Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

CZECH
UNIVERSITY
OF LIFE SCIENCES PRAGUE

Bachelor Thesis

Personal digital identity management

Paola Vannesa Gamarra Burgoa

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Bc. Paola Vannesa Gamarra Burgoa, BS

Informatics

Thesis title

Personal digital identity management

Objectives of thesis

The objective of the thesis is to identify and summarise the best practices for personal digital identity management in selected scenarios.
Partial goals of the thesis are:
- to make a literature review of the current state of the art and trends in digital identity management;
- to identify and evaluate main practices for digital identity management in real world scenarios;
- to formulate future recommendations and conclusions;

Methodology

The thesis is based on the literature review in the theoretical part of the work. The practical part will consist of the case studies with demonstrations of managing digital identity on real world scenarios.

The scoring method will be applied to evaluate and compare various approaches to digital identity management. As a result, the best practices recommendations will be identified and formulated in the conclusion of the thesis.

The proposed extent of the thesis

30-40 pages

Keywords

Digital identity management, online presence, personal data, data protection.

Recommended information sources

COVER, Rob. Digital identities: Creating and communicating the online self. Academic Press, 2015. ISBN: 9780128004272.

EC. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [online] Available from: http://eur-lex.europa.eu/eli/reg/2016/679/oj

LEHMANN, Anja, et al. Privacy and Identity Management. Facing up to Next Steps. Springer, 2017. ISBN 978-3-319-55782-3

MAHALLE, Parikshit Narendra; RAILKAR, Poonam N. Identity Management for Internet of Things. River Publishers, 2015.

Expected date of thesis defence

2017/18 SS – FEM

The Bachelor Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 18. 12. 2017

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 21. 12. 2017

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 06. 03. 2018

Declaration

I declare that I have worked on my bachelor thesis titled "**Personal digital identity management**" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on March 2018 ______________________________

Acknowledgement

I would like to thank Ing. Miloš Ulman for their advice and support during my work an this thesis.

Personal digital identity management

Abstract

The thesis identify and summarize the best practices for personal digital identity management, making a review of the current state of the art and trends in digital identity management, identifying and evaluating main practices for digital identity management and based on real cases recommendations were given. The thesis is based on the literature review in the theoretical part of the work. The practical part based on case studies with demonstrations of real examples of managing digital identity. Results of this recommendation were evaluated with the multicriteria analysis that implies the identification that is relevant or that reflects importance in the final decision, the scoring method will be applied. As a result, the best practices recommendations were identified and formulated the conclusion of the thesis.

Keywords: Digital identity management, online presence, personal data, data protection, social networks.

Index

List of tables

1 Introduction

Human identity can be defined as the set of features that makes a person be who they are and what distinguishes them from others while allowing one to interact in their respective environment (1). It is built according to the conditions of the person and also of the events and experiences, in fact, human identity is only fully realized in terms of the interactions with external environments and is a reality that evolves over time.

Today new technologies related to information and communication are expanding the concept of identity and is complete with the digital identity then personal digital identity distinguishes between information explicitly disclosed by the person.

The personal information that moves on the Internet is growing and every day millions of people use services such as social networks, forums, shopping pages, etc., leaving a trail of activity, tastes and preferences, and finally the behavior and way of being in a digital identity. In this way the digital identity that is formed of each individual can say a lot about a person, but cannot distinguish facts of the presence that are authentic or not at the moment. (11)

This research work based on the use of personal data that people upload to social networks, and in general to the Internet world, give an affirmation or negative about the correct or incorrect use of the actions of people, in order to give a suggestion for the best privacy management.

2 Goals and methodology

The main objective of the thesis is to identify and summarize the best practices for personal digital identity management on social networks. The project will focus mainly on recommendations based in the new General Data Protection Regulation.

Firstly, a literature review will be made to describe the current state of the art and trends in digital identity management in order to make a good recommendation for the administration of personal data when it is uploaded to the web.

In order to identify and evaluate the main practices for digital identity, it can be observed that simple mistakes that result in carelessness can cause great damage, in people who are involved in the self-identity impersonation by an unknown person.

To formulate future recommendations and conclusions we can see that the upload of personal information to social networks must be conscious and responsible. Also, it must take into account the purposes with which profiles are opened as well with the people who wants to communicate to keep good control of the administration of data and personal information.

The thesis is based on the literature review in the theoretical part of the work. The practical part will consist of the case studies with demonstrations of real examples of managing digital identity and look the mistakes that people did to enter in impersonation.

Based on the multicriteria analysis that implies the identification that is relevant or that reflects importance in the final decision, the scoring method will be applied. As a result, the best practices recommendations will be identified and formulated.

