Social engineering: Application of psychology to information security

Del Pozo, Ivan
Universidad Nacional De Colombia
Bogotá, Colombia
imdelf@unal.edu.co

Iturralde, Mauricio
Universidad San Francisco de Quito
Quito, Ecuador
miturralde@usfq.edu.ec

Restrepo, Felipe
Universidad Nacional De Colombia
Bogotá, Colombia
ferestrepoca@unal.edu.co

***Abstract*— Psychology and computer science are two scientific disciplines that focus on identifying the specific characteristics of information processing. The first analyzes human behavior, while the latter focuses on the construction of a technical tool that seeks to emulate the brain: the computer. Therefore, psychology is strongly tied to the moment people choose their passwords. Deceptive advertising often compensates through money, free products, services or other self-esteem tests to influence a product or service to appear on your social network, in order to increase their consumption among its followers and to take personal information without your consent. Security is subjective, and each individual will perceive security differently, since each person has different weaknesses. Subjectivity should not be the one who meditates to manage his own measures of protection against the Social Engineering, which refers to psychological manipulation of people into performing actions or divulging confidential information. This project is also based on the need to prevent attacks of information subtraction by obtaining and decrypting the keys of access, or in the worst case, obtaining passwords directly to the different services, bank accounts, credit cards of individuals, based on the information that a people exposed or share on their social networks. Additionally, it focuses on how attackers could obtain or decipher their passwords based on personal information obtained from such advertisements; providing a better vision of how hackers use the psychology applied to information security.**

Keywords*— *Psychology, Social Engineering, Information security, Deceptive advertising, Passwords, Social networks

I. INTRODUCTION

The rise in popularity of social networking platforms are creating enormous amounts of data [1] where both children's and adults' emotions are constantly expressed in real-time [2]. There have been several unknowns of Psychological phenomena regarding human behavior, the internal and external stimuli. Psychologists have used various research strategies [3] to approximate as close as possible to where it arises and how our thoughts are processed, and the relationship that it has with our behavior. Some studies refer to a comprehensive understanding of threats to human security [4]. with an appropriate balance between structured improvements to defend human weaknesses and security training and security awareness focused efficiently [5]. But none of them deals specifically with the direct application of social engineering in the weakest link [4] in the security chain; to psychologically manipulate the person by using social networks combined with deceptive advertisements and in this way obtain confidential data from it. So that is why we must discover how vulnerable people are to deceptive advertising on social networks. And, how attackers could obtain or decipher their passwords based on personal information obtained from such advertisements. This is paper is an exploratory research project, which is quantitative, and it will be executed in four phases described below.

Section II will present a Literature Review about the relationship between social engineering with psychology, deceptive advertisements, passwords and people confidence. With a short related work explanation.

Section III introduces our proposed strategy, which will be used to design and develop an ethical attack on one popular social network.

Section IV presents statistical analysis and numerical results regarding the number of people who are vulnerable to deceptive advertising; and how computer attackers can obtain an advantage with the information achieved from the ethical attack to break user's passwords.

Finally, Section V, sets out recommendations and conclusions, granting safety recommendations between functionality and security.

II. LITERATURE REVIEW

Over the last few years, enormous progress has been made in developing and implementing technological tools to earn money through the internet. We belong to a society that coexists daily with digital technologies [6]. Part of these technologies are social networks. Through them, companies and organizations have the opportunity to reach an audience that was beyond their reach through traditional media.

A. Social engineering and psychology

Psychological phenomena are unknowns related with human behavior, because each person is a completely different world from each other [3]. However, all people have more affinity to certain common of influence patterns, as is the case of social engineering. There are different incentives and motivators in people who allow social engineers to take their victim to action [23].

978-1-5386-7810-7/18/$31.00 ©2018 IEEE
DOI 10.1109/W-FiCloud.2018.00023

The majority fall within six basic categories which will be explained on figure 1 [23].

