Current Trend of End-Users' Behaviors Towards Security Mechanisms

Yasser M. Hausawi(✉)

Department of Information Technology,
Institute of Public Administration, Jeddah, Saudi Arabia
hawsawiy@ipa.edu.sa

Abstract. End user's Security-related behaviors are key factors on success or failure of information security mechanisms' application. Such security mechanisms are being rapidly modified sophisticatedly. Consequently, end-users' behaviors are being changed, newly developed, and/or innovated as a result of the modifications of the mechanisms. Therefore, tracing the change of the end-user's security related behaviors is an essential activity that should get continual attention from the security professionals. Unfortunately, behavioral studies on information security are out of most security professionals' scope, despite the common believe that end-users must be involved in security mechanisms' development. This article focuses on tracking the current trend of both positive and negative behaviors of end-users who are not security experts. The tracking process is based on semi-structured interviews with security experts who deal with end users on daily bases.

Keywords: Security · Usability · Human computer interaction · HCI · HCI-SEC · Security-related behaviors · Security enhancement approaches

1 Introduction

Among security community, there has been a wide spread conceptual thought that end-users are the enemies of security mechanisms. Therefore, a considerable amount of studies have been conducted to figure out if such a hypothesis is true. There are many famous research studies such as [1,7,12] have been conducted to investigate whether end- users are the enemies of security or not. As a result of the studies, it became clear that end-users are divided into two groups, legitimate end-users and adversaries [3], and it became even clear that the legitimate end-users are not the enemies, while the adversaries are the real enemies of security mechanisms. However, despite the fact that the legitimate end-users are not the enemies, they also behave in ways that can affect security mechanisms both positively and negatively citemayron2013secure. Having two different possible behaviors, it is important to distinguish between the behaviors that can be considered as positive and those that can be considered as negative. In the cases that the users perform negative behaviors during their interaction with security mechanisms, there is a set of important concerns raised. These concerns are:

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 140–151, 2016.
DOI: 10.1007/978-3-319-39381-0_13

- Whether legitimate end-users, who behave negatively against security, be considered as enemies or not;
- Whether we should differentiate between the legitimate users themselves and their behaviors or not;
- The best security approaches to be followed in order to promote the positive behaviors of the legitimate end-users, and limit their negative behaviors.

To clear up all of the above concerns, a series of consecutive studies should be conducted such as the work of Stanton et al. in [8,10]. It is important to be aware of the fact that during the last decade, there has been rapid change in the development of user-security interaction. Sequentially, end-user behavior toward security is being changed frequently as well. Therefore, there is a continual need to frequently investigate end users' behaviors and to not rely on the previously studied behaviors of users toward security.

To begin this research, an initial exploratory study has been conducted to investigate the current state of end-users behaviors when interacting with security mechanisms. Human-computer interaction Behavioral researchers in [2,4,6] recommended interviews and focus groups as the best initial exploration research methods used to help in better identifying problems. Therefore, the previously mentioned research methods are the best ways to identify legitimate endusers' positive and negative behaviors towards security mechanisms.

This study focuses on identifying the current state of legitimate end-users' behaviors and the best approaches to deal with such behaviors. To this end, a set of interviews have been conducted to survey security experts' experiences and interactions with end-users and digital security.

The reminder of this article is structured as follows: Sect. 2 presents the related work on investigating end-users' behaviors towards security mechanisms.

2 Related Work

According to Stanton et al., successful application of security mechanisms relies on the behaviors of end users who interact with such mechanisms [8]. While Security professionals and administrators are responsible for creating, developing, and configuring practical security mechanisms, end-users are responsible for practicing and appropriately using the mechanisms [5]. Accordingly, Whitten and Tygar stated that security mechanisms can only be a as effective as should be if they are used correctly [12].

Unfortunately, the research work on security-related behavior is very limited despite its importance on making security mechamesms applicable [11]. However, Stanton et al., conducted an interview study that involved 110 participants (managers, IT professionals, and regular employees), the result of their study was a collection of 94 security related behavior list that nine of which were then used in a following survey study. Among those selected behaviors, sharing and writing credentials were among the common negative security related behaviors [9]. In addition, Stanton et al. transformed 91 out of the collected 94 security-related behaviors into a more manageable six-element taxonomy [10].