3 Literature review

3.1 Identity

The Identity is all the traits of an individual or community. These features characterize the subject or the community against the other. The formation of identity is a process that begins to take shape from certain specific conditions of the person, present from birth and, from there, changes according the facts and experiences that occur along his life. (4)

The identity could be divide by:

- Social identity
- Cultural identity
- National identity
- Gender identity
- Online identity

3.1.1 Online Identity

An online identity can be as permanent as an offline one, pseudonymous users often identify themselves in different social networks using the same account name. But because their handles are not based on real names, they can deliberately delineate their identity accordingly, and reassert anonymity if they wish. (1)

In this way there are two types of user information for the online identity, one that can be captured by social networking sites and information that is obtained through the electronic tracking. The users who share information in general aspects includes:

- Photos and other data
- Age and sex
- Bibliographic Information
- Updates or posts

- Contacts
- Interests
- Geographic location

3.2 Entity

A Credential Service Provide (CSP) is an entity that creates, issues and maintains credentials of subjects and provides partial identities, CSP forms part of an authentication system, most typically identified as a separate entity in a Federated authentication system. (5)

3.3 Role

It is the context in which the identity of an individual person may have many partial identities depending on the area in which the individual is located. (5)

3.4 Digital identity attributes

Identity attributes are characteristics of an identity and it can be classify in: (5)

- Legal documents
- Demographic
- Financial
- Biometric
- Transactional

3.5 Authentication

The authentication is applied in policies forms that define the required level of identity authorization. Authentication policies control the identity accuracy for a given transaction. The authentication method defines the mechanisms by which the subject can access the required service. (5)

3.6 Authorization

The authorization is a permission that someone gives to allow go through a certain actions, those are define most of the time in policies which explain the conditions in which subjects are allowed to access given identity service and data.(5)

3.7 Digital Identity Life Cycle

An identity life cycle is a term for the complete life cycle of this identity or for the access of a user in a given and determined system. A digital identity is the set of information about an individual, organization or electronic device that exists online. (5)

3.8 Software tools of Digital Identity

Software tools are a computer programs, those programs are employed in the development software and in digital identity are automated in software verification routines, software tools can assist in all activities of all phases of the software life cycle, including management and quality-assurance activities. (5)

3.9 Profiles

Much of the early current literature on social networks describes the conscious, use of an online technology related to social applications, then the process of performing identity occurs within a narrative of coherence over time, motivated by a cultural demand or imperative that are coherent, intelligible, and recognizable to others in order to allow social participation which include common axes of discrimination such as gender, ethnicity, ability, and age but might also be comprised of spurious experiences that are less easily categorical and less well demarcated in an identity difference dichotomy.(3)

Social networking sites can therefore be understood as sites through which identity categories are most effectively performed becoming a profile, then social net-works are built around individual user profiles, even though these are always produced and utilized in relation to others. The first step for the creation of any given profile is to engage in a form filling process, a process that now occurs countless times over one's lifetime.

Then we can recognize that this information may be made public in different ways. A user can choose to have the information published is public. Certain information may be public by default, social network sites can change its privacy policy at any time without user authorization. The context that was published with limited privacy settings might be visible when the privacy policy is altered. (20)

3.10 Privacy

Privacy is something that a person held in a reserved area. Therefore, some person is entitled to maintain their privacy away from other people, ensuring the confidentiality of his or her private things. (3)

3.11 Individual Security

Individual security could refer how to avoid becoming a victim of a single attack then a person needs to be aware of the places and situations where attacks can occur, in order to avoid them. (4)

Individual security could be related with personal safety means knowing the facts. Personal attacks may suffer them anyone, anywhere and anytime, in public or at home, day or night.

3.12 Social Networks

A Social Network is a network of individuals, organizations or entities that are connected by one or more types of relationships in social structure. (4)

Internet social networks are in websites that allow people to connect with a group of people, virtually, and share content, interact, create communities of similar interests: work, readings, games, commercial relations, etc.

In these communities, an initial number of participants send messages to members of their own social network based general contact email or inviting them to join the site. New participants repeat the process, and so grow the total number of members and network links. (4)

3.13 GDPR – General Data Protection Regulation

The processing of personal data must be designed to serve humanity. The right to the protection of personal data is not an absolute right and is related to its role in society and to maintain balance with other rights, taking into account the recognized principles of protection and privacy is taken in particular the respect of private and family life, home and communications, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom of enterprise, right to privacy effective judicial protection and a fair trial, and cultural, religious and linguistic diversity. (2)

It is then that this Regulation is applied to the total or partial treatment of personal data that will be treated in a lawful, loyal and transparent manner in relation to the interested party.

All processing of personal data must be transparent for information and communication regarding the treatment of such data is easily accessible and their rights in relation to the treatment. Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are treated.

This Regulation does not require that each individual treatment be governed by a specific rule. The purpose of the treatment must also be determined by the law of the Union or of the Member States.

The processing of personal data must also be considered lawful when necessary to protect an interest essential to the life of the interested party or that of another natural person. In other hand, the personal data processed that is automated must have been allowed by the interested parties who have provided this data in a structured format, generally mechanical reading.

If the personal data is processed for direct marketing purposes, the interested party may object to say treatment, including the elaboration of profiles in so far as it is related to say direct marketing.

In case of illegality with the personal data of an individual who does not take adequate measures in time, and if the breaches of the security of the personal data entail physical, material or immaterial damages for the physical persons, the person in charge must give constancy to notify the violation of the security of personal data to the competent control authority, unless the responsible party can demonstrate, based on the principle of proactive responsibility, the improbability that the violation of the security of personal data entails a risk for the rights and the freedoms of natural persons. (2)

In relation to non-EU countries the Commission may decide, with effects for the whole Union, that a third country or an international organization offers an adequate level of data protection, thus providing legal security and uniformity across the Union in what refers to the third country or international organization that is considered to offer such a level of protection.(2)

If the Commission recognizes that a third country, or an international organization no longer guarantees an adequate level of data protection, the transfer of personal data to that third country or international organization should be prohibited, unless the requirements of this Regulation relating to transfers based on adequate guarantees, including binding corporate rules.

