Kymatio®

White Paper - Social Engineering

SOCIAL ENGINEERING, ARE WE READY?

KYMATIO - ACTIVATE HUMAN FIREWALLS

Social Engineering, what is it?

Nowadays, the information security field is highly dynamic, in which both the prevention measures and the attack methods are constantly adapting to changes in the environment. For **every advance in security, criminals break through, creating new ways to achieve their goals**. This results in a cyclical process of continuous updating and development.

In this way, given the constant increase in the complexity of attacks, the need to develop increasingly advanced protection programs is generated. However, in recent years, the target of criminals has not only been computer systems, but people are gaining prominence. The reason is very simple: on many occasions, 'hacking' a person is easier than hacking a system.

This is known as **social engineering**, and it is a method to which an accurate protection response has not yet been achieved. In this type of attack, criminals take advantage of human vulnerabilities by making use of various manipulation techniques (Mouton, Leenen, & Venter, 2016; Hinson, 2008; ACCISI, 2018).

Social engineering is defined as the **manipulation of people** through direct contact and/or technology, in order to obtain sensitive information or other data that could compromise its availability, confidentiality or integrity. It could happen both in the personal or organizational spheres and, in the case of the latter, manipulation can occur by someone external or internal to the company.

Social engineering in numbers

There is no doubt that this method is on the rise, endangering both the capital and the reputation of organizations and, in many cases, even their continuity.

Ponemon Institute carried out a study on it in 2020. The results were, to say the least, shocking: **79% of the companies that participated admitted to having suffered at least one social engineering attack**. Furthermore, in 67% of the cases the consequences were significant or very significant.

In the light of these results, it is worth wondering if the root of the problem could be found in the level of awareness of the workforce.
Only half of these companies provide their employees with awareness training. This alone already constitutes a critical point in security, but it is not the only one. If the other half do carry out programs to fight social engineering, how can such a high percentage of incidents exist?

It is clear that **awareness methods are not giving any effective results**, and this is something companies themselves are aware of: the confidence they have on their ability to respond to these attacks has decreased from a 31% to a 23%.

The way to protect ourselves from these threats must evolve and cover new necessities, changing the main approach until now. However, to establish new guidelines, first of all, it is necessary to deeply understand the problem.

Different techniques, different attack vectors

Social engineers seek to manipulate people, often motivated by money, and to do so they rely on various techniques to favor the success of their attacks. Some of them are:

Phishing. One of the most common ones. It consists on sending an e-mail, often impersonating trusted entities or people, in order to deceive the recipient and make them download an infected file, click on a link or give certain sensitive information (Krombholz, Hobel, Huber & Weippl, 2015). In addition, thanks to the rise of social network, they have also become a widely used means in these kinds of hoaxes (Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019). These are usually mass mailings with generic messages so that, although the success rate is not exactly high, the number of people who fall victim to fraud is significant enough (Salahdine & Kaabouch, 2019; Gupta, Singhal & Kapoor, 2016). However, when looking to hunt down a specific person or organization, attackers turn to evolved spear phishing. It consists of fully targeted messages that provide real data such as names or titles to increase credibility and thus make it easier for the potential victim to lower their guard (Salahdine & Kaabouch, 2019).

Vishing. Its name comes from voice phishing and its characteristics are the same as with phishing, except for the channel used. In this case, the target is contacted through phone calls to convince them to take the actions sought by the criminals (Ollmann, 2007; Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019).

Smishing. This technique has many similarities with the previous two, since it deals with fraud through text messages (Yeboah-Boateng & Amanor, 2014; Altwairqi, AlZain, Soh, Masud & Al-Amri, 2019). Although originally only SMS was used for this (hence its name), the proliferation of instant messaging applications such as WhatsApp or Telegram open new windows through which social engineers might want to enter. The use of shortened malicious links or account theft are the most used methods.

