Proceedings of the World Congress on Engineering 2013 Vol II,
WCE 2013, July 3 - 5, 2013, London, U.K.

# A Framework to Assess the Computer Security Skills of People in the Information Society

Antoni Martínez-Ballesté, Juan Francisco Martínez-Cerdà and Agusti Solanas

***Abstract*—The so-called Information Society is founded on information and communication technologies (ICT). A wide variety of people use ICT to create, distribute, consume and manipulate information in a daily basis. Although there are experts skilled in security issues, most ICT users have not got a vast knowledge and understanding of the risks that a wrong employment of ICT might imply. Notwithstanding, it is not apparent how to measure the actual level of awareness of the users and their computer security skills.**

**With the aim to address this problem, we propose a framework to assess the computer security skills of ICT users. First, we identify a set of *assessment areas* to consider. Second, we define the *indicators* that allow the computation of *area indexes* with which we can value the computer security skills of ICT users. Our proposal has been tested in practice and we present the study and the obtained results.**

**Thanks to the proposed framework, it is possible to gather precise information about the security understanding of people. As a result of this knowledge, specific actions could be taken on the analysed subjects. Thus, we provide a comprehensive analysis tool for IT managers, CTO and e-Government experts interested in improving the computer security skills of their staffs within their departments, companies and administrations.**

***Index Terms*—ICT Skills, Internet Security, Social Studies.**

## I. Introduction

The Information Society is founded on the massive access to the Information and Communication Technologies (ICT) by very diverse people: from highly educated professionals to primary school children, from retired people that have just started discovering the Internet to technology geeks that countdown the days to the next smartphone launch. They all use computers and Internet services. For instance, in 2012 72% of the European citizens declared to have used Internet in the last three months and, in 2011, around 40% participated in social networks [1]. Although ICT offer an unprecedented way of knowing, sharing, creating and living, the reality is that users and their information are not immune to being attacked by technology offenders.

In the beginning of the Internet, attackers were focussed on mainframes and servers. On the contrary, nowadays, the most precious targets are millions of users that are exposed to losing their data or even their money as a result of successful attacks. In addition, attacked systems can unconsciously take part in large scale distributed denial of service attacks against services and critical infrastructures. Consequently, guaranteeing the *security* of users' devices is crucial to the security of these services and infrastructures.

Martínez-Ballesté and Solanas are with the Dept. of Computer Eng. and Maths of Universitat Rovira i Virgili. Martínez Cerdá is with the Department of Journalism and Communications Studies of Universitat Autònoma de Barcelona.

Corresponding author: antoni.martinez@urv.cat

The massive use of ICT paves the way to a simple gathering of private data. Those data con be analysed with intelligent data mining algorithms to obtain personal information about ICT users. As a result, privacy is endangered by an unprecedented number of threats: from eavesdroppers that profile users upon their requests to a location-based service, to the Big Brother effect that entails the use of massive Internet search engines and e-mail services. Clearly, *security* and *privacy* issues related to the use of ICT must be thoroughly considered in order for the Information Society to become feasible and sustainable in the long term.

The knowledge and abilities of ICT users have evolved as fast as the very ICT did. During the 1990's, an average ICT user was supposed to be proficient in using an operating system (specially managing files and folders), in writing with a word processor, in working with spreadsheets and having some knowledge of multimedia formats [2], [3]. Notwithstanding, with the wide adoption of the Internet and its related technologies, some more skills were added to the former list (for instance, sending e-mails and surfing the web), and the list of skills and common ICT activities keeps growing with each passing day. Unfortunately, security and privacy issues have been traditionally considered out of the scope of the average ICT user. That started to change in the beginning of 2000, when the concept of security of ICT users gained importance; especially after the publication of several reports [4], [5], [6], [9] that captured the attention of governments and institutions [7], [8].

