UNDERSTANDING USER TRUST PROCESSES IN INTERNET APPLICATIONS

by

Anis Ghazvinian

Submitted in partial fulfillment of the requirements
for the degree of Master of Human Computer Interaction

at

Carleton University
Ottawa, Ontario
January 2020

Contents

List of Tables

List of Figures

Abstract

People appear to be inconsistent when deciding what to trust online. They are cautious in online dating platforms but are often naive and careless when acessing online services. We conducted two user studies to better understand this difference: one on evaluating online dating profiles and another on evaluating online service portals. We found that users follow the same trust processes while using different online platforms. The inconsistent observed behavior is due to people having the option of conversing with a potential date online; with online services, sensitive information must be given without any identity-confirming dialog. To bridge this gap we propose an authentication browser which allows the user to verbally interact online platforms in order to ask identity-confirming questions of the service before authenticating to the service. Here we present the results from our user studies and an initial design for an authentication browser extension.

Acknowledgements

First, I would like to thank my parents Hadi and Manije and my brother Ehsan who supported me not only through my Master's journey but also my whole life and stayed with me in all the ups and downs.

Many thanks to Anil Somayaji who inspired and guided me throughout my research work and having many discussions and input in my thesis.

Special thanks to the members of my committee, Robert Biddle and Kasia Muldner, and David Barrera for chairing my defence. I appreciate all their valuable feedback and suggestions which helped me to improve this research work. Special thanks is due to Robert Biddle for opening my way into HCI.

I would like to thank all of the members of Carleton Cloakware Security Research Lab (CCSL) for being such a wonderful, helpful and cheerful labmates.

Finally, many thanks to my amazing friends especially Becky, Nora, Sanaz, and Behnaz who were so supportive and understanding throughout my Master's degree, and created fantastic memories for me.

Chapter 1

Introduction

> "... trust is a social good to be protected just as much as the air we breathe or the water we drink. When it is damaged, the community as a whole suffers; and when it is destroyed, societies falter and collapse." Bok, 1978, pp 26 and 27 [11]

Have you ever trusted someone or something in such a way that you have felt instant regret and asked yourself "Why did I do that?"

Trust is one of those feelings that is easy to express or have destroyed, but difficult to develop and maintain [72]. Trust has numerous meanings which can vary in different situations [8, 23–25, 46, 59, 68, 72, 78–80]. Researchers have proven that a human's brain can take just three hundredths of a second to decide to consider a person trustworthy or not [38]. In the realm of human interaction with computer security, trust can be defined as "an integral component in many kinds of human interaction, allowing people to act under uncertainty and with the risk of negative consequences" [4]. Some of those negative consequences encountered in the online world would be in the form of identity theft or an act of fraud; however, if an online introduction leads to an in-person interaction the consequences would be more significant such as rape or death [74].

By looking at the other research works, their result reveals that users attempt to act cautiously and carefully in some platforms such as online dating services [74] while behaving naively, even carelessly when using other online platforms, entering their sensitive information on an obviously fraudulent website or clicking on a suspicious link provided in an email from unfamiliar sender [61]. This contradictory behavior while facing trust decisions made us wonder why users are acting wisely on some platforms while acting foolishly on others? Are users following similar trust processes in different contexts or do those processes differ depending upon the person and the platform?

While online dating and online services might appear to be very different domains, they have a number of similarities. With both, users are interacting with strangers, with strangers being in the form of unfamiliar humans or potentially fake services. In both contexts, people initially form opinions based on appearances (how attractive they find the pictures, how legitimate a website

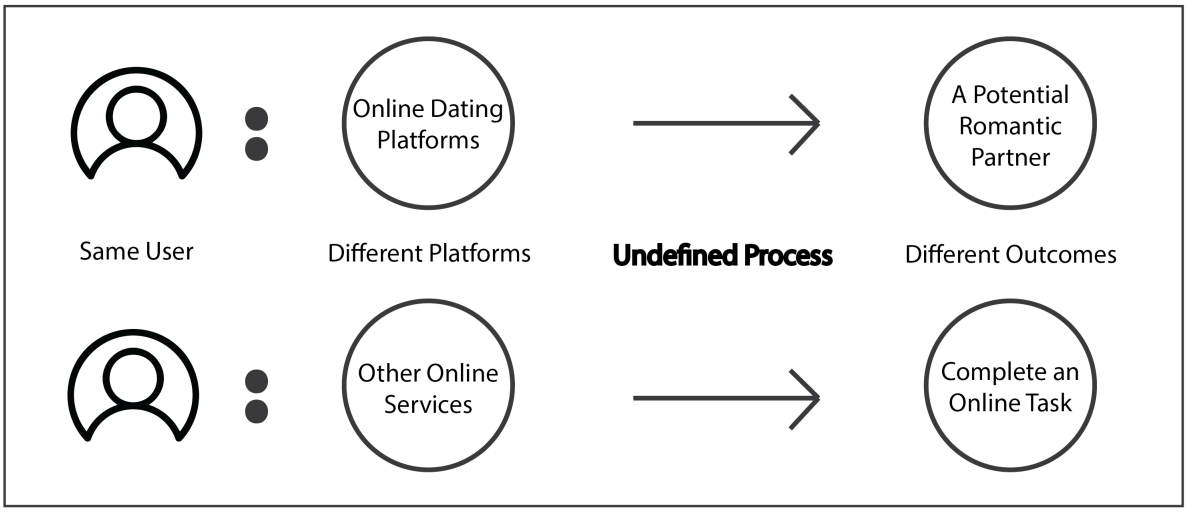


Figure 1.1: Authentication Process in Two Different Scenarios

looks) but then must go beyond appearances to determine trustworthiness. Whether it is deciding whether to go on a date or whether to enter in a password, users must decide whether to engage in a potentially risky action by assessing information presented to them online that may be misleading or even fraudulent.

To investigate the process of how the online dating users decide whether to trust a person met online and continue the process of the introduction in real life, we conducted our first study with two parts consisting of a semi-structured interview and a Tinder profile simulation. To be able to make the comparison between the trust process in online dating platforms to other online services, we conducted our second study which explored the users trust process in other online services, specifically how they determined they were interacting with their intended service (See Figure 1.1).

Based on past work, we expected that people would engage in a rigorous process when evaluating potential dates but would be much more trusting and would do less verification when connecting to online services. What we want to investigate was the source of these differences, specifically whether it was due to different trust processes or differences in context.

The key insight from our studies was that users have a chance to verbally interact with strangers in online dating platforms and have appropriate mechanisms to assess whether they can trust that person or not, but this stage and interaction is missing from other online platforms. Users are unable to ask question or validate presented information through conversation with other online services. This deficit forces users to trust websites blindly and hope for the best. We hypothesize

this blind trust is a key enabler of harms such as phishing attacks, online financial fraud, and online identity theft.

To cover this gap between the trust process people use in social contexts and when interacting with services online, we propose a new browser-based authentication mechanism which allows users to interact with the browser before sharing sensitive information or engaging in important transactions. We propose an authentication chatbox design based on our results and user experience (UX) guidelines. This authentication virtual assistant would activate when the user visits a website that requires sensitive information. While this proposal has not been implemented or evaluated as part of this research, it is useful as a design exercise and can serve as a basis for future work.

1.1 Research Questions

Our research objective is to identify and understand the process that users must go through to trust a stranger, a network connection, or unfamiliar provider (when we say "unfamiliar provider", we are referring to websites which are not commonly use and well known). Therefore, our main research question is: **"What are the processes that users follow before they are willing to take risks with potentially untrustworthy parties online?"**. The main research question explored through two sub-questions of: **"What factors do dating site users use to determine whether a profile is legitimate?"** for the first study sessions and **"What are the processes the users use to determine whether an online service provider and the connection to that online provider is trustworthy or not?"** for the second research study.

1.2 Contributions

Our contributions to the security and user experience field are as follows:

- We conducted the first study of trust processes in validating dating profiles.
- We conducted the first study of trust processes in visiting online websites.
- We did the first comparison of trust processes in different online contexts.
- We were the first to study the gap in trust process outcomes online through comparing the results of our two studies.

- We present a novel design for a verbal interaction-based interface for web browsers to verify the identity of online services.

1.3 Chapters Outline

In Chapter 2 we discuss related background regarding offline trust. We continue with background with online trust in Chapter 3. Our research methodology, requirements, and description of our research ethics protocol is found in Chapter 4. In Chapter 5 we present the findings and categories of the trust process. Our recommendation of adding verbal interaction to a web browser is presented in Chapter 6. In Chapter 7 we discuss the limitation of our study design, ethical responsibilities, and future research considerations. Research materials for our two user studies are presented in the appendices.

Chapter 2

Background: Offline Trust

To better understand how trust works and the differences between offline trust and online trust, we reviewed research on offline trust, online trust, trust indicators, and trust in computer mediated introductions, divided into two chapters of offline trust and online trust.

In this chapter, we start with a review of the concept of trust from different angles and the importance of trust in our day-to-day lives. Then the chapter covers in-person trust and cues of deception in face-to-face conversation. After, we talk about the world before the Internet and cues of deception in physical letters or texts.

2.1 History of Trust

"We trust when we are vulnerable to harm from others yet believe these others would not harm us even though they could" [41]. Trust issue is a fundamental psychological phenomenon developed by faithful interactions. Trust is a feeling that seems to be simple to express but is difficult to develop. It may be one of the first feelings demonstrated noticeably by infants soon after birth, expressed when recognizing their caretaker by smell or voice. Hence it can be a challenge to deal with this delicate fundamental feeling scientifically.

Misztal in her book "Trust in modern societies" discusses different approaches towards a definition of trust. Misztal describes the concept of trust as either "the property of individuals, the property of social relationships or the property of the social system explained with attention to behavior based on actions and orientations at the individual level" [72]. In this context a few approaches are suggested by Misztal. She she considers that feeling and loyalty should be the first approach, arguing that these are very personal and depend on an individual's personality. Whereas the second approach considers the collective attribute, meaning that trust is seen as social resource which helps a group of people reach their goals. It is worth mentioning that Misztal named Fordism as a "low trust system" in comparison with flexible specialization or post-Fordism which she specified as a "trust dependent system". The third approach looks at trust in a larger scale and refers to the actions and responses of the members of a society. In this attribute Misztal explains about the

macro and micro distinction. She basically says that the interactions and building micro trust leads to making macro trust in the end. For example, if a person develops trust in his/her physician by frequently visiting that physician, that person's trust in his/her physician can lead to having trust in the whole health care system of a country. Deutsch also believes that "the extent to which one party is willing to depend on something or somebody in a giving situation with a feeling of relative security, even though negative consequences are possible" [23]. Later, Bacharach and Gambetta also explained that "In general, we say that person 'trusts someone to do X' if she acts on the expectation that he will do X when both know that two conditions obtain: if he fails to do X she would have done better to act otherwise, and her acting in the way she does gives him a selfish reason not to X" [6].

Trust by itself is vague and has numerous meanings [8, 23–25, 46, 59, 68, 78–80]. Trust also changes whenever the point of view and situation changes. However, in general it can be said that trust is the appropriate behavior or response to what we expect and believe in to get from our perspective or point of view. We also demonstrate or construct our expectations and beliefs, that are the two big aspects of trust, by daily negotiations, gestures or social interactions and hence reflecting this in our relationship with other people.

2.2 In-person Trust and Cues of Deception in Face-to-Face Conversation

We all make trusting decisions in our lives, with most of us make those decisions daily [66]. Each time we decide to trust someone or something, we expose ourselves or our belongings to betrayal [53].

Humans intentionally or unintentionally observe behavioural cues as well as physical attributions when they meet someone in person. Then they try to find attributes that provide evidence of that person's trustworthiness and use a combination of them in aggregate to decide whether that person is trustworthy or not [8,23–25,46,59,68,78–80]. Imagine a scenario where your car breaks down in the middle of the road. A person with a truck who wears overalls like the one mechanics wear at the garage offers to help you. At that time you are most likely to trust that person and let him take a look at your car. In contrast, if they were someone else wearing only a t-shirt and jeans, you may not let them take a look at your car [70].

Valley et al. [99] found that people are more likely to tell the truth face to face rather than talking or negotiating over the telephone or writing a text. Face to face conversations appeared to elicit a higher than normal level of candor and build an atmosphere suitable to manifest clear

relationships.

Deception in humans can cause "guilt, stress, and fear of detection" [32]. Guilt, stress and fear of detection can be displayed in a person's behavior either verbally [2,7] or non-verbally [32,101]. Researches has shown that one of the physical elements that can reveal deception is an increase in the level of the voice [56] or tone [97], but this can be attributed due to stress as well. Other physical elements that may show deception are negative effect (unethical behaviour), cognitive load, sweating, arousal, and blinking [115]. Assessments of trustworthiness can be very fast, potentially requiring only 100 ms [108].

In next part we will look at the elements that matter in verbal communication between humans through physical letters or text before we look at their counterparts in the online world.

2.3 Text - Based Communication before the Internet

As aforementioned earlier, deceptive speech has some non-verbal characteristics such as tone and facial expressions. However, when deceptive information turns into deceptive messages, the message recipients can see neither the facial expression nor hear the changed tone of the deceiver [97]; therefore, that situation can be misleading for the message recipients and can lead them to wrong decision making [57]. Before talking about deceptive text-based communication, we should define what offline text-based communications are. Text-based communications are one of the most important types of communication [69]. Examples can range from a billion dollar business contract to a written will that someone wrote at their death bed. Various types of text-based communications exist, such as contracts, letters, reports, bulletins, newspapers, wills, and brochures. Unfortunately, for the development of an appropriate trust relationship, the readers of text-based communications are not able to detect deception via seeing facial expressions, feeling the stress, or hearing the change of tone of the author on a letter or a brochure. However, there are still some other gestural or verbal deception foot prints that can be relied on.

