Proceedings of the Ninth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2015)

Online Fraud Defence by Context Based Micro Training

J. Kävrestad and M. Nohlberg

The School of informatics, Högskolan i Skövde, Skövde, Sweden
e-mail: {joakim.kavrestad; marcus.nohlberg}@his.se

Abstract

Online frauds are a category of Internet crime that has been increasing globally over the past years. Online fraudsters use a lot of different arenas and methods to commit their crimes and that is making defence against online fraudsters a difficult task. Today we see continuous warnings in the daily press and both researchers and governmental web-pages propose that Internet users gather knowledge about online frauds in order to avoid victimisation. In this paper we suggest a framework for presenting this knowledge to the Internet users when they are about to enter a situation where they need it. We provide an evaluation of the framework that indicates that it can both make users less prone to fraudulent ads and more trusting towards legitimate ads. This is done with a survey containing 117 participants over two groups where the participants were asked to rate the trustworthiness of fraudulent and legitimate ads.. One groups used the framework before the rating and the other group did not. The results showed that, in our study, the participants using the framework put less trust in fraudulent ads and more trust in legitimate ads.

Keywords

Online fraud, fraud defence, awareness, micro training

1. Introduction

Over the past years online fraud has evolved to be an increasing crime that is targeting a large portion of the Internet users. This fact is being reported in many countries including Sweden and the USA (Brottsförebyggande rådet,2013; IC3, 2013). As one example it was estimated that one third of the American adults experience victimization annually (Pratt, Holtfreter, & Reisig, 2010). Online frauds come in many different forms and are occurring in several different arenas including e-mail, social networks, online auction houses and telephones. The great variety of the modus operandi of the fraudsters makes online fraud defense a difficult task.

Previous research makes it clear that online fraud is not a crime that target specific groups of Internet users. Rather, it seems as if anyone that is present on the arenas were frauds are being executed faces the risk of not only being targeted by a fraudster, but also to fall for the fraudsters actions. This is shown in the research by Wilsem (2013).

The common suggestion on how to defend yourself against online fraudsters in to gather the knowledge and skills you need to avoid being defrauded before you

encounter a fraudster, as exemplified by usa.gov (2013) *"The best way to fight Internet fraud is to learn how to avoid becoming a victim"*.

Today, this knowledge is often presented on governmental and business webpages and the users are expected to identify and make use of the information on their own. This puts the responsibility of defense on the users rather than the actors hosting the arenas were the frauds can take place.

In this paper we suggest a model for online fraud defense that aims at educating users that are encountering a potentially fraudulent situation. The education is taking place in the moment were the fraud may be executed and is tailored to learn the user about the specific fraud attack he is currently in the risk of facing. This methodology is influenced by the concept of situated learning as described by Herrington & Oliver (1995).

With this approach we believe that the users will make use of the information because it is relevant for their current situation. It has also been discussed that when you acquire knowledge in a situation where you use that knowledge, the overall learning process provides are better result compared to if you are learning in a theoretic manner, i.e. by reading from a book or webpage (Brown et al, 1989). Further, as shown by Davinson & Sillence (2010), being aware of the possibility of being defrauded will reduce the risk of being victimized. It is our belief that presenting information about online frauds just before the user enters an arena where frauds are being executed will make the user more aware and thus further reducing the risk of victimization. Similar effect was discussed by Davinson & Sillence (2010) who researched the effects of anti-phishing training. They discussed if the users behaviour was enhanced due to actual training or due to that the users awareness was increased just by being confronted with a training program.

Within this paper we also present an evaluation of the defense model that indicates that it can change user behavior in potentially fraudulent situations. The evaluation is done in an online auction house scenario.

The remainder of this paper presents our suggested defense model and our evaluation of the model

2. Proposed defence mechanism

Several researchers argue that knowledge is the best defense against online fraudsters. In example see Arachchilage and Love(2014) and Garg and Nilizadeh (2013). The same is stated by several governmental web pages including usa.gov (2013). While we do not argue with this fact we have seen that this knowledge often comes in the form of informational websites, thus creating a situation where the potential victims are required to acquire the knowledge they need before they encounter a potentially fraudulent situation.

We also believe that knowledge is the best countermeasure to online fraud but in our opinion the current situation introduces the following three issues:

- The potential victims are expected to gather knowledge before they encounter a potentially fraudulent situation. This implies that common Internet users must gather knowledge about something they may not be aware of.

- Internet users are supposed to read about online frauds in a context were the knowledge is not usable.

- The responsibility is put on the users rather than on the owners who hots the arenas were online frauds are taking place.

With our defense mechanism we make use of the ideas of situated learning that states that a learning experience is more meaningful if the learning is taking place in a context were the information is immediately useful (Herrington & Oliver, 1995). We call our approach context based micro training.