3 Methodology

3.1 Interview Design

The semi-structured strategy is used to design the interview. The reason for using the semi-structured strategy is to get the benefits of both using a rigid script of well-defined, ordered questions to control the flow and consistency of the interview, and keeping the interview opened up for both depth and breadth topic exploration [4]. To give the interviewee the freedom of answering questions, five of the questions (62 %) are open-ended, two are unstructured-closed questions, and one is a structured-closed question. Among the five open-ended questions, two of them are followed with the two unstructured- closed questions. The structured-closed question is followed by another related open-ended question. The flow of the questions is structured based on the five following major topics: security compromising, negative behaviors, positive behaviors, security enhancement approaches, and open topics of mind. Table 1 shows the questions, their topics, and their types.

3.2 Participants

Thirty-one expert from the U.S and Saudi Arabia (23 males and 8 females) participated in the study; all are security experts and have experience with end users. Their work experience is between 8 and 30 years, with an average experience of 19 years. Their daily interaction with end-users ranges from 1 to 7 h, with an average 4 h.

3.3 Tools

Rigid scripts were used by the interviewers to keep the interview consistent and controlled. The scripts consist of an introduction part and set of questions in an organized and well-defined order. Moreover, the scripts were provided with noting areas for each question. At the top of the scripts, there is a field to record the code the interviewee. It is worthwhile to state that the interviewers read from the scripts, while the interviewees had no scripts to reference, rather, the questions were read one by one to them by the interviewers. Figure 1 depicts the script. The interviews were voice recorded in order to make sure that all the important information is not missed and also to double check the hand-written recorded data after the end of each interview. Microsoft Excel 2013 was used to store and analyze the collected data.

3.4 Analysis and Evaluation

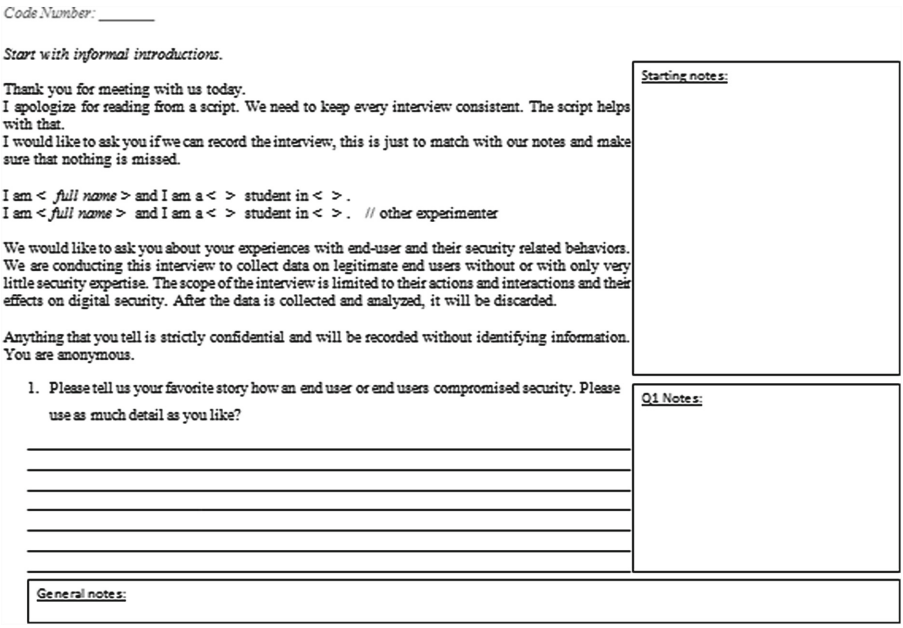
Because of the nature of the exploratory semi-structured interviews and having a lot of open-ended questions, the collected data are grouped, categorized, organized, and then displayed. The open-ended and the unstructured-closed questions are analyzed based on the following steps:

