"Don't Break My Heart!": User Security Strategies for Online Dating

Borke Obada-Obieh
Carleton University
BorkeObadaObieh@cmail.carleton.ca

Sonia Chiasson
Carleton University
chiasson@scs.carleton.ca

Anil Somayaji
Carleton University
soma@scs.carleton.ca

***Abstract*—Online dating sites require users to reveal information about themselves to find potential matches, yet users must also be wary of potential security and privacy threats. We conducted semi-structured interviews with 10 participants to better understand the various methods they employ to maintain their personal security and privacy while arranging to meet strangers in person. Specifically, we asked questions about how they validate the legitimacy of potential partners, how they safeguard their online information, and their overall experiences with dating sites. We found out that though users are familiar with most of the traits exhibited by scammers, they do not have sufficient security measures to protect themselves from being scammed. Users also have no principled means of balancing the need to share information with their need to stay safe. Our results suggest that better security and privacy mechanisms are needed to improve the online dating experience.**

I. Introduction

Dating sites are a popular social media tool enjoyed by many. Unfortunately, like most online platforms, dating sites are susceptible to scams by attackers preying on vulnerable users. The sole purpose of online dating sites is to put in contact people who do not know each other. As a result, identifying unsolicited and spontaneous messages that are the core of traditional anti-fraud online activities does not have any meaning when applied to online dating sites. Even worse, dating site scammers are known to exploit the vulnerable emotional state of unsuspecting users, making their attacks more effective [9].

While past research on online dating has primarily focused on the variety of risks people face in using these services [4], [5], [7], [8], [13], [17], there has been little work regarding users' perception of those risks or on understanding the strategies they use to mitigate those risks.

Through semi-structured interviews with ten subjects and qualitative data analysis, we explored how users of online dating sites address their privacy and security concerns. The goals of this study were as follows:

1) Understand the security and privacy precautions taken by users in online dating sites.
2) Understand how users balance the need for sharing information with the need to protect themselves.
3) Explore situations where users discover others were untruthful in their representations and how this might endanger them.
4) Explore how users gauge the accuracy of information revealed by others on dating sites.

We found that dating site users are aware of the risks and take a variety of steps to protect themselves, such as being wary of weird requests and investigating a potential date's social media presence. Unfortunately, none of these strategies offer sufficient protection against serious scammers.

The rest of this paper proceeds as follows. In Section II we introduce online dating and discuss past work on online dating security. Section III presents the methodology of our study. We present our results in Section IV and discuss their implications in Section V. Section VI concludes.

II. Background

While online dating sites have been around since the early days of the World Wide Web (Match.com was founded in 1995 [1]), in recent years online dating platforms have become increasingly mainstream. Although their precise format and target audience vary widely, their basic format remains the same. Individuals create profiles for other users of the site to browse. While these profiles do not contain an individual's name, address, or other standard identifying information, these profiles do contain demographic information, personal statements, answers to standard questions, and (perhaps most importantly) pictures. Typically, other users of the site can search for and view these profiles. When a suitable profile is found, a user can send the profile's owner a pseudonymous message, thus beginning a conversation. Sometimes the online conversation is the goal; more commonly, though, the conversation's goal is to determine whether to proceed to the next step—meeting in person. Online dating sites thus facilitate highly personal interactions between people who otherwise would be strangers.

As of 2013 one in every ten American had used a dating site or application, and 66% of these users had gone a step further to set up dates with people they met on these platforms [20]. As as 2014 it was reported that 38% of single adults in the US had used an online dating site [11]. New reports emerged in 2015 that the use of dating sites had increased from 10% in

USEC '17, 26 February 2017, San Diego, CA, USA
Copyright 2017 Internet Society, ISBN 1-891562-47-9
http://dx.doi.org/10.14722/usec.2017.23046

2013 to 27% among users ranging from 18–24 years old. The use of the platform also doubled from 6% to 12% among users ranging from ages 55–64 [19]. Rosenfeld et al. and Couch et al. [7], [18] both highlighted the importance of this relatively recent type of interaction, noting that online dating has partly displaced family gatherings, schools, and parks as places to meet potential partners.