Fig. 1. The six universal truths of influence

Cybercriminals who use social engineering seek to deceive their victims so they voluntarily give out their personal information [7]. The vulnerability of legitimate users is stipulated by their needs (money, self-affirmation) and weak points of each (self-esteem, social approval) [8]. Social engineering has been established based on psychological and security terms [9] by various organizations and experts, as taking advantage of vulnerable people's naivety via influence, in different aspects such as persuasion and manipulation to obtain vital information [10]. It is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information [9]. By knowing the personal information or the likes of a person, they become defenseless so the attackers will know the structure of their passwords [11]. Social network users such as users of Facebook, Instagram, Youtube, Twitter, blogs, and other users of current social media, use social networks as a world window in which they expose multiple aspects of their day to day [11], for various purposes, some of them, clearly commercial [12]. Nowadays, cybercrime is introduced by hackers through social networks, because they have the ability to identify methods to forward spam messages for advertisement purposes in an illegal way. [12].

B. Social engineering and deceptive advertising

Responsibility for misleading advertising operates in a simple way, only presenting what it is, that advertising does not correspond to reality or because it is insufficient and has the ability to mislead and even confuse the consumer. This raises the question regarding who is responsible for misleading advertising on social networks orr how to recognize if an ad is authentic or misleading. That is why many tests have been carried out and methods designed to distinguish between genuine and fraudulent advertising.

According to [13], the authors presented several works and methods focused on the identification of vulnerabilities to security and privacy in regards to social engineering. The most outstanding are:

- Fake Form Elicitation
- Spear-Phishing money transfer
- Phishing web service attack.

The methodologies mentioned have a very strong documentary structure and are specially designed for in-depth Information Security Audits:

- OSSTMM (Open Source Security Testing Methodology Manual).
- ISSAF (Information Systems Security Assessment Framework).
- OWASP (Open Web Application Security Project).

A complete analysis to distinguish legitimate and malicious posts using Netbeans IDE is presented in [6]. With 91.01% of accuracy identifying legitimate posts. This technique can find legitimate posts effectively.

In [14], the authors demonstrate an intimate knowledge about deceptive advertisement. They implement a system which can efficiently detect deceptive ads and phone scams by taking advantage of our unified framework on deep neural network with convolutional neural network. The work challenges is in the appliance of the same system throughout the different internet services.

In [15], the authors present an actual scamming and spamming ethical attack through e-mails and a social network. It begins when the victim receives an unsolicited e-mail, social request, or letter often concerning of an African nation containing either a money laundering or other illegal proposition.

In [16], the authors carried out a series of preliminarily studies on users' preference distribution. Collecting 479,048 user's information. It presents 6,276,422 particular preference items in total. Facebook classifies users' preferences into 11 types as Music, TV, Movie, Activity, Book, Interest, Athlete, Game, Team, Sport and the people who Inspire you. But it does not present anything regarding vulnerability on social networks.

In [11], Gather Facebook user data from participants via their access token, i.e., 'like' pages and 'share' posts. For each user, compute the frequency of each behaviors on the pages with respect to each category. They identified 204 different pages categories, which are provided by Facebook. In addition, it obtains their user preferences to be used as class attributes.

Despite all the information that has been collected through the use of the different social networks, the work is incomplete. More research is needed to better understand of the direct application of social engineering through deceptive advertisements. In that way analyze how vulnerable users are of becoming victims of fraud, using social networks is necessary and feasible.

C. *Social engineering and passwords*

When a user wants to create a bit more complex passwords, the user relies, even unconsciously, on symbolic references such as his birthday, his children's, or the date of his wedding. In this way, one makes it easy for hackers to access sites such as Facebook, [11] see some of these data and, from there, search for the combination of entry to personal services. After entering the password, it is important to check that it does not contain personal tracks. Regarding the username, the "professionals in breaking keys" know that almost everyone uses the same one that has in their email address [12]. So it is therefore appropriate to be much smarter, be one step forward and shield what is now almost like an open book [4].