For example, there exist some features of text-based communication whose presence increase perceived trustworthiness, such as a signed and sealed letter, a stamped and initialed contract, an advertisement with recognizable logo, or a bill of money printed on special paper. Although these features are accepted by people as increasing trust, there are still ways to manipulate them. Therefore, carefully reading and being aware of textual cues in the content of a letter is necessary even if it is sealed and signed. Williams and Muir [107] proposed a model users follow to explore whether they received a deceptive text-based piece of information or not (see Figure 2.1). Williams

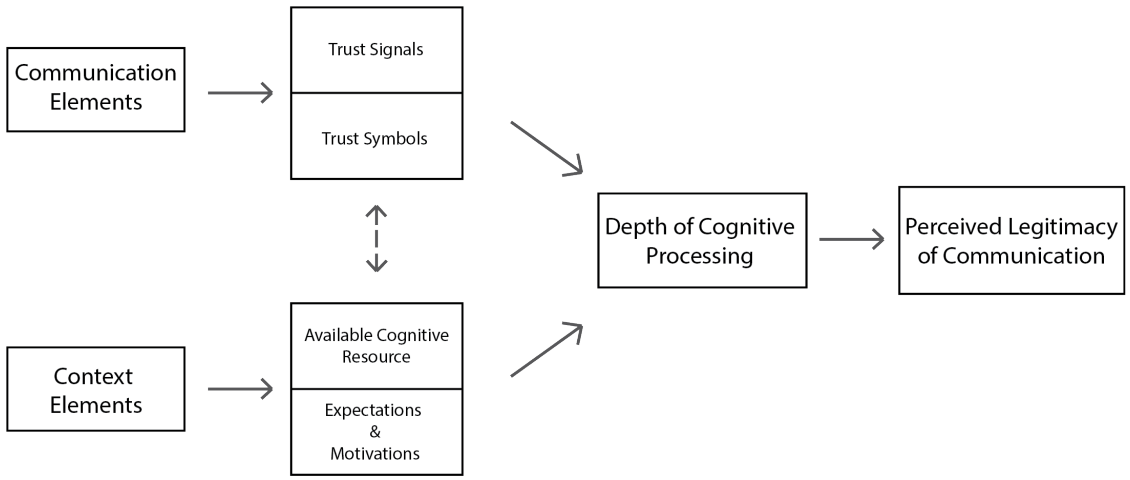


Figure 2.1: An initial model of how receiver trust may be manipulated by deceivers [107]

and Muir believe that each piece of text-based information is a combination of "communication elements" and "context elements" [107]. As we mentioned earlier, there are some symbols and signals of trust that people consider trustable aspects of text-based communication.

When the receivers of the text-based information are more suspicious about the received information, then they may consider investigation for cues of deception in the context of the information [107].

There are different kinds of lies; some are less harmful, such as "white lies" which, for example, constitute being polite and appreciative when you receive a gift that you don't like, and some are more harmful, for instance when you receive a letter with a bad intention [17].

Many techniques of linguistic and graphology exist, and some organizations such as law enforcement, intelligence agencies, and forensic scientists can detect deceptive information while normal individuals would not usually have such awareness [67]. Therefore, individuals may just rely on some simple facts such as the letter being sealed or looking at the logo or signature.

In text-based communications, verbal clues are maybe one of the most reliable facts that humans can use to judge whether the other side of the conversation is telling the truth or intending to deceive the text reader [81]. The analysis on synchronous text-based communication revealed that deceivers tend to use more words in their communication, more sense-based vocabulary, and use other-oriented pronouns rather than self-oriented pronouns [48].

In the field of interpersonal psychology, when a study is conducted regarding the deceptive behaviors for both verbal and non-verbal performances, the participants are usually asked to distinguish between the deceptive statements and the truthful ones. The outcomes of these studies shows

that people are not good at detecting deceptive statements [100] and on average, just slightly over half (54%) succeeded in detecting the deception within the total of 100 examinations considering over 1000 participants since each session conducted with a group of participates [22]. As a result, some researchers believe that people have little ability to detecting written deceptive messages [35].

In conclusion, in this chapter we looked at the both in-person and text-based communication and the cues that people look when attempting to detect deception. During in-person conversation, people are more focused on non-verbal behaviors and studies showed that people are quite successful in detecting deception through non-verbal behaviours. However, when the deception occurs though text-based communication such as a letter or a brochure, then the person has to focus on some other syntactic and semantic attributions. Research has proven that the detection of deception in text-based communication by humans is an inherent skill they lack.

Chapter 3

Background: Online Trust

In previous chapter we talked about the offline trust and how dealing and entangling with trust challenges in our day-to-day life made us good at recognizing the trustworthiness. However, nowadays our life is not just limited to offline world and most of us are members of both offline and online worlds.

Research studies on offline trust have shown that trust is a key element in having a successful reciprocal relationship with one another and also makes it easy to cooperate with them [41]; however, in the recent decade researchers realized that having trust in one's online environment is of critical importance, especially trust between online users and information websites, transactions websites, and applications [18, 74]. As discussed in the previous chapter, finding or building in-person trust can be hard but it is feasible. As Donath et al. [28] said "one body, one identity", people are able to use their common sense and non-verbal facts which they can see with their eyes and judge whether something is trustworthy or not.

The online world is different from the offline world. The information spreads, diffuses and is stored in multiple locations across the online world. In communication being aware of whom we are talking with plays an important role to build trust; thereby, in online communities the identity of the person who we are interacting with can be ambiguous and that may allow opportunist to take advantage of that and may create many different characters for themselves [28]. In the other words, we can say that the online trust is more limited than offline trust because the end users have to rely on some limited key mechanisms. Those mechanisms are such as URL and Domain Name, HTTP/HTTPS, Transport Layer Security (TLS) Certificate, and some other ones which we are talking about them in this chapter. We also talk about the harms that may happen by neglecting those mechanisms after each one.

3.1 Trust Indicators and What May Happen by Neglecting Them

Technology offers some ways and methods to increase the security and protection of users from online harms and attacks. In this section we will cover some of those ways and methods.

3.1.1 URL and Domain Name

Uniform Resource Locator (URL) is used to specify resources on the World Wide Web (WWW). A URL is the fundamental network identification for any resource connected to the web. All URLs contain the followings:

- Scheme name: the connection protocol, today it is almost always http or https
- Location of the server: host name or IP address with an optional port
- The requested resource, a pathname followed by optional arguments

A URL has the following syntax:

scheme://hostname:port/resource-on-server?querystring=1

Note that the first part of each URL, the hostname, specifies *who we are talking to* and the rest of the URL specifies *what we are saying*.

Having some knowledge regarding URLs, particularly domain names, is fundamental and necessary for those who are using online services, as many attacks involve malicious hostnames in URLs, as we explain in the following sections.

3.1.2 Phishing Attacks

A phishing attack happens with the combination of social engineering as well as technical trickery [30, 83]. A phishing attack occurs when users are fooled into disclosing personal information such as passwords or credit card numbers, by receiving a forged email or entering their credentials into a fraudulent website. These fraudulent websites or emails are very similar in appearance to legitimate ones. Sometimes websites even provide their victims with the same URL as the legitimate website [10]. Therefore, users may think such emails or websites are safe to use due to having a familiar appearance and providing them some portions of their sensitive information [54]. These attacks take advantage of human errors and lack of user knowledge. Users may not have the requisite knowledge of how to identify phishing URLs, where to look for cues in websites and web browsers, and how to use search engines to find the original and legitimate websites [86]. Many phishing prevention strategies rely on users recognizing potential threats. Therefore, there are recurring proposals on ways to educate users. Some of the suggested ways are through games,

system training, and alternatively, traditional ways of educating and passing the knowledge to one another [63].

Garera et al. [44] conducted a study on detecting patterns in phishing attacks using a black list of phishing URLs maintained by Google. They found that the most of phishing websites follow similar rule and have one or more of these four features:

- Replacing the host name with an IP address in the URL
- Normally the URL contains a domain name and a path. In a phishing attack, the URL contains a domain name which looks like a valid domain but instead contains a redirect in the path to make the URL appear valid
- The long domain names in URLs which is normally a large string of words and domain name comes after the host name (e.g. `https://www.google.com/search?q=example+of+of+very+long+url&oq=example+of+of+very+long+url&aqs=chrome..69i57j0.13131j1j8&sourceid=chrome&ie=UTF-8`)
- Unknown or misspelled domain names

To decrease the chance of end users getting phished by attackers, Google has implemented a change to how URLs are presented to users by shortening it [50]. Google announced that users will no longer see the "https" scheme or the "www" sub-domain while using Google Chrome. The URL will also begin with the domain name. If the user wants to see the scheme and the sub-domain, they can double click on the URL bar and see the complete version of that URL [50, 82]. This new visual trend can not only decrease the confusion [50] but it can also help the user to detect the phishing websites.

3.1.3 Unicode

Another attack that may happen to the end users by neglecting the URL and the domain name is Unicode. For information processing and to record and represent our language, we use symbols and characters. Many years ago, in order to have easier interaction with computers, Latin characters were represented in binary codes and each character was mapped to its own individual seven-digit binary code. While that idea was a major technological advancement forward at that time, soon people realized that there are 6500 languages other than English, which exist all around the would.

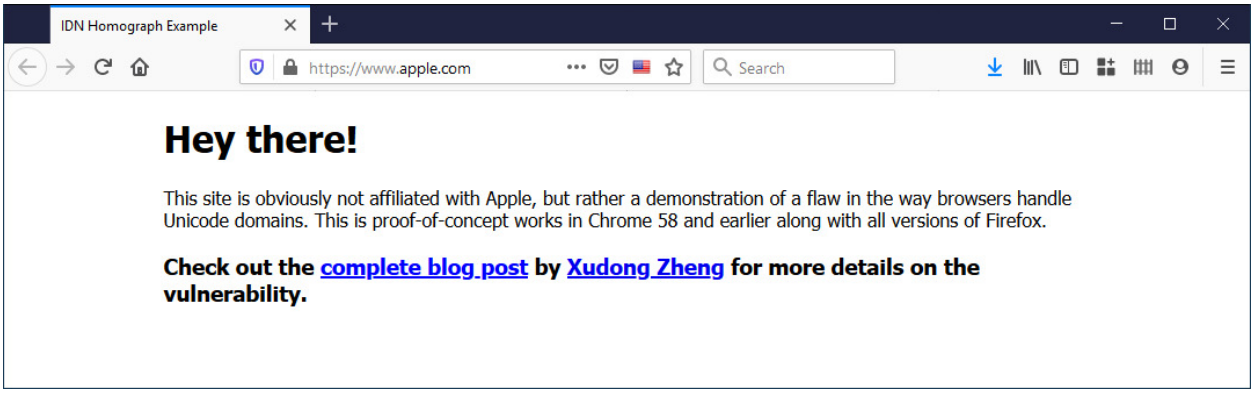


Figure 3.1: The URL appears as "**http://www.apple.om**" while the description of the page shows reveals that the URL includes some Unicode characters.

Due to different character sets, people had to install additional software to use the specific binary code for their language. Therefore, Unicode was created to represent all human written language digitally.

While Unicode was an important development, it also enabled new kinds of phishing attacks due to the similarity between the characters and symbols between languages [42, 71]. It is quite easy to generate numerous similar/fake Unicode strings from any given one in order to carry out Unicode attacks [113, 114] (3.1).

3.1.4 HTTPS and Certificates

Another online trust indicator is HTTPS. When a URL starts with "https://" (rather than "http://"), the connection to the website is secured using TLS (Transport Layer Security, formerly SSL). By clicking on that or the lock icon that is often displayed near the URL, the user will be able to view the details of the certificate with respect to that particular website. HTTPS was designed to encrypt and authenticate data sent between a web browser and a web server, including sensitive data such as usernames, passwords, or cookies, preventing attackers from observing or modifying them [75].

Having an certificate is important for domain owners because the certificate tells their customers two things. The first is that the website verifies who they claim to be and the second is that it provides an indication that the connection is secure between the website and the customer.

TLS, however, only works if the website's certificate is genuine. A faked certificate can result in secure communication with an attacker, meaning the attacker can now simply ask for the information they wish to steal. Unfortunately, it can be very difficult to determine whether a certificate

is genuine for a user, and browser-based checks (using built-in certificate authorities) can be circumvented. Certificate transparency [15] is the current effort to ensure certificates are legitimate; in its current form, however, it is not very usable by regular users.

If a connection between a website and the end user is not secure, users may end up at a fraudulent website (as happens in a phishing attack) or an attacker may actively intercept communication, as happens in a Man-in-the-Middle attack. A Man-in-the-Middle attack occurs when an attacker inserts himself in between both ends of a communication, forwarding traffic back and forth between both parties. Doing this ensures that the attacker can filter, modify, and steal personal information.

3.1.5 The Padlock Icon

We mentioned earlier that one way indicating a secure connection to a website is by adding "https" to the beginning of the address in the browser's URL bar. The padlock icon is the metaphor for HTTPS which indicates that the connection is secure. However, there are several studies that demonstrate users do not notice the presence or absence of the "https" URL prefix or the padlock icon in the URL bar [26, 29, 40, 84, 102]. Schechter et al. [84] conducted a study within which they removed the "https" preamble from the beginning of an online bank website address . They then asked the participants to enter to the website using their username and password to complete the task and surprisingly, all 63 participants completed the task without noticing the lack of "https" in the URL bar [84]. On the other hand, Noemí Benítez-Mejía and Toscano-Medina also point out that there exists the possibility of a phishing attack even when a malicious website appears legitimate due to its adherence to the same layout, and the same URL as it's counterpart legitimate website, as well as a certified padlock icon [10].

In most browsers, the lock icon indicates a secure connection. A good user interface experience of the browser would ensure that upon clicking on the lock icon a user should be able to obtain more information regarding the website's certification. The majority of users who are not aware of the technical terms and just rely on the padlock icon, are unaware of these browser features with regard to certificates [26, 29, 102] and lack an understanding of the concept behind them [26].

3.1.6 Reputation System

A reputation system exists as a third party which attempts to boost trust for both sides of a communication pathway (from user to provider and vice versa) via the mechanism of using past experience to predict future behaviour. Trust and reputation are directly correlated which means that

trust can both lead to a good reputation and on the other hand, a good reputation can give birth to trust [27, 74].

Reputation systems traditionally existed in the offline world. Nowadays people use reputation systems for online stores such as eBay or Amazon. Since Amazon and eBay made their transactions clear to the end user and there is no hidden fees, the user trusts them. Also, potential customers are able to see comments and reviews from other users which they can then use to assist in their decision to make a purchase or not [12]. As another examples we can point out for reputation system usage are all kinds of places where regular people offer services such as: Uber, Airbnb, hotels, and/or restaurants (See Section 3.3).

In the early 2000, two reputation mechanisms were proposed by Zacharia et al [111]. These two mechanisms, called Sporas and Histros addressed the trust issues of e-communities as well as other online contexts. In the Sporas mechanism, new users have a standard reputation value and as transactions are being carried out according to reputation feedback, the users' value could either increase or decrease. The Histtos mechanism is a web-of-trust based mechanism. It operates in such a way that users trust other users due to the fact that other users have previously tried the providers platform and shared their experience with others. The importance of the trust and how it can help reduce threats in online e-commerce communities also acknowledged by Li Xiong et al [110]. They proposed "PeerTrust", a feedback-based reputation model, as a reputation system to assist in measuring the trustworthiness of users involved in online communities.