To make sure that data protection is correctly Each EU country has to have at least one data protection supervisory authority. (2)

3.14 Social networks and their privacy policies and terms of use

3.14.1 Facebook

The Facebook security policy collects the place where it was made, pictures, the date of creation, in addition the type of content and the frequency and duration of the activities that a person has in his or her account as well as activity with other users information with other users of the service. Facebook collects information about people and groups to which is connected the frequency that she or him interact with them, collects information of the contacts, synchronizes or imports this information from any device.

Regarding the used devices Facebook collects information about computers, telephones or other devices where from where it is accessed, as well as the information generated by such devices as the operating system, the hardware version, the configuration of the device and the names and types of computer programs and files, also battery charging, signal strength, as well as device identification data. (6)

In the geographic information Facebook collects locations of the device, information about the connection of the mobile operator or internet service provider, the browser type, the language, the time zone, the mobile phone number and the IP address. Facebook specifies the uses of this information is to display relevant advertisements and share information with specific public, it affirms to provide information to external partners about any account in order to prevent fraud and illicit conduct, inside and outside its Services. (6)

Facebook says that once the security policy is accepted, permission is granted to use the name, profile photo, content and information related to commercial, sponsored or related content. This allows a company or other entity to display a name and / or profile picture with the content or information without the owner knowledge and user of the account won't receive any compensation for it.

Regarding the information collected within the European Economic Area ("EEA"), it can be transferred to external countries for the described purposes using standard contractual clauses approved by the European Commission, and adopting according to the European Union legislation and obtaining consent for legitimize the transfer of EEA data to the United States and other countries. (6)

3.14.2 Twitter

In Twitters' privacy policy reported that the information of each user is collected for the use of the company. The user, through his or her consent, allow the transfer of this information to the United States and / or to other countries for storage, processing and use by Twitter.

Twitter suggests to create strong passwords and they will not be held responsible for improper entry into the accounts.

Twitter affirms that the responsibility for all content, public or private is user’s responsibility and they do not supervise or control the content. By the agreement with the users "The user understands that their Content may be retransmitted by associates who also have the right to access, read, preserve, and make public any information as reasonably necessary to satisfy any applicable law, regulation, legal process or government request, enforce the Terms, including the investigation of potential violations thereof, detect, prevent, or otherwise cause fraud, security or technical problems, respond to requests for user support, or protect the rights, property or security of Twitter, users and to the public." (7)

3.14.3 LinkedIn

LinkedIn uses the information provided from the users to generate aggregate data that identifies them, such as generating statistics in terms of professions or paid occupations, taking into account the number of impressions on the ads as well as the demographic distribution of visitors to a website.

It also uses the user's data if necessary by the company for security and to investigate possible frauds or other violations of its conditions of use or its privacy policy, and / or attempts to harm our Members or Visitors. In case of irregularities, the company is granted the right to disclose information when required by law, in a subpoena or other judicial procedure, to enforce the conditions of use, and if it were to protect the rights and safety of LinkedIn and other Members. (19)

4 Practical part

The identity impersonation or falsification of data used in the creation of the profiles occurs when a person is another person before a third party, generally with an illegal purpose or with the intention of causing harm. Identifying three specific cases and ten suggestions for the best administration and profile creation, it is included the general requirements that the websites request for the creation of a profile through the scoring method, the results and conclusions of the trends that a user can have are given**.**

4.1 Leah Palmer Mar 5, 2015 BBC

She is a British girl, single, in her twenties, who lived in Dubai for the time of the case. Actually, Leah Palmer does not exist.

The woman who appears as Leah is Ruth Palmer and she is married.
Ruth discovered that during the last three years someone has been stealing her personal pictures in social networks and setting up in the network of false profiles for communicate with people.

The person, who calls herself Leah Palmer, described Ruth's husband as "psychotic ex" in this version of the fake profile on social networks made meetings with at least six different men.

While the authentic Ruth Palmer has 140 followers on Instagram, Leah has more than 800 and all her photographs more than 900 are of Ruth and her friends.

"One of them had broken up with a real girlfriend to have a relationship online with this girl who they thought was me." Said Ruth

The police offered her support, but since no crime had been committed and the person did not use Ruth's full name, they could not do much.

Ruth says she always kept her accounts with the maximum privacy settings.

4.1.1 Assessment

According to (8), following aspects were observed.

- What went wrong

In social networks anyone can register without any requirement beyond an email, it is in that way any false profile can appear.

The fact that photographs appear in the social networks without user consent is most probably because the person shares these with other users of the network without filtering publication requirements.

Most probably she posted pictures with under any security and complete public.

- How to prevent it

The privacy policy conditions and terms of use of the social network should be read carefully before starts to use it.

The right to one's own image is aimed at protecting not only privacy. Anyone can prevent a photograph in which she appears without your consent. Said consent must be expressed in a document signed by both parties.

- Lessons learnt

When a picture or image is published in a social network, it must be taken into account that certain rights like the use of the name, profile picture, content and information into this accounts are being transferred to them, and then the images belong to that social network.