Assessing the computer security skills of ICT users is paramount to properly evaluate the health of the Information Society. To that end, agencies and governments have been publishing reports on the security aspects of computers and their users. Those reports tend to measure technological aspects (*e.g.*, the use of antivirus software) and issues that are not straightly related to security (*e.g.* having several partitions on the disk). Moreover, to our knowledge, there is no methodology that allows the assessment of security of ICT users in a holistic way, this is, taking into account the user's attitudes and behaviours.

### A. Contribution and Plan of the Paper

In this paper, we present a framework to assess the computer security skills of ICT users. To that end, we identify several *areas* of interest and describe a set of *indicators* that allow the assessment of the security skills of users within those areas. By using these indicators we compute the *ICT User Security Index* (ICT-USI) and other related values. Our framework provides a comprehensive assessment of relevant areas in ICT, specifically those Internet technologies accessible via personal computers.

The rest of the article is organised as follows: Section II summarises the context in the methodology of our study.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

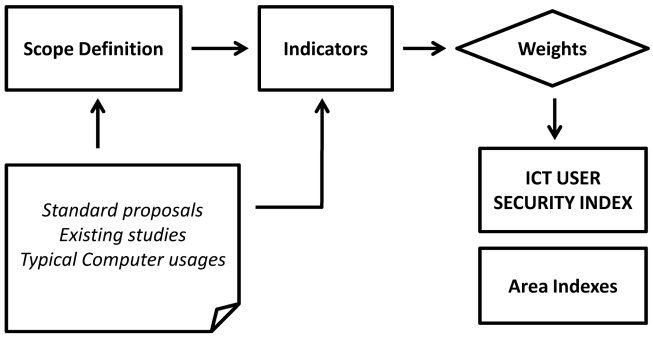


Fig. 1. The process for elaborating the ICT User Security Index.

Section III describes the studied assessment areas. Next, Section IV elaborates on the indicators used to assess each area and Section V explains how the ICT-USI and other indexes are computed. We show the results of a real study in Section VI and we conclude the paper in Section VII.

## II. Context and Methodology

The proposed assessment framework was conceived under a research project conducted by the Universitat Rovira i Virgili and FOBSIC [9], an organization aiming at analysing the impact of the ICT on the Catalan [1] society. The work was developed by a group of computer scientists, experts in social studies and ICT users educators.

To define the methodology of our study, we followed the process illustrated in Figure 1. During sections III, IV and V we elaborate on the above processes. The first step consisted in studying some of the relevant existing resources for ICT and computer security assessment, mainly reports of statistical agencies and other organizations [4], [5], [6], [8].

Upon analysing the aforementioned reports, we obtained a list of questions and their corresponding *indicators*, which were evaluated aiming at averting overlaps (*i.e.* different questions from different questionnaires measuring very similar indicators). In a second step, we categorised those elements/questions into six *assessment areas* (see Section III) and came up with some new indicators and aspects to be evaluated that were not taken into account in the analysed reports. We iterated on the list of indicators (fusing them, removing them, etc.) until the number of indicators could fit into a 15-minute questionnaire.

Finally, in a third stage, we assigned a value to the indicators according to their *level of knowledge*. To that end, we used a simplified model of Bloom's Taxonomy [10] consisting in *knowing*, *doing* and *behaving*. Thus, we assigned weights to each indicator so as to obtain the final ICT-USI index. Additionally, we also computed a specific index for each assessment area.

## III. Assessment Areas

The definition of assessment areas is important in two aspects. On the one hand, it clearly allows the easy classification of the indicators into groups and, more importantly, it allows computing *area indexes* aiming at comparing skills according to a specific area. Next, we describe the six assessment areas that we have defined for this framework.

