SOCIAL ENGINEERING AND RISK FROM CYBER-ATTACKS
Today, many people are facing the risk of losing information and sensitive data. For criminals/hackers, social engineering is one of the most prolific and effective means to induce people to carry out specific actions or to divulge information that can be useful for attackers.

This article will discuss the basics of social engineering by giving a general overview of social engineering. We will discuss the specific details relating to the most common techniques used by attackers to access seemingly secure systems. Also, at the end of this article, we explain why it is important to be certified against ISO standards and what benefits this can bring in relation to security.

Even though a lot of people use the web and all the services that go with it, general awareness about the cyber world and safe practices to be followed while online is very low. Social engineering is a kind of art; it is the art of manipulating people and one of the most effective means of gaining access to secure systems and obtaining sensitive information. In general, social engineering is the process of deceiving people into giving confidential, private or privileged information or access to a hacker. There is really not a lot of difference between the techniques used for social engineering and the techniques used to carry out traditional fraud. From a technical perspective, social engineering is simple, because it does not require advanced technical knowledge. Instead, social engineering is based on using human psychology such as curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy that in this case are used as weakness.

Attackers use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). The types of information they seek can vary and the techniques they use range from little sophisticated techniques that can be easily identified such as bulk phishing emails to highly targeted and multi-layered techniques.

According to the results of a survey of cyber-security conducted by ISACA and RSA in the first quarter of 2015, it shows that phishing and some other kind of social engineering attacks were the most common attacks within enterprises in 2014. Almost 70% of respondents declared that phishing, was exploited in the enterprise, and 50% declared other social engineering attacks, including water-holing attacks, SMS phishing and so on.
What is concerning is that the number of attacks is rising year by year. Based on the “Global State of Information Security Survey 2015” conducted by PricewaterhouseCoopers (PwC), it shows that the number of detected information security incidents rose 66 percent year-over-year since 2009. On the other side, the survey of 2014 reported that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013.

As cybersecurity incidents increase and breaches become more significant, they cause an increased financial impact. For more information about financial cost cyber-crime in 2015 read the report that derivates from the study of the Ponemon Institute, sponsored by Hewlett Packard Enterprise.

### COMMON SOCIAL ENGINEERING ATTACKS

**Phishing attempts.** Phishing is one of the most prolific forms of social engineering; it is estimated that 37 million users have reported phishing attacks in 2013. Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate popular company, bank, school, or institution, as well as other methods of communication, including social media, but email phishing is the most common. Email phishing vary from unsophisticated, which can be easily identified, to very sophisticated, emails appearing legitimate. Phishing emails often ask the user to follow a link to a website, to open an attachment, or require the user to donate money for charity. Despite the fact that email phishing is becoming very sophisticated, there are still some indicators letting the user know the email is false:

- Messages are unsolicited
- Messages are vague, not addressed to the target by name, contain little other specific or accurate information to build trust
- Contain incorrect or poor versions of an organization’s logo, and may contain web links to sites that, whilst perhaps similar, are not ones used by that organization.

**Baiting** is in many ways similar to phishing attacks. Baiting attackers use online adverts and websites and have very unrealistic offers, too good to be true, or send urgent warnings like pop-ups that purport to have detected a problem with the victim’s system which by clicking on the pop-up will solve the issue. But, in fact by clicking the provided link, the user is tricked into giving away personal information, or by clicking the link user’s machine may automatically download malware. Another form of baiting is the use of false free Wi-Fi hotspot, where attackers create Wi-Fi that is labeled as free. Although, they provide internet connection, all the data sent over this connection can be captured by attackers.

**Watering hole attack** is one of the most sophisticated (the most sophisticated form in 2013) social engineering techniques as it requires some more technical knowledge. This attack technique requires the attackers to infiltrate a legitimate site visited by their target, plant malicious code, and then lie in wait. As with other targeted social engineering attacks, the attacker will research their intended victim(s) and identify one or more trusted websites that they are likely to access. After they identify the suitable website, they look for vulnerabilities within the server that hosts the website and later they insert the code within the server to enable malware to be downloaded.

When a website is compromised, the attackers will be able to monitor almost everything from activity logs (to see who is visiting the website) to the victim’s IP.
WHY IS IMPORTANT TO BE CERTIFIED AGAINST ISO STANDARDS AND HOW CAN ORGANIZATIONS BENEFIT?

Bill Gates once said: “There will be 2 types of business in the 21st century: those that are on the Internet and those that no longer exist.” He was not wrong, because currently the vast majority of the businesses are carried out online or at very least organizations have an online presence. Being on the Internet means that the risk from cyber-attack is always permanent, and as explained, social engineering works by manipulating normal human behavioral traits. So, a good way to be protected and ready to handle such attacks (technical and non technical) is to implement fundamental processes and controls based on ISO/IEC 27001.

A key part of this is about raising awareness as how both humans and computer systems can be manipulated. ISO/IEC 27001 determines requirements for an information security management system (ISMS). ISO/IEC 27001, Annex A has 114 controls that help organizations keep information assets secure, even though not all of which are related to technologies, but indirectly, all of them are related to information security. Since ISO/IEC 27001 only contains a brief description of each control, more information about cybersecurity can be found in ISO 27032, which is guidance for cybersecurity inside the ISO 2700 family of standards. ISO 27032 provides a framework for coordination and exchange of information, which is important while managing cybersecurity-related incidents that can occur.

Further other ISO 27001 series standards can provide greater help such as ISO 27034 which covers the processes for developing secure software and ISO 27035 which gives the guidance and how to detect and react to security (including social engineering) incidents.

The Ponemon Institute’s study, implies that certification against industry-leading standards can save companies up to US$549,620, while other activities that are promoted by ISO/IEC 27001 can result in even further savings such as:

- employing expert personnel (US$1,458,736)
- appointing a high-level security leader (US$1,291,810)
- training and awareness activities (US$1,150,951)

Finally, it can be concluded that having a certified ISO/IEC 27001 ISMS supported by other key ISO standards such as ISO 27032, ISO 27034 and ISO 27035 can benefit organisations by improving resilience, seizing opportunities to use technology well, keeping risks under controls and actually decreasing security costs.

ABOUT THE AUTHORS:

Graeme Parker is an experienced professional in Cyber Security, Risk Management and governance fields with proven experience in implementing and developing effective management systems, and also performing various kinds of security testing for small and large organizations. He is the Managing Director of Parker Solutions Group, the PECB representative in the United Kingdom.

Vlerar Shala is an Account Manager for Information Technology and Service Management at PECB. He is in charge of conducting market research while developing and providing information related to the Information Technology and Service Management systems at PECB. If you have any questions, please do not hesitate to contact: marketing.itsm@pecb.com.