Two different types of reputation systems exist. These are social navigation systems and recommender systems [27]. The social navigation system gives enough information to the users which guide and inform them but do not change their decision. The social navigation systems also trace the information left from previous users to the current users [27]. Kuwabara [64] conducted three studies whose subject matter determined whether a particular reputation system has any affect on a customer's decision making process. He realized that the reputation system has positive affects on the process of customers decision making and enabled them to trust the platform more.

3.1.7 Verification System

A verification system refers to the validation of identification that users will receive through platform providers. In the other words "An individual identification verification system is provided for person to verify their identity to third persons who they meet in various internet sites in a safe, confidential manner and wherein the extent and manner of information are controllable by

the person whose identity and background is being verified" [3]. This verification system requires potential users to voluntarily submit their personal identification to platform providers to verify themselves [5].

One of the most popular places that a verification system applies is within online dating platforms. Secondly, they are also applied on social media platforms. Normally online dating platforms verify all their users during initial sign up (or registration). A code is sent to them via text message or email to perform this verification. Another method of verification system uses Facebook information to verify individuals when they register [96]. Having Facebook account information or a cell phone number can be a simple initial step in verifying users, Caluwaert believes that photographic, bio-metric, and documentation identification protocols are necessary in order to verify the identity of the users [16]. Therefore, some platforms step forward and give the user a choice of being verified. This privilege grants them the use of holding a verified badge after the receipt of an email or a picture by the platform. On the other hand, some online dating platforms just provide verified badges for public figures such as celebrities, or influencers (is a person who has the ability to influence potential buyers of a product or service by promoting or recommending the items on social media). The consideration due for sharing personal identification and sensitive information with providers requires recalling the meaning and interpretation of verified badges in different contexts for different platforms. This can be exasperating, frustrating and confusing [37].

In this chapter we looked at some ways that technology offered to protect users and some relevant harmful attacks occurring online due to either negligence or naivety. Although these trust indicators are designed to make the users aware of any potential or possible danger, research revealed that users are negligent toward these trust elements. Friedman and et al [40] conducted a study with 72 individuals and the result shows that many users mistakenly evaluate whether a connection is secure or not. Other studies have also shown that a website may carry all those trust indicators but the user is still vulnerable to those attacker's exploits [1, 10]. As a result, some questions arise here such as: How can the user rely on trust indicators? Is there any trust process that exists before the user decides to trust an online platform? If there is a process, why is the outcome of that process not satisfying?

3.2 Usable Security

In previous section, we talked about some of the security indicators and assurances on online platforms; however, when a security design gets in between the users and their workflow or the

task that they are trying to complete, users often think about ways to work around them, making the designs less secure. The field of usable security is looks at security design and the human interaction or behaviour towards that. There has been numerous researches done on the human aspects of security and privacy systems. One of the primary and most effective ways to decreasing the severity of security and privacy threats is to make the users aware of the potential threats and the harms that they may suffer through those threats or attacks. There are many successful proposed and tested methods of educating the users such as teaching the threats and how to prevent them though a game [87] or educational comic or posters [112].

There are many threats that users may face while using online platforms, but some of the main security and privacy threats are phishing attacks [31, 85], password hacking [60], and man-in-the-middle attacks [109]. Usable security research has an an important role in protecting users from such threats.

Reducing the security responsibility of system users, enabling more secure defaults, providing clear and concise instructions, describing security contexts, and generally training users to adopt best practices are the summarized usable security progress guidelines that proposed by Garfinkel and Lipford in 2014 [45]. To support them, Garfinkel and Lipford [45] proposed usable security progress guidelines. Earlier in 1999, Whitten and Tygar [105] proposed the usable security principles with four main priorities:

- Ensuring that the users can easily understand what security tasks are required,
- Explaining clearly how they are able to successfully complete the tasks,
- Designing ways to prevent dangerous security errors, and
- Making the design easy to use that the users be comfortable to use it again.

Freitas and et al. [39] also designed and developed a system called “Online Neighborhood Watch”, to give alternative trustable suggestion as well as trustworthy advice when a user wants to download potentially malicious software. The result that they gathered revealed that providing and suggesting alternative trusted software can improve security.

However, Carnor [20] propose the “human-in-the-loop” security framework to keep the users aware of the security processes that automation would not be able to solve and requires communication pertaining security warnings, notifications, status indicators, or training to ensure that the security information dissolved by the users and can be appropriately processed with completing a

task. But a question arises here which is, what if the user would not be able to understand those warnings?

There are some other solution proposed and already exist to visually assist the users in order to be able to manage avoiding the online threads. One of the most famous security indicator called HTTPS or also known as padlock or lock icon which is embedded in the chrome side of the browsers [102]. Another visual suggestion was made by Lin and et al. [65] to highlight the domain name within the URL address bar which makes it easier for the users to look and realise the mistake in a case of phishing attack. However, Stojmenović and et al. [95] recently conducted a study to explore the effectiveness of simpler certificate interfaces on the users by showing two different interface prototypes, one with identity-verified elements but simple interface and the other one without any identity verification but sophisticated interface design. Their findings revealed that presenting the identity information was helpful in distinguishing between the real and fraudulent website; however, some users were suspicious about the notification and/or just relied on the appearance and aesthetics of the website. The fact that the security indicators are making the difference is recognizable, but the users may require some help and brief education regarding the security and the correct meanings of trust indicators to be able to truly distinguish real from fraudulent websites [93].

Many researches conducted on user understanding and mental model development [93, 94], educating users regarding what to trust online [93, 112], and proposing the idea of trusted expert advice for the users [39], but to our knowledge the usable security literature lacks work focused on trust processes in on online applications.

By looking at the literature in previous chapter, Offline Trust, we found that humans are good at detecting deception in the offline world; however, in this chapter the literature has shown that human beings do not do well at detecting deception online. Therefore, we decided to look at an area which users are introduced to each other online but continue that interaction offline.

3.3 Computer Mediated Introductions Trust

Computer Mediated Communication (CMC) is referring to the human communication via computers with using any kinds of tool such as text, image, audio, and video [52]. E-commerce is one of the biggest use of CMC. According to research, conducted by Boyd [12] on eBay it has been successful to build the trust between the platform and the clients. This success was due to reputation system which allows the user to give their feedback and share that with the other customers [74].

Li Xiong et al. [110], also introduced "PeerTrust", which is a reputation system that allows the customers to rate their transaction and the overall rate is the sum of all the ratings that aggregated in duration of six months. Nowadays, all platforms which either provide goods or service to the users (e.g. Amazon, eBay, Uber, and etc) use reputation systems [74]. This way buyers rate sellers and sellers rate buyers which allows the the good services or providers get rewarded while the low rate services or providers get punished [55].

Computer mediated introductions (CMI) is a branch of CMC, but it is a connection between the online and offline worlds. Users utilize these platforms in order to get introduced to another person and continue that introduction offline and in real life [74]. When two or more strangers interact online, the worst thing that can happen is identity theft. Information leakage while using CMI can result in real life disasters such as rape or even death [74]. Therefore, CMI users are required to pay more attention to whether the other person is trustworthy or not. The platform providers have proposed some guidelines for the users such as: "Carefully read through information, on member profiles and ask questions about anything that's unclear" [19] or "Ask questions! Have conversations!" [19]. While providing these guidelines are a way to warn the users to pay more attention, are the questions enough? What do their users actually need?

Young adults seek attachment, where "Attachment" is an inborn system inside the human brain which has control and influence on motivational, emotional, and memory processes. These are usually influenced by the caregiver or parents of a child [88]. More and more, it is found that the Internet, particularly CMIs, or in everyday terminology: online dating platforms are now playing an ever more significant role in serving young adults' yearning for attachment [36].

There are so many studies done on attachment from different angles. Attachment and the proximity between children and their care givers or parents was one of the most important area that the researchers have been focused on for decades and the they believe that the children consider their care giver or parents as the secure place in facing the undefined item or situation [88]. Youth who are looking to become independent and rely less on their attachment to their parents or care givers; tend to rely on their peers to serve their yearning for attachment [88].

Although online dating platforms are accessible and commonly in use by the youth, they may convey a false sense of security to their users [36]. Trustworthiness has deeper meaning in online dating platforms. Users may misrepresent themselves, usually in providing their age or height [13,33,98], since they want to impress and attract their mate through showing the perfect image of themselves [33]. While daters may provide deceptive information, they might not lie about crucial

attributes [98].

In fact, Quiroz [77] explored that the popularity of these platforms and by being more accessible by the users due to shifting those platforms from websites to the cellphone application, they can create an illusion of "Thin Trust". Quiroz defines thin trust as the assumption of considering other online dating users trustworthy just because they appear to have the same need and being in the same social circle [77]. Quiroz also later talked about "Thick Trust" which means that some individuals who are using those online dating platforms believe that by presents of thin trust, developing the thick trust would be easier and can lead to a meaningful form of relationship [77] when needed.

There are numerous researches done on online dating and how to apply more trust into those platforms. Researchers proposed many ideas such as using a fiend-of-a-friend (FOAF) social network model [91], user-centered design of an interface called Certifeye [73], introducing "FaceTrust" which is a system using social tagging games to build assertion validity scores for profile information [89], and many others. However, to our knowledge there is no research done regarding what are the trust processes that the users of online dating will take to call a person trustworthy.

Chapter 4

Methodology

There is a considerable amount of research done on trust, trust indicators in online dating platforms, and trust indicators on the other online services such as email providers, financial services, and social media mediums; however, we found that there is a lack of research on the trust processes and what steps users take to trust a person on online dating platforms or a website on the other online services and providers. To find out those processes and establish design recommendations regarding more effective ways of distinguishing the legitimacy from fraudulent acts, we conducted two user studies. Our first study was on one of the most famous online dating platforms in the North America called Tinder [21]. Other online providers such as email providers, financial services, and social media mediums were our area of focus in our second study. In this chapter, we present the details of the research questions and methodology of these two studies.

4.1 First Study: Trust Indicator In Online Dating Applications

The main research question in this thesis was "What are the processes that users follow before they are willing to take risks with potentially untrustworthy parties online?" This question was explored through some sub-research questions divided into two studies. The research question in the first user study was "What factors do dating site users use to determine whether a profile is legitimate?"

All materials, forms, and questions for the first study are in Appendix A.

4.1.1 Summary of study

Each study session took 45 minutes on average. We started with asking demographic questions with the purpose of both making the participants comfortable talking with us and getting some information about current status of the participants (e.g. if they are currently using Tinder, if not how long they used it for). We continued with asking more in dept questions about the participants experience using Tinder and how they would used it. Through asking those questions we were able to understand the mindset of the participants and understand what they were looking for while

using the platform. After that we asked some question regarding other online dating platform to see whether the participants are using the same technique or trust process across online dating platforms. The participants were willing to share their own personal experience or the stories that they heard from their friends, families, or even read that somewhere. After asking all semi-structured interview questions, the researcher handed ten simulated Tinder profiles (Appendix A) to the participants and observed how they react toward each Tinder simulated profile. The aim of this exercise was to watch the way that participants would interact with the simulated profiles, what are the points that they would notice at first glance and what elements would help them to make decision in order to proceed with a profile or not. The participants sometimes had stories to share by looking at those simulated profiles as well.

We explain the steps of the study in more detail below.

4.1.2 Ethics and Recruitment

Carleton University Research Ethics Board-B (CUREB-B) reviewed and cleared our research methodology with the clearance number of 109951. The first study involved 15 participants. The participants recruited through social media, a recruitment poster, and snowballing methods. The study was advertised on the Carleton Research Participants Facebook group and in public areas of Carleton University campus. Participants who expressed interest through sending an email to the researcher received an invitation email to participate in the study. The criteria for being eligible to participate in the study included age between 18 to 59, being comfortable with English, had used Tinder for at least a month, and had went on at least a date through the application. The research sessions took place at the Carleton Computer Security Lab (CCSL). Prior to the start each study, a printed consent form was given to each participant to read and sign. After each study to appreciate the participants' time, each participant received a ten dollar gift card.

4.1.3 Materials

For the first study, we used ten simulated Tinder profiles. The profiles were created on Adobe Photoshop. The pictures used in creating the stimulated profiles were downloaded form a stock photo website "istockphoto.com". To make more realistic simulated profiles, we randomly opened 10 different Tinder profiles and used their description. We made sure to remove any specific or revealing personal facts in the description, omitting them or replacing them with more generic ones.

4.1.4 Protocol

After participants had provided their informed consent, the study sessions included two segments of semi-structured interview followed by the experiment, the evaluation of simulated Tinder profiles.

4.1.5 Consent

Prior to the start of each session, participants who agreed were asked to read and sign the consent form. In the consent form, they were reminded that the session would be audio recorded. To make sure the participants read the consent form carefully and they are aware of their right, the researcher again verbally explained the purpose of the study as well as the participants right of withdrawal if they wish at any time prior to beginning of the session.

4.1.6 Study Steps

1. **Semi-structured interview:** The participants were asked thirty questions, starting with general questions to get to know them and then questions related to their experience using Tinder. At the end they were asked if they had had similar experiences with other online dating applications.

2. **Experiment:** After the interview, participants were given ten simulated Tinder profiles. The researcher asked the participants to look at each profile carefully and decide whether each profile goes to “the left” (not trustworthy) or “the right” (trustworthy). The swiping to the right or left in this study were affordances which already exist in the nature of the most online dating applications, particularly Tinder. Participants were encouraged to think aloud and explain the rationale for their placement of the simulated profiles. That information helped the researcher to understand their reasoning and get familiar with the participants’ mental models. If the participants were quiet or ambiguous, the researcher attempted to ask open ended questions such as “Why?" or “Why would you think that?" If participants were not able to explain the reasons behind their decisions, the researcher asked for any examples they had that they wished to share.

4.1.7 Data Collection

We asked questions verbally and recorded responses and took notes on Microsoft Word. Each session was audio recorded individually on separate memory cards and transcribed by the primary researcher. After transcription the recording files were deleted.

4.1.8 Data Analysis

In this study we gathered data from transcribed audio recording and the activity comments and notes taken by the primary researcher from our 15 participants.