The activity of an individual in social networks will give the final intention, so it must be clear what kind of relationship achieve with should be achieved with those people who decide to share the profiles.

4.2 Sweetie Published on Nov 7, 2013 BBC

Sweetie is a 10 years old virtual girl from Philippines. The image of Sweetie was generated by graphic designers from the humanitarian group in the Netherlands.

According to Van Santbrink a member or humanitarian group, the organization gave the police the identities of those who showed interest in this project.

The virtual girl served as a bait to identify at least 1,000 of the sex offenders, out of a total of more than 20,000 from more than 70 countries who responded to the offer to interact with her in exchange for money.

The predators feel safe and anonymous they use fake names, live far away and can pay with untraceable prepaid credit cards that anybody can buy anywhere.

They contact kids on dating sites social networks and public chat rooms. The organization used bits of information and they were able to identify them in Google, Facebook and other sources social network. The organization collect their names, phone numbers, pictures and video footage during the communication with this virtual girl. (9)

4.2.1 Assessment

- What went wrong

  The anonymity of the Internet allows any person with any intentions to modify their real identity to catch someone, in this case just to chat. While this is an experiment that could show how lack of the application of basic security rules in private web cams are, then it can be seen that malicious people fake their identity, it is then that they can be displayed without restriction through the Internet with almost any content, taking care that on the webcams, the video can be recorded on the other side.

- How to prevent it

To make minors aware of the use of technology in terms of communicating with people, taking care of their image through the Internet, so that in the near future, young people should be able to preserve their autonomy and privacy.

- Lessons learnt

It is very important to educate children when they start to learn to read and write how to use personal and family data when they will use internet. In social networks and chat rooms, anyone can pose as a fake person to obtain information about schedules, activities, addresses and others.

4.3 Fingerprints of a selfie

Isao Echizen, a researcher at the National Institute of Informatics of Japan, says that “by placing the index and middle fingers in front of the camera, they can steal our identity”. According to the specialist, the new technologies allow to enlarge the images easily and get to scan the fingerprints graphically, especially if the fingers are "exposed to strong lighting". (10)

4.3.1 Assessment

- What went wrong

Pictures with angles showing the palms and fingers of the hands could be possible copy.

- How to prevent it

Not to expose the palms hands in pictures with direct light.

- Lessons learnt

Although copying fingerprints is possible, experts in biometrics say that is still a complex process is required

4.4 Evaluation of approaches to personal identity management on social networks

Based on the multicriteria analysis to get and identify the final decision in what people pay attention, three people were questioned according to the recommendations established based on the real cases already presented.

Person A is 20-year-old without a university studies, he is not married, he works for a private company and uses social networks at least 5 times a week.

Person B is 36 years old, a married woman with 2 children under the age of 10 years old, she works in a private company and uses social networks at least 3 times a week.

The person C is 45-year-old adult professional engineer who works for the state, he is not married and he uses social networks at least once a week.

4.4.1 Multiple criteria

Alternatives

The alternatives are based on the general requirements or criteria that any person has to follow when is going to upload information to create a profile or account in to the social networking sites, based on three cases presented above, following criteria will be examined by the scoring method and reforcing by Saaty's method. The criteria are basic and general parameters that must be followed to have an account in social networks.

Table 1 Criteria

Criteria	Weight
Fill out forms	3
Age	3
Email	3
Verify data	1
privacy policies	5
Password	1

To identify the weight requirement in multicretira method, it was observed that in the social media is more important to accept the privacy policy for get an account, other criteria are not so relevant, even though these social networks recommend paying attention to the password. (17) - (16)

Table 2 - Weight requirement

weight requirement	
5	High
3	Medium
1	Low

Alternatives

A. Read carefully the privacy policy.
B. Be aware of the use of technology in terms of communicating with people
C. Be careful about pictures posted on social networks
D. Limit the audience of all your publications.
E. Monitor what is published about you.
F. Evaluate the attitudes of the contacts.
G. Customize, know and configure in detail the privacy options.
H. Never communicate your personal data, especially to strangers.
I. Only accept friend requests from people you know.
J. Protect your password.

4.4.2 Scoring method

Table 3. Person A - scoring method

Person A	Weight	A	Score	B	score	C	score	D	Score	E	Score
Fill out forms	3	3	9	5	15	5	15	5	15	5	15
Age	3	5	15	3	9	5	15	5	15	5	15
Email	3	1	3	1	3	3	9	1	3	5	15
Verify data	1	5	5	5	5	5	5	5	5	5	5
privacy policies	5	3	15	5	25	5	25	3	15	5	25
Password	1	5	5	5	5	5	5	5	5	5	5
Total			52		62		74		58		80

Person A	weight	F	Score	G	score	H	score	I	Score	J	Score
Fill out forms	3	1	3	5	15	5	15	1	3	5	15
Age	3	5	15	5	15	5	15	5	15	5	15
Email	3	5	15	3	9	1	3	3	9	1	3
Verify data	1	5	5	5	5	5	5	5	5	5	5
privacy policies	5	5	25	5	25	5	25	1	5	5	25
Password	1	5	5	5	5	5	5	1	1	5	5
Total			68		74		68		38		68