- *Computer System (CS).* This area is related to the use of security tools that affect the very computer equipment and the information it contains. This could be simply addressed by asking *Do users take care of their computers?* For example, the update of the operating system and the presence of antivirus software are considered. This area is important for several reasons, *e.g.* the possibility of becoming part of a botnet is directly related to some of the aspects evaluated in this area.
- *Information Access (IA).* Their indicators measure the awareness of users while browsing the web. Certainly, this is the main activity of average users while using the Internet (in some scenarios, users spend more time surfing the web than watching TV [11]). Moreover, most of the current Internet services are offered trough the browser.
- *Electronic Mail (EM).* Personal communication using the e-mail service is also considered as a specific assessment area. Whether the e-mail service is accessed from the browser or from a specific user agent software, the fact is that the attitudes and cautions taken while sending and reading e-mails are closely related to security.
- *Passwords (PW).* Indeed, passwords are the most widely used identity authentication techniques, partially due to the scarce adoption of biometrics and electronic certificates. Hence, passwords (and specifically their strength and management) deserve a specific assessment area.
- *Social Networking (SN).* The number of users registered to social network services is steadily approaching the number of Internet active users. Social network activities in the most popular services entail well-known privacy risks. Moreover, the everyday social activities through the web involve a series of specific habits and behaviors. For all these reasons, the attitude and skills of users when living their web-side of life must be assessed.
- *Electronic Certificates (EC).* Governments and organizations are investing resources to provide citizens with electronic certificates, aiming at making eGovernment fully feasible. When assessing the quality of the security in the Information Society, this linchpin aspect must be addressed.

In the next section, we elaborate on the indicators considered in each assessment area.

## IV. Indicators

We have defined 31 indicators to assess the security skills of ICT users. On the one hand, we have tried to achieve a comprehensive overview in each of the aforementioned assessment areas. On the other, we believed that this quantity of indicators would fit into a 15-minute questionnaire. Certainly, the resulting survey took approximately 15 minutes to be completed via a telephone call. Note that we included in the questionnaire some questions aiming at categorising the nature of the respondent.

In order to evaluate a indicator, we designed a specific multiple choice question. Depending on the answers chosen,

[1] Catalonia, Catalunya in Catalan language, is a nationality inside Spain. Its population is around 7.5 million people. It is situated in the north-eastern part of the Iberian Peninsula and its capital and largest city is Barcelona.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

the indicator was classified into *achieved* or *not achieved* by the individual. The elaboration of the survey is out of the scope of this paper.

Furthermore, each indicator was assigned a punctuation according to the involved level of knowledge. Hence, an indicator is assigned a '1' value if it only entails knowing some theoretical concepts, is assigned a '2' value if it involves some procedural skills, and a '1' if it is related to the attitude/behaviour of users. An indicator involves theoretical knowledge when the user knows a concept (knows what is a cookie, knows how to determine a strong password...). The indicator implies a procedural knowledge when the user has reached an ability to perform an action. Finally, the indicator is related to attitude if it is a matter of fulfilling it voluntarily. If the indicator involves several kinds of knowledge, their values are added. The weighting of these indicators entailed a sound work by the experts on ICT involved in the project.

In the remaining of this section, we enumerate and describe the indicators included in our framework. For each element, we point out some comments and specify their assigned weight.

### A. Computer Security

1) *The operating system is updated at least once per month.* The operating system must be updated so security patches can be applied as software manufacturers discover security flaws in their products. Value=3 (procedural, attitude).
2) *There is some antivirus software running on the system.* This is a necessary software to be taken into account, specially under Windows environments[2]. Value=3 (procedural, attitude).
3) *There is some antispyware software running on the system.* People must be aware that spyware can be as annoying as viruses. Currently, security products comprise a comprehensive set of antimalware tools. Value=3 (procedural, attitude).
4) *There is some firewall running on the system.* The existence of a firewall (currently also embedded in the operating system) is necessary to avoid several attacks, such as worms and spying. Value=3 (procedural, attitude).
5) *Takes care of making backup copies.* This is to evaluate the cost of suffering an attack on the user data. Clearly, if users take care of their data backups, they can recover faster from malware attacks. Value=3 (procedural, attitude).
6) *Somebody takes care of computer's maintenance.* Taking care of the maintenance is essential, for instance, to detect if the system is a potential victim of malware. Value=1 (attitude).