Qualitative Approaches

We enforced the best practises of analysis methodology [34, 62, 106] into analyzing our collected qualitative data. Before initiating the analysis, to get a better understanding and having the bigger picture of the result of the analysis, we read the transcribed responses. After getting a better sense and understanding of the overall result, we imported the analysis into a software called 'NVivo 12 Pro' [76] provided by the MacOdrum Library at Carleton university. Using an inductive approach, we colour coded the interview responses. We then created nodes, categorized them and placed the similar responses into related clusters. We used abstraction to come up with our main points, combining similar responses into a category and then refined the sub-categories to the main head categories. By using this methodology, we were able to identify the participants' thematic mind map and how they justified whether they can trust a person/profile or not. Thematic mind mapping is a method that helps to obtain a better understanding of the data and the relation between them through visual organization [104].

Quantitative Approaches

After categorizing and clustering the collected data set, we counted the frequency of each category and ordered them based on highest to lowest rank. We used this ranking to discover further patterns in our data.

4.2 Second Study: Human Patterns In Trustworthy Internet Navigation

The research questions in our second study was "What are the processes the users use to determine whether an online service provider and the connection to that online provider is trustworthy or

not?" The materials, forms, and questions for the second study are in Appendix B.

4.2.1 Summary of study

For the second study, we contacted the participants who agreed to be contacted for the follow up study in the first study's consent form. In order to validate whether a user follow the same or different processes while using different online platforms, it was important to have a few of same participants in our second study. At the beginning, we asked some background questions to understand their level of expertise and how familiar are the participants with technology and using the Internet platforms. knowing the participants' level of expertise in using the Internet would help us to have better understanding of our participants and asking the follow up questions accordingly. Next we gave six scenarios to participants and asked them to show us how they would reach to different platforms. The rationale behind each task was to understand how the participants would reach to requested platform, whether they look for any trust assurances, whether they question regarding the authenticity of the websites or trust it without asking any question. The participants were confident to show their processes that they would take to reach to their destination via using website as well as sharing the alternative ways they may use to get to the same platform. In general each session took approximately 30-35 minutes in average and participants were willing to share their experiences or mostly what they read or heard about those platforms with the researcher.

We explain each of the steps in our study below in more detail.

4.2.2 Ethics and Recruitment

The second study focused on online platform that requires trust such as email providers, online sopping services, online banking services, and social media platforms. We received approval for our study from the Carleton University Research Ethics Board-B (CUREB-B) with clearance number of 111234.

The second study involved 12 participants. The participants in the first study were asked if they agreed to be contacted for the follow up research and 12 out of 15 said yes. We sent an invitation email to those 12 interested participants and seven participants were confirmed that they were still interested to participate in the second study. We then recruited the rest of the participants through snowballing methods. Participants who were expressed their interest through sending an email to the researcher received an invitation email to participate in the second study.

The requirement of eligibility to participate in the second study were being aged between 18

to 59, comfortable with English, able to use online shopping platforms, online banking platforms, social network mediums, and email services.

The Carleton Computer Security Lab (CCSL) at Carleton campus was again the location for the research sessions. Each session started by asking the participant to read and sign a hard copy of the consent form and the researcher verbally described what we were doing during the session if the participant were new to user experience studies. In appreciation for the participants time, each received a ten dollar gift card and the cost of parking for an hour if they needed a parking space at Carleton Campus.

4.2.3 Materials

We used the cognitive walk-through method [103] in the second study to find out what is the process that the users take to trust a connection to an online platform. To find out that process, we prepared a test plan including the background questions, six activities, and debriefing questions. We used one of the CCSL's computers running Ubuntu 16.04 and the Firefox browser as tools for the participants to show us what steps they would take to get to online platforms such as their email providers, online shopping sites, and social media platforms. The participants were advised that they are not required to enter any username or password at the beginning of the study session.

4.2.4 Protocol

Participants started their session with providing their consent. After getting their consent the researcher started recording the session and then the participants were asked background questions, engaged in the six tasks, and answered debriefing questions.

4.2.5 Consent

We provided the consent form to participants in advance via email upon request and in hard copy form at the start of each study session. Participants had to review and sign the form before the session would continue.

4.2.6 Study Steps

1. **Background questions:** The participants were asked 4-5 background questions with the purposes of both feeling more comfortable to talk to the researcher and to get to know more

about their level of expertise in terms of using technology.

2. **Six cognitive walk-through tasks:** After the background section, participants were given six tasks with a scenario before each to make the task easier for them (Appendix B).

    - Task 1: Imagine today is Saturday. You just woke up and you want to check your email via using the website and not the application on your phone. Could you please show me how would you get there?
    - Task 2: Imaging while you are checking your email, you will see that you have received an email from your bank. How would you get to your online banking account via using their website?
    - Task 3: After checking your email and your online banking account, now is time to check your social media/ networking accounts. Can you show me how would you get to the sign in page?
    - Task 4: While you are checking your social media/ networking account, you will see that you have two notifications. The first one indicates that a random person sent you friend request. What would you do?
    - Task 5: The second notification says that next week is your best friend's birthday. However, you are too busy and don't have time to go shopping. Therefore, you will decide to order something online. Your friend is interested in a book/a travel mug, or an electronic gadget/other. (Please note that you should choose something that you have never ordered that before.) Can you show me the whole process from finding to order the good online?
    - Task 6: After you ordered your friend's gift, you remember that you need something (something you already ordered it before) for yourself as well. Can you show me the whole process from finding to order the good online?

We asked the participants to show us the steps that they follow to get to different platforms and/or providers at each time, then we asked them if they are confident that page is the actual and legitimate website. If yes, is there any assurance in that page which they can share it with us? During the whole time we encouraged them to think aloud and tell us what their rationale behind their actions are. In a case of rambling responses or confusion, we asked them follow-up or leading questions to get back to the topic of our study.

3. **Debriefing questions:** The purpose of asking debriefing questions was to go back to the general topic and get some more information regarding how concerned the participants were about their privacy and security.

4.2.7 Data Collection

The questions were asked verbally in each session and the researcher tried to take notes as much as possible at the same time. Along with taking notes by the researcher each study session was audio-recorded with the participants consent on separate and individual memory cards. We transcribed the recordings afterwards, deleting the audio files once transcription was finished.

4.2.8 Data Analysis

After gathering the data and transcribing them, we analyzed them with both qualitative and quantitative approaches.

Qualitative Approaches

This time we printed off all the responses and used different colour of highlighters to highlight the same or similar responses. For example, we used yellow to show 'when participants talk about trust or authentication indicators', blue to show 'when participants talk about technical tools', and pink for 'when participants mentioned reputation or history'. After that we wrote all the highlighted responses on a whiteboard and tried to cluster them. We then chose names for each group. By applying this thematic analysis methodology to our research, we were able to understand our participants mental model regarding the process they take on online platforms to figure out whether that website is trustworthy or not.

It is worthwhile to mention that the reason we changed our analysis methodology in the second study was that "NVivo 12 Pro" was time consuming and we were more comfortable doing the analysis using a manual approach.

Quantitative Approaches

In the second study, we had two kinds of quantitative approaches of frequency and Likert scales. We used the frequency to rank the responses and understand which responses are the most and least common. We also had two questions of five points balanced Likert scale in our questions,

one for understanding how familiar they were with the technology, and another one to understand how satisfied they were with the current online services in terms of security. We choose the five points balanced with the purpose of both having neutral in the middle and not giving them too many option to choose. The Likert scale options were:

- Very Unfamiliar, Unfamiliar, Average, Familiar, Very Familiar
- Very Unsatisfied, Unsatisfied, Neutral, Satisfied, Very Satisfied

Chapter 5

Results

In the following section we will analyze the data that we gathered from our participants during both user studies, "Trust Indicator In Online Dating Applications" and "Human Patterns In Trustworthy Internet Navigation".

5.1 Participants

In total of two studies we had 27 participants aged between 20–35 years old, 15 in the first study and 12 in the second. All the participants were affiliated with Carleton University through being an undergraduate, graduate student, or an alumnus. All participants considered themselves familiar with technology and daily usage of different online platforms.

5.2 Trust Indicator In Online Dating Applications (First Study) Results

Our first research study revealed that more than two third (13 out of 15) of the participants have not noticed any verified badge on Tinder and 12 participants confessed they are not aware of how the verified badge works or how they can get one on Tinder.

> "*I did not recognize that (verified Badge) maybe because it's been a while since I have used that.*" MM18100

> "*I feel like I have maybe not, I don't know.*" THM7530

> "*I don't know, but I can relate to some other website not the dating applications. Some other websites like LinkedIn, Twitter, Facebook, if a person who is very famous then they are going to have that tick to show that is a real person or real page.*" MM18100

> "*I think if you give them email and then confirm it by email maybe or phone number, I'm not sure.*" THM71230

Not seen Verified badge on Tinder	13 out of 15
Not aware of how the verified badge works on Tinder	12 out of 15

Table 5.1: The Number of Not Seen or Not Aware of Verified Badge Participants on Tinder

I would not trust that person	7 out of 15
I don't care about verified badge	6 out of 15
I would trust that person even more	2 out of 15

Table 5.2: The Participants Reaction If They See a Profile with Verified Badge on Tinder

Based on our participants feedback, if they saw a profile on Tinder which was carrying a verification badge (Table 5.1), they either would not consider that profile trustworthy at all (since our participants were believed that getting a verification badge is an extra step. Therefore, If a person is willing to do that extra effort, this action reflects that the person is not feeling trustworthy and needs to get that badge to show-off and pretend the trustworthiness) or they ignored the verification badge and having the verification badge did not make them to trust that profile more (Table 5.2).

> "*It depends on how they works, but I think on Bumble is like by email or phone number so if I see that I might say okay this is a real person but that is not going to effect my decision to swipe right or left on them but I think I'm more leaning towards left because that is just like okay good job you are having the bare minimum of being real person. For me looks, age and bio are more important than verified badge.*" THM71230

> "*I google them first to see if they are somebody famous or somebody important or something, but my first feeling would be a little bit of suspicious, maybe that's the company an put their own verification badge to get message out or try to sell something but I think if that turns out to be a real person I would ask about it and I would be curious.*" THM71100

While we started our first study with intention of both finding the effect of trust indicators on the online dating platforms and the trust processes, we explored that the users are following an authentication process to define and consider a profile trustworthy or untrustworthy since the trust indicator turned out not to be trustworthy (see Table 5.2).

To better understand what the trust processes that users use in online dating platforms, we first tried to cluster the similar responses together and came up with the title for each category. After organizing the groups, we explored four final categories of 'Fact Check', 'Verbal Check',

'Verification Check', and 'Verbal Interaction'. We found that online dating users are usually using this four step authentication process to validate whether other profiles are legitimate or not. Almost all of our participants reported that they were happy with the quality of their screening process's ability to exclude fake profiles.

> "*I've gone on a few dates through Tinder and I'm pretty sure they were okay because I'm not going to go on a date unless I chat with them for a while and I think I'm really good at figuring out if they are creepy or not. I never creeped out with whoever I end up meet them but defiantly I have creeped out by people who I've talked*" THM7330

> "*I liked Tinder and I think it was fine, I found that the messaging function was fine, and honestly I didn't give out my phone number in the Tinder, I kept chatting with them until I was comfortable to meet them in-person and I gave them my number after I meet the person, and I used that app to keep in touch.*" THM71230

> "*I don't think I came across the person who is different from his profile and who I end up meeting. My dates were pretty accurate to what I expected from their profile and our chats, but I heard from other people who use Tinder that defiantly some creepy profiles exist.*" THM71100

The most reliable stage in terms of understanding the authenticity of other profiles happens in 'Verbal Interaction' while the 'Verification Check' has the least act on implying the feeling of trust onto the users.

Below we talk more about each category.

5.2.1 Fact Check

In the 'Fact Check' category we clustered the responses which were most like a personal checklist. The participants were using their own checklists to find out the reliability of a profile as soon as they would see the profile (Table 5.3).

The top two preferred parameters on that checklist were 'Having bio' (having a written profile) and 'Having picture(s)' which mentioned by all of the participants. At this stage, the users are not paying attention to the details, they just want to make sure a profile meets their minimum requirements. They may look at 'Age', 'Mutual friends' or 'Location' after putting a mental check mark in front of 'Having bio' and 'Having picture(s)'.

Fact Check	Number of Participants who mentioned that	The frequency of Repetition of the item
Having bio	15	44
Having photos	15	40
Age	7	11
Mutual friends	4	9
Location	4	9

Table 5.3: The Participants Check List to Consider Other Profiles Legitimate (Section 5.2.1)

"*Having picture and bio, there were nothing more than that to rely on, but sometimes distance too. I was first looking to find whether they have both picture and bio, then look at all of their pictures and if I would attract to the person then I would go to the bio.*" FM81100

5.2.2 Verbal Check

At this stage the users start developing the feel of trust and want to know more about the other profiles. Therefore, they look at the pictures and read the bio in more depth, paying attention to the details.

"*Having stock photos, or very professional taken photos, photos that lack veracity and diversity in like location, cloths or action, people who are just alone in the pictures, or they are look like an actor portfolio or a model portfolio, those seems fake account, also if their bio has something small or look like a copy and paste paragraph or even nothing at all, I think are fake profiles.*" THM71230

"*Sometimes people are sketchy and you can just ignore them or block them. Sketchy mean they profile is fake or they have some weird thing on their picture, like picture with dead animals or holding gun or hunting guns or resist propaganda yeah these are sketchy and you don't want to interact with them in general.*" TM5200

"*Defiantly their biography, I think that the most important thing is biography, if someone has appealing pictures but he does not have a biography it's a no go. You have to be interesting as a person and as much as a photo says 1000 words, if he can't talk about himself and if he can just show his muscle, that's not a appealing personality.*" THM7330

Therefore, they look to answer questions such as:

- How many pictures?
- What kind of activities are portrayed in the pictures?
- Are the pictures taken by a professional or an amateur?
- Does the person pose in the pictures or are they natural?
- Do the activities in the pictures match the interests in the bio?
- What is included in the bio?
- Is the bio self-written or does it look copy and pasted from somewhere else?
- Are there any offensive, racist, or sexist comments or jokes in the bio?

5.2.3 Verification Check

After finding the answer to most of the questions in the previous stage, users may feel more trust than before and move on to the next step which is checking to see whether the profile is verified by Tinder or not. This step was skipped by many participants due to lack of knowledge regarding verified badges on Tinder (Table 5.2).