Table 4. Person B - scoring method

Person B	weight	A	Score	B	score	C	score	D	Score	E	Score
Fill out forms	3	3	9	3	9	1	3	3	9	1	3
Age	3	3	9	3	9	3	9	5	15	3	9
Email	3	3	9	5	15	3	9	3	9	5	15
Verify data	1	5	5	3	3	1	1	1	1	3	3
privacy policies	5	1	5	1	5	3	15	1	5	5	25
Password	1	3	3	3	3	3	3	3	3	1	1
Total			40		44		40		42		56

Person B	weight	F	Score	G	score	H	score	I	Score	J	Score
Fill out forms	3	1	3	3	9	1	3	1	3	1	3
Age	3	5	15	3	9	5	15	5	15	3	9
Email	3	5	15	3	9	5	15	5	15	3	9
Verify data	1	5	5	5	5	1	1	3	3	3	3
privacy policies	5	1	5	5	25	1	5	3	15	3	15
Password	1	1	1	5	5	5	5	5	5	5	5
Total			44		62		44		56		44

Table 5. Person C - scoring method

Person C	weight	A	score	B	score	C	score	D	Score	E	Score
Fill out forms	3	5	15	1	3	1	3	3	9	1	3
Age	3	5	15	3	3	1	3	3	9	1	3
Email	3	5	15	5	15	5	15	5	15	5	15
Verify data	1	3	3	3	3	1	1	3	3	3	3
privacy policies	5	5	25	3	15	1	5	5	25	1	5
Password	1	3	3	5	5	5	5	5	5	5	5
Total			76		44		32		66		34

Criteria C	weight	F	score	G	score	H	score	I	Score	J	Score
Fill out forms	3	1	3	1	3	3	9	1	3	5	15
Age	3	5	15	3	9	1	3	3	9	1	3
Email	3	3	9	5	15	5	15	5	15	5	15
Verify data	1	3	3	1	1	3	3	3	3	1	1
privacy policies	5	1	5	3	15	1	5	1	5	5	25
Password	1	5	5	5	5	5	5	5	5	5	5
Total			40		48		40		40		64

4.4.3 Saaty's matrix

This method was proposed by Thomas Saaty. It is a procedure of comparison by pairs of the criteria that starts from a square matrix in which the number of rows and columns is defined by the number of criteria to be weighted. This establishes a comparison matrix between pairs of criteria, comparing the importance of each of them with others. (14) In this way the three people were questioned taken the as criteria the recommendations given.

Table 6. Saaty's matrix criteria weights

1	Equally preferred
3	Moderately preferred
5	Strongly preferred
7	Very strongly preferred
9	Extremely preferred

Ordered list of criteria

Table 7. Person A - Saaty's matrix results

D	E	G	C	J	F	H	B	I	A
0,21	0,17	0,16	0,12	0,08	0,07	0,06	0,05	0,05	0,04

Table 8. Person B - Saaty's matrix results

G	I	B	J	H	A	E	F	D	C
0,24	0,18	0,12	0,1	0,08	0,07	0,07	0,06	0,04	0,03

Table 9. Person C - Saaty's matrix results

A	D	J	B	E	F	G	H	I	C
0,31	0,19	0,13	0,12	0,07	0,04	0,04	0,04	0,04	0,03

5 Results and discussion

Based on the scoring method result, the most important recommendation to take care in the case of person A, who is a person of 20 years old, it is to monitor what is published about him, in the case of person B who is a person of 36 years old, it is to customize, know and configure in detail the privacy options and in the case of person C who is a person of 45 years old, it is to read carefully the privacy policy. Based on Saaty's matrix result, the most important recommendation to take care in the case of person A, is to limit the audience of all the publications, in the case of person B and person C, results are the same as scoring method.

This study does not present recommendations to avoid scams and the use of credit cards, payments or transactions in these social networks.

The most common and accessible social networking websites recommend choosing a secure password using a combining of at least six numbers, letters and punctuation marks (such as! And &) even though the most important thing for them is to accept the security policy. They also recommend closing the sessions of the devices, especially if they belong to other people. These companies are not responsible for the content that the user uploads to the network unless they do not follow the agreement in the policy.

If we take into account that for these companies a very important and safe way is the password, it can be seen that in the results of the three people, none of them places the use of a secure password as the first importance.

Then to look in attention and results in both methods used it was taken general basic information to show that uses of internet has the tendency of growing so statistical study from U.S. showed that (14) as for false accounts there are about 81 million false accounts on Facebook 88% of companies with more than 100 employees use Twitter for marketing purposes. 59% of Americans, with social media accounts, think that customer service through them, has facilitated the obtaining of answers to questions and problems. More than 56% of adults who use the Internet use more than one social network.

According to the university texts of the University of Barcelona, the recommendations for the creation of a profile on a website are: to know the differences between the various social networking sites and how to use them, know what use we can give to the materials that are in the network and to find and adjust the privacy settings of social networking sites. (12)

"Being aware of the privacy of personal data on the Internet and the use that can be made of this data becomes a key element for the effective management of digital identity" .It is observed that these recommendations are a summary of the recommendations established based on the cases analyzed.

According to an article of the University of Valencia, based on an application of a questionnaire to 170 adolescents aged from 12 to 16 years old, a certain lack of knowledge of the protection and privacy mechanisms offered by social networks has been perceived.