Hackers know how to apply social engineering, through psychological elements that influence an individual to do a particular task of which he is not aware Despite users having different levels of computer experience, familiarity with technology, backgrounds, ideologies, religions, and gender; It is apparent that social networking sites are not restricted to any type of user [4]. Nowadays, it should not be unexpected that social networking sites present a market for information security threat agents such as phishers or hackers.

D. *Social engineering in relation to people's confidence*

There are up to six different disciplines: sociology, psychology, economics and management, security, law and education. All are related to each other and each point addresses a sensitive psycho-social and computer security information in order to gain the trust of the people [23]. Unlike traditional hacking methods, where the attacker needs to be technically equipped to carry out a sophisticated attack, a social engineer needs to focus on his social skills, in their behavior, in their tastes, in their ideology [5][9]. A word, or registration in a social network, are facts that for those who mention it may not be of any importance. But for an expert in social engineering it may be the key that opens the Pandora's Box of the protection of sensitive information [18]. Most elements recognized as effective in phishing [5] commonly use persuasion principles such as authority and distraction which represent dominant attitudes, people of strong character, which will be able to manipulate the victims at their whim. A self-inflicted abduction of one's privacy based on a user's ignorance and lack of skill for social relations and on the capacity of the social engineer to take advantage of them based on using human psychological characteristics such as curiosity [23] (what moves us to look, to respond and touch where we should not), fear (to fear, we seek help in any way or fall easier in the traps because we cannot reason with peace), trust (we feel safe at the slightest sign of authority).

E. *Importance of understanding the relationship of psychology with social engineering*

The most valuable treasure that exists today is the data [19] and the knowledge that can be obtained from another person because of the rapid change and development of web and social network sites. While technological know-how certainly plays a large role in enabling attackers to hack any given code system, network or individual, what is often overlooked is that some tricks of the trade, like social engineering, are also psychological games [15]. Cybersecurity attacks are increasingly based primarily on social engineering techniques, the use of psychological manipulation to trick people into disclosing sensitive information or inappropriately granting access to a secure system. That is why it makes it one of the most complex techniques to avoid and is undetectable or questionable given that it handles aspects of psychology that could not be factually proven [9].

III. PROPOSED STRATEGY

To examine the deceptive operations and techniques used in social engineering and phishing, the study has designed an ethical attack. That will be performed from the perspective of an attacker.

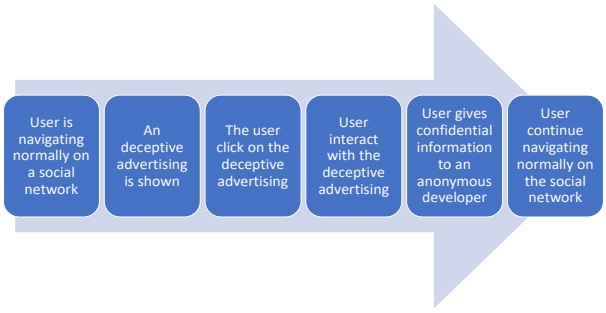

Fig. 2. Proposed strategy implemented

The purpose is to collect personal information through deceptive advertising in order to use for different purposes. The entire flow will be divided into six stages, as is shown in figure 2.

A. *Stage 1 - User normal navigation*

In principle, the main purpose of the Internet was communication, [16] creating an efficient channel of communication allowing the human communication with others without barriers, which does not take into account the space, or borders, distances, societies. The Internet is full of communication in all areas. Any type of visual communication that we can imagine is on the World Wide Web. [22]

- The world population in March 2016 was 7.4 billion.
- Internet has 3.17 billion users.
- There are 2.3 billion active users on social networks.
- 91% of retail brands use two or more social media channels.
- Internet users have 5.54 social media accounts on average.
- Social network users grew 176 million last year.
- There are 1 million active users of social networks on new mobile phones every day. That is, 12 every second.
- Facebook Messenger and WhatsApp handle 60 billion messages daily and Facebook has 1.71 billion users

Based on these statistics and according to the study conducted, it can be concluded that given the considerable number of users interacting with social networks, it is quite possible that a significant percentage of users could be susceptible to these types of illicit activities. For the purpose of this case of study, we will examine the social network with the most users: Facebook.