### B. Information Access

7) *If the browser shows a warning message, it is carefully read so user can act consequently.* This is a specially delicate matter. For instance, warning messages related to certification authorities are usually hard to understand by a significant part of ICT users. Hence, we proposed to detect if individuals pay attention to these warning messages. Value=3 (procedural, attitude).
8) *Erases cookies at least once per month.* Tracking cookies can be seen as a threat to users' privacy. To that end, some browsers allow modes for private browsing. However, it is important that users take care of deleting these cookies from time to time. Value=3 (procedural, attitude).
9) *Gives importance to web quality seals.* Internet is a huge source of information. However, users must know that there are quality seals that accredit the quality of the website and the information it contains. Value=2 (theoretical knowledge, attitude)
10) *Knows the meaning of HTTPS.* It is essential for users to be aware of the protection mechanisms to send information through the web securely. Value=1 (theoretical knowledge).
11) *Is aware of several ways of being infected by malware.* There are several ways of being infected by viruses and other malware (to name just a few: sharing pendrives, clicking banners in certain websites, installing "friendly" plugins, etc.). Value=1 (theoretical knowledge).
12) *Is aware that P2P sharing and illegal downloading can result in downloading pornography and malware.* Users must also be aware of this way of getting these particular kinds of content. Value=1 (theoretical knowledge).

### C. Electronic Mail

13) *Never reads the emails from suspicious or unknown senders.* Clearly, reading suspicious emails may entail a variety of annoyances or even attacks. Value=3 (procedural, attitude).
14) *Never opens the attachments in the emails from suspicious or unknown senders.* Opening these kind of attachments may pave the way for being infected via Trojan horses. Value=3 (procedural, attitude).
15) *Hides the recipients' addresses when sending massive emails.* Email messages with a large number of addresses can be used by spammers to obtain email addresses. Value=3 (procedural, attitude).
16) *Deletes the chain of addresses when forwarding a message.* This is straightly related with the previous indicator. Value=3 (procedural, attitude).
17) *Does not receive junkmail or just a few because of using a filter.* The user is aware that there is an antispam filter functioning in the email service. Value=2 (theoretical knowledge, attitude).
18) *Never forwards emails massively or sends them to a small number of users.* This is related to the behaviour of people when using the email services. Value=1 (attitude).

### D. Passwords

19) *Does not write down passwords in papers, or stores them in encrypted files.* Having a set of robust passwords might be useless if these passwords are written on a note besides the computer display. Value=3 (procedural, attitude).

[2]When the survey was launched few people were using Linux.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

20) *All the passwords are robust.* The robustness of the password is essential to avoid the success of a variety of attacks (namely brute force attacks, dictionary attacks, etc.). Value=2 (theoretical knowledge, attitude).
21) *Uses more than a password.* Although using several passwords may suppose a memory challenge, the fact is that using a set of different passwords restricts the success of social engineering attacks (*e.g.*, if an attacker gains access to the email password, the attack will be limited to the email service of the user). Value=1 (attitude).
22) *Has never given a password to another person.* Behaving like this is essential to avoid the success of social engineering attacks. Value=1 (attitude).

### E. Social Networking

The aim of this area is focused on social networks such as Facebook. If users were members of social network services, they were asked to answer according to their experience. On the contrary, if they were not users of social networks, they were asked to answer according to what they think.