In addition, this questionnaire showed that there has been a lack of awareness of the problems that can lead to misuse of these tools both to their personal privacy and their own image. (13)

6 Conclusion

The best practices for personal digital identity management before deploying it, were formulated based on real cases. Those recommendations are taken keeping that the digital identity is measured by the impact of what is shared or displayed in social media. In the social media environment, digital identity, information, privacy and security are aspects that go together as seen in the three real cases exposed, it is then that in order to correctly manage the digital identity, privacy and information must be taken in consideration.

Based on the multi criteria analysis to get and identify the decision in what people could take attention, three people were questioned according to the recommendations established based on the real cases already presented, none of those get the information share as was recommended by social networks. Depending on the nature of the data uploaded on social sites, the perception of users regarding the degree of privacy is different for everybody. Therefore, it can be found from information that users do not perceive as private data and whose knowledge by third parties or companies is not seen as a negative aspect, including data that are considered very sensitive and that can be transmitted or used outside the original environment.

The services that require the user to enter personal information always have been associated with policies reflected in the terms of privacy that must be signed and accepted by users when hiring or accessing these services. On many occasions, users do not read these conditions even if they know that they will allow to share personal information and, therefore, do not know to what extent their data can be used. In this aspect, it is important to inform and educate children about the use of their personal data, so it is recommended to inform them not to share more information than is necessary and to take care of personal information.

7 Bibliography

1. COVER, Rob. Digital identities: Creating and communicating the online self. Academic Press, 2015. ISBN: 9780128004272.

2. EC. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (online) Available from: http://eur-lex.europa.eu/eli/reg/2016/679/oj

3. LEHMANN, Anja, et al. Privacy and Identity Management. Facing up to Next Steps. Springer, 2017. ISBN 978-3-319-55782-3

4. MAHALLE, Parikshit Narendra; RAILKAR, Poonam N. Identity Management for Internet of Things. River Publishers, 2015. ISBN 8793102909

5. ELISA BERTINO, Kenji Takahashi, Identity Management. Concepts, Technologies, and Systems, Artech House Publishers, 2011, ISBN 9781608070404

6. Facebook. Facebook companies. 2018. Retrieved on 25.1.2018 from: https://www.facebook.com/help/111814505650678

7. Twitter. Twitter companies. 2018. Retrieved on 25.1.2018 from: https://about.twitter.com/en_us/safety/enforcing-our-rules.html

8. ZOE KLEINMAN, Who's that girl? The curious case of Leah Palmer. Retrieved on 29.1.2018 from: http://www.bbc.com/news/technology-31710738

9. ANGUS CRAWFORD, Computer-generated 'Sweetie' catches online predators. Retrieved on 29.1.2018 from: http://www.bbc.com/news/uk-24818769

10. GARETH DAVIES. How YOUR selfies are allowing crooks to steal your identity... by zooming in on your FINGERS: HD lenses mean thieves can replicate your fingerprints. Retrieved on 29.1.2018 from: http://www.dailymail.co.uk/news/article-4104918/How-selfies-allowing-crooks-steal-identity-zooming-FINGERS-HD-lenses-mean-thieves-replicate-fingerprints.html

11. LORNA CAMPOS. STATISTICS IN SOCIAL NETWORKS THIS 2017. Retrieved on 29.1.2018 from: https://www.postedin.com/2017/07/19/estadisticas-en-redes-sociales-este-2017

12. GIONES VALLS. The management of digital identity: a new informational and digital skill. Retrieved on 25.1.2018 from: http://bid.ub.edu/24/giones2.htm

13. LORENA RODRIGUEZ GARCIA. Perspective of young people on security and privacy in social networks. Retrieved on 25.1.2018 from: https://icono14.net/ojs/index.php/icono14/article/view/885

14. THOMAS L. SAATY. Mathematical Methods of Operations Research, McGraw - Hill,2004, ISBN 0-486-49569-8

15. https://www.mitre.org/ . Retrieved on 25.1.2018 from : http://www2.mitre.org/worxk/sepo/toolkits/STEP/files/ScoringMethodsContent.pdf

16. EVANGELOS Triantaphyllou, Springer Science+Business Media Dordrecht. Multi-criteria Decision Making. Publisher: Springer US 2000 ISBN 978-1-4419-4838-0

17. Department for Communities and Local Government: London, January 2009. Multi-criteria analysis. January 2009. ISBN: 978-1-4098-1023-0

19. LinkedIn. LinkedIn companies. 2017. Retrieved on 25.1.2018 from: https://www.linkedin.com/legal/privacy-policy

20. IAN LONG. The New Rules. Jordan Publishing, 2016. ISBN 1784732133, 9781784732134

8 Appendix

Table 10. Person A - scoring method results

Person A	E	C	G	F	H	J	B	D	A	I
Fill out forms	15	15	15	3	15	15	15	15	9	3
Age	15	15	15	15	15	15	9	15	15	15
Email	15	9	9	15	3	3	3	3	3	9
Verify data	5	5	5	5	5	5	5	5	5	5
Privacy policies	25	25	25	25	25	25	25	15	15	5
Password	5	5	5	5	5	5	5	5	5	1
Total	80	74	74	68	68	68	62	58	52	38