A key challenge in any online dating interaction is establishing sufficient trust to move the interaction from online to in person. While safety concerns could in principle cause individuals to obfuscate or outright lie in their online profiles and interactions, in practice this is often not the case. Online daters are relatively truthful about their physical attributes [12], and they tend to reveal a significant amount of personal information—enough to potentially make them susceptible to scammers [15]. Indeed, people are sometimes traumatized by their experiences with online dating. Sometimes the trauma comes from going on "bad dates," or from ending up in abusive relationships. However individuals are also traumatized by being outright scammed [22]. Online dating scams can result in financial losses for victims and forms of blackmail such as sextortion [9]. Sometimes these scams aren't even conducted directly by humans. Instead, chatbots can deceive individuals into disclosing enough sensitive information with which to mount an attack [14]. While users can be proactive in limiting what they disclose, they can also take risks just by installing an app on their phone. Although dating apps such as Tinder limit accuracy when disclosing the distance to other nearby users of the app, techniques such as trilateration can be used to help locate a targeted individual [10].

Even though dating sites may try to detect scamming-related behavior, they face significant barriers beyond the obvious privacy-related ones. Many times scammers make an initial connection with a potential victim through the online dating site but then convince the victim to continue the conversation on a different messaging system. As a result, online dating site administrators do not even see the scam, as the attacker has changed his communication channel [14].

The most closely related work to our current research was conducted by Couch et al. [7] with data collected in 2008–2009. They conducted online interviews with participants (mostly from Australia) to gather perceived risks and dangers encountered. Their participants generally viewed online dating as risky and were primarily concerned with deceit, emotional vulnerability, and sexual risks. They framed risks in terms of dangerous 'others' who could cause them harm and they worried about international scammers.

Our research explores similar themes, several years later, when online dating has become mainstream. We also go beyond the exploration of perceived risk to study users's knowledge of specific types of scams and the strategies users employ to protect themselves.

III. Methodology

After receiving clearance from our University's Research Ethics Board, we recruited 10 participants, primarily through a university-wide email announcement and subsequent snowballing. The participants included six females and four males with ages ranging from 18-50 years old. Six participants were students while the rest were university staff. All participants had used a dating site at some point for at least a month. The participant demographics are summarized in Table I.

ID	Gender	Age	Occupation
P1	Female	22	Masters Student
P2	Female	18	Undergraduate Student
P3	Male	21	Undergraduate Student
P4	Male	19	Undergraduate Student
P5	Female	24	Research Assistant
P6	Female	20	Undergraduate Student
P7	Female	49	Administrator/Advisor
P8	Male	20	Undergraduate Student
P9	Male	23	Trainer
P10	Female	50	Staff

Table I. Demographics summary of participants

We conducted individual semi-structured interviews with participants. While the interview was structured around a question guide, digressions were allowed so participants could expand upon their experiences where appropriate. We chose this approach because it offers participants the freedom to express their view in their own terms, providing more reliable, comparable qualitative data [6].

Participants completed a demographic questionnaire before their interviews. Interview sessions were audio-recorded. Participants were asked to discuss the various activities they have carried out on dating sites and the end results of those activities. Participants could skip any question they were not comfortable answering. Participants were further encouraged to share additional dating site experiences they may have that could be of benefit to the research. Each session lasted approximately 20 minutes.

The questions covered:

1) The sites they use, whether they pay for these services, whether their online interactions have resulted in real life meetings or relationships.
2) The completeness and accuracy of their profile information, and how this affected their experiences.
3) The precautions taken to avoid scammers.
4) Any situations where they have dealt with scammers, untruthful others, or dangerous situations.

We conducted qualitative analysis on the interview data. From the users' responses, we extracted relevant incidents and common themes, paying particular attention to issues of security, privacy, and safety. We also tabulated common responses as an indication of their frequency. We note that these numbers represent a lower bound since some participants may also have similar behavior or opinions but not have explicitly mentioned it since responses were open-ended.

IV. Results

Participants' responses have been grouped into themes, focusing on security, privacy, and personal safety issues.