> "*If a person is verified, makes me feel more comfortable that is a real person probably.*" WM27400

> "*I would not think of that person any other ways. I mean I won't attracted to a person because that person has a verified badge but maybe I feel more comfortable talking to that person. Because maybe Tinder take care of some stuff and I won't be that much worried anymore. My concern was that maybe she won't be what she is said she is but I want Tinder check that and tell me is telling the truth or not.*" TM18600

5.2.4 Verbal Interaction

Out of all the stages of the trust process before meeting in person, this stage is the most important step to validate the legitimacy of profiles. To validate profiles using verbal interaction, they again

Criteria	Number of Participants who mentioned that	The frequency of Repetition of the item
The Flow of Conversation	15	37
Respond too Fast/ Start chatting right away	13	32
Keep going back to one subject of discussion	13	28
Short responses (one way conversation)	11	11
Copy and past texts (too long)	11	11
Too General messages	11	11
Racist, governmental comments or political propaganda	8	9
Spelling or grammar mistakes	3	5

Table 5.4: The Participants Verbal Interaction Check List (Section 5.2.4)

have some criteria. The participants mostly evaluated the other person by the flow of the conversation, how soon or late they responded, and whether the other person answers with short or long responses (Table 5.4).

> "*I would go on a date if there is a nice conversation, and it has flow. But if they are boring, I mean their answer is very short or if I ask a question and she just answer that question then that's too hard to carry a conversation then I won't be inclined to meet with that person.*" TM18600

Although the flow of the conversation is very important to our participants, they indicated that starting the conversation as soon as they got matched or going back to the same topics may convince them that person is not trustworthy, or is trying to sell them something.

> "*Actually as soon as we match I won't reply right away and I'll wait few hours before, to see if they send me a message first, because I have got some messages before which after we matched they invited me to a bar with cover or something like that and they were trying to advertise for their nightclub or whatever. And whenever I get messages like that, I just unmatched right away because I'm not interested in that kind of thing. I think they are just advertising. They probably send that message to everybody who matches with them.*" THM7200

5.3 Other Approaches

There are always different methods and ways to get to a destination. That insight applies to our study as well. For example, some people believe that to be successful in online dating platforms, they should have the high number of "I would like to date this person". If they got the match then they would go back to the person's profile and do the trust process.

> "*Most of the time, I don't really bother to looking in-depth and just keep swiping right because it is a number game, but sometime if there is something catching my eyes I would look into their bio or their other picture and make decision based on that. Sometimes if the first photo looking suspicious, I might look other pictures and I might swipe left.*" THM7200

Some other users are attraction oriented. Those users first look for physical attraction then they consider safety.

> "*The way I decide to start talking to a person on online dating application is if I attracted by the photo swipe right, if I didn't attract by the photo swipe left, if it is a maybe I would decide by the bio.* WM27400

5.4 Human Patterns In Trustworthy Internet Navigation (Second Study) Results

After getting the result from the first study and understanding about the four step verification process for dating profiles, we went back to the literature to determine if there has been any research about the trust process on other online platforms. We realised that other researchers mostly focused on trust indicators and end user interfaces, not the process that users take to understand whether a connection to an online platform is trustworthy or not. Therefore, we initiated our next phase of study and our mission was to understand this trust process, following the methodology outlined in Section 4.2.

After each of the six tasks, participants were asked what factors they can rely on and making decisions about whether to trust that website. Eleven (92%) of the participants reported the visual appearance and professionalism of the website as a factor that they can rely on and make trust decisions based on. But all twelve of them (100%) admitted that if they see anything malicious or different then they will read letter by letter the address of the website (URL) then look for the

traditional lock icon and/or https indicators. Four participants (33.5%) also mentioned that they look at the content of the website company for security information, logos, and sometimes change the language of the page to their first language to see if it is done professionally or not.

At the end of the user experience study sessions, participants were also asked whether the machine that we had them use is trustworthy or not and they all responded with something such as:

> "*Well, we are doing the study here, and I'm pretty sure you had to go through some kind of process to do it so you have to protect my information.*" 2T1709

> "*I don't know if this machine is safe or not, also this is Linux and I'm not familiar with it so that means I can't even check but I trust you and I'm here for the research so it should be okay.*" 2S1509-2

> "*Honestly I have seen very unsecured machines that a lot of pop-up notification comes up but I normally judge by the person to be honest. If I trust the person and that person is good with technology then I may trust but if I know that person is really bad and their machine has a lot of virus then no I won't use it*" 2S1409

They had some similar responses about the popular websites and the huge companies behind them.

> "*I trust it because I trust the company but I think there can be indicators as we talked earlier like the grammar mistake or layout but there are some transaction pages that there are very bare-bone for example the presto card transaction page, it looks very basic to me and how can I really trust this but I put my initial trust in it because I trust who is actually provide this and also there are some assurances like if something goes wrong I can get my money back through my bank or contacting the actual company.*" 2T1709-2

The participants' responses showed us that they mostly trust the person/companies behind the websites. However, we drilled down more into the gathered data from our participants and we narrowed the data down to a list, clustering them and named each category. These categories are shown in Table 5.5.

User Interface	Technical Tools	History and Reputation
Familiar layout of the page	URL	Company's website reputation and size
Logo	Green lock/https	Bookmark
Colour	Certificate	Checking the rating and reviews
Font		Being at the top of the list in search page
Changing the language		Different colour in the search page (shows that you have been there before)
Contact us (or phone number)		Leave your account open
Deposit protected sign		Save your information on the platform
MFDA protection sing		
Legal		
Privacy and security		
Copyright sign		

Table 5.5: The Participants Response List

These results convinced us that the users also have a clear process to distinguish the malicious websites from the legitimate ones. According to the gathered data, the participants are following three stages while evaluating online platforms.

- Looking at the layout of the page, logo, font, and etc.
- Looking at the URL and texts.
- Looking at the indicators such as the lock icon.

Therefore, if we compare these three steps with our four stage authentication process in online dating applications and try to name each level:

- Looking at the layout of the page, logo, font, etc. $\rightarrow$ Fact Check
- Looking at the URL and texts $\rightarrow$ Verbal Check
- Looking at the indicators such as the lock icon $\rightarrow$ Verification Check

In the following section we talk more about the comparison between our findings in the two studies and how they complement each other.

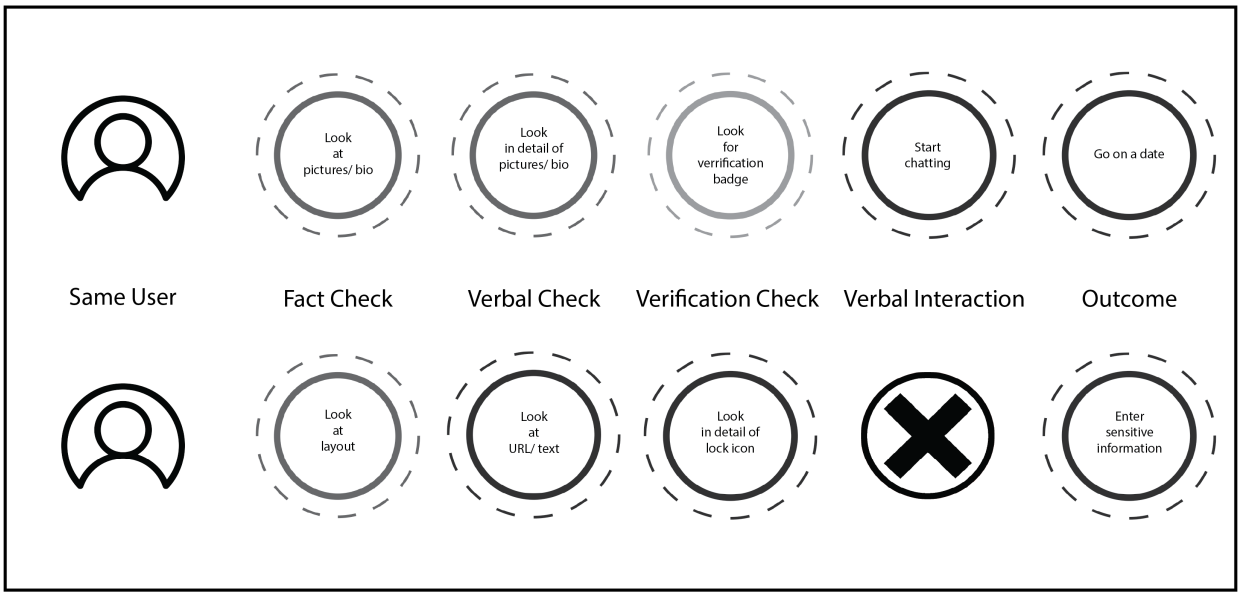


Figure 5.1: Comparing of Trust Process in Online Dating Applications and Other Online Services. The greyness is indicating the frequency of that action reported from our participants.

5.5 Results Comparison

Figure 5.1 shows a high-level comparison of the differences in the authentication processes of online dating profiles and other online providers that we discussed previously. Before looking at these differences in detail, we first should examine the whole authentication processes in both contexts. Figure 5.2 shows the whole trust process of users evaluating new profiles while using online dating services. The process starts with the task of visiting a person's profile and it will continue until the user agrees to go on an in-person date. The process that the users of online platforms such as email providers, financial services, and/or social media mediums take to trust and share their sensitive information is presented in Figure 5.3. In this trust process the users initiate with entering to a website which requires entering their sensitive information such as password or credit card number in order to complete the task.

Interestingly, apart from the initial and the completion stage of each environment authentication process, the core steps appear similar.

The core steps of the authentication processes include four steps of: Fact Check, Verbal Check, Verification Check, and Verbal Interaction. It is worth mentioning that the darkness of each step