With context based micro training we developed a framework for introducing precise and tailored knowledge to Internet users in the situation were they may need it. To make the information as useful as possible to the users, the framework states the following about the information that is presented to the user:

- Relevant in the users current situation, i.e. if a user is entering an online auction house, where frauds has taken place, he will receive information about how to identify and avoid fraudsters in online auction houses.

- Interactive information meaning that the information module will require active participation from the users. As stated by Herrington & Oliver (1995) this approach increases the users awareness

The processes in the framework are shown in Figure 1.

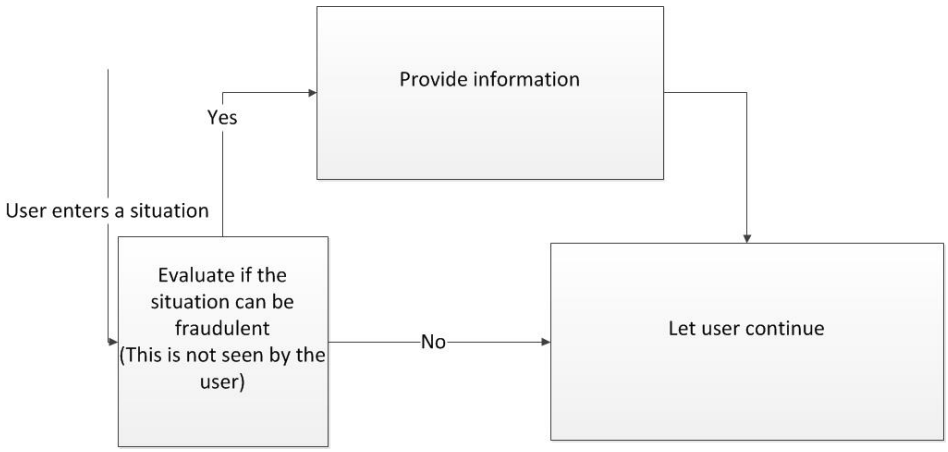

Figure 1: Overview of the processes in our framework

With this approach we aim to put precise information into a user's mind just before the users enters a potentially fraudulent situation. Since the information is tailored to the users current situation and requires participation from the user we believe that users that make use of this framework will be educated and prepared for the situation they enter and they will also be more aware of online frauds.

3. Research aim and limitations

The aim of this study is to evaluate the presented defense mechanism for use against online fraudsters. As described, the aim of the model is to provide knowledge "in the moment" and for that reason long time effects of the mechanism is not in the scope of the study. Rather, this study aims at providing a proof of concept for the direct effects of the proposed defense mechanism. Further, this study evaluates the defense mechanism in an online auction house environment. While we strongly believe that it can be used in other environments as well, effects of the mechanism in other environments is beyond the scope of this study and could be explored in the future. Also, this study does not provide a technical solution for how to implement the mechanism. While the actual implementation is not in the scope of this study we suggest that the mechanism can, for instance, be implemented in the following ways:

- As an interactive game or questionnaire when a user in an online auction house is entering a category of goods where the owner of the auction house is currently aware of ongoing frauds.

- As a way of countering telephone related frauds by warning users that are calling or receiving calls from numbers that are related to fraudulent behavior. This can be accomplished by matching incoming calls to a database of numbers that has been reported for fraudulent actions.

The aim of this study was reached by exploring the following questions in a controlled environment:

Q1: Can the defense mechanism help users identify fraudulent ads?

Q2: Will the mechanism make the users more likely to falsely identify legitimate ads as fraudulent?

4. Research model

To generate truly reliable results one could argue that this research is best conducted with a real-world approach by testing user's behavior in authentic situations. However, it is hard to conduct such study in an ethically appropriate manner. As example see Dittrich & Kenneally (2011) and Schrittwieser, Mulazzani & Weippl (2013). The guidelines proposed in those articles were followed in this study.

Instead, the research questions were explored in a survey-style environment. A central point in conducting a survey is that the sample of participants should represent the characteristics of the surveys intended population (May, 2001). In this case the intended population was everyone, in Sweden, that uses the Internet. May (2001) argues that the only way to generalize from the results of a survey is to use a probability sample. However May (2001) also states that using this kind of sample is not always possible. One requirement that a sample must fulfill in order to be called a probability sample is that every person in the population has an equal chance of participating in the survey. In this survey that is impossible because of the size of the population that holds a large portion of the Swedish population. A more convenient way of sampling would be to use a convenience sample where the sample is taken from people close to the researcher (Robson, 2011). Using such a sample will, however, generate less generalizable results (Robson, 2011). Since it was not feasible to use a probability sample in this study the aim was to get participants from different geographical places and with different demographic attributes. In order to achieve this, the surveys was be marketed over the Internet through social networks. This did not generate a probability sample but the sample did likely contain respondents with different backgrounds resulting in a more generalizable result than if convenience sampling where to be used.