23) *Takes care of protecting several parts of the profile from public access.* Users must be able to manage these relevant tools to control the public side of their profile and activities. Value=2 (procedural).
24) *Does not publish personal data in the profile.* Despite the privacy controls, sensitive information (such as phone numbers and home addresses) could be leaked in case of attacks. Value=2 (theoretical knowledge, attitude).
25) *All the contacts in the social network are real-life friends or acquaintances.* This can be considered a proper behaviour of social network users, specially in Facebook-like social networks. Value=1 (attitude).
26) *Checks the identity before accepting new contacts.* This is related to the previous indicator. It is feasible to create false profiles in a social network. Value=1 (attitude).
27) *Asks contacts for permission before publishing information concerning them.* Certainly, social networks allow to control the privacy aspects of the own accounts and profiles but, in general, it is not straightforward to inform users on the real amount of *their* data being published by other people. Value=1 (attitude).
28) *Does not publish information concerning unknown people.* Users can communicate with their contacts before publishing information concerning them. Moreover, they can make use of tagging tools to automatically notify these contacts that they are appearing in a picture. However, this is not possible with unknown people. Value=1 (attitude).

### F. Electronic Certificates

29) *Has some electronic certificate.* This is the first step to analyse the area of electronic certificates. However, having an electronic certificate (such as Spain's eDNI [12]) does not imply that the user knows how to make the most of it. Value=1 point.
30) *Has used the electronic certificate between one and four times during the last year.* If users have utilized their electronic certificate, then we can assume they know how to use it. Value=3 points.
31) *Has used the electronic certificate more than four times during the last year.* The more frequently they use their certificate, the more skilled in this are they are. In fact, in the survey we asked for the number of times the electronic certificate had been used during the last year and we lately computed a threshold value to classify between casual users and frequent users. Value = 6 points.

TABLE I
SUMMARY OF THE NUMBER OF INDICATORS AND WEIGHTS FOR EACH ASSESSMENT AREA.

| Assessment area | #indicators | Aggr. values | Weight |
|---|---|---|---|
| Computer System (CS) | 6 | 16 | 25% |
| Information Access (IA) | 6 | 11 | 17% |
| Electronic Mail (EM) | 6 | 15 | 23% |
| Passwords (PW) | 4 | 7 | 11% |
| Social Networking (SN) | 6 | 8 | 13% |
| Electronic Certificates (EC) | 3 | 7 | 11% |
| Total | 31 | 64 | 100% |

Table I summarises, for each assessment area, the number of indicators and their aggregated values (*i.e.* the sum of the values of all the indicators in the assessment area). The relative weight of the area with respect to the values for the 31 indicators (64) is also shown.

## V. The Index and Area Subindexes

In this section we elaborate on the computation of the indexes that measure the assessment of the ICT computer security skills of individuals. The ICT-USI value is expressed as:

$$\text{ICT-USI} = \frac{10}{64}\sum_{i=1}^{31} v(i)$$

where $v(i)$ is the value of the $i$-th indicator if this is achieved by users and 0 if the indicator is not achieved. Note that the value of ICT-USI ranges from 0 to 10.

Additionally, we also propose computing indexes for the different assessment areas. Specifically:

- Computer System area

$$\text{CS-USI} = \frac{10}{16}\sum_{i=1}^{6} v(i)$$

- Information Access area

$$\text{IA-USI} = \frac{10}{11}\sum_{i=7}^{12} v(i)$$

- Electronic Mail area

$$\text{EM-USI} = \frac{10}{15}\sum_{i=13}^{18} v(i)$$

- Password Strength area

$$\text{PW-USI} = \frac{10}{7}\sum_{i=19}^{22} v(i)$$

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE II
RESULTS FOR THE ICT-ISU INDEX AND THE OTHER ASSESSMENT AREAS INDEXES, FOR THE AVERAGE INDIVIDUAL AND BY CATEGORIES (CATALONIA, 2010). BOLD VALUES INDICATE ARE THE MAXIMUM VALUES FOR EACH CATEGORY.