A. Security And Privacy Precautions

Participants generally felt a need to protect themselves while on dating sites or on dates. They reported several strategies and precautions, as summarized in Figure 1. We observe that females reported more protective strategies than

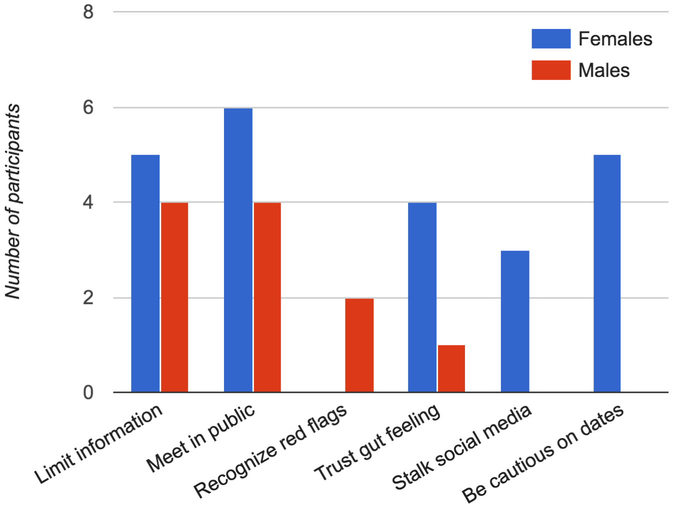

Figure 1. The number of participants reporting each precaution.

males. Next, we describe these strategies and offer exemplar quotes from participants describing their approaches.

1) Providing Limited or Incorrect Information: 9 participants (5 females and 4 males) reported omitting information when filling out their profiles on dating sites. No one felt that this had negatively affected their dating site experiences.

Not all participants omitted information solely for security or privacy reasons. Two participants (1 male and 1 female), said they omitted information in order to invoke some form of mystery. P2 explains, *"If you put out all of the information at once, what are you going to say when you meet the person?"*. Therefore 7 participants omitted information as a precautionary security and privacy measure. Participants claimed they left out information that was too readily identifiable or revealing, such as their home address, occupation, date of birth and income. P3 commented, *"If you call your bank at anytime, the first thing they would ask you is your date of birth, hence I never put up my correct date of birth when filling out profiles"*. One participant, P5, explained that in addition to omitting information about herself, she also gave misinformation to stay safe, saying, *"I always fill out a wrong digit or two in my mobile number whenever I need to put it up"*.

The remaining participant, on the other hand, said she truthfully fills out all fields and uploads her most recent pictures when filling out profiles. She explains, *"I am always 100% true... there is nothing you can do if people recognize your picture from a dating site, it's the price you have to pay."*

Interestingly, all 10 participants uploaded their pictures. When asked whether they considered photos personally identifiable, none of the participants could defend this practice, acknowledging that it was a concern but believing it was a necessary risk. P5 explained "Yeah, they can trace me... but no one's going to talk to you if you don't have your picture up, that's how dating sites work."

2) Sharing Further Information: As a security measure, participants delayed sharing some information until they felt they could trust their matches better. Participants, however, had varying ideas on how long the waiting period should last before exchanging more personal information or agreeing to meet in person. P5 explained that she would talk to a match for at least a week before exchanging phone numbers. P2, on the other hand, said she would never exchange phone numbers or further personal details until she met the match in person. P10 was of the opinion that it was best to collect the match's phone number but to never give hers and hide her caller ID whenever making calls to the match.

3) Setting Up First Dates: All 10 participants believed that a first date should be set up in a public location, for example, at a coffee shop. However, strategies for when to meet potential matches varied. Two female participants said that for security reasons, it was better to meet sooner rather than later. P5 narrated an experience of how a dating site user she was starting to like kept postponing their date. She soon discovered the user was a scammer. She explained that scammers would rather not meet and that if a match repeatedly postponed the meeting time then you should be suspicious. However, three other participants were of the opinion that to be safe, it was better to meet only after talking for an extended period of time. P2 thought three weeks was sufficient to know a person, after which she would set up a date. P1 insisted that two months was the best time frame.

4) Recognizing Weird Requests As Red Flags: Two female participants stated that as a security measure, they stayed away from guys who made 'weird' requests such as asking for nude pictures or monetary assistance. They believed those type of guys were mostly scammers. To further illustrate her point, P10 said, *"One guy I was chatting with online claimed he was staying at Sussex Drive [in Ottawa]... only the Prime Minister [of Canada] stays there! It was then I discovered he was a scammer... and soon enough he started requesting money."* She further explained other cues that she utilizes to identify potential red flags in her conversations with other dating site users, such as location or time differences. In staying safe online, half of the participants (4 males and 1 female) mentioned that going with their gut feeling was critical as it was usually never wrong.