B. *Stage 2 - Attracting user attention*

Advertising on Facebook is already starting to be used by some companies that are trying out this tool to attract customers [22]. Advertising on Facebook consists of purchasing small advertising spaces that appear on the Facebook page. By clicking on this ad, you will be redirected to a company's Facebook page, or to an external page [22]. Therefore, based on how Facebook presents an advertisement and according to the study conducted, it can be concluded that, presenting a deceptive advertisement on the home page will attract many users of all kinds of ideologies, professions, religions, etc.

C. *Stage 3 - The deceptive advertising*

An advertisement posing the question "Share what you are going to eat and / or drink" will run; and will appear as "¿Qué tan buen borracho eres?" which means "How good of a drunk are you?" This is a test which discovers first if you like to drink, and if it is affirmative, it is to say you like to drink, and then to determine if you have a good behavior while you are drunk. The advertisement presents an initial message, which it is intended to persuade the user, capture his attention and encourage him to do this alluring quiz [14]. The deceptive ad was published in a particular Ecuadorian Facebook fan Page. This fan page has as particularity that it publishes false news, jokes and ridicule of characters of show business or politics. As a result, this Fan Page has a large number of followers, which is perfect to carry out our implementation of malicious advertising

D. *Stage 4 - Interaction with the deceptive advertising*

It consists of fillable form made up of ten basic mixed questions formed by a multiple-choice option and filling information in a text box to persuade the user, and through this form collect the information need for the study. This test will be performed in Spanish. Question 1, 2, 3, 4, 9 and 10 are distractors to divert the user's attention and give a meaning that is a formal survey; and question 5, 6, 7 and 8 will be used to obtain personal information. All this information will be saved in one .txt file.

E. *Stage 5 - Retrieve confidential information*

Finally, a pop-up window will appear, so the user is asked to write their email and their password, so it means that he may try to login and because of this, the user will give his personal information, which will be saved on a second .txt file on the server. At this part of the proposed strategy, the user does not realize that everything is false. Despite that the screen is identical to the original, trusted Facebook page.

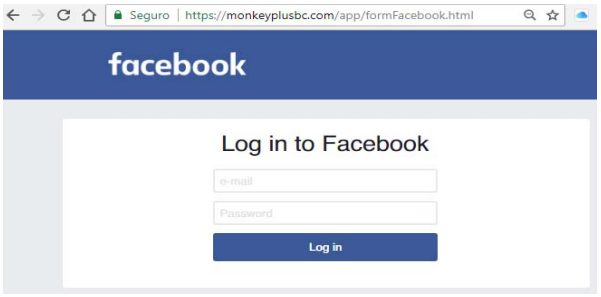

Fig. 3. Fake Facebook window at the final stage of deceptive advertisement

This is how deceptive advertising works. Which because of false or inaccurate data, or because of its ambiguity, omission, similarity with reality or other circumstances, induces or may mislead its addressees about essential elements of the confidential information of the persons.

F. *Stage 6 - User continue his normal navigation*

On Stage 6 the ethical attack will finish, and the user will continue navigating normally on the social network without realizing that he has just been a victim of theft of valuable confidential information.

G. *Implementation*

The strategy implemented understands about usability and how to create a site that customers want to navigate around [20]. The general architecture of proposed strategy implemented is shown in the Figure 4 as a normal Client – Server architecture with the additional component that on the server is stored the user personal information. All the personal information collected from the test of the deceptive advertisement is subjected to an analysis that the user never finds out and, in this way, to be able to fulfill the purposes of the attacker.