| | | ICT-USI | CS-USI | IA-USI | EM-USI | PW-USI | SN-USI. | EC-USI |
|---|---|---|---|---|---|---|---|---|
| **Average value** | | 5.0 | 7.1 | 4.5 | 4.8 | 7.0 | 4.1 | 0.9 |
| Gender | Male | **5.2** | **7.4** | **5.1** | 4.7 | **7.1** | 4.0 | **1.0** |
| | Female | 4.9 | 6.7 | 4.0 | **4.9** | 6.8 | **4.2** | 0.8 |
| Age | 16 - 24 | 5.4 | **7.7** | 4.9 | 4.4 | 7.3 | **5.9** | 0.8 |
| | 25 - 34 | **5.5** | 7.3 | **5.1** | 4.8 | **7.4** | 5.6 | **1.0** |
| | 35 - 44 | 5.0 | 6.8 | 4.6 | **5.1** | 6.7 | 3.5 | 0.9 |
| | 45 - 54 | 4.6 | 6.9 | 4.0 | 4.7 | 6.7 | 2.3 | 0.9 |
| | 55 - 74 | 4.3 | 6.2 | 3.2 | 5.0 | 6.4 | 1.9 | 0.6 |
| Education level | Primary school | 4.2 | 6.1 | 3.4 | 4.4 | 5.7 | 3.0 | 0.6 |
| | Secondary School | 5.1 | 7.1 | 4.0 | 4.7 | **7.3** | 4.2 | 0.6 |
| | Higher Education | **5.4** | **7.5** | **4.9** | **5.1** | 7.2 | **4.4** | **1.4** |
| Frequency of Internet use | Daily | **5.3** | **7.3** | **4.8** | **4.9** | **7.2** | **4.5** | **0.9** |
| | Weekly | 4.0 | 5.9 | 3.4 | 4.3 | 5.4 | 2.3 | 0.6 |
| | Monthly | 3.3 | 4.9 | 2.0 | 3.4 | 6.5 | 1.4 | 0.2 |
| Self-perceived skills | High | **5.4** | **8.0** | **5.7** | 4.1 | **7.2** | 4.3 | **1.3** |
| | Good | 5.5 | 7.7 | 5.3 | **5.2** | **7.2** | **4.6** | 1.0 |
| | Average | 4.6 | 6.5 | 3.8 | 4.5 | 6.7 | 3.8 | 0.7 |
| | No | 4.2 | 5.4 | 3.0 | 4.8 | 7.0 | 3.3 | 0.7 |
| Has some ICT degree | No | 4.9 | 6.9 | 4.3 | 4.7 | 6.9 | **4.1** | 0.8 |
| | Yes | **5.5** | **7.8** | **5.2** | **5.1** | **7.2** | **4.1** | **1.3** |

- Social Networking area

$$\text{SN-USI} = \frac{10}{8} \sum_{i=23}^{28} v(i)$$

- Electronic Certificates area

$$\text{EC-USI} = \frac{10}{7} \sum_{i=29}^{31} v(i)$$

## VI. RESULTS

Once we have defined the framework to obtain the assessment indexes, we show the results for a survey on the security in ICT of the population of Catalonia. The survey was conducted in 2010 and 1,015 questionnaires were analysed, so the results could be representative for the population of Catalonia (CATI methodology, error=$\pm 3,1\%$, confidence=95%, $\sigma = 2$, $P = Q = 50\%$). The questionnaire allowed us to classify the individuals according to their gender, age, education level and frequency on the use of Internet, among others. The survey was only conducted with individuals, between 16 and 74 years old) that had been active on the Internet at least once during the last month.

Now, we discuss the results of the survey. Table II shows the value for the ICT-USI index for the average individual, as well as his/her assessment area values. Moreover, this table also shows the values according to different categorizations, namely gender (male, female), age (from 16 to 24, from 25 to 34, from 35 to 44, from 45 to 54 and from 55 to 74), education level (primary school, secondary school, higher education) and frequency of Internet use (daily, weekly, monthly). Additionally, we have added two categories: on the one hand, the self-perception of computer security skills (ranging from no skills to high skills); on the other hand, we have categorised the results depending on whether the individual has earned some degree related to ICT (for instance, computer science degree, professional courses on telecommunication systems, etc.)