5) Stalking Social Media: Three female participants admitted to carrying out social media stalking as a precautionary measure to uncover details about potential matches. P2 explained, *"[before agreeing to meet up] I'm good at stalking, I look up people on Facebook, Twitter, Instagram... everywhere!"* P10 further asked questions to verify if potential matches can back up what they shared online; she explains, *"I always do my research online, then I ask them direct questions to confirm if what they wrote is true."*

6) Being Cautious While On Dates: Five female participants took additional precautions while on dates, such as making sure a third party was present. P1 commented *"... (my match) came to my apartment for the first date, but I made sure my roommate was in."* P2 agreed, saying she always went on dates with a friend, *"Whenever I go to Starbucks for the dates, I always went along with my friend... he [the date] would never know my friend and I know each other... my friend sat out of sight watching us all through the date."*

Others made sure that someone knew the details of the date and sometimes made it clear to their dates that this was the case. P6 explained, *"I would give my friends his picture* *and they will always know where we are meeting…like when I wanted to go with a guy on a first date, I took a picture of his license plate number. He didn't know. I then texted my friends the make of the car. During the date, I kept telling him I'm updating my Facebook status. It was like making a subtle threat to him"*. P5 also explained *"My roommates always knew where we were headed."*

B. Balancing Privacy and Sociability

Participants struggled with how to fulfill their desire for privacy with the purpose of the dating site, which is to meet people, socialize, and get to know each other. In many cases, they sacrifice their privacy when faced with a choice between the two. This is clearly a situation where the security and privacy are hindering the user's primary task [21].

Three participants (2 males, 1 female) agreed that there is such a thing as "too much information" when using dating sites. But none could give a definite answer on where they draw the line on how much information is considered "too much." Those who considered omitting information from their profiles were asked how they decided what should be included and what should be left out, but no consensus emerged. P3 noted, *"There's nothing you can really do to keep safe online cause it's online…they could always hack into it anyway…so…"*. He further explained, *"When using dating sites, sometimes I would put up sensitive information…in my head I'm like you shouldn't be doing that, but there's not much you can do."* P5 went on to say, *"I just assume that people at the other end are also as sincere as I am and are looking to just date too"*. P10 and P5 explained that it was only when they were *"less protective and loosened up"* that they found suitable matches. P10 explained, *"I was very careful not to give out too much information, but then it could restrict you…so I loosened up…you just have to be wise."* P5 commented, *"I started to have lots of success when I started joking about it and let down my guard."*

Participants thus compromised between the need to share information and the need to stay private and secure. In these circumstances, participants clearly believed that one had to be sacrificed for the other since they saw positive results when they revealed more information than they initially wanted.

C. Detecting Scammers and Gauging Truthfulness

Participants had developed several strategies for identifying potential scammers, mostly based on social cues from the potential match. Figure 2 summarizes these strategies.

1) Trusting A Gut Feeling: Four participants (all male) claimed they relied on their gut feeling to know if the information provided online is true or whether a scammer is at play. They recognized, however, that this was not a foolproof strategy. P3 commented, *"it's tough…I mean if you are a good judge of character that may help, but really you never know."*

2) Relying On Social Norms: Participants relied on characteristics of the conversation and interaction to identify potential threats. When these varied from the expected social norms, this was a cause for concern.

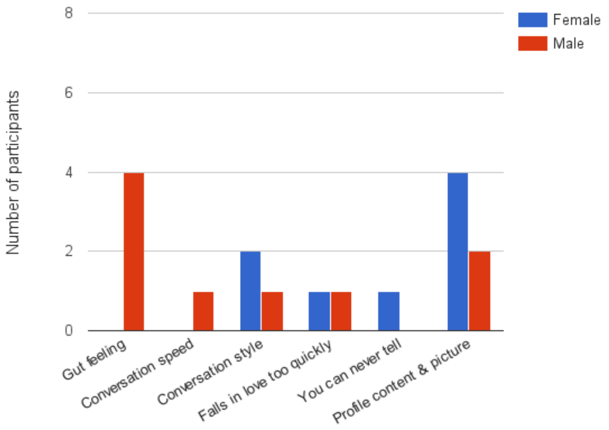

Figure 2. Shows the male and female ratio of how participants gauged the accuracy of information shared online