Table 1. Interview's questions

No.	Question	Topic	Type
1	Please tell us your favorite story on how an end user or end users compromised security. Please use as much detail as you like	Compromising Security	Open-ended
2	What are some other behaviors that you have encountered that users make that negatively affect security?	Negative Behavior	Open-ended
3	Which of these activities, in your opinion, has the most impact on security, and which one the least?	Negative Behavior	Unstructured-closed
4	On the other hand, could you please tell us about some things that users do that in your experience, improves security?	Positive Behavior	Open-ended
5	Which of these activities, in your opinion, has the most impact on security, and which one the least ?	Positive Behavior	Unstructured-closed
6	Of the following four approaches, which one do you think is most effective for enhancing security? a. Enforcing security policies, b. Training users, c. Motivating users, d. Rewarding users	Security Approaches	Structured-closed
7	Is there another approach that you think is effective?	Security Approaches	Open-ended
8	Is there anything else that you would like to add?	Open Topic	Open-ended

1. Counting the number of behaviors cited in each question.
2. Ordering (descending) the behaviors for each question.
3. Rating the behaviors for each question.
4. Display the results of the rating.

The structured-closed question is analyzed based on the following steps:


Code Number: _____

Start with informal introductions.

Thank you for meeting with us today.
I apologize for reading from a script. We need to keep every interview consistent. The script helps with that.
I would like to ask you if we can record the interview, this is just to match with our notes and make sure that nothing is missed.

I am < *full name* > and I am a < > student in < > .
I am < *full name* > and I am a < > student in < > . // other experimenter

We would like to ask you about your experiences with end-user and their security related behaviors. We are conducting this interview to collect data on legitimate end users without or with only very little security expertise. The scope of the interview is limited to their actions and interactions and their effects on digital security. After the data is collected and analyzed, it will be discarded.

Anything that you tell is strictly confidential and will be recorded without identifying information. You are anonymous.

1. Please tell us your favorite story how an end user or end users compromised security. Please use as much detail as you like?

Starting notes:

Q1 Notes:

General notes:

Fig. 1. A snapshot of the Interview's Script

1. Creating four groups of rankings as the following:
   (a) First choice (4 points).
   (b) Second choice (3 points).
   (c) Third choice (2 points).
   (d) Fourth choice (1 point).
2. Putting each approach in one of the four based on each interviewee ranking. Where represents an approach.
3. Counting the number of occurrence for each approach in each group.
4. Multiplying the total count of each approach of each group by that groups' point.
5. Summating approach's results from each group.
6. Listing the four approaches along with their results.
7. Ordering the approaches.
8. Rating the approaches.
9. Displaying the results of the rating.

4 Interview Results

The results of the interview study are presented based on the five major topics that are: security compromising, negative behaviors, positive behaviors, security enhancement approaches, and open topics of mind.

4.1 Security Compromising Stories

Sharing Credentials: There are many different security-compromising stories all share one common incident that is sharing credentials. The following are summarized descriptions of the stories:

- A project team having one credential to share accessing the same resources.
- Faculty staff members give their credentials to IT support staff member when fixing their banners. The IT support staff member writes the credential on a paper and access to the faculty staff's banner and look at students' grades.
- Single sign-on credential sharing.

Over Trusting: There are two types of over trusting in digital security, one is over trusting people by not protecting self's security related stuff protected (such as credentials and devices), another is over trusting technology by not investigating whatever software brings up (such as pop-ups and default configurations and installations). Another form of over trusting technology is when users believe that devices are self-secured properly. The following are summarized descriptions of the stories:

- Clicking OK without reading the contents of the messages.
- Grandfather clicks OK on fake security popups coming through emails from trusted people.
- Storing sensitive data in USBs.

Lack of Knowledge and Awareness: Sometimes important security decisions alert end-users in the form of a pop-up, the pop-up asks the user if they would like to accept or reject security actions that the end-user lacks knowledge and awareness of. As a result, end-users prefer not choose any. The following are summarized descriptions of the story:

- End users try to get rid of the pop-ups in a safest way by cancelling the pop-up or closing it. The reason for that is because end users don't know the right answer.