From these figures we can derive some interesting results for the Catalan society with respect to their skills in computer security:

- The best skilled segment of population is the one between 25 and 34 years old, with some higher education degree, that uses the Internet daily.
- In almost all areas, the highest skilled people is below 35 years old.
- Individuals with high or good self-perceived skills on computer security, certainly have the best results. On the contrary, users stating they have no skills or average skills present the lowest results.
- The areas of Computer System and the use of Passwords are significantly the ones with highest values, for all the categories.
- The weakest area is Electronic Certificates.
- The frequency of use of Internet is directly related to the value of the indexes, except for the Password area.
- The skills in all the areas are higher for people with higher education (except for the password area, whose difference with people with secondary school is negligible). People with only primary school degree, present the lowest results.
- People with a degree in ICT have the highest value for ICT-USI and all the area indexes.

The indicators proposed in our framework can also be individually analysed. Figure 2 shows the indicators and their degree of achievement, grouped by assessment areas.

Furthermore, the indicators can be ranked aiming at knowing the most and less achieved indicators. For our study, the five most achieved indicators are:

- Has never given a password to another person (96.2%)

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

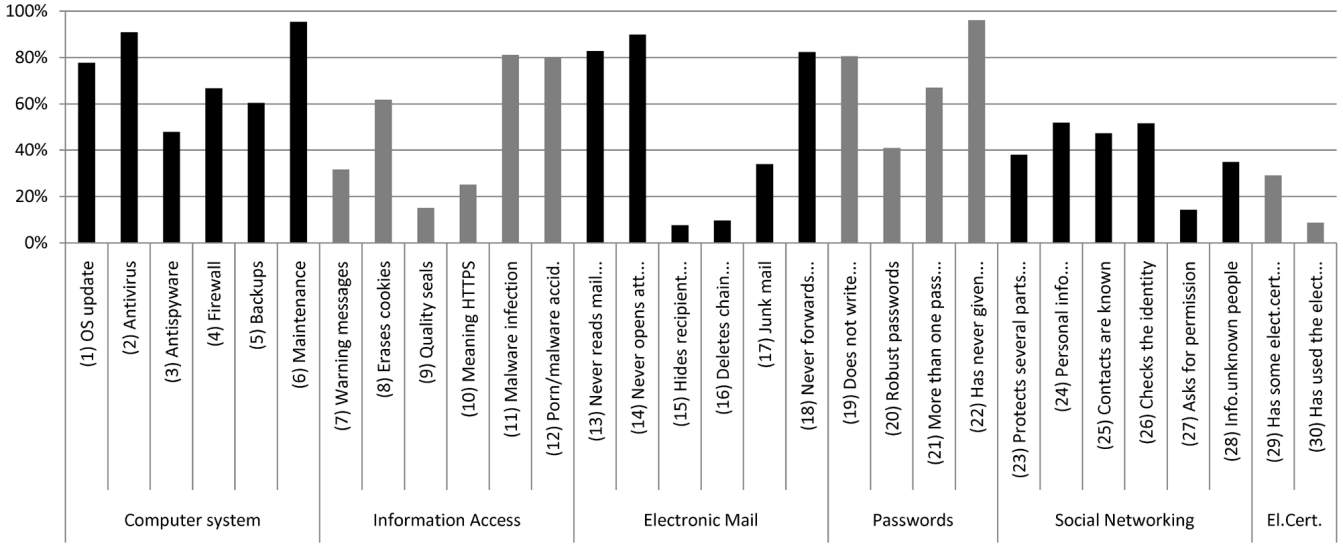


Fig. 2. The indicators studied in our framework according to their percentage of achivement. Indicator (30) includes the value assigned for indicator (31).