Three participants (2 females, 1 male) claimed that the topic and pace of conversation could sometimes help them determine if a potential match is a scammer. P1 commented, *"Creepy ones always start the conversation way off the line."* P4 explained, *"if a first conversation starts with 'Hey baby, how you doing?'…I'm like 'really'?"* Two females were alarmed if matches consistently requested nude pictures. One male participant (P4) was strongly believed that if the conversation speed was too fast, then the person was most likely a scammer. He explained, *"People who reply way too fast or way too often are definitely scammers"*. P2 elaborated, *"If they ask to hang out too soon, they are scammers!"*

Others thought that displays of emotion that seemed out of sync with the stage of the relationship were suspicious. Two participants (1 male, 1 female) strongly believed that if a match professed falling in love very fast, it was another sign of a scam was underway. P7 comments, *"All of a sudden they are in love with you…they want to meet you right away, those are fake people."*

3) Noticing Inconsistencies in Profiles: Six participants (4 females and 2 males) believed that inconsistencies in normal profile content and picture could signal a scammer. Participants attributed weight to the profile pictures, expecting them to depict 'average' people and expected profile descriptions to provide sufficient detail about the person. Two females felt that if a profile picture is too cute then the profile is suspicious. Three participants (2 males, 1 female) said weird pictures accompanying weird profile descriptions were a cause for concern. To illustrate this, P4 explained *"Some people have like a dog as profile picture…and write as description 'I'm a dog'…those are completely fake…"* P6 claimed sighting multiple profiles for the same person was also a red flag, *"I found same person multiple times, but I can tell it's a different person because of the way they speak and respond."*

4) Requesting Proof: In some circumstances, participants who were already suspicious took extra steps to determine whether they were interacting with a scammer. Two participants (1 male, 1 female) believed that asking for proof of identity was one of the major ways to detect whether a person was a scammer. They did not expand on how they determined the authenticity of the provided proof. P8 explains, *"It's hard to do [detect scammers]... I ask them to prove it [their identity] by sending maybe a picture or something specific."* P10 shared her experience with a scammer, *"So the Nigerian scammer that claims he stays at Sussex Drive started asking me for money that he was stuck somewhere, I told him to scan his passport and send to me... I never heard from him again."*. It is unclear what her next steps would have been had the scammer provided a photo of a passport.

5) You Can Never Tell: One female participant held on to the thought that there was no way you could tell if a potential match was a scammer solely through online interactions. P6 explained, *"It's really hard to do. It's only if you are going to meet someone, you would know if the person is scammer or not. You just have to meet in a public place."*

D. General Dating Site Experiences and Feedback

Looking at outcomes, participants seemed to have had reasonable success with dating sites despite their concerns about privacy and security. Overall, eight participants (6 females, 2 males) had set up dates with people they met on dating sites. The most dates set up by a participant was 30 dates within a space of six months. Six participants (5 females, 1 male) were currently in a relationship with someone they met on a dating site. Two participants said they met people online, who, even though it did not result in a romantic relationship, were still very close friends. P3 explained that even though he had never gone on a date personally, he knew a lot of his friends had been successful at using dating sites.

Interestingly, their opinions seemed to contradict this apparent success. When asked what advice participants would give a friend who was considering using a dating site, half of the participants (4 males, 1 female) advised that people stay away completely from using dating sites. Two claimed that there was a social stigma attached to using dating sites and that people were better off without them. P2 explained further, *"Don't use it [dating site], it's a waste of time... imagine my parents asks me where we met? I would then say dating site?... it makes one look irresponsible."* P4 also remarked, *"Don't go do it [dating sites]... don't go there... it gets you down. It's also easy to waste your time and very emotionally draining"*. P3 cautioned, *"Try as hard as you can not to use it... stay off completely from it, it's not worth it... try and meet someone in real life"*. P6, who was in support of using dating sites, advised, *"Also don't go into it thinking you would have a long term thing, go with the mindset that you want to have fun and if it works that long term way good... else good."*

P5 also recommended that dating sites should adopt additional verification of users at registration to reduce the number of scammers. She would like users to scan their passport or driver's license as a way of verifying their identity. She also worried about her past interactions on dating sites. She worried that her previous dating site may be hacked and all her sensitive sexual information would be made available to the public. She continues, *"I didn't think hard about that until when I was done with it [the dating site]. I was like, I shouldn't have been so truthful with these questions, what if they come back to haunt me in future?"* As dating sites become more popular, these types of regrets and anxiety about potential attacks are likely to increase.