Dumpster diving. Not all social engineering attacks have a technological component, and this is one of those cases. It is based on searching the victim's garbage for some type of sensitive or, at least, useful information to be able to continue with the deception later (Granger, 2001; Mitnick & Simon, 2003; Krombholz, Hobel, Huber & Weippl, 2015; Salahdine y Kaabouch, 2019). Some examples might be notes with written passwords, schedules, or printed reports. Shoulder surfing. Sometimes attackers don't have to go very far to get the information they want - just looking at the target's screen while they are working can be enough (Krombholz, Hobel, Huber & Weippl, 2015; Salahdine y Kaabouch, 2019).

Tailgating: It occurs when the social engineer walks next to or behind a person who has authorization to enter the company or a sensitive area to access at the same time when they open the door (Dey, 2016). In this way, the attacker would gain access to the facilities to damage them, steal information or even eavesdrop while other people talk about sensitive topics. (Heikkinen, 2006).

Baiting. It is a somewhat different method from the others, since the attacker does not contact or even come close to the victim. It consists of infecting a removable device, such as USB drives, with a malware (malicious program) and leaving it in a place where it can be easily found (Salahdine y Kaabouch, 2019). In this way, the moment someone picks it up and connects it to their computer, the malware will begin to work, be it damaging files, hijacking them, or monitoring the actions carried out on the computer.

These are the techniques that criminals use to carry out their attacks, but none of them would work if it weren't for the fact that there is something that prompts the victim to act as expected. So, how do they do it?

Why do the attacks work?

Just as hackers constantly search for **vulnerabilities** in computer systems to carry out their attacks, social engineers do the same with people. There is no one who is totally infallible, so it is only necessary to use the right message to greatly increase the chances of success.

Therefore, it is worth wondering what these vulnerabilities are that they are trying to exploit.

These openings are nothing more than our **motivations**. It is not necessary to go to especially complex desires, but you can start with something very simple: what is more effective in us, punishments or rewards?

There are people who are especially sensitive to punishment; that is, they are more motivated to avoid negative consequences than to achieve positive ones. Others, on the other hand, work in a totally opposite way. This does not mean that they are exclusive: all people are happy when something positive happens, and nobody likes anything bad happening to them.

However, this preference does exist, and it is determined by the brain. This is what is called the Behavioral Inhibition System (BIS) and the Behavioral Activation System (BAS), present in all people (Gray, 1981). Although it depends on the situation, we all have a tendency. For example, when someone offers a reward without any negative consequence, no one would turn it down. However, in more complex situations that have both pros and cons, the balance does not always tip to the same side depending on who is evaluating them.

In addition to this basic distinction, there are other factors that come into play. Although they are less simple motivations, they also have their basis in psychology (Eysenck, 1970; Costa and McCrae, 1992), and are born from the combination of different characteristics of people, such as their level of emotionality in the face of different situations or orientation towards others.

Thus, five large groups of motivations are identified to which social engineers appeal to carry out their attacks, namely:

1. **Altruism**. It is the desire to help other people. An alleged colleague who is in a hurry, a person with his hands full who seems to want to enter the office, a request for direct help for a good cause ... Any of these pretexts can be used to carry out a deception, in which those people with a greater orientation towards others will fall more.
2. **Fear**. Inspiring fear is one of the techniques preferred by criminals and has to do with the aforementioned about sensitivity to punishment. You just have to introduce an undesirable consequence in the message if the instructions are not followed so that a large percentage of people consider, at the very least, to pay attention to what they are told.
3. **Curiosity**. It is about appealing to the contrary: the rewards. Just by appealing to curious facts or that can report some type of benefit, it is enough to think about accepting what is proposed, such as offering something for free.
4. **Authority**. There are people for whom it is very important to follow the rules and comply with direct requests from those who have a certain authority. Obedience to this type of figure is something natural for many, which makes it easy to be the victim of an attack in which the identity of one of them is impersonated.
5. **Self-esteem**. Wanting to preserve our sense of worth is something important for everyone, although more for some people than for others. Therefore, when someone recognizes our abilities or, on the contrary, we feel that they are attacked, a need arises to bring out how much we are worth. This opens a new vector of entry for social engineers who decide to use this factor to achieve their objectives.