Other Stories: There are some security compromising stories narrated by the interviewees such as:

- A web administrator wrote his credentials on his screen. The students got the credentials and changed the site contents.
- Compromising an official public website to perform a security homework assignment.
- A project team having one credential to share accessing the same resources.

Table 2. Negative behaviors

No.	End-users' negative behaviors
1	Sharing credentials
2	Over trusting people
3	Writing credentials down
4	Clicking OK without reading
5	Not logging off
6	Downloading programs
7	Not having security software
8	Allowing auto remembering of credentials via browsers
9	Bypassing security
10	Keystrokes
11	Lack of awareness of importance of security
12	Not applying least privileges
13	Not checking default configurations
14	Not locking screens
15	Not updating security software
16	Reusing credentials
17	Sending stuff to wrong resource
18	Setting easily security questions
19	Signing on from unsecure networks
20	Turning software programs off without turning them on again
21	Using jump drives

4.2 End-Users' Negative Behaviors

A total of 21 different negative behaviors were collected. Table 2 lists the collected behaviors, and Fig. 2 shows the percentage that each behavior got.

Among the 21 negative behaviors, 6 negative behaviors were chosen by the experts to be the most behaviors that negatively impact security (Sharing credentials, Over trusting people, Clicking OK without reading, Not having security software, Turning software programs off without turning them on again, and Lack of awareness of importance of security), where sharing credentials behavior got the highest attention.

On the other hand, among the 21 negative behaviors, 5 negative behaviors were chosen by the experts to be the least negatively impacting behaviors (Sharing credentials, Downloading programs, Keystrokes, Not locking screens, and Writing credentials down), while sharing credentials behavior got the highest attention. It is worthwhile to mention that one answer was missed, because the interviewer forgot to ask the interviewee about the least negative impact behavior.

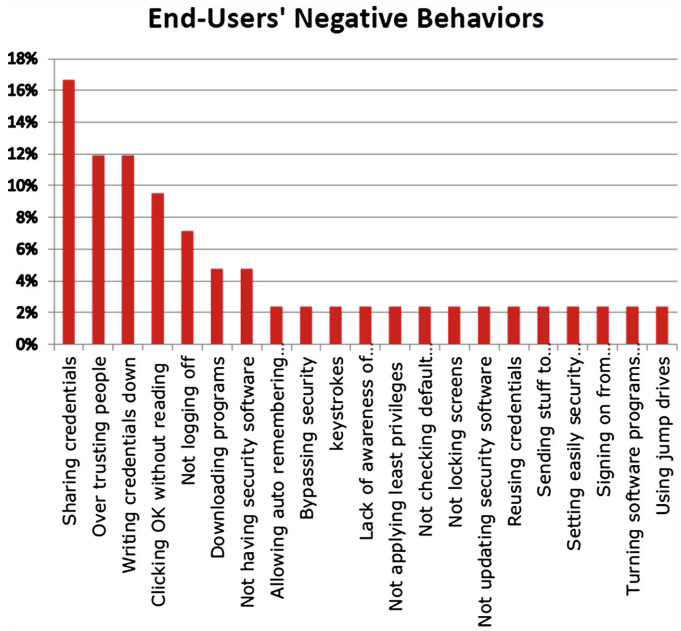


Fig. 2. Negative behaviors' percentage

4.3 End-Users' Positive Behaviors

A total of 15 different positive behaviors were collected. Table 3 lists the collected behaviors, and Fig. 3 shows the percentage that each behavior got.

Among the 15 positive behaviors, 5 behaviors were chosen by the security experts to be the behaviors that most positively impacts security (Complying with security policy, Keeping software updated, Layering security, Paying attention to security alerts, and Self-awareness), where self-security awareness behavior got the highest attention.

Among the 21 positive behaviors, 4 behaviors were chosen by the security experts to be the behaviors that positively impact security the least, whereas protecting personal security stuff behavior got the highest attention. It is worthwhile to mention that 3 answers were missed, because the interviewers forgot to ask the interviewees about the least positive impact behavior.