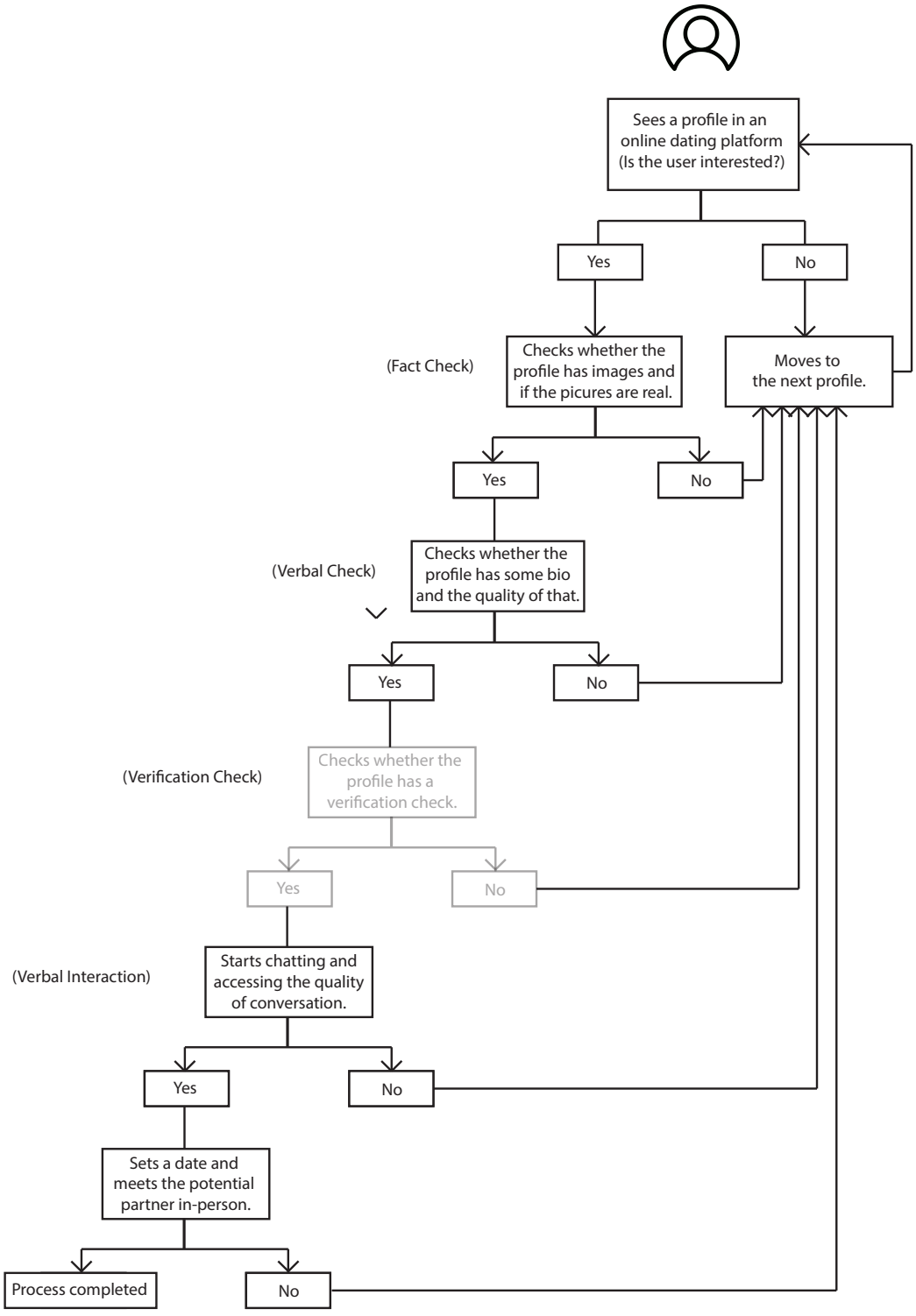


Figure 5.2: Authentication Process of Online Dating Applications

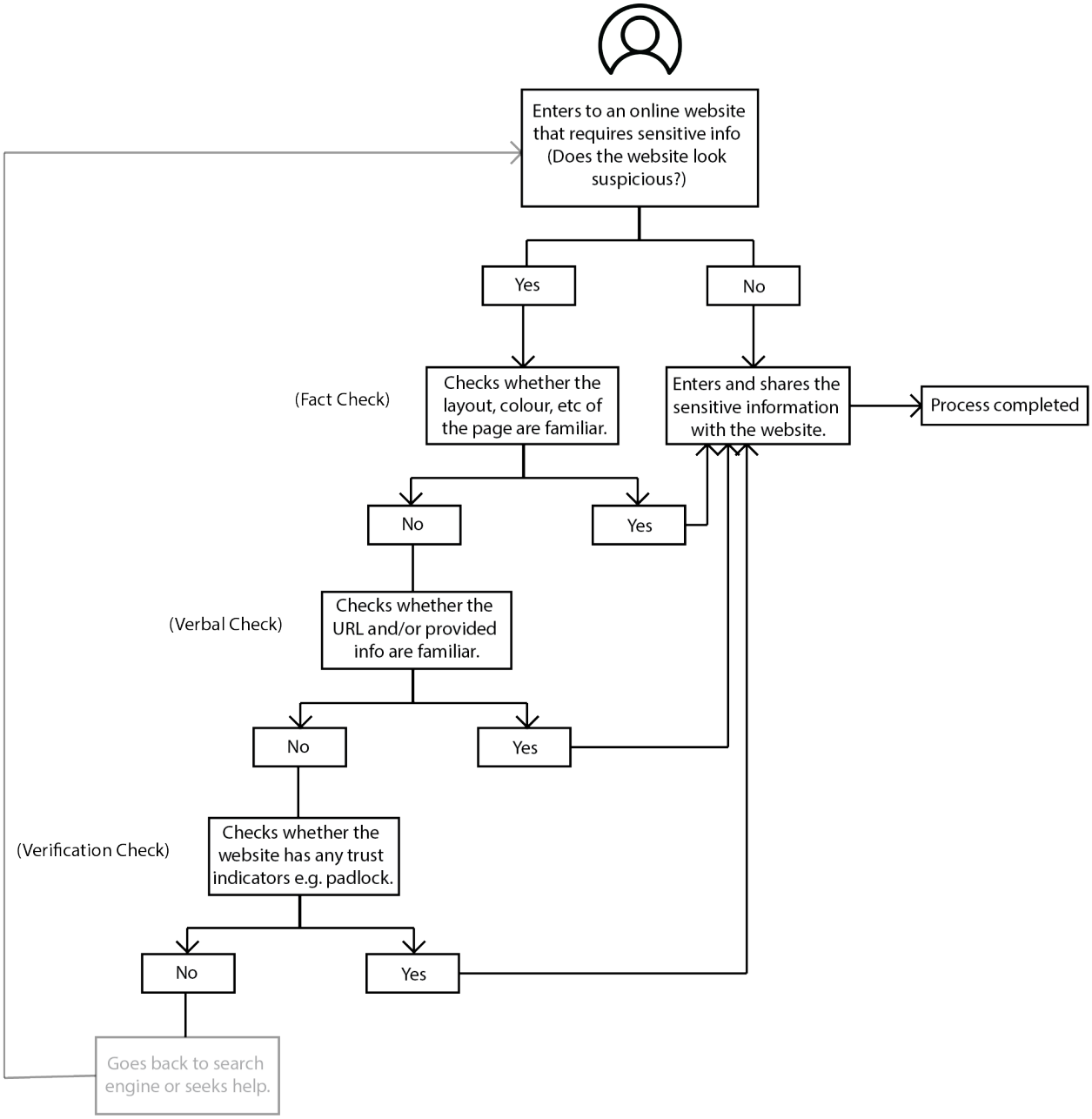


Figure 5.3: Authentication Process of Online Platforms Such as Email Providers, Online Banking Services, Social Media Mediums, and Online shopping Platforms.

indicates the level of reported usage of that step by our participants. For instance, 'Verbal Interaction' has the highest rank of indicating whether the other person is legitimate or not in Figure 5.1; however, 'Verification Check' has the lowest rank.

Let's go back to a couple of trust definitions and remember who we consider as a trustworthy person according to Bacharach and Gambetta:

> "*In general, we say that a person 'trusts someone to do X' if she acts on the expectation that he will do X when both know that two conditions obtain: if he fails to do X she would have done better to act otherwise, and her acting in the way she does gives him a selfish reason not to do X"* [6].

Gambetta also describes a trustworthy person as:

> "*Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly when we say that someone is untrustworthy, we imply that probability is low enough for us to refrain from doing so"* [43].

These definitions suggest why 'Verbal Interaction' appears to be most important when building trust. Because in that stage the user can start interacting with the other person and quickly understand whether the other person is a real human or a bot, whether the other person trying to sell something or get very specific information, or even the user may check to see whatever the person talks about matches with what they wrote in their bio.

As we can observe, the highest rank of reliability belongs to 'Verbal Check' and 'Verification Check' in the other online platforms authentication process (Figure 5.1). Recall that even if users check the URL letter by letter and verify it uses HTTPS, they may still get phished [40]. If we pay a closer attention to the definition of HTTPS, we will understand that is just talking about the secure connection and not about the legitimacy of a website. Therefore, one can create a fraudulent website and get HTTPS for a minimum or even no monetary cost.

Figure 5.1 also displays that the other online platforms trust process is missing the “Verbal Interaction” which we consider to be the most important stage in the online dating authentication process.

To solve the gap of lacking “Verbal Interaction” in the other online process, we came up with a recommendation. According to our findings and user experience (UX) principals, we came to conclusion of designing an “Authentication Browser” which allows the user to communicate with the browser. We explain the details of this proposal in the next chapter.

Chapter 6

Adding Verbal Interaction to a Browser

We found in our research that the authentication process of online providers and platforms is missing "Verbal Interaction". As we presented in Section 5.2.4, the stage of "Verbal Interaction" is the key step in online dating application due to giving the ability to virtually interact and have a chance to assess the authenticity of the other party. In online dating platforms, users consider each behaviour (such as how long the other person takes to reply, the writing style, the usage of emojis, or how the other person starts the conversation) as an indicator of whether or not the other profile is trustworthy. Verbal interaction can help the users of other online services to detect the deceptive information by providing them the information that may missing, giving them warning if the website seems to be malicious, or telling them if they never visited a page that they think they regularly did. During the verbal interaction, the users will get benefit of sharing their concerns and asking questions to make sure they are safe.

Therefore, to solve the problem we came up with adding verbal interaction to the web browser. This new feature of the web browsers can provide the ability of the communication between the web browser and the user. The web browser will have and authentication indicator which will activate and turn into either green or red when the user enters a website that requires sharing the sensitive information, e.g. sign-in pages. In fact, when the browser considers a website not trustworthy and the authentication indicator turns red, the browser will also provide a pop-up notification to warn the user as well as opening the authentication virtual assistant chat-box. In the case of need, when the user is uncertain about the authentication of any website, the user can also communicate with the browser and get more information about the website's certification, authentication, and whether a website was visited by the user before or not (this action will be possible by just clicking on the authentication indicator at the top right corner of the screen).

It is worth to mention the reason that we chose the authentication chatbox over including some trust indicators are:

- Our participants were not paying attention to indicators and neglecting them.
- Most of our participant were not fully aware of the functionality of the trust indicators.

- When aware, most of our participants misinterpreted the indicators.

To design the authentication browser, we adapted a set of user experience (UX) guidelines of designing a chatbots by Budiu [14] and used the insights from our research and came up with a potential design for the authentication chat-box. It is worth mentioning that we have not implement or tested the authentication chat-box design with the users; such testing is left to future work.

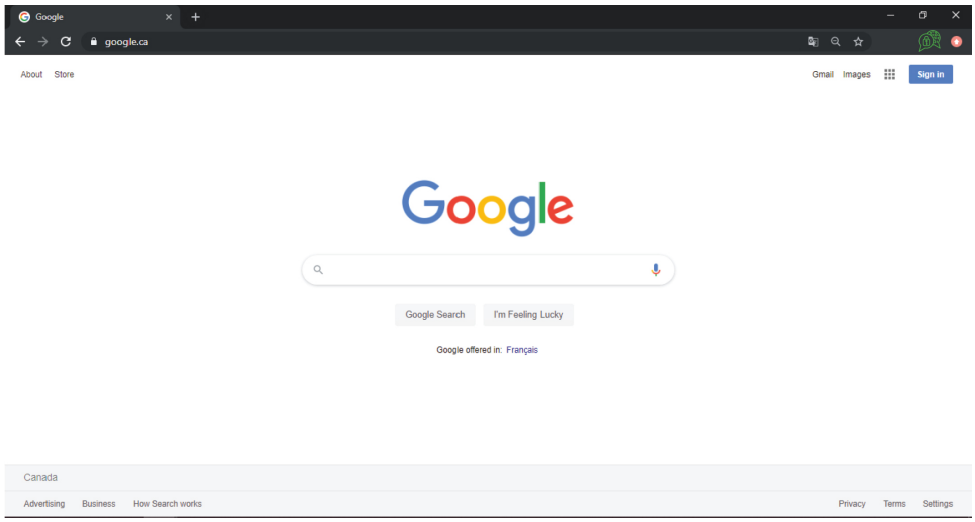


Figure 6.1: Adding the Authentication Chat-box into the Browser

We decided to add the Authentication chat-box into a browser, in our example we used Google Chrome (Figure 6.1).

If the user chooses to use the authentication browser mode then the Authentication chat-box icon will appear on top right corner of the browser. We decided to place the icon on the browser toolbar which is separate from a website's interface, to prevent malicious websites from duplicating or pretending that a website has the authentication indicator in an attempt to fool the users (Figure 6.2). (Note this is a weakness of the design, as we know that users are not good at distinguishing between information displayed by the browser versus the website.)

In case the need of evaluation and authentication assessment rises, the users can click on the authentication icon, and the authentication virtual assistant will start introducing itself. The authentication virtual assistant will continue the introduction with revealing its ability and capability according to the aforementioned UX guidelines of designing a chatbots by Budiu [14] (Figure 6.3).

The authentication virtual assistant will have limited ways of responding to the user's questions. The reason of this limited responses is due to technical limitations and to protect users from some kinds of attacks. By using the authentication virtual assistant for a short while, the user will

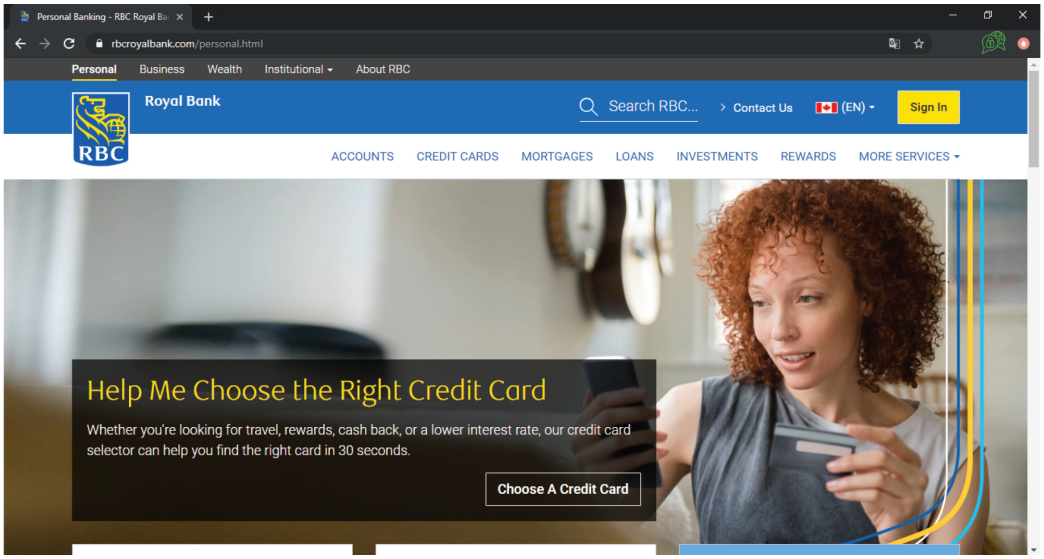


Figure 6.2: Authentication indicator icon will appear on every page but will be activated when the website requires sensitive information to proceed.

learn those ways of responses, and ideally those responses will be customizable by the end user; therefore, in the case of receiving any responses other than what the user learnt and is used to, will warn the user that there is something suspicious.

The authentication virtual assistant is able to search, evaluate, and validate the authentication of each website according to the valid TLS certificate, correct domain name, and secure connection. It is also able to provide users with information on whether or not they visited the same website before, when was the last time that they visited that website, and how frequently they visit it as well as pointing out if the website is part of their bookmarks or favorites. Detecting the frequency of visiting a website will assist the authentication browser to direct the user to the right page. For instance, if a person uses their online banking account once a week and one day they misspelled the domain name, the authentication browser will direct them to the correct destination since it is aware of how frequent the user visits their online banking account.

On the other hand, if the authentication virtual assistant cannot validate the authenticity of the website, or if the user never used that website before, the colour of both the chat-box and the authentication indicator will turn red to make the users aware. In that case, the user and the authentication virtual assistant may communicate, either to allow the authentication virtual assistant to provide detailed information regarding the current malicious website and then guide the user to the right place, or if the user is sure about the website being legitimate, ask to add the information into the browser's store of trusted websites.

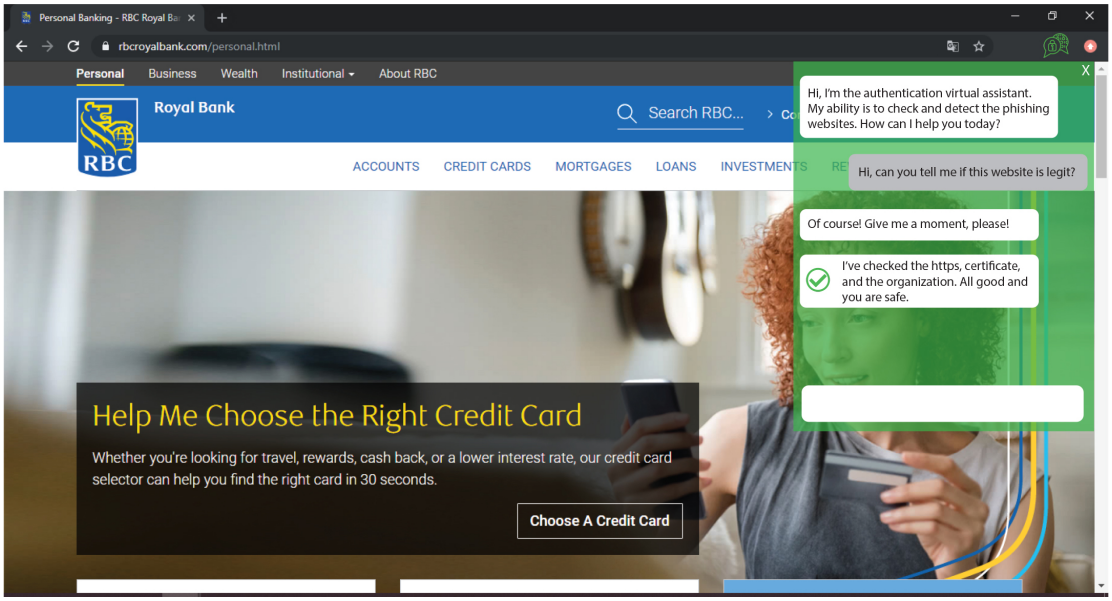


Figure 6.3: An authentication agent helps confirm that the website is legitimate. Note the conversation is simplified for presentation purposes.

