victim’s acquainted friend or company. There is a link that, when clicked on, directs the e-mail receiver to a false site where someone’s information can be stolen, or a computer be infected by some virus able to collect information, such as, bank data, passwords, and documents, and send them to criminals.

Phone Phishing - It is a technique similar to phishing, and that many times starts with an email. The victim receives a false email or letter asking her/him to call her/his bank service, for example. After digitating the data and password on the phone, the private information is automatically sent to the criminal.

Baiting - It works as a Trojan Horse, making use of the victim's curiosity. In this case, the criminal creates a CD or a pendrive or any media that can make carry out the boot operation (turn on and off) in the computer – bearing a title as "photos of the surprise party" or "the team's salary" - and leave it in public places where possible victims will be curious enough to pick these medias up and insert them in their computers.

Thus, the simple insertion of the media in the computer will infect it by installing a malware that will give access to the victim's machine, generating invasion breaches in the system or even picking up the data contained in the machine and sending them to the attack creator.

There are a lot of other techniques based on the discovery and exploration of people's vulnerability, and who end up being involved in situations that seem legitimate, but that in fact are mere manipulator-planned creations.

One of them involve calling several numbers of a company pretending to be a technical support technician and asking about the possible computer problems, and, after the user's approval, a breach in the system is open.

The data exposure in social networks put individuals at risk, for it facilitates the digital criminals' work. A simple dating application, such as, Tinder, for example, that uses Facebook or Instagram information can open breaches for raising other people's data through the Internet.

Some users also openly expose their cellular phone numbers, snapchat, social network, and several details of their lives in small biographies in Tinder. For example, when obtaining a person's snapchat, one can follow in real time his/her daily activities, when accessing his/her Facebook, and pick up information on where he/she studies, works, lives, or relative's names, etc.

The access to this information depends directly on the exposure level that people accept and the data that they publish in their social networks. This overexposure in the social networks has developed a shop-window-exposed society, where everyone can see and comment on one another.

A tendency observed in the current applications and social networks indicates that the funnier they are, the more private information they will require from the users in exchange. The objective is to arrange, manipulate, and even sell data as a form of financing the service rendered. Companies like Facebook and Google already do this with their users' information.

Therefore, we have to be alert towards the constant use of networks, cell phone applications, and even dating site, for example. After all, everything we use in the Internet exposes us more and more and makes us vulnerable to virtual crimes. Or even makes us possible crime victims in a real world, due to the use of the virtual world data by criminals of all kinds.

Marvin Ferreira *has graduated in Computing Sciences from PUC São Paulo; MSc in Computing Engineering at the School of Engineering of the University of São Paulo; and a CEST researcher.*

Journalist in-charge: Edson Perin
Coordinator: Edison Spina

This article is a result of the author's ascertainment and analysis, without compulsorily reflecting CEST's opinion.