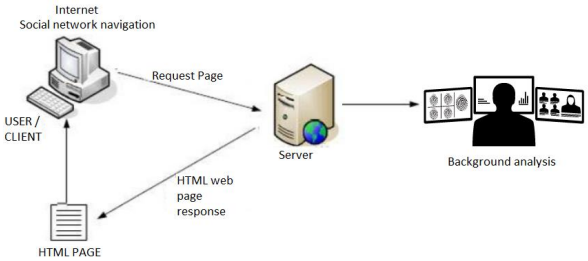

Fig. 4. General architecture of proposed strategy implemented

The parameters and statistics that will be evaluated will be:

1. Length of the password
2. Number of uppercase characters
3. Number of lowercase characters
4. Number of digits
5. Number of specials characters
6. Composed by two or more words
7. Root of the password
8. Match with information of the form (hobby/ favorite drink/ birthday / color)
9. Composed by the email user

IV. Numerical Results

A. *Analysis about vulnerability of deceptive advertising*

Cybercrimes share some similarities with crimes that have existed for centuries before the arrival of cyberspace. Therefore, for the purpose of our research, the first analysis takes place in stage 3, in order to determine the population that is vulnerable to a deceptive advertisement, and at least click on it.

$$\forall\, n \in \mathbb{N}\ \exists\{n | n\ = total\ population\}$$

$$n = 228250\ people$$

228250 Represents the number of people how follows the page. From of all this population we have:

$$\forall\, m \in \mathbb{N}\ \exists\{m | m\ = users\ which\ have\ accessed\}$$

$$m = 11645\ people$$

So we can say that it represent:

$$= 5.101\ \%$$

Based on the previous analysis and taking into account that Facebook has "1.71 billion users" [22]

$$if\ n\ \rightarrow 1.71\ billon\ Facebook\ users$$

$$\Rightarrow k\ \rightarrow\ 87\ \ million\ users\ (aprox)$$

This is a greater number of users to access to this fake web site. However, it should be considered that the study was carried out in Latin America. Where people have a different education level from other continents and countries of the first world, where religion prevails against science and many other cultural determinants for research. So the impact of deceptive advertisement in social networks is not easy to determine and generalize for the entire world. Moreover it should be considered that if this deceptive test is left for longer on the web it can be distributed more quickly to a larger number of people. But what can be concluded is that:

$$\forall\, n\ \wedge m \in \mathbb{N}\ \exists\{n | n\ = total\ population\}$$

$$\wedge\ \exists\{m | m\ = users\ which\ have\ accessed\}$$

For the second purpose of our research, this analysis takes place in stage 4 and 5, in order to determinate how many people give confidential information to hackers.

$$\forall\, j \in \mathbb{N}\ \exists\{\, j |\, j\ = users\ who\ did\ the\ questionnaire\}$$

$$j = 9823$$

$$\forall\, k \in \mathbb{N}\ \exists\{k |\ k\ = users\ who\ tried\ to\ re\ login\ on\ Facebook\}$$

$$k = 127$$

Taking in account the previous conclusion, it should be considered that if this deceptive test is left for longer on the web, there is a small probability that more users will deliver the confidential information of the email and the password. To support our results, a confidence interval is presented with 95% of confidence [20]. With 95% confidence level and using the Binomial proportion confidence interval with the Wilson score interval, which is an improvement over the normal approximation interval in that the actual coverage probability is nearest to the nominal value [20].

$$\hat{p} = 0{,}05101$$

$$z = 1{,}961$$

$$\frac{\hat{p} + \frac{z^2}{2n}}{1 + \frac{z^2}{n}} \mp \frac{z}{1 + \frac{z^2}{n}} \sqrt{\frac{\hat{p}(1-\hat{p})}{n} + \frac{z^2}{4n^2}}$$

$$= 0.051007 \mp 9.021 * 10^{-4}$$

There are numerous victims of cybercrime, all stemming from very different demographics, and this number represents the percentage of people that are potentially vulnerable and are good targets of social engineering attacks. In just one week; almost the twenty percent of the population was tricked by deceptive advertising, which is the first step for computer frauds. These users are more susceptible to be distracted and deceived by visual elements, fooling their minds and playing with their psychology to get information easily. To believe in any advertisement in any of the advertising distribution methods depends on whether we can distinguish between realistic advertising, well-applied advertising, and advertising that is simply misleading. Moreover, understanding who the criminal is likely to target can assist in taking preemptive actions to forewarn and prepare for all forms of attack.