In the survey, the participants were presented to six ads from a Swedish online auction house called Tradera.se. Three of the ads were known to be fraudulent and three were supposedly legitimate. The fraudulent ads were supplied by the Swedish online auction house Tradera and the other ads were randomly chosen from the same site. The participants was asked to rate the trustworthiness of each ad on a sex-graded scale were 1 meant that the ad was not trustworthy at all and 6 meant that the ad was completely trustworthy. The participants were guided to a website containing the survey and were randomly assigned to one of two groups called DM and non-DM. A total of 117 participants went through the full survey, 70 in the non-DM group and 47 in the DM group. The participants in the different groups performed the following tasks:

- DM: The participants in this group went through three learning modules designed according to the proposed defense mechanism before rating the ads. The learning modules were in the form of slideshows that presented a dialogue between a buyer and a seller. The participants were asked to

decide if the buyer was in a potentially fraudulent situation or not. Based on the participants answer they received feedback describing if the buyers behavior was insecure and in that case why.

- Non-DM: The participants in this group rated the ads without going through the defense mechanism or being presented to any training.

5. Results

This section provides the results from the survey and conclusions related to the research questions. Figure 2 shows the average answers from both groups for the fraudulent ads. The column names are formatted in the following way: *"question number – group"*

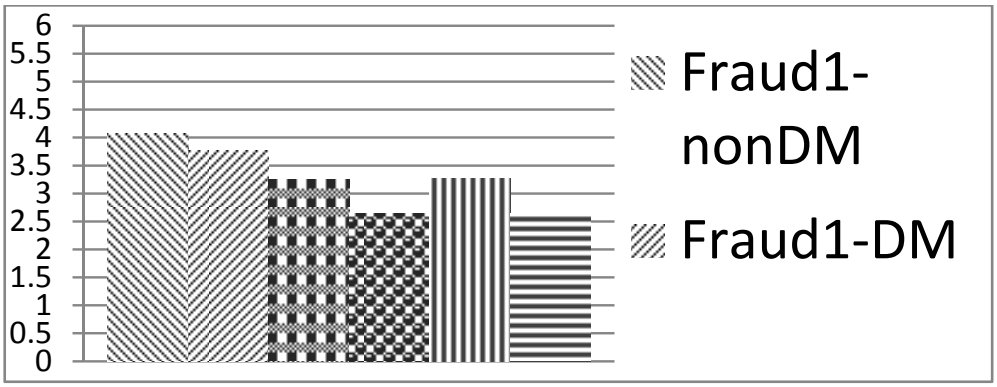

Figure 2: Overview of results for the fraudulent ads

As seen in the figure the participants in the DM group rated all three fraudulent ads as less trustworthy compared to the rating from the group non-DM. This result does show that the defense mechanism can, in a controlled environment, make users better at detecting fraudulent ads. This is the answer to Q1: Can the defense mechanism help users identify fraudulent ads?

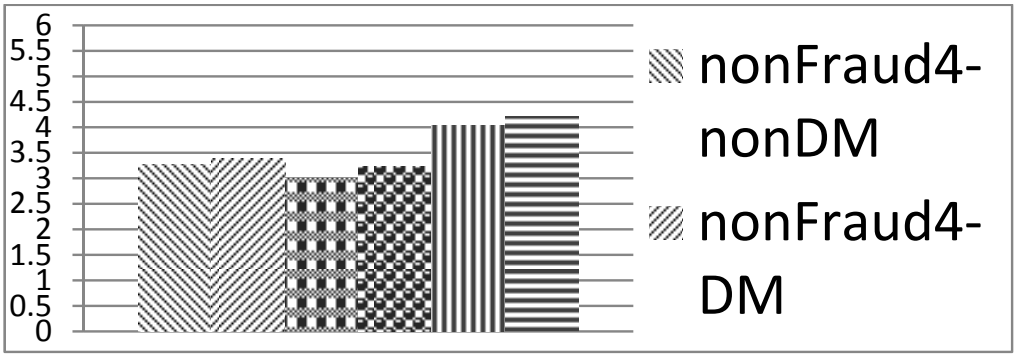

Figure 3: overview of the results for the legitimate ads

Figure 3 reflects the average answers for the randomly chosen supposedly non-fraudulent ad.

As seen in the figure the participants in the group DM rated these ads as more trustworthy than the participants in the non-DM group. Thus, based on the results from this study the answer to Q2 ”Will the mechanism make the users more likely to falsely identify legitimate ads as fraudulent?” appears to be no. On the contrary the participants who used the defense mechanism actually placed more trust in the supposedly legitimate ads than the participants who didn’t.