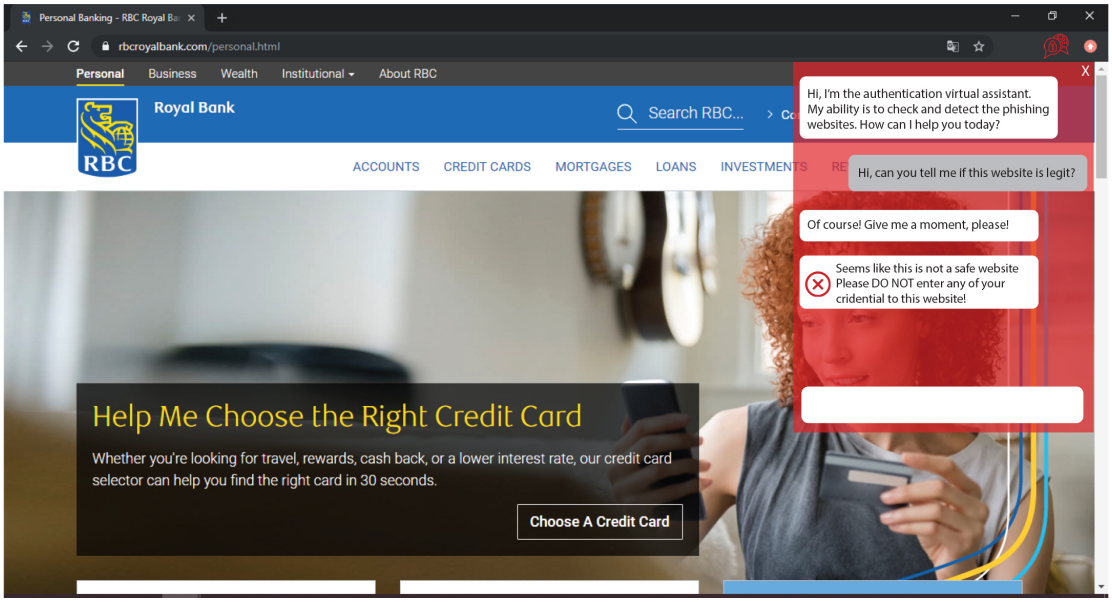


Figure 6.4: An authentication agent gives a warning about a phishing website. Note the conversation is simplified for presentation purposes.

6.1 Sample Conversation Between Agent and User

Positive Response

- A: Hi, I'm the authentication virtual assistant. My ability is to check and detect phishing websites. How can I help you today?
- B: Hi, can you tell me if this website and domain is associated with RBC Royal Bank?
- A: Of course! Give me a moment, please!
- A: This domain is registered as RBC Royal Bank Canada and you have visited this domain 14 times this month. Your last visit was October 24, 2019. Do you want to see more information about this domain?
- B: Yes
- A: The domain provider updated the interface of this website at October 26, 2019. Do you want to more about the domain certificate?
- B: Yes, please.
- A: This domain holding V3 certificate, Issued by: DigiCert Global CA G2, Issued to: rbcroyalbank.com, Valid from 2019-09-25 to 2021-09-26, and the certificate status is: "This certificate is OK." Would you like to know more about this domain?
- B: No, thanks.

Negative Response

- A: Hi, I'm the authentication virtual assistant. My ability is to check and detect phishing websites. How can I help you today?
- B: Hi, can you tell me if this website and domain is associated with RBC Royal Bank?
- A: Of course! Give me a moment, please!
- A: I cannot recognize this website. You usually use "www.rbcroyalbank.ca". would you want me to add this new link to your bookmarks, blacklist it, or forget it? Do you want to know more details about this link?

- B: Yes
- A: The domain certificate is invalid and there are 20,743 reports about that online "https://www.google.com/search?sxsrf...". Do you want me to open it?
- B: No, but can you block this link for me?
- A: Yes, I just block the link "www.RBCroyalBank.com". Would you want me to open "www.rbcroyalbank.ca"?
- B: Yes please.

First Time Usage Response

- A: Hi, I'm the authentication virtual assistant. My ability is to check and detect phishing websites. How can I help you today?
- B: Hi, can you tell me if this website and domain associate with RBC Royal Bank?
- A: Of course! Give me a moment, please!
- A: I cannot recognize this website and this is your first time using this domain. Would you want me to add this domain to your bookmarks?
- B: Yes
- A: I have added this domain to your bookmarks. Would you want me to save your username and password for this domain?
- B: Yes. can you give me more details about this domain?
- A: Of course, this domain holding V3 certificate, Issued by: DigiCert Global CA G2, Issued to: rbcroyalbank.com, Valid from 2019-09-25 to 2021-09-26, and the certificate status is: "This certificate is OK." Would you like to know more about this domain?
- B: No, thanks.

One may think that on online dating platforms, users are trying to find out whether the other person is legitimate, real, trustworthy or not; however, by using the authentication browser, the users are already aware that they are talking to a bot. So why do we need to have that authentication

browser and what is the rational behind that? That assumption of the users are trying to validate the existence of the other person on online dating platforms through communication is correct but the purpose and usage of the other online platforms are different. It is not necessary that the users talk to an actual human to validate whether or not a website is legitimate while the authentication virtual assistant can access and provide information to prevent users from attacks or fraudulent acts.

6.2 Alternative Trusted Paths to Online Services

There are some ways to protect users from phishing cyberattacks such as bookmarking the website or using the applications of the platforms installed through app stores.

Those ways seem promising and secure but bookmarks cannot help when people click on a link provided in an email and offer no help when the user visiting a website for the first time. App stores also can be beneficial; however, again only if they are the exclusive way users interact with the service (which is not the case in practice). In fact, for downloading an application or bookmarking a page, the user should use a legitimate platform to search, find, download, and then install that application on the device or bookmark the page. Any such tool should ideally provide ways for a user to validate the presented information, bringing us again to the problems addressed in this chapter.

6.3 Ethical Responsibility

Despite the fact we believe that the authentication browser can be very useful to many users, what are the variables and data that the authentication browser will collect and keep? And who will have access to those information? Therefore, the user should be aware of what information will collect, save, or use within the context of their communication and whether the browser company will release the information to the government, police, or any other interested organizations [51, 58]

To prevent the attacks, we suggest that to keep the user aware of all the transactions and interactions. We also suggest that the authentication browser should have a recognisable language and behaviour with users. That way we will have two-way authentications and the users can identify every time whether they are talking with the authentication browser assistant or the system is experiencing some manipulations.

6.4 Potential Sources Of Information For The Authentication Virtual Assistant

As per we mentioned earlier that the authentication virtual assistant is able to search, evaluate, and validate the authenticity of a website as well as remembering whether or not the user have visited a website before, if the user visited that website before when was the last time, and how frequent the user visited that website. In order to response correctly to the users' questions, the authentication virtual assistant needs to be able to have access to some resources such as:

- **Google transparency report** [15], the Google transparency report share the information such as issuance and existence of SSL/ TSL certificates open to scrutiny by domain owners, Certificate Authorities, and domain users.

- **Browser history and track record** [47], the browser history and track record can remember whether a user visited a website, when was the last time, and how frequent the user uses that website. Those information would help the authentication assistant to direct the user to the correct website in case of Unicode or phishing attack.

- **URL blacklists (marginal benefit)**, Since the URLs and the domains are constantly changing; therefor, URL blacklist may not be so useful in a case of phishing attacks. In another words, a list of bad websites may not contain the latest version of malicious websites. Checking the URL blacklists may worth checking, which the browsers already do, but it may not going to be so much helpful. Therefore, checking the reputation of a domain can be much more helpful.

- **Reputation of the Certificate Authority (CA)**, all the CAs have to pass some audits to be recognizable and authentic; however, there so many CAs that caused serious and critical security errors. Therefore, they are not all equal [90].

- **Age and issuer of the TLS certificate** [9], the TLS certificate is now just valid for maximum of two years; therefore, the age can help to understand whether the TLS certificate is expired or still valid, and knowing who issued the certificate will show how authentic is the issuer and the certificate.

- **The information on the process that the CA used to vet the certificate**, When a person applies to get a certificate, what are the processes that the CA go through and check in order to understand whether that person is who he says he is. For example, When Microsoft

asks for microsoft.com and wants the company name to say Microsoft, how does say Entrust make sure that they really are Microsoft (and are authorized to register the certificate)? Some CAs just make sure you can change what appears on the website, but others for Extended Validation (EV) certificate will have to check out more in dept about the business.

- **Search engine result ranking when searching for company name**, normally the first hit when searching for a famous and sensitive providers, for example RBC Royal Bank.

6.5 Suggested Test Plan To Evaluate The Proposed Authentication Browser Design

As discussed before, we proposed the idea of adding verbal interaction to the browsers; however, we have not implemented or tested this design idea. In general, it is always better to test a design before spending a huge amount of time and money on a design which may or may not be successful. Therefore, we suggested a test plan to evaluate the proposed idea of adding verbal interaction into the browsers. Is is worth to mention that our proposed design is the first draft of this idea and the design may change and adjust in response to users input. In order to improve the design, the next research fellow may need to follow a process such as:

- Prior to initiate a session, the researcher should educate the participants regarding the new option/ design and what is able and capable to do by giving them some examples and defining the benefits of having that new option. *This approach allows the participants become aware of existence of that feature as well as understanding how to use it*.

- The researcher may give some tasks to the participants to complete and the research fellow may observe the participants whether or not using the new option/ design. *This approach allows the researcher to observe when the participants are aware of existence and capability of this new feature and have chance to use it, what would be their choice*.

- If the participants would not use it, the researcher may ask them what was their rational of not using that. *The responses of this step will be one of the most important output to understand what the users want and what was wrong with our design that they would choose to not use it*.

- If the participants would use the new option/ design, the researcher may observe and gather what kind of questions they would ask from the authentication virtual assistant. *Those questions would help he developer to figure out what sources is needed for the authentication virtual assistant to be able to respond to those questions*.

- The researcher may observe to find out that after the communication of asking questions and receiving the answers between the participants and the authentication assistant, whether the answers were clear and understandable by the participants? If the responses are not clear for the participants, why is that? *These information will help to improve the level of communication and humanize the answers*.

- One of the most piece of information for the researcher in this study is to see what the participants reaction would be after they received the response from the authentication assistant. For example, if the authentication assistant says that the website is untrustworthy, would the participants hesitate to share their sensitive information or they would neglect the warning? *This information actually will indicate whether the users are trusting the authentication virtual assistant. If the users chose to not trusting the authentication assistant, what is their reason behind that and what elements would make it trustable for them*.

Chapter 7

Discussion

In this chapter we first discuss our contributions, limitations, recommendations, and future work.

7.1 Contributions

In this thesis, we presented the first studies on the processes that people use to assess the authenticity of a website or online dating profile. We developed a novel a four step process model of authentication based on the results of our studies. Using this model, we proposed a new interface design for user verification of online services using a conversational interface.

7.2 Study Design Limitations

Our studies had the following key limitations:

- **Limited, Biased Sample:** Any person who is older than 18 can use the online dating applications or anyone who has access to the internet and signed up for online platforms, can use them. However, we mostly advertised our study at Carleton University campus and its Facebook group which were more convenient for us, and we only obtained a total of 22 unique subjects between the two studies.

- **Focus on Just One Online Dating Application:** In our first study, we mostly focused on Tinder while there are plenty of other online dating applications exist. Other dating apps may have better ways of building trust between users. We chose Tinder application due to being more famous in the North America.

- **Laboratory conditions:** Our research took place in a laboratory environment which may led the participants to not behave naturally during the studies, due to have the feeling of being watched. Thus their reported trust behaviors may differ from those they use in practice. Further, self-reported behavior may differ from real-life choices.

In addition, due to ethical reasons, we designed the studies in a way where participants were aware of what will happen next, what and why we are asking our questions. In real life, the users would be on their own and they may not be aware of what will be the consequences of their decision.

- **Cultural Differences:** Our research has been done in North America (Ottawa) and based on North America's cultural beliefs and behaviors. Therefore, this research may have very divergent results due to cultural and geographic differences.

7.3 Recommendations

This work presented the data gathered from our participants perception of both online dating platforms and other online providers in terms of authentication and security. Based on our finding and inspiration from the literature, the follow design suggestions have been developed.

7.3.1 Educating Users

Our gathered data from the real users showed us the serious lack of knowledge which sometimes lead to making wrong decisions. In our both studies, the participants confessed that they are not aware of how the indicators work and the meanings behind them. For instance, verified badge in online dating applications or the green lock icon on websites. This lack of knowledge may lead the users to make the wrong decisions in different situations. For example, in our first study 12 Tinder users confessed that they are not aware of how verified badge works, seven out of 15 participants mentioned that they would not trust profiles with the verified badge on Tinder, and another six participants admitted that they do not care about seeing verified badge on other profiles since they are not aware what the purpose of that verified badge is and how the other user got that.

As Harley mentioned on the Nielsen Norman Group [49], Since there is an absent of standard usage for most of icons, the user needs to have a good understanding of what an icon does or tries to indicate. So the idea of better understanding an icon will be feasible by adding labels or some text to that icon. Therefore, the online dating applications or the other online providers that require the users' trust may need to add some descriptions or notifications regarding how those indicator works and what is the purpose of having those.

Based on this finding we agree with Kumaraguru and et al. [63] and Stojmenoviæ and et al. [93] on the need for user education. However, when we are talking about the educating users,

we believe the focus should be on giving users a checklist to follow before sharing any personal and/or sensitive information online. Education on indicators should be intergrated with a checklist approach, something that has not been suggested in past work.

7.3.2 Design an Authentication Browser

Considering our findings and the UX best practices guidelines, we proposed the idea of designing an authentication browser which gives the ability of direct communication between the users and the browser. The authentication browser should include an authentication indicator and an authentication virtual assistant which would be accessible through a chat-box.

The authentication indicator and virtual assistant should activate when the users visit websites that require personal and sensitive information from the users in order to proceed to a task.

The authentication browser will be able to search, evaluate, and validate the authentication of each website according to the valid TLS Certificate, correct domain name, and secure connection. It has also the ability of recognizing websites that the users were visited before as well as how frequent the users visited that website. Other than the technical benefit that the authentication browser can provide for the users, it is also potentially better integrates with the trust processes that the users are used to. Moreover, since not all online users are aware of high level technical abilities and functions that a browser can offer, they can easily ask the authentication virtual assistant in the chatbox and it could translate that technical information into a more accessible form, assuring the user when needed.

7.4 Future Work

Considering our results and comparing them with some those of other researchers showed us that there are some areas to be worked on in the future to resolve open questions.