B. Analysis about password elaboration

Passwords are one of the pillars of cybersecurity, since they are the primary tool users have for the device or service with which they interact to identify us, but the user is still not aware of the need to have a robust password in their digital life to protect their personal and confidential information. In order to analyze the password in detail, we used the information retrieval technique "Single pass in memory indexing" using inverted index with counts. It uses term instead of termID's, writes each blocks dictionary to disk and then starts a new dictionary for next block [23]. Additionally this implementation supports better ranking algorithms and works as follows:

```
1 output_ file = NEWFILE ()
2 dictionary = NEWHASH ()
3 while (free memory available)
4     do token ← next (token_stream)
5              if term (token) /∈ dictionary
6                then postings_list = ADDTODICTIONARY(dictionary,
      term(token))
7              else postings_list = GETPOSTINGSLIST(dictionary,
      term(token), counter)
8              if f ull(postings_list)
9        then       postings_list=DOUBLEPOSTINGSLIST(dictionary,
       term(token), counter)
10    ADDTOPOSTINGSLIST (postings_list, docID(token))
11 sorted_terms ← SORTTERMS (dictionary)
12 WRITEBLOCKTODISK (sorted_terms, dictionary, output_ file)
13 MERGEBLOCKS (f1, . . . , fn; fmerged)
14 return output_ file
```

Single pass in memory indexing using inverted index with counts is called repeatedly on each that we will consider as token, until the entire collection has been processed. All tokens are processed one by one as we can appreciate it at line 4 during each successive call of Single pass in memory indexing using inverted index with counts. When a term, or a word or character, occurs for the first time, it is added to the dictionary, and a new postings list is stored as we can appreciate it at line 6. The call in line 7 returns this postings list for subsequent occurrences of the term. Each postings list is dynamic, and it is immediately available to collect postings. This has two main advantages: it is faster and saves memory because there is no sorting required, and we keep track of the term a postings list belongs to, which makes it easier for us to get the number of repetitions of each term.

When the memory had run out, the index of the block, which consists of the dictionary plus the postings lists to disk at we can appreciate at line 12. We sort the terms at line 11 in order to facilitate the final merging step. So, the last step of Single pass in memory indexing using inverted index with counts is then to merge the blocks into the final inverted index at line 13. Then

our output file is ready to be used for the attacker. Once all the output files are saved and taking in account the previous analysis k=127; we have this passwords. As general data, the single pass in memory indexing using inverted index with counts program used shows that none of the password is a unique dictionary word (compared with our dictionary). All of them are composed by two terms or more.

Password Characteristic	***Percentage***
4 characters	3,150%
5 characters	3,937%
6 characters	11,020%
7 characters	7,874%
8 characters	9,449%
9 characters	14,960%
10 characters	8,661%
11 characters	16,540%
12 characters	3,937%
13 characters	7,087%
14 characters	3,937%
15 characters	4,724%
16 characters	2,362%
22 characters	0,787%
28 or more characters	1,574%
1 capital letters	51,970%
2 capital letters	3,150%
3 capital letters	3,937%
4 capital letters	1,575%
1 lowercase letters	2,362%
2 lowercase letters	2,362%
3 lowercase letters	4,724%
4 lowercase letters	8,661%
5 lowercase letters	11,020%
6 lowercase letters	13,390%
7 lowercase letters	10,240%
8 lowercase letters	6,299%
9 lowercase letters	7,874%
10 lowercase letters	3,937%
11 lowercase letters	5,512%
12 lowercase letters	4,724%
13 lowercase letters	4,724%
14 lowercase letters	0,787%
15 lowercase letters	1,575%
20 lowercase letters	0,787%
21 lowercase letters	0,787%
30 or more lowercase letters	0,787%
1 numbers	2,362%
2 numbers	14,960%
3 numbers	3,937%
4 numbers	11,020%
5 numbers	0,787%
6 numbers	2,362%
7 numbers	0,787%
8 numbers	3,937%
9 numbers	0,787%
10 numbers	3,937%
11 numbers	0,787%
1 special characters	9,449%
2 special characters	3,150%
3 special characters	3,150%
5 special characters	0,787%
6 special characters	0,787%
only lowercase letters	16,540%
only numbers	6,299%

