The Cyber Trust of Norwegian Online Flea Market: An Ethnographic Study on Fraud

Yushan Pan

Organisation
yushan.pan@ntnu.no

Abstract. This work-in-progress paper reports an ethnographic study on how cyber trust could be designed to prevent online fraud. A yearlong ethnographic study was conducted with a group of victims who were frauded in online shopping. I discuss how-to re-build cyber trust by linking different interests of actors, such as sellers, the police, the consumer council, the person registers authority, the national collection agency, and the classified advertisements website provider, towards an anticipated safety for online shopping. Through the actor-network theory, the paper unpacks the mechanism of payment method of classified advertisements website which caused the cyber trust to be unsuccessful. Reasons behind it is the interests of different actors are not probably translated which caused the safety-vulnerability and gave chances to the scammer. I assert that a better understanding of the social aspect of technology use will provide fruitful insights on societal changes in information society for better living.

Keywords: Ethnography, safety, online shopping, social computing.

1 Introduction

The interaction between work practice and technology has always been a central research focus within information systems, with its aims to design information systems to support human interaction in cooperative environment. Ethnographic studies of information-systems-in-use have described how successful information systems were inseparable from the situated activities in which they existed, and user-centered and situated design was advocated [1–3]. Such situated, worker-oriented design might involve further development, such as safety concerns in cooperation [4]. When investigating information-systems-in-use we see unexpected unsafe results which points to the deviations from the original design goals and objectives and the unintended consequences of using online shopping platform, such as Norwegian online flea market.

However, different with regular online stores that controls unsafe purchasing in their own platforms, the online flea market kicks off some part of the responsibility for the safety control outside the platform due to various reasons, alternatively, the platform suggests both buyers and sellers to use common sense, avoid prepayment, and carefully deal with personal information. For example, if a buyer comes across an offer that is too good to be true, the buyer should notice that ads probably is a fake

one. The buyer should not prepay to the seller before asking the seller to verify his/her users on the platform through the personal identification systems. And both buyers and sellers should be careful to share personal information but the platform suggests that if one shares first name, address and telephone number, it would be safe enough [5].

Thus, the role of information systems as a platform has been little focused on cooperative safety. Although empirical studies have focused on the safety in technology use, most of them only focus on the privacy. There is still a lack of empirical studies that investigate how safety mechanism could be designed in sociotechnical information systems for online shopping where information systems and work practices evolve together.

The importance of understanding this safety mechanism may become more evident if we consider the change within information technology in recent years. For example, in the maritime domain safety issues happened sometime neither technical problems of systems nor the issues of human organizations. Safety issues occurs during the cooperation among the networked human, information systems, and interactions among humans and systems [4, 6]. This understanding of safety mechanism is deviating from the safety studies in information systems. For example, safety is considered as ethical and political [7–14], as well as highly reliable human organizations [15–20]. Neither, such safety mechanism is different with those understandings where safety is part of the systems and applications' attributes in systems models.

When safety issues happen during the cooperation, there is lack of mechanism for protecting the rights for the buyers, and sellers, unsafe online purchase will happen. If the seller certified their personal ID on the platform and the buyer trusted the ads, when both sides make a deal of how to finish the purchase, such as the buyer pays a half of asking price and pay the rest when received the item. Or, the seller trusts the buyer and posts the item first. Both solutions have high risks which go beyond the current argument of ethical, privacy, and security issues in the support platform. In other words, the platform provider offers less secure information systems to the market. This paper reports an ethnographic study on the Norwegian online flea market. Through investigating a real case, the aim of the paper is to identify several breakdowns when an online fraud happens in use of an information system which provided by one of the largest online market provide in Norway.

The paper is structured as follows: In section 2, methodology is presented, which include the case, the research site and method. In section 3, the paper describes the ethnographic study with victims who helped themselves to find a solution to find out the scammer and convince the other actors to act on the cases until they finally catch the scammer and request money back. In line with our ethnographic description, the paper reflects on how to design a better information systems platform for online flea markets to providing better safe and secure experiences for both buyers and sellers in very practical terms in section 4. The paper concludes in section 5.

2 Methodology

2.1 The Case and the Research Site

The Norwegian online flea market was established in 1990s with sections devoted to second-hand housing, cars, and for sale. The purpose is to classify advertisements to provide straightforward information from the seller to the buyer. Different with business to customer model, the online flea market builds upon the integrity mechanism and seeks both buyers and sellers have highest integrity during a transaction. Such flea market also differs from eBay, and there are no payment methods. That means no secure payment in between sellers and buyers.