4.4 Security Enhancement Approaches

The topic of security enhancement approaches is designed in a different structure than other security topics. It is more controlled despite the fact that it is an open area of study. The reason for this type of design is to get the best of the currently available approaches first, then with a follow up question the interviewee is given a chance to add approaches not yet listed or to propose new approaches.

Table 3. Positive behaviors

No.	End-users' positive behaviors
1	Complying with security policy
2	Self-awareness
3	Having unique credential per system
4	Asking before acting
5	Keeping software updated
6	Reporting to security officers
7	Protecting personal security stuff
8	Deleting unknown emails
9	Paying attention to security alerts
10	Differentiating between self and technology
11	Layering security
12	Changing credentials frequently
13	Not trying to discover new things that are not for tasks
14	curiosity about security
15	Education

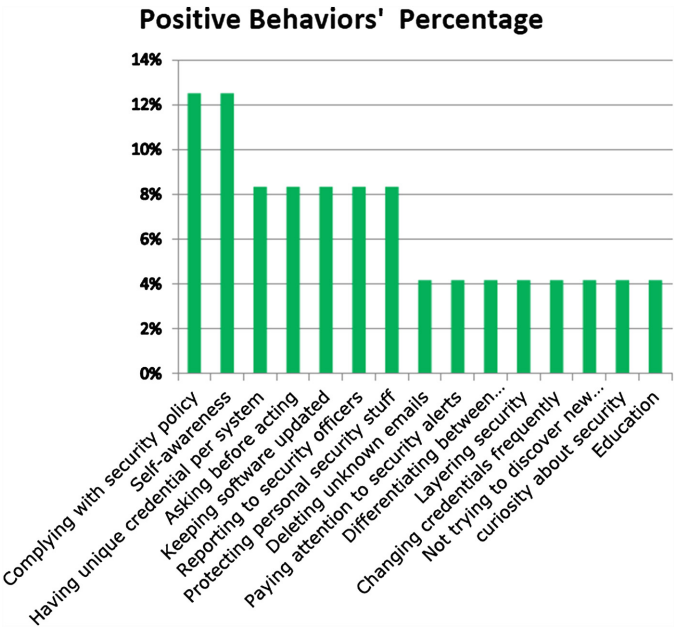


Fig. 3. Positive behaviors' percentage

Among the 4 listed approaches (Training users, Motivating users, Enforcing security policies, and Rewarding users), training users was the most recommended by the interviewees (34 %), second, motivating users (29 %), then enforcing security policies (26 %), and the least recommended approach is rewarding users (11 %). Figure 4 illustrates the ratings.

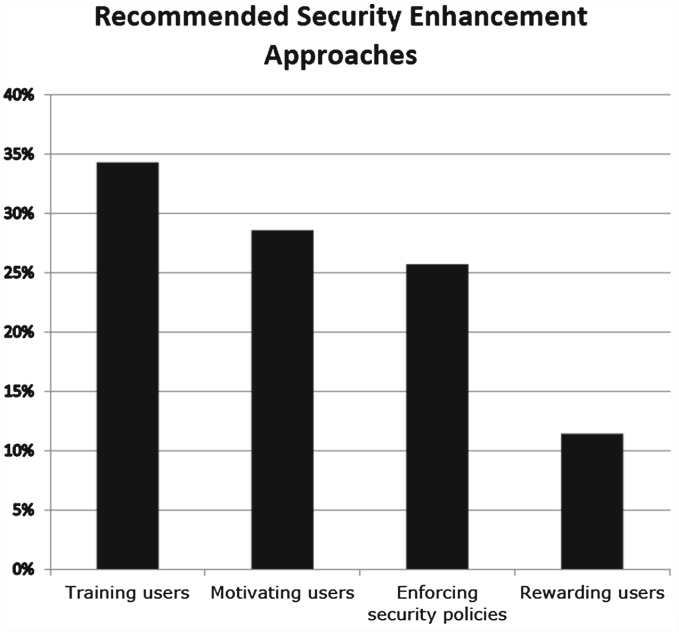


Fig. 4. Security enhancement approaches percentage

In addition, the interviewees added a set of approaches as the following:

- Assessing security
- Promoting users self-awareness
- Restricting security
- Punishing users
- Turning technology off
- Educating users
- Designing simpler user interfaces
- Designing informative security systems
- Hiring IT staff with security experience

4.5 Open Topics

The interviewees talked about very important issues related to end users' behaviors that usually are not considered when security mechanisms are designed and developed. The issues are listed as the following:

- Security policies must be usable.
- Improving user decision-making by having better design.
- People have to address their level of security.
- Security designers must understand the users' needs.
- Balancing quality attributes is a very important issue.
- Security officers should be nice with legitimate end-users, as they are not security enemies.

5 Discussion

Looking at the above results, it is clear that sharing credentials, over trusting people and technology, writing credentials down, and clicking OK without reading are still the most wide-spread negative behaviors end-users exhibit that negatively impact security. This is despite the huge amount of research and development focused on enhancing security. This finding should bring the attention to a fact that: it is important to review the way that security mechanisms are currently being designed and developed. Perhaps some of the issues that are mentioned by the security experts at the open topics question can help in redesigning security mechanisms that address the negative behaviors that are yet to be mitigated.

One interesting result about the most and least impacting negative behaviors is that: sharing credentials is the only behavior that is considered as both the most and least impacting behavior that negatively affects security simultaneously. Such a contradicting result indicates that sharing credentials is an important behavior that needs further investigation. In some cases, security experts, themselves, perform the same negative behaviors such as sharing credentials or writing credentials down! This infers that there might be design flaws in security mechanisms' designing methodologies.

6 Conclusion and Future Work

This initial exploratory interview was conducted to collect data on legitimate end-users with or without very little security knowledge from security experts' viewpoints. A total of 21 negative, and 15 positive security-related behaviors had been collected and analyzed. Four well-known security enhancement approaches had been investigated and ranked to find the best among them. Moreover, nine other proposed enhancement security approaches have been proposed and need to be investigated in further research. A set of six design principles had been gathered from the security experts that may help in enhancing security mechanisms design, most of which are user-centered. Future step is to get the end-users' viewpoints about the causes for performing both of the negative and positive behaviors when interacting with security mechanisms. Then the results are interrelated and analyzed with the results of this interview to create a solid foundation for new design methods for security mechanisms. When this is finished an experimental study will be conducted to evaluate the new security methods.

Acknowledgment. The author would like to thank the Institute of Public Administration (IPA) in Saudi Arabia and Florida Institute of Technology in the U.S. for their support of this work.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999)
2. Converse, J.M., Presser, S.: Survey Questions: Handcrafting the Standardized Questionnaire, vol. 63. Sage, Thousand Oaks (1986)
3. Hausawi, Y.M.: Towards a usable-security engineering framework for enhancing software development (2015)
4. Lazar, J., Feng, J.H., Hochheiser, H.: Research Methods in Human-Computer Interaction. Wiley, New York (2010)
5. Ng, B.-Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: A health belief perspective. Decis. Support Syst. **46**(4), 815–825 (2009)
6. Ritter, F.E., Kim, J.W., Morgan, J.H., Carlson, R.A.: Running Behavioral Studies with Human Participants: A Practical Guide. Sage Publications, Thousand Oaks (2012)
7. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the weakest linka human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)
8. Stanton, J.M., Mastrangelo, P.R., Stam, K.R., Jolton, J.: Behavioral information security: Two end user survey studies of motivation and security practices
9. Stanton, J.M., Stam, K.R., Guzman, I., Caldera, C.: Examining the linkage between organizational commitment and information security. In: IEEE International Conference on Systems Man and Cybernetics, vol. 3, pp. 2501–2506 (2003)
10. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**(2), 124–133 (2005)
11. Stephanou, A.: The impact of information security awareness training on information security behaviour. Ph.D. Thesis (2009)
12. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX Security, 1999 (1999)