To summarize; this survey indicates that using the defense mechanism we propose in an online auction house environment can make the users less susceptible to fraudulent ads. Moreover the results indicate that the users will also put more trust in legitimate ads. However it must be said that there was a great spread in the answers for all groups over all ads. This is shown in Table 1 that presents the standard deviation for each ad and group. This shows that with or without training it is hard to distinguish a fraudulent ad from a legitimate with only the actual ad as information.

Question	Standard deviation
Fraud1-nonDM	1,48
Fraud1-DM	1,56
Fraud2-nonDM	1,51
Fraud2-DM	1,35
Fraud3-nonDM	1,64
Fraud3-DM	1,38
Fraud4-nonDM	1,60
Fraud4-DM	1,56
Fraud5-nonDM	1,65
Fraud5-DM	1,73
Fraud6-nonDM	1,68
Fraud6-DM	1,37

Table 1: Standard deviation for all survey questions

6. Discussion

This study presented a framework for defense against online fraudsters and provided a proof of concept for that framework by testing it in a controlled environment. In this particular study the framework was tested in an online auction house environment. For that reason it is not possible to tell about the effects of the framework in another setting. Furthermore we want to mention that making this kind of studies in a controlled environment is troublesome since several factors that are present in a real world situation are difficult to imitate. After all, the participants in this study did never face any real risk of actually being defrauded. Also, they did not have all the opportunities to really investigate the seller that you would have in a real situation. For one, calling the seller and offer to meet and conduct the transaction in person can be an effective way of avoiding fraudsters.

With that said the study does provide the results that we set out to find by generating a proof of concept for the defense mechanism that we propose. This is done by showing that in our test:

- A person who uses the mechanism is better at identifying a fraudulent ad than a person who does not use it and,

- A person who uses the mechanism does not falsely identify legitimate ads as fraudulent more frequently than a person who does not use it. On the contrary the results actually indicated that a person using the mechanism places more trust in legitimate ads than a person that does not use the mechanism.

7. Future work

One could argue that to generate really strong results when researching online fraud you would have to conduct research in real life scenarios. Since this would involve actually tricking real persons without their knowledge and consent it is of course impossible without breaking many of the ethical guidelines set by the research community.

Even with these problems we acknowledge that conducting studies that imitates real life scenarios is crucial in order to generate a strong basis of research with reliable results. It is our understanding that more research within the area of online fraud prevention with a focus on the users behaviors is necessary. For future research within this domain we suggest that researchers make use of gamification as a part of the methodology. While we cannot recreate a real life situation using surveys or likewise we believe that making the actual study into a game, where the participants are encouraged to do good in order to get a high score or likewise, can make the participants feel the same risks as they would in a real life situation.

8. References

Arachchilage, N.A.G. and Love, S. (2014), "Security awareness of computer users: A phishing threat avoidance perspective." *Computers in Human Behavior*, Vol. 38,pp304-312.

Brottsförebyggande rådet (2013), "Bedrägerier och ekobrott.", http://www.bra.se/bra/brott--statistik/bedragerier-och-ekobrott.html, (Accessed 1 may 2014)

Brown, J.S., Collins, A. and Duguid, P. (1989), "Situated cognition and the culture of learning.", *Educational researcher*, Vol. 18, No. 1, pp32-42.

Davinson, N. and Sillence, E. (2010), "It won't happen to me: Promoting secure behaviour among internet users." *Computers in Human Behavior,* Vol. 26, No. 6, pp1739-1747.

Dittrich, D. and Kenneally, E. (2011), "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research", *US Department of Homeland Security*.

Garg, V. and Nilizadeh, S. (2013), "Craigslist scams and community composition: Investigating online fraud victimization." *Security and Privacy Workshops (SPW), 2013 IEEE* pp. 123-126.

Herrington, J. and Oliver, R. (1995), "Critical Characteristics of Situated Learning: Implications for the Instructional Design of Multimedia.", *ASCILITE 1995 Conference,* pp253-262.

IC3. (2013), "2012 - Internet Crime Report", https://www.ic3.gov/media/annualreport/2012_IC3Report.pdf (Accessed 30 marsh 2015)

Pratt, T.C., Holtfreter, K. and Reisig, M.D. (2010). "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory.", *Journal of Research in Crime and Delinquency*, Vol. 47, No. 3, pp267-296.

Schrittwieser, S., Mulazzani, M., & Weippl, E. (2013), "Ethics in Security Research - Which Lines Should Not Be Crossed?", *Security and Privacy Workshops (SPW), 2013 IEEE,* pp1-4.

USA.gov. (2013),"Internet Fraud", http://www.usa.gov/Citizen/Topics/Internet-Fraud.shtml, (Accessed 1 may 2014).

Wilsem, J.V. (2013), "'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization.", *European sociological review*, Vol. 29, No. 2, pp168-178.