The market platform also does not use any third-party platform during the purchases. To secure a purchase, the recommended option is to meet in person. However, this might inconvenient for sellers and buyers who are not in the same place. In this case, the platform suggests a few tips that both buyers and sellers can ensure the deal is somehow protected. This is means that if the buyers intend not to pay, the buyers could ask the platform to help with the crime case if the police engaged in. Also, if the sellers do not post the goods after the buyers make payment, the buyers could ask the platform to help with the case too.

However, if a fraud happens, no one could solve the problem until someone could decide. Unluckily, in this study, the fraud is never happened since no one can close the case. A buyer wants to buy a mobile phone, but he decides to check on the flea market since sometimes the price is reasonable than a brand new one. He finds a phone which he wants to buy. Then he sends an email to the seller, as suggested by the online platform, asks the following questions – why you want to sell, do you have receipt for this phone, if we could not meet how we could reach a deal. Soon, the seller replies that the reason she wants to sell the phone is because her boyfriend betrayed her and gave this phone as a gift. However, she decided to sell the gift since she did not need it. She also shows the receipt where she brought the phone with her name printed on the paper. However, she wants the buyer to pay full price before she posts the phone to the buyer's address.

In this situation, the buyer checks if the seller is recognized with her national ID before he decides whether to pay or find another option. He found that the seller was registered her national ID, but he still has some doubt, so he replied to the seller that he would not pay but choose to sign a standard contract which is provided by the customer council of Norway. While, the seller does not want to sign the contract, she provides another solution that the buyer can pay half of the total amount immediately, otherwise there is no deal. Since the buyer have checked all suggested information and really wants to buy the mobile phone, he accepts the solution. Then, the seller sends her bank account number to buyer.

The buyer paid a half price to the seller including the post fee, then the seller sends a tracking number of the package to the buyer. And agreed that when the buyer receive the mobile phone, he pays the rest of amount. All these activities happened on Sunday. Regarding to Norwegian Banks, no transaction could be made immediately but you can register it online. This is means that you could not see who you are trans-

fer money to but only account number. The owner of an account will only be visible after two working days. In this time, if the buyer has any doubt, he could cancel the transaction. And this is the last chance if he finds this is a fraud. However, everything goes so smoothly, and he believes that he will receive the package on Monday, or at least on Tuesday. He will have more information on where the package is and to whom he paid for.

On Monday, the buyer finds the package is not addressing to him regarding to the post service since the address is another city which thousand kilometers away from the buyer's address. He questions the seller what is wrong. The seller, now pretends, she sends to a wrong place and she promises to correct it with the post office. She did correct it but told the buyer by email, saying that she could not take photos because her mobile has dropped on floor, now the phone has some problems on taking pictures. The buyer chose to believe her unfortunately. He still believes that he will receive the mobile phone. He chooses to wait for another two days since in that time if everything is correct, he will receive the package. While, two days later, the package stopped to a wrong destination.

This time, he chose to ask the post office, if the package was really addressed to him. The post office confirms that the package addressed to no one. The address also is not address to the place the buyer lives. Then the buyer logon to his bank account to ask the bank to send him a receipt where the money goes. The bank returns a paper form showing the money was sent to a man who is living in even different places compared to the seller's registered address on the online platform. Now, the buyer knows this must be a fraud. He warns the seller via email, saying that return the money, or doing the right thing to finish the deal. However, this time there is no reply anymore.

The buyer decides to report the case to the online platform. The online platform requests the buyer to indicate all information exchanged between the buyer and the seller. In the meantime, the platform helps to check again if the seller has registered any national ID. The conclusion from the online platform via their internal email systems, stating that the buyer needs to contact the customer council of Norway and the police because regarding to the law the online platform has no rights to further process a fraud case. The only thing the online platform could provide is a case number, showing that this is an online fraud.

The buyer later contacts with the police and the customer council with the case number provided by the online platform. The police reply that they receive the case and now investigates it. A half year later, police notices the buyer the person who cheated online is now on trails and now a lawyer engaged in the case. When the case will be closed, there is no clear answer. And police suggest the buyer does not contact anymore since it is a low priority case. If there is an update, they will notice the buyer. In the same time, through a half year investigation, the customer council decides to close the case because for the council it is impossible to process it further if the seller never respond their requests. They tried to send email, post mail, and call the seller, there were no reply. Thus, they must get back to the buyer and suggest the buyer to close the case. But the buyer has the right to reopen the case if there is any update from the police, then the council can request money back from the seller.

2.2 Method

Ethnography is a good foundation for integrating of online and offline data gathering in Internet, in order to obtain the 'overflowing description' [21]. Around 40% of the author's off work time during the past year was spent online and offline, talking with the buyer, the online platform, the police, and the costumer council. Also, I observe and listen to the conversation between the buyer and bank, police, costumer council and online platform. Also, I read the exchanged information between the buyer and these organization, under the permission of the buyer.