E. Awareness of Security and Privacy Risks

Participants were sufficiently aware of security and privacy issues arising from online dating to correctly identify the major traits exhibited by dating sites scammers and their scams as identified in the literature.

Huang et al. [14] discussed how dating site scammers make use of multiple profiles with the same fake content. Six participants correctly identified this scam. They noted that unusual profile content and multiple profiles with the same content could belong to scammers. Huang et al. further explained how scammers use very attractive profile pictures to attract unsuspecting users; our participants also noted this as suspicious. 30% of participants also correctly identified that unusual requests from dating site users such as request to share nude pictures or money could be a red flag that something is fishy, a characteristic previously noted in the literature [14]. Also, 10% of participants identified that the speed at which dating sites' users respond to conversations could also verify if the user is a scammer (see [14], [16]). Whitty et al. [22] noted that a dating site user who falls in love too fast or almost immediately, could be a sign that the user is a scammer. 20% of participants correctly recognized this trait.

On how users gauge the accuracy of information shared online and how they protect themselves from scammers, Barber et al. [2] identified using basic instinct as one of the main methods. This was correctly identified by 40% of participants. However, gut feeling may not be sufficient to judge the accuracy of information put online or to determine another user's sincerity.

Whitty et al. [22] noted that dating site users should take precautions before meeting new people, including taking time to get to know individuals and letting others know they are going on a date. 60% of participants let someone know their plans when going on a date. All participants (100%) were of the opinion that meeting someone from a dating site should be done in a public place. Also 90% of participants correctly identified that sharing limited information could help protect one's self from scammers.

Like McRae et al. [15], our participants were unable to come to a conclusion on how much information sharing was too much.

V. Discussion

Bonabeau et al. [3] noted that though intuition plays an important role in decision making, it can be dangerously unreliable in complicated situations. Using intuition to judge the accuracy of information shared on a dating site may be even more dangerous because, as previously stated, scammers tend to exploit the vulnerable emotional state of users [14], leaving their gut feelings clouded. Our results indicate, however, that intuition, directly or indirectly, is key to how users of online dating sites keep themselves safe.

They look for "weird" requests and deceptive profiles based on heuristics derived from regular profiles. They observe whether correspondents reply too quickly. They determine what to share, and what not to share, on an ad-hoc basis depending on how safe they feel in a given interaction. These methods can all lower the risks of normal threats, i.e.

avoiding the “creeps” and the “crazies.” Con artists, however, are adept at taking advantage of such emotionally-driven decision making, and the relative anonymity and data analysis opportunities of online dating gives purveyors of scams plenty of opportunities with which to operate.

While none of our participants were deceived by an outright scam in their online dating experiences, this may be a result of our relatively small sample size. Even so, virtually all of our participants encountered some level of deception in online dating at a sufficient level that a common refrain was “you can never know.” Mechanisms that can reduce the ability of individuals to deceive each other in online dating thus have significant potential for improving the quality of the entire experience.

Any such mechanism needs to go beyond protecting users' locations and preventing data breaches. An ideal online dating site would allow users to engage in zero-knowledge-like interaction proofs with potential partners such that private information is only disclosed to individuals who are potentially good matches. The dating site itself would not know the content of the interaction, and individuals would have guarantees that they are interacting with a real human with sincere motives. Further, the reputation of individuals would be clear (while also being anonymous yet impossible to spoof), such that knowledge of bad behavior can be appropriately spread and acted upon without turning into a tool for harming innocents.

From this framing it should be clear that the challenges of online dating are hardly unique. In fact the problems of reputation, trust, and privacy are central to virtually every interaction we have online. With online dating, however, the challenge is acute because of the nature of the interaction. The difference is one of degree, though, not kind.

More practical approaches are needed to help dating sites users better gauge the accuracy of information shared, as the available ones are not sufficient to protect users and to prevent them from falling prey to scamming attacks. They also need help in sharing information about themselves in a way that protects their privacy and safety while also helping them find potential partners. It is possible, then, that mechanisms that fit the requirements of online dating may have significantly wider applicability.