- Somebody takes care of computer maintenance (95.4%)
- There is some antivirus software running on the system (91.0%)
- Never opens the attachments in the emails from suspicious or unknown senders (89.9%)
- Never reads the emails from suspicious or unknown senders (82.9%)

The five least achieved indicators are:

- Gives importance to web quality seals (15.1%)
- Asks for permission to contacts before publishing information concerning them (14.3%)
- Deletes the chain of addresses when forwarding a message (9.7%)
- Has used the electronic certificate (8.8%)
- Hides the recipients' addresses when sending massive emails (7.7%)

There were some other interesting results obtained from the survey that, for the sake of brevity, are not addressed in this paper.

## VII. Conclusions

In this paper we have presented a framework to evaluate the users' skills in computer security. We have shown the process of selecting the indicators to be evaluated, from a variety of existing sources and surveys. We have proposed different assessment areas. Besides the ICT-USI value, we have computed specific indexes for these assessment areas, aiming at a more comprehensive comparison. The utility of this framework is, on the one hand, to gather precise information on the skills (note that the achievement of each indicator is in fact measured). On the other hand, the knowledge extracted can be used to focus the training courses that specific people may need.

To illustrate how this framework has been successfully used, we have shown the results for a survey for the population of Catalonia. We have demonstrated that, from this set of indicators and areas, we can obtain valuable results. This framework could be used to detect the flaws in computer security in a variety of target groups: a company's staff, incoming students in a high school, etc. Hence, we provide an analysis tool for IT managers, CTO and e-Government experts.

## Acknowledgements

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES" and project TIN2011-27076-C03-01 "CO-PRIVACY", and by the Government of Catalonia under grant 2009 SGR 1135.

## References

[1] Eurostat, the statistical office of the European Union (2012) ICT usage in households and by individuals http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables

[2] A. Martínez-Ballesté, F. Sebé and J. Domingo-Ferrer, "Computer Skills Training to (Middle-aged) Adults: Problems and Program", in *International Conference on Information Technology: Coding and Computing* (ITCC 2004), pp.146–150, IEEE Computer Society.

[3] R.W. Morrell, C.B. Mayhom and J. Bennet, "A survey of World Wide Web Use in Middle-Aged and Older Adults", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol.42, no.2, pp. 175-182, 2000.

[4] Eurostat, *Community Survey on ICT Usage in Households and by Individuals*, 2002. ttp://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/compreensive_databases

[5] Gallup Organization, *Flash Eurobarometer 250: Confidence in the Information Society*, 2008. http://ec.europa.eu/public_opinion/flash/fl_250_en.pdf.

[6] Princeton Survey Research Associates International, "Leap of Faith: Using the Internet Despite the Dangers, 2005. http://www.psrai.com/news.aspx?titleId=1016

[7] Commission Nationale de l'Informatique et des Libertés (CNIL), http://www.cnil.fr

[8] Instituto Nacional de Tecnologías de la Información (INTECO), http://www.inteco.es

[9] A. Martínez-Ballesté, J.F. Martínez Cerdá *et al. Estudi sobre la seguretat de la informació a les llars i ciutadans*. Barcelona: FOBSIC (Fundació Observatori per a la Societat de la Informació de Catalunya). http://www20.gencat.cat/docs/empresaiocupacio/17\%20-\%20Telecos\%20i\%20SI/Documents/Dades\%20i\%20estadistiques/2010/Seguretat_llars/TICSEGURALLARS_informe_complet.pdf

[10] S. Bloom *et al.*, *Taxonomy of educational objectives: the classification of educational goals*, Handbook I: Cognitive Domain, Longmans, Green, 1956.

[11] European Travel Commission, *New Media TrendWatch*. http://www.newmediatrendwatch.com/markets-by-country/17-usa/123-demographics

[12] Documento Nacional de Identidad electrónico (Spain's Electronic National Identity Number Document). http://www.dnielectronico.es/