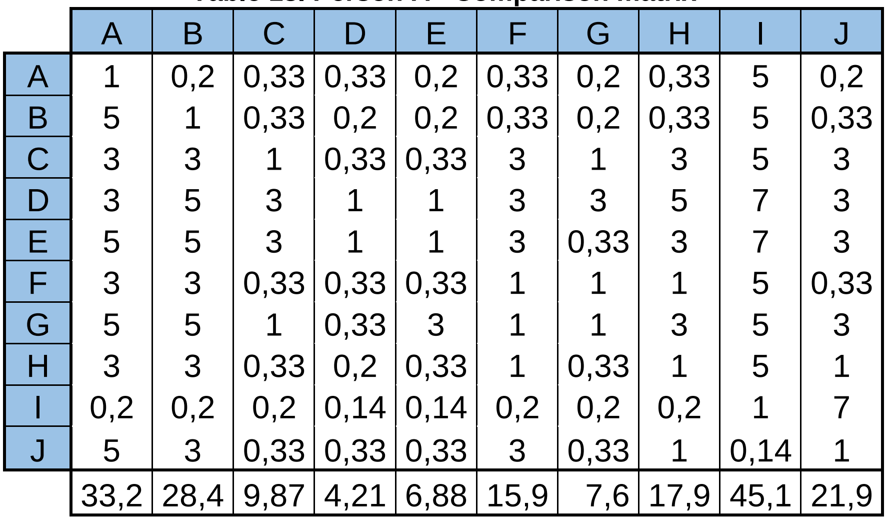
Table 11. Person B - scoring method results

Person B	G	E	I	B	F	H	J	D	A	C
Fill out forms	9	3	3	9	3	3	3	9	9	3
Age	9	9	15	9	15	15	9	15	9	9
Email	9	15	15	15	15	15	9	9	9	9
Verify data	5	3	3	3	5	1	3	1	5	1
Privacy policies	25	25	15	5	5	5	15	5	5	15
Password	5	1	5	3	1	5	5	3	3	3
Total	62	56	56	44	44	44	44	42	40	40

Table 12 Person C - scoring method results

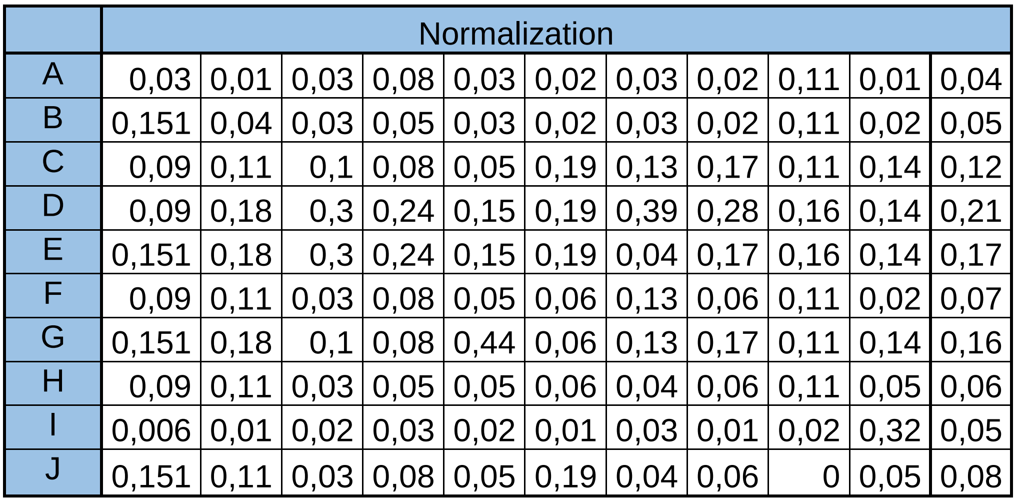
Person C	A	D	J	G	B	F	H	I	E	C
Fill out forms	15	9	15	3	3	3	9	3	3	3
Age	15	9	3	9	3	15	3	9	3	3
Email	15	15	15	15	15	9	15	15	15	15
Verify data	3	3	1	1	3	3	3	3	3	1
Privacy policies	25	25	25	15	15	5	5	5	5	5
Password	3	5	5	5	5	5	5	5	5	5
Total	76	66	64	48	44	40	40	40	34	32

Table 13. Person A - Comparison matrix



	A	B	C	D	E	F	G	H	I	J
A	1	0,2	0,33	0,33	0,2	0,33	0,2	0,33	5	0,2
B	5	1	0,33	0,2	0,2	0,33	0,2	0,33	5	0,33
C	3	3	1	0,33	0,33	3	1	3	5	3
D	3	5	3	1	1	3	3	5	7	3
E	5	5	3	1	1	3	0,33	3	7	3
F	3	3	0,33	0,33	0,33	1	1	1	5	0,33
G	5	5	1	0,33	3	1	1	3	5	3
H	3	3	0,33	0,2	0,33	1	0,33	1	5	1
I	0,2	0,2	0,2	0,14	0,14	0,2	0,2	0,2	1	7
J	5	3	0,33	0,33	0,33	3	0,33	1	0,14	1
	33,2	28,4	9,87	4,21	6,88	15,9	7,6	17,9	45,1	21,9