As with the Behavioral Inhibition System and the Behavioral Activation System (sensitivity to punishment or reinforcement, respectively), each person will present one of these vulnerabilities to a greater extent, although it does not mean that they cannot present the others.

In addition to these, there are a number of techniques used to increase **persuasion**; that is, to increase the chances that the attacker will get the victim to act according to their plans. These techniques are explained by Cialdini in his book *Influence. The Psychology of Persuasion* (1984), in which he himself admits: "All my life I've been a patsy. For as long as I can recall, I've been an easy mark for the pitches of peddlers, fundraisers, and operators of one sort or another. (...) With personally disquieting frequency, I have always found myself in possession of unwanted magazine subscriptions or tickets to the sanitation workers' ball". They are normally used to support the previous ones, and are:

1. **Liking**. We tend to accept requests from those we like, so on many occasions, attackers will try to make a good impression on the victim.
2. **Reciprocity**. "You scratch my back and I'll scratch yours" is a very widespread mantra among the population, to the point of being almost an unwritten norm. So, when someone does something for us, we feel compelled to reciprocate in some way.
3. **Commitment**. Showing a commitment or, at least, a previous favorable attitude towards what is asked, increases the chances of acting accordingly.
4. **Social proof**. In situations of uncertainty, when we do not know what to do, we look at the behavior of others. This is because we seek to be approved by other people, so if we are presented with a request that would be socially welcomed (such as helping someone), we are more likely to accept.
5. **Authority**. It has already been commented previously: when the request comes from someone with some authority over us, we will tend to obey. This is something that Milgram already, in 1963, studied in his laboratory. The experiment consisted of asking the participants to provide electric shocks, each time of higher voltage, to another person if he did not correctly answer the questions that were asked. The shocks were not real, but this is something that the participants did not know. Even when the supposed voltage was so high as to threaten the life of the other person, most of the participants applied the shock when the authority figure (the person responsible for the experiment) asked them to do so.
6. **Scarcity**. When offered something for a limited time, many people feel the urge to get hold of it while they still can. This is because they do not want to be without it later, or because they seek to be part of that exclusive group that possess the product. In any case, it is clear that the probabilities of acting as they ask us increases the moment they give us a deadline to do so.

To all these rules and personal characteristics, it is necessary to add something else: the situation in which each one finds themselves. Although it is a subject to be addressed in subsequent analyses, it should be noted that the environment has a great influence on people, since our reasoning capacity is not the same under a stressful situation as in a relaxed one, for example.

Are we ready?

Social engineers are aware of the different **techniques** and our **vulnerabilities**, taking advantage of them to achieve their goals. For this reason, it is important that **we know ourselves** to be able to detect in what kind of situations we may be more exposed to deception.

This is not an easy solution, much less at the organizational level, where many people are still unaware of the scope and dangers of social engineering. However, there is no doubt that **current approaches are not enough** to slow the progress of these attacks, and this is due to the low level of personalization of awareness programs.

As explained throughout this document, not all people have the same motivations. For this reason, **a program that meets the needs of each individual in a particular and personalized way** is necessary.

Personalized awareness, **targeted** simulations, training on how social engineering works and how can each of us **protect ourselves** against it knowing our own **vulnerabilities**... that is the path to success if we want to get one step ahead of the attackers.

Only then can we activate our ***human firewalls***, protecting both our personal information and that of the organization.

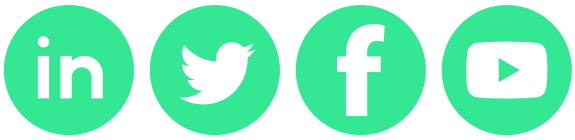
About Kymatio

Kymatio is a SaaS solution for managing cyber risk associated with the human factor, based on interactions with employees and automatic and personalized awareness.