Table 1: Password characteristic percentage

As global statistics we have the results shown in Table 1. This represents that much of the population k=127 use 1 capital letter in their password. A standard password of eight characters can be discovered in less than one minute by a current computer and if we add that it only uses letters, and only lowercases letters, it makes it easier for the attacker to generate a much more efficient comparison dictionary, without much work or effort required. Analyzing each password individually we have that:

Parameters	*Bool Type*	*Frequency*	*Percentage*
Match with information of the form:	T	53	41,73%
Composed by the email user	T	8	10,16%

Table 2: Analysis about password elaboration

As we can appreciate passwords that contain personal information (the name or birthday, a pet, or a personal identification number) may or may not be found through an attack based on dictionary passwords. However, if the attacker knows him personally (or is motivated enough to investigate his personal life), he may be able to guess his password with little or no difficulty. In addition to dictionaries, many password crackers also include common names, dates and other information in your password search.

Therefore, even if the attacker does not know that his dog's name is such, they may still discover that his password would be based on his pet, with a good password decoder. Because you upload many photos of your pet, and everybody know that the puppy has a preferential treatment. If people continue using passwords based on their hobbies, tastes, ideologies, birthdays, id numbers, among others, there will be no need to extract the password directly, because the attacker knows the behavior of

the victim, and only to analyze them fully, the attacker can deduce passwords for the rest of services. It is important to consider that many times people for the sake of simplicity to remember passwords use the same users of your email in order not to get confused Which for this particular case represents the 10, 16% from the 127 people who gave the confidential information. At first glance it seems that it is a low range, nevertheless we are generating a huge security gap for any person. In other words it means those people are easy targets to be victims of an attack of social engineering. It is reasonable to conclude that with the half of the population using one capital letter in their password, attackers will induce always to put the first letter of the password in capital letter.

V. CONCLUSIONS AND FUTURE WORK

The human mind becomes a resource for storing sensitive information and can be attacked by cybercriminals through social engineering at an electronic and personal level. In this exploratory research project through the study, it is shown that people are vulnerable to deceptive advertisements. Presenting even greater risk, they give their personal information to unknown sources or people. As seen in the evidence previously discussed, psychology plays a fundamental role in both conceptions of social engineering, since it is from the use of psychological techniques that the implementation of them is possible, and how easy it is to manipulate a person to do what we want them to do.

Another view is that necessary information is omitted for the adequate understanding of commercial advertising, because they never ask for credentials. The results show that our proposed strategy clearly reflects that there is great vulnerability to misleading advertising on social networks. Furthermore, Social Engineering is an art that few develop because not all people have social skills. Human nature plays a role in shaping social life while the social structure in turn, with its habits, norms, and customs; also exerts an influence on people, which handled in dangerous hands triggers an attack of social engineering. Moreover, this project also shows us that our passwords are still very functional rather than secure.

Through our study we are able to draw a number of recommendations for deceptive advertisings and some tips for choosing a secure and functional password:

- Do not trust if the website asks you for personal data in confusing tests of dubious origin and to share them. Even worse if you are asked to rewrite your password even though you were already browsing normally in the social network.
- Beware of open sessions or to fake URL.
- Do not use dictionary words or names in any languages.
- Do not use common misspellings of dictionary words related with your personal affinities, hobbies, ideologies, id numbers, phone numbers or pet names.
- Never use only numbers.
- Do not use just one capital letter.
- If possible use special characters, such as ! @ # $ % ^ & *

This proposed strategy has been implemented for obtaining user email and password through a social network. Further work must focus on deceptive advertisements in other countries. Also on online payments to verify if when there is money in between, people are psychologically not so easy to manipulate, reject deceptive advertising and, as a result social engineering loses its influence. Moreover make a phishing attack with the emails obtained from this deceptive advertising.