3 No Money Comes Back

The buyer, himself, investigated if the seller is a scammer. He found there was a safety logo after the seller's name (Anonymous in this paper, although the name used online was a fake one). That means, the seller logged in the classified advertisements website with an authorized ID. Such an ID is commonly used in Norway as biometric authorization for logging on public services as well as financing services. To name a few, bank, insurance, health information system, digital post, and many others. All the victims are affected by such a logo. The reason is because of the website says if anyone who is registered an address in Norway and with a BankID, if wanted log in with BankID will lead to a verified user status [22]. In line with this verified status, all victims build up trust on others even though they noticed there is no trustable payment method between the buyers and the sellers. However the website does not promise even though the ID is correct the seller or buyer still can be a scammer.

All victims paid to the scammers through bank transfers due to living in different locations and impossible to meet in person. The banks have recorded where the money goes, for example account owner, owner's registered address, email and telephone number. When addressing how the banks could help the victims, I followed the victim I met to the bank. However, the back cannot get the money back but can only show a letter to indicate who is possible a scammer. Noted that, on the letter, it shows a different name, a different email, a different telephone number, and a different registered address. Then, he contacts both the website and the Customer Council. This is surprised because if such personal information is different with the registered user name on the website. Is it still trustable the BankID verification? What the purpose the website allows sellers or buyers to use a different user than the registered name associated with BankID? Unlikely, the website refuses to tell more information about that scammer due to data protection policy.

Such kind of freedom to use different name without associate with the BankID gives chances to scammers to cheat, without a payment method powered by the website makes the deal even risky. At the same time, the Customer Council confirms the case reporting. However, the Customer Council calls the victim and says they could not help too. In their experience, they suggest the victim to give up since they are unable to find the scammer.

The victim collected all the material as many as he can. Now, he has materials from the Customer Council, the bank confirmation letter, the screenshots of the advertisement, and the email exchanges between the scammer and him. He tried the last hope – the police. He sends all materials to the police and ask for a help. The police confirmed that they received the report and created a crime case by post. In that post letter, the police also notify the victim that a notification will be sent if investigated is finished.

However, this is not the end of the case. Money is still not back. Although the police said that the person was arrested and the case was forwarded to the national collection agency where the victim can get the money back. However, the victim got another letter from the national collection agency, requesting to fill out the form. In the form, the victim is promised to be credited the lost money into his account. The victim sends back the form and wait for the money. Nothing happens after that. Since this is a working in progress paper, I still collect data and hope I could interview with the national collection agency soon.

4 The Cyber Trust

In the length analysis, I address contexts of cyber trust which goes beyond purely technical issues of security design in computer systems as well as the interaction of those computer systems. As seen, the scammer bypassed the biometric authorization and legally registered and verified himself on the classified advertisements website. Since the website allows use nickname rather than the real name which is associated with the BankID, the scammer could use fraudulent name, email, and telephone number to cheat. This is the biggest flaw on the website.

In user experience research, Mertzum [23] argues that organizational usability is about the match between the user and the system, between the organization and the system, and between the environment and the system. Organizational usability must be evaluated in situ. The computer systems must be used for real work. The same could applies to the organizational cyber trust. The fraud does not happen due to technical failures in online shopping. Victims do not face failures of the system, they could easily log in and see the advertainments. Victims also do not face identification and authentication problems. Instead, their trust of identification and authentication techniques caused them to believe the scammer. The two faces of identification and authentication techniques empowered the scammer as a good user. In this manner, no failure and errors are about wrong passwords, wrong identification tokens, misuse of the biometrics. The fact is that the algorithms for identification and authentication discriminate the victims during their interactions with the scammers through the website. I do not mean that the algorithms have any technical problems. The problems are hidden in practices. Cyber trust in such practices is only about individual interaction with cybersecurity systems. More than that, it is about re-examine cybersecurity technology from a holistic point of view. Only zoom out from a single technical issue, should we have the ability to see the problem in the whole information infrastructure.

5 Concluding Remarks

This article presents an ethnographic study on cyber trust from a user's perspective. The study analyses the problematic areas in information systems that are proposed to support a safe environment for dealing purchase of secondhand goods online. By analyzing different actors in the information systems, their interests, and the website's interpretation of cyber trust, an outline of reconsidering cyber trust is suggested. The article asserts that cyber trust is more than technical solutions to protect attacks and misuse of user cases from the phase of human-interface interaction. The evaluate of cyber trust must be put into real use. Only these methods could reveal inviable problems that are hidden in cooperation, organization, and above technical solutions in cybersecurity issues of information systems for e-commerce. To conclude, the article suggests combining both technical and social aspects of safety concerns when addressing on cyber trust.