VI. Conclusion

Improving the trust in online dating is now more important than ever, as its influence and popularity continues to grow throughout the world [9]. To this end, we conducted a semi-structured interview with 10 dating site users. The results show that though users correctly identify traits of scammers, they do not have sufficient security measures to protect themselves. While their experiences were largely positive, users were unable to balance information sharing and staying safe online on anything but an ad-hoc basis. We thus hope this work encourages future research into improved security and privacy mechanisms for online dating.

Acknowledgement

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through the Discovery Grant (Chiasson, Somayaji) and Canada Research Chair Programs (Chiasson).

References

[1] “About match.com,” http://www.match.com/help/aboutus.aspx?lid=4, accessed December 14, 2016.

[2] G. Barber and A. Bigham, “The perils and pitfalls of online dating: How to protect yourself,” 2013.

[3] E. Bonabeau, “Don't trust your gut.” *Harvard Business Review*, vol. 81, no. 5, pp. 116–23, 2003.

[4] R. J. Brym and R. L. Lenton, “Love online: A report on digital dating in canada,” 2001.

[5] B. E. Cali, J. M. Coleman, and C. Campbell, “Stranger danger? women's self-protection intent and the continuing stigma of online dating,” *Cyberpsychology, Behavior, and Social Networking*, vol. 16, no. 12, pp. 853–857, 2013.

[6] D. Cohen and B. Crabtree, “Qualitative research guidelines project,” 2006.

[7] D. Couch, P. Liamputtong, and M. Pitts, “What are the real and perceived risks and dangers of online dating? perspectives from online daters: Health risks in the media,” *Health, Risk & Society*, vol. 14, no. 7-8, pp. 697–714, 2012.

[8] J. E. Donn and R. C. Sherman, “Attitudes and practices regarding the formation of romantic relationships on the internet,” *CyberPsychology & Behavior*, vol. 5, no. 2, pp. 107–123, 2002.

[9] S. Edmunds, “Scammers & online dating fraud: 2015 trends and tactics,” 2015.

[10] M. Feltz and M. Chow, “The security of tinder,” 2015.

[11] K. Gatter and K. Hodkinson, “On the differences between tinder$^{\text{TM}}$ versus online dating agencies: Questioning a myth. an exploratory study,” *Cogent Psychology*, vol. 3, no. 1, p. 1162414, 2016.

[12] J. T. Hancock, C. Toma, and N. Ellison, “The truth about lying in online dating profiles,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2007, pp. 449–452.

[13] M. Henry-Waring and J. Barraket, “Dating & intimacy in the 21 st century: The use of online dating sites in australia.” *International Journal of Emerging Technologies & Society*, vol. 6, no. 1, 2008.

[14] J. Huang, G. Stringhini, and P. Yong, “Quit playing games with my heart: Understanding online dating scams,” in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 216–236.

[15] B. McRae and J. McKnight, “Privacy and online dating,” *Convenient of Invasive–The Information Age*, 2007.

[16] Y. Park, J. Jones, D. McCoy, E. Shi, and M. Jakobsson, “Scambaiter: Understanding targeted nigerian scams on craigslist,” *system*, vol. 1, p. 2, 2014.

[17] A. Rege, “What's love got to do with it? exploring online dating scams and identity fraud,” *International Journal of Cyber Criminology*, vol. 3, no. 2, p. 494, 2009.

[18] M. J. Rosenfeld and R. J. Thomas, “Searching for a mate the rise of the internet as a social intermediary,” *American Sociological Review*, vol. 77, no. 4, pp. 523–547, 2012.

[19] A. Smith and M. Anderson, “5 facts about online dating,” http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/, 2016, accessed December 11, 2016.

[20] A. Smith and M. Duggan, “Online dating & relationships,” http://www.pewinternet.org/2013/10/21/online-dating-relationships/, 2013, accessed December 11, 2016.

[21] A. Whitten and J. D. Tygar, “Why johnny can't encrypt: A usability evaluation of pgp 5.0.” in *Security Symposium*. USENIX, 1999.

[22] M. Whitty and T. Buchanan, “The psychology of the online dating romance scam,” *A report for the ESRC. In*, p. 23, 2012.