REFERENCES

[1] D. S. Terzi, R. Terzi, and S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," *2017 Int. Conf. Comput. Sci. Eng.*, pp. 592–597, 2017.

[2] M. T. Aziz, "Sentiment Analysis On Facebook Group Using Lexicon Based Approach," pp. 8–11, 2016.

[3] B. Atkins and W. Huang, "A Study of Social Engineering in Online Frauds," *Open J. Soc. Sci.*, vol. 1, no. 3, pp. 23–32, 2013.

[4] R. Heartfield, G. Loukas, and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 1–1, 2016.

[5] A. Ferreira and G. Lenzini, "An analysis of social engineering principles in effective phishing," *2015 Work. Socio-Technical Asp. Secur. Trust*, pp. 9–16, 2015.

[6] C. Ekta Science, "Reputation Based Technique to Distinguish Posts in Facebook Social Network," 2016.

[7] C. S. Centre and A. Jones, "Information Security and Digital Forensics in the world of Cyber Physical Systems," pp. 10–14, 2016.

[8] I. Kotenko, M. Stepashkin, and E. Doynikova, "Security Analysis of Information Systems taking into account Social Engineering Attacks," 2011.

[9] C. E. L. Grande and R. S. Guadrón, "Social Engineering : The Silent Attack," no. Concapan Xxxv, 2015.

[10] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches," *2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud*, pp. 145–149, 2016.

[11] J. Rachsuda, "User preferences profiling based on user behaviors on facebook page categories," pp. 248–253, 2017.

[12] K. Bhise, "A Method For Recognize Malignant Facebook Application," pp. 41–44, 2016.

[13] A. Zingerle, "How to obtain passwords of online scammers by using social engineering methods," 2014.

[14] T. H.-D. Huang, C.-M. Yu, and H.-Y. Kao, "Data-Driven and Deep Learning Methodology for Deceptive Advertising and Phone Scams Detection," 2017.

[15] O. B. Longe, V. Mbarika, M. Kourouma, F. Wada, and R. Isabalija, "Seeing Beyond the Surface, Understanding and Tracking Fraudulent Cyber Activities," *Int. J. Comput. Sci. Inf. Secur.*, vol. 6, no. 3, p. 12, 2010.

[16] L. Wang, X. Han, and L. Chen, "An Empirical Study on Preference Distribution of Facebook Users," *2016 Intl IEEE Conf. Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People, Smart World Congr.*, pp. 1069–1073, 2016.

[17] H. Zou, "Protection of personal information security in the age of big data," pp. 5–8, 2016.

[18] E. D. Frauenstein and S. V Flowerday, "Social Network Phishing : Becoming Habituated to Clicks and Ignorant to Threats ?," pp. 98–105, 2016.

[19] I. Del Pozo and M. Iturralde, "CI: A new encryption mechanism for instant messaging in mobile devices," in *Procedia Computer Science*, 2015.

[20] Z. Qian, B. Shen, W. Mo, and Y. Chen, "SatiIndicator: Leveraging User Reviews to Evaluate User Satisfaction of SourceForge Projects," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, pp. 93–102, 2016.

[21] M. Iturralde, R. Maldonado, and D. Fellig, "An approach to detecting text autorship in the Spanish language," *2016 8th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2016*, 2016.

[22] Smith, K. (august, 2016). 96 statistics and incredible data from social networks for 2016. Accessed on October 28, 2017 from <https://www.brandwatch.com/es/2016/08/96-estadisticas-redes-sociales-2016/>

[23] Cialdini, R. (1984). Influence: The Psychology of Persuasion. HarperCollins e-books. ISBN 978-0-06-189990-4.

[24] Manning, C. D., Raghavan, P., & Schütze, H. (2008). Introduction to information retrieval. Cambridge: Cambridge University Pres