Table 14. Person A - Normalized matrix



	Normalization										
A	0,03	0,01	0,03	0,08	0,03	0,02	0,03	0,02	0,11	0,01	0,04
B	0,151	0,04	0,03	0,05	0,03	0,02	0,03	0,02	0,11	0,02	0,05
C	0,09	0,11	0,1	0,08	0,05	0,19	0,13	0,17	0,11	0,14	0,12
D	0,09	0,18	0,3	0,24	0,15	0,19	0,39	0,28	0,16	0,14	0,21
E	0,151	0,18	0,3	0,24	0,15	0,19	0,04	0,17	0,16	0,14	0,17
F	0,09	0,11	0,03	0,08	0,05	0,06	0,13	0,06	0,11	0,02	0,07
G	0,151	0,18	0,1	0,08	0,44	0,06	0,13	0,17	0,11	0,14	0,16
H	0,09	0,11	0,03	0,05	0,05	0,06	0,04	0,06	0,11	0,05	0,06
I	0,006	0,01	0,02	0,03	0,02	0,01	0,03	0,01	0,02	0,32	0,05
J	0,151	0,11	0,03	0,08	0,05	0,19	0,04	0,06	0	0,05	0,08

Table 15. Person B - Comparison matrix

	A	B	C	D	E	F	G	H	I	J
A	1	1	3	3	1	1	0,2	1	0,33	1
B	1	1	3	3	1	1	0,2	1	5	1
C	0,33	0,33	1	0,33	1	1	0,14	0,33	0,33	0,33
D	0,33	0,33	3	1	0,2	0,33	0,2	1	0,14	0,2
E	1	1	1	5	1	1	0,2	1	0,2	1
F	1	1	1	3	1	1	0,2	1	0,2	1
G	5	5	7	5	5	5	1	1	3	1
H	1	1	3	1	1	1	1	1	0,33	1
I	3	0,2	3	7	5	5	0,33	3	1	3
j	1	1	3	5	1	1	1	1	0,33	1
	14,7	11,9	28	33,3	17,2	17,3	4,48	11,3	10,9	10,5

Table 16. Person B- Normalized matrix

	Normalization										
A	0,068	0,08	0,11	0,09	0,06	0,06	0,04	0,09	0,03	0,09	0,07
B	0,068	0,08	0,11	0,09	0,06	0,06	0,04	0,09	0,46	0,09	0,12
C	0,023	0,03	0,04	0,01	0,06	0,06	0,03	0,03	0,03	0,03	0,03
D	0,023	0,03	0,11	0,03	0,01	0,02	0,04	0,09	0,01	0,02	0,04
E	0,068	0,08	0,04	0,15	0,06	0,06	0,04	0,09	0,02	0,09	0,07
F	0,068	0,08	0,04	0,09	0,06	0,06	0,04	0,09	0,02	0,09	0,06
G	0,341	0,42	0,25	0,15	0,29	0,29	0,22	0,09	0,28	0,09	0,24
H	0,068	0,08	0,11	0,03	0,06	0,06	0,22	0,09	0,03	0,09	0,08
I	0,205	0,02	0,11	0,21	0,29	0,29	0,07	0,26	0,09	0,28	0,18
J	0,068	0,08	0,11	0,15	0,06	0,06	0,22	0,09	0,03	0,09	0,1

Table 17. Person C - Comparison matrix

	A	B	C	D	E	F	G	H	I	J
A	1	5	7	3	9	7	7	7	7	3
B	0,2	1	5	0,33	3	5	5	5	5	0,33
C	0,14	0,2	1	0,14	0,33	0,33	0,33	3	0,33	0,14
D	0,33	3	7	1	3	5	5	5	5	3
E	0,11	0,33	3	0,33	1	3	3	3	3	0,2
F	0,14	0,2	3	0,2	0,33	1	1	1	1	0,33
G	0,14	0,2	3	0,2	0,33	1	1	1	1	0,33
H	0,14	0,2	3	0,2	0,33	1	1	1	1	0,33
I	0,14	0,2	3	0,2	0,33	1	1	1	1	0,33
J	0,33	3	7	0,33	5	3	3	3	3	1
	2,69	13,3	42	5,94	22,7	27,3	27,3	30	27,3	9,01

Table 18. Person C - Normalized matrix

	Normalization										
A	0,371	0,38	0,17	0,5	0,4	0,26	0,26	0,23	0,26	0,33	0,31
B	0,074	0,08	0,12	0,06	0,13	0,18	0,18	0,17	0,18	0,04	0,12
C	0,053	0,02	0,02	0,02	0,01	0,01	0,01	0,1	0,01	0,02	0,03
D	0,124	0,23	0,17	0,17	0,13	0,18	0,18	0,17	0,18	0,33	0,19
E	0,041	0,03	0,07	0,06	0,04	0,11	0,11	0,1	0,11	0,02	0,07
F	0,053	0,02	0,07	0,03	0,01	0,04	0,04	0,03	0,04	0,04	0,04
G	0,053	0,02	0,07	0,03	0,01	0,04	0,04	0,03	0,04	0,04	0,04
H	0,053	0,02	0,07	0,03	0,01	0,04	0,04	0,03	0,04	0,04	0,04
I	0,053	0,02	0,07	0,03	0,01	0,04	0,04	0,03	0,04	0,04	0,04
J	0,124	0,23	0,17	0,06	0,22	0,11	0,11	0,1	0,11	0,11	0,13