Using neuropsychology and cybersecurity as the basis of its technology, Kymatio AI interacts with people, offering them a personalized awareness appropriate to their needs, maintaining the level of alert and strengthening the areas in which they may be most vulnerable.

At the same time, it provides organizations with visibility into human risk based on different metrics such as level of awareness, functions and access to information, level of well-being, response to simulations or analysis of accounts exposed in breaches.

To learn more, contact us at **contact@kymatio.com** or ask us for a meeting at **https://calendly.com/kymatio**

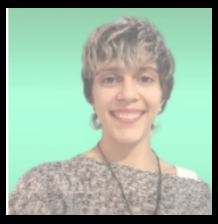


About the authors

Andrea Zamorano
https://www.linkedin.com/in/andrea-zamorano/

Cyberpsychology Manager at Kymatio, she investigates the human side of cybersecurity and develops the necessary algorithms for the platform to be able to accurately measure the factors involved, so that risk can be evaluated and personalized recommendations can be presented based on the needs of each employee. She is also a teacher at the UAM School of Economic Intelligence (La_SEI) as an expert in indirect personality profiling. She is a psychologist, having studied at the Autonomous University of Madrid (UAM), and later graduated from the Master's degree in Economic Intelligence and International Relations at La_SEI. She also has an Expert in Organization and Human Resources degree from the Autonomous University of Madrid.

Sara Dorado
https://www.linkedin.com/in/sara-dorado/



Sara Dorado works as a Neurostrategist at Kymatio, developing the scientific basis that supports the validity and effectiveness of the tool designed to detect vulnerabilities and personalized needs of users. In addition, she is also an expert in indirect personality profiling and intelligence analyst at the School of Economic Intelligence (La_SEI), where she also does teaching functions. She graduated in Psychology at Universidad the Autonomous University of Madrid (UAM) and completed her studies with a Master's degree in Criminal Analysis and Investigation at the Forensic Science and Security Institute (ICFS).

References

- ACCISI. (2018). Seguridad informática-Hacking ético. Conocer el ataque para una mejor defensa (4ª edición). Barcelona: Ediciones Eni.
- Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Four Most Famous Cyber Attacks for Financial Gains. International Journal of Engineering and Advanced Technology, 9(2), 2131-2139.
- CERT Insider Threat Center. (2013, September 30). The Latest CERT Research of Unintentional Insider Threats: Social Engineering. Software Engineering Institute, Carnegie Mellon University. Retrieved from: https://insights.sei.cmu.edu/insider-threat/2013/09/-the-latest-cert-research-of-unintentional-insider-threats-social-engineering.html
- Costa, P. T., y McCrae, R. R. (1992). Four ways five factors are basic. Personality and individual differences, 13(6), 653-665. doi: 10.1016/0191-8869(92)90236-I
- Dey, P. K. (2016). Prashant's algorithm for password management systems. International Journal of Engineering Science, 2424.
- Eysenck, H. J. (1970). The structure of human personality (3.ª Ed.). Londres: Mathuen.
- Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18.
- Gray, J. A. (1981): A critique of Eysenck's theory of personality. En A model for personality (pp. 246-276). Berlin: Springer.
- Gupta, S., Singhal, A., & Kapoor, A. (2016) A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA2016), pp. 537-540. Doi: 10.1109/CCAA.2016.7813778.
- Heikkinen, S. (2006). Social engineering in the world of emerging communication technologies. In Proceedings of Wireless World Research Forum (pp. 1-10).
- Hinson, G. (2008). Social engineering techniques, risks, and controls. EDPAC: The EDP Audit, Control, and Security Newsletter, 37(4-5), 32-46.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
- Milgram, S. (1963). Behavioral study of obedience. The Journal of abnormal and social psychology, 67(4), 371.
- Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. Indianapolis: John Wiley & Sons.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209.
- Ollmann, G. (2007). The vishing guide. Retrieved from InfoSec Writers: http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf
- Ponemon Institute (2020). Seventh Annual Study: Is Your Company Ready for a Big Data Breach?
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. Doi: 10.3390/fi11040089
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.