In the present study, several authorities failed to help the victims due to various reasons. However, the most important reason is the privacy protection policy. It is understandable that the website does not able to share the core information of the scammer with the victim. It becomes a problematic that if one could use BankID to verify himself or herself, should it a problem to share information in between Bank, the Police, the Customer Council, and the National Collection Agency. It might out of the scope when addressing relative laws. However, it would helpful if the website could find a payment method which build upon the BankID and enable tractability if fraud happens. Such method might be a useful tool for secure both buyers and sellers from a user's perspective. Then the cyber trust will go beyond the discussion on human-interface interaction but combining technical and social aspects of safety concerns within an infrastructure of dependency, identification and authentication, privacy, and usability at large. In turn, such an infrastructure could serve as a mechanism between users and security techniques from a social-technical aspect to protect all stakeholders' goals and views.

References

1. Greenbaum, J., Kyng, M.: Design at Work: Cooperative Design of Computer Systems. Lawrence Erlbaum, New Jersey, USA (1991).
2. Suchmann, L., Blomberg, J., Orr, J.E., Trigg, R.: Reconstructing Technologies as Social Practice. Am. Behav. Sci. 3, 392–408 (1999).
3. Aanestad, M.: The Camera as an Actor Design-in-Use of Telemedicine Infrastructure in Surgery. Comput. Support. Coop. Work. 12, 1–20 (2003).
4. Pan, Y.: From field to simulator: visualizing ethnographic outcomes to support systems developers, (2018).
5. FINN.NO: Nyttige tips for en trygg handel, https://hjelpesenter.finn.no/hc/no/articles/115005831409-Nyttige-tips-for-en-trygg-handel.
6. Pan, Y., Finken, S.: From Offshore Operation to Onshore Simulator: Using Visualized

Ethnographic Outcomes to Work with Systems Developers. Informatics. 5, (2018).
7. Abokhodair, N., Vieweg, S.: Privacy & Social Media in the Context of the Arab Gulf. In: Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS ’16. pp. 672–683 (2016).
8. Yarosh, S., Bonsignore, E., McRoberts, S., Peyton, T.: YouthTube: Youth Video Authorship on YouTube and Vine. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW ’16. pp. 1421–1435 (2016).
9. Hoyle, R., Das, S., Kapadia, A., Lee, A., Vaniea, K.: Viewing the viewers: publishers’ desires and viewers’ privacy concerns in social networks. In: CSCW 2017. pp. 555–566 (2017).
10. Zytko, D., Lingel, J., Birnholtx, J., Ellison, N., Hancock, J.: Online Dating as Pandora’s Box: Methodological Issues for the CSCW Community. In: CSCW 2015. pp. 131–134 (2015).
11. Forte, A., Andalibi, N., Greenstadt, R.: Privacy, anonymity, and perceived risk in open collaboration: a study of Tor users and wikipedians. Proc. Comput. Support. Coop. Work Soc. Comput. 1800–1811 (2017).
12. Raval, N., Dourish, P.: Standing Out from the Crowd: Emotional Labor, Body Labor, and Temporal Labor in Ridesharing. In: CSCW ’16. pp. 97–107 (2016).
13. Ozcan, K., Jorgenson, D., Richard, C., Hsieh, G.: Designing for targeted responder models: exploring barriers to respond. In: CSCW 2017. pp. 916–924 (2017).
14. Wisniewski, P., Ghosh, A.K., Xu, H., Rosson, M.B., Carroll, J.M.: Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety? Proc. ACM Conf. Comput. Support. Coop. Work. CSCW. 51–69 (2017).
15. Perrow, C.: A society of organizations. Theory Soc. 20, 725–762 (1991).
16. Perrow, C.: Normal Accidents: Living with High Risk Technologies., (1985).
17. Weick, K.E.: Organizational Culture as a Source of High Reliability. Calif. Manage. Rev. 29, 112–127 (1987).
18. Harper, R.R., Hughes, J.A., Shapiro, D.Z.: Harmonious working and CSCW: Computer technology and air traffic control. In: Studies in Computer Supported Cooperative Work. pp. 225–233 (1991).
19. LaPorte, T.R., Consolini, P.M.: Working in Practice But Not in Theory: Theoretical Challenges of “High-Reliability Organizations.” J. Public Adm. Res. Theory. 1, 19–48 (1991).
20. Bentley, R., Hughes, J., Randall, D., Shapiro, D.: Technological support for decision making in a safety critical environment. Saf. Sci. 19, 149–156 (1995).
21. Sade-Beck, L.: Internet ethnography: online and offline. Int. J. Qual. Methods. 45–51 (2004).
22. FINN.NO: Hvordan blir jeg en verifisert bruker? [How do I become a verified user?], https://hjelpesenter.finn.no/hc/no/articles/202612752-Hvordan-blir-jeg-en-verifisert-bruker-.
23. Hertzum, M.: Three contexts for evaluating organizational usability. J. Usability Stud. 14, 35–47 (2018).