The result in our first study suggest that people are good at detecting scam or fake profiles; however, some researchers strongly believe that human beings are generally bad at detecting deception over text [35]. Therefore, one area of future research would be to investigate whether this difference is due to the online dating context since small lies are not as important as being a legitimate person on those platforms.

It is worth mentioning that, although we believe that users are better in assessing and distinguishing trustworthiness in online dating platforms than others have reported, those platforms

are still carrying high amount of fraudulent activity [92]. Therefore, they require improving their current safeguards as well as developing new ones, in order to provide the users with safety and security.

Some research has shown that the users are neglecting the absence of the security indicators [26, 29, 40, 84, 102] while our results suggest that users will pay attention to existence of those security indicators but they don't have enough knowledge to use them effectively. Therefore, we also suggest further research on this disparity and identify why people often neglect security indicators when they have trust concerns. The other question here is whether the users are neglecting the indicators on all of the websites or just some of them. If yes, what is their rationale behind that behavior?

We also proposed a design of an authentication browser to help users communicate with the browser to make sure they reached the right website. However, we suggest further research to assess the feasibility of our design in terms of technology and usability, particularly whether users are comfortable talking and sharing information through a chatbox.

Chapter 8

Conclusion

Although extensive research has been done on both online dating platforms and other online providers such as online shopping platforms, email services, and financial providers, the process and what steps users take to trust the platform or a person on online dating platform had not been previously studied.

By looking at the literature we found that users act more suspicious using online dating platforms but at the same time are much more trusting when interacting with other online platforms, even though both environments can be considered as vulnerable environments. This contradictory behavior led us to want to know what the processes are that user takes to trust a website or a person.

We broke our main question to two sub-questions of "What factors do dating site users use to determine whether a profile is legitimate?" and "What are the processes do users use to access whether an online service is trustworthy or not?" and conducted a study for each of those sub-questions to be able to answer our main research question. While users following similar authentication process for both online dating platforms and other online service environments, the other online platforms are missing one step called “Verbal Interaction” to compare with online dating providers. We believe that the absence of “Verbal Interaction” step from the authentication process of other online services is the reason of users acting naive in interacting with those platforms. Therefore, to fulfill that gap we proposed an authentication browser which allows the user to interact with the browser to validate whether that website is trustworthy or not.

Bibliography

[1] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *22nd ACM Conference on Computer and Communications Security*, 2015.

[2] Joanne Arciuli, David Mallard, and Gina Villar. "um, i can tell you're lying": Linguistic markers of deception versus truth-telling in speech. *Applied Psycholinguistics*, 31, 2010.

[3] Jeffrey Arndt and Daniel Seidler. Personal internet identity verification system, 2005. US Patent App. 10/632,492.

[4] Donovan Artz and Yolanda Gil. A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, 5, 2007.

[5] Warren Austin and Otto Coppen. Secure online dating support system and method, July 17 2007. US Patent 7,246,067.

[6] Michael Bacharach and Diego Gambetta. Trust as type detection. In *Trust and deception in virtual societies*. Springer, 2001.

[7] Joan C Bachenko and Michael J Schonwetter. Method and system for the automatic recognition of deceptive language, 2010. US Patent 7,853,445.

[8] Annette Baier. Trust and antitrust. *ethics*, 96, 1986.

[9] Kevin Benton, L Jean Camp, and Chris Small. Openflow vulnerability assessment. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pages 151–152. ACM, 2013.

[10] Diana Benítez-Mejía, Alejandro Zacatenco-Santos, Linda Toscano-Medina, and Gabriel Sánchez-Pérez. Https: a phishing attack in a network. In *ICICM 2017: Proceedings of the 7th International Conference on Information Communication and Managemen*, pages 24–27. ACM, 2017.

[11] Sissela Bok. *Lying: Moral choice in public and private life*. Vintage, 1978.

[12] Josh Boyd. In community we trust: Online security communication at ebay. *Journal of Computer-Mediated Communication*, 7, 2002.

[13] Robert J Brym and Rhonda L Lenton. Love online: A report on digital dating in canada. *MSN. ca, February*, 6, 2001.

[14] Raluca Budiu. The User Experience of Chatbots. Nov 25, 2018.

[15] Transparency Report by Google. Https encryption on the web. https://transparencyreport.google.com/https/certificates?cert_search_auth=&cert_search_cert=&cert_search=include_subdomains:false;domain:www.ccsl.carleton.ca&lu=cert_search.

[16] Laurie A CALUWAERT. Online identity verification platform and process, September 12 2019. US Patent App. 16/423,544.

[17] Jinwei Cao, Janna Crews, Ming Lin, Judee Burgoon, and Jay Nunamaker Jr. Can people be trained to better detect deception? instructor-led vs. web-based training. *AMCIS 2003 Proceedings*, page 76, 2003.

[18] Cynthia L Corritore, Beverly Kracher, and Susan Wiedenbeck. On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58, 2003.

[19] Couchsurfing. How can i have a safer couchsurfing experience? https://support.couchsurfing.org/hc/en-us/articles/200639130-How-can-I-have-a-safer-Couchsurfing-experience-, 2019.

[20] Lorrie F Cranor. A framework for reasoning about the human in the loop. *Carnegie Mellon University*, 2008.

[21] Tinder | Match. Chat. Date. Online dating application. https://tinder.com/?lang=en.

[22] Bella M DePaulo, Kelly Charlton, Harris Cooper, James J Lindsay, and Laura Muhlenbruck. The accuracy-confidence correlation in the detection of deception. *Personality and Social Psychology Review*, 1, 1997.

[23] Morton Deutsch. Trust and suspicion. *Journal of conflict resolution*, 2, 1958.

[24] Morton Deutsch. The effect of motivational orientation upon trust and suspicion. *Human relations*, 13, 1960.

[25] Morton Deutsch. Cooperation and trust: Some theoretical notes. *American Psychological Association*, 1962.

[26] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006.

[27] Andreas Dieberger, Paul Dourish, Kristina Höök, Paul Resnick, and Alan Wexelblat. Social navigation: Techniques for building more usable systems. *interactions*, 7, 2000.

[28] Judith S Donath. Identity and deception in the virtual community. In *Communities in cyberspace*. Routledge, 2002.

[29] Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, 2006.

[30] Zakir Durumeric, James Kasten, Michael Bailey, and J Alex Halderman. Analysis of the https certificate ecosystem. In *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013.

[31] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074. ACM, 2008.

[32] Paul Ekman and Wallace V Friesen. Nonverbal leakage and clues to deception. *Psychiatry*, 32, 1969.

[33] Nicole Ellison, Rebecca Heino, and Jennifer Gibbs. Managing impressions online: Self-presentation processes in the online dating environment. *Journal of computer-mediated communication*, 11, 2006.

[34] Satu Elo and Helvi Kyngäs. The qualitative content analysis process. *Journal of advanced nursing*, 62, 2008.

[35] Thomas H Feeley and Melissa J Young. Humans as lie detectors: Some more second thoughts. *Communication quarterly*, 46, 1998.

[36] Kyla C Flug. Swipe, right? young people and online dating in the digital age. *Sophia, the St. Catherine University*, 2016.

[37] Simon Fong, Yan Zhuang, Luke Lu, and Rui Tang. Analysis of general opinions about sina weibo micro-blog real-name verification system. In *The First International Conference on Future Generation Communication Technologies*. IEEE, 2012.

[38] Jonathan B. Freeman, Ryan M. Stolier, Zachary A. Ingbretsen, and Eric A. Hehman. Amygdala responsivity to high-level social information from unseen faces. *Journal of Neuroscience*, 34(32):10573–10581, 2014.

[39] Bruna Freitas, Ashraf Matrawy, and Robert Biddle. Online neighborhood watch: The impact of social network advice on software security decisions. *Canadian Journal of Electrical and Computer Engineering*, 39(4):322–332, 2016.

[40] Batya Friedman, David Hurley, Daniel C Howe, Edward Felten, and Helen Nissenbaum. Users' conceptions of web security: a comparative study. In *CHI'02 extended abstracts on Human factors in computing systems*. ACM, 2002.

[41] Batya Friedman, Peter H Khan Jr, and Daniel C Howe. Trust online. *Communications of the ACM*, 43, 2000.

[42] Anthony Y. Fu, Xiaotie Deng, Liu Wenyin, and Greg Little. The methodology and an application to fight against unicode attacks. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06. ACM, 2006.

[43] Diego Gambetta et al. Can we trust trust. *Trust: Making and breaking cooperative relations*, 13:213–237, 2000.

[44] Sujata Garera, Niels Provos, Monica Chew, and Aviel D. Rubin. A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM Workshop on Recurring Malcode*. ACM, 2007.

[45] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[46] David Good. Individuals, interpersonal relations, and trust. *Trust: Making and breaking cooperative relations*, 2000.

[47] Abrar Haider and Andy Koronios. *Authenticity of Information in Cyberspace: IQ in the Internet, Web, and e-Business.* PhD thesis, Citeseer, 2003. Proceedings of the Eighth International Conference on Information Quality (ICIQ-03).

[48] Jeffrey T Hancock, Lauren E Curry, Saurabh Goorha, and Michael Woodworth. On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes*, 45, 2007.

[49] Aurora Harley. Icon Usability. July 27, 2014.

[50] Nick Heath. Google Finally Chops 'www' from Chrome's Address Bar Despite Backlash Over 'Confusing' Change. August 1, 2019.

[51] James Hendler and Alice M Mulvehill. *Social machines: the coming collision of artificial intelligence, social networking, and humanity*. Apress, 2016.

[52] Susan C Herring. *Computer-mediated communication: Linguistic, social, and cross-cultural perspectives*, volume 39. John Benjamins Publishing, 1996.

[53] Lars Hertzberg. On the attitude of trust. *Inquiry*, 31, 1988.

[54] Lance James, ProQuest (Firm), and Inc Books24x7. *Phishing exposed*. Syngress Pub, 1 edition, 2005.

[55] Nick Janetos and Jan Tilly. Reputation dynamics in a market for illicit drugs. *arXiv preprint arXiv:1703.01937*, 2017.

[56] PN Juslin, KR Scherer, J Harrigan, and R Rosenthal. The new handbook of methods in nonverbal behavior research, 2005.

[57] Surinder Singh Kahai and Randolph B Cooper. Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality. *Journal of management information systems*, 20, 2003.

[58] Clare-Marie Karat, John Karat, and Carolyn Brodie. Why hci research in privacy and security is critical now. *International Journal of Human-Computer Studies*, 63, 2005.

[59] Lars Bo Kaspersen. Anthony giddens: The consequences of modernity. *Politica*, 23, 1991.

[60] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE symposium on security and privacy*, pages 523–537. IEEE, 2012.

[61] Engin Kirda and Christopher Kruegel. Protecting users against phishing attacks. *The Computer Journal*, 49(5):554–561, 09 2006. Copyright - Copyright Oxford University Press(England) Sep 2006; Document feature - ; Charts; Illustrations; Last updated - 2014-05-16; CODEN - CMPJAG.

[62] Klaus Krippendorff. *Content analysis: An introduction to its methodology*. Sage publications, 2018.

[63] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[64] Ko Kuwabara. Do reputation systems undermine trust? divergent effects of enforcement type on generalized trust and trustworthiness. *American Journal of Sociology*, 120, 2015.

[65] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2075–2084. ACM, 2011.

[66] Niklas Luhmann. *Trust and power*. John Wiley & Sons, 2018.

[67] Daoshan Ma et al. Linguistic methods to detect lies. *Open Access Library Journal*, 2, 2015.

[68] Michael W Macy and John Skvoretz. The evolution of trust and cooperation between strangers: A computational model. *American Sociological Review*, 1998.

[69] Ashley D. Manker. What Is Written Communication in Business? - Definition, Types & Examples.

[70] Stephen Paul Marsh. *Formalising trust as a computational concept*. PhD thesis, University of Stirling, 1994.

[71] Jason Milletary and CERT Coordination Center. Technical trends in phishing attacks. *Retrieved December*, 1(2007), 2005.

[72] Barbara A. Misztal. *Trust in modern societies: the search for the bases of social order*. Polity Press, 1996.

[73] Gregory Norcie, Emiliano De Cristofaro, and Victoria Bellotti. Bootstrapping trust in online dating: Social verification of online dating profiles. In Andrew A. Adams, Michael Brenner, and Matthew Smith, editors, *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013.

[74] Borke Obada-Obieh and Anil Somayaji. Can i believe you?: Establishing trust in computer mediated introductions. In *Proceedings of the 2017 New Security Paradigms Workshop*, pages 94–106. ACM, 2017.

[75] Paul Pajares and Gelo Abendan. Trendlabs security intelligence blog.“, 2014.

[76] NVivo 12 Pro. `https://www.qsrinternational.com/nvivo/nvivo-products/nvivo-12-pro`. Tool for qualitative analyses.

[77] Pamela Anne Quiroz. From finding the perfect love online to satellite dating and ‘loving-the-one-you’re near’ a look at grindr, skout, plenty of fish, meet moi, zoosk and assisted serendipity. *Humanity & Society*, 37, 2013.

[78] Julian B Rotter. A new scale for the measurement of interpersonal trust 1. *Journal of personality*, 35, 1967.

[79] Julian B Rotter. Generalized expectancies for interpersonal trust. *American psychologist*, 26, 1971.

[80] Julian B Rotter. Interpersonal trust, trustworthiness, and gullibility. *American psychologist*, 35, 1980.

[81] Victoria L Rubin and Niall Conroy. Discerning truth from deception: Human judgments and automation efforts. *First Monday*, 17, 2012.

[82] Emily Schechter. Feedback: Eliding www/m subdomains. `https://bugs.chromium.org/p/chromium/issues/detail?id=883038#c114`, Sep 11 2018.

[83] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor’s new security indicators. In *2007 IEEE Symposium on Security and Privacy (SP’07)*, pages 51–65. IEEE, 2007.

[84] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor’s new security indicators. In *2007 IEEE Symposium on Security and Privacy (SP’07)*, pages 51–65. IEEE, 2007.

[85] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382. ACM, 2010.

[86] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99. ACM, 2007.

[87] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99. ACM, 2007.

[88] Daniel J Siegel. *The developing mind: How relationships and the brain interact to shape who we are*. Guilford Publications, 2012.

[89] Michael Sirivianos, Kyungbaek Kim, Jian Wei Gan, and Xiaowei Yang. Assessing the veracity of identity assertions via osns. In *2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012)*. IEEE, 2012.

[90] SSLShopper. Choosing the right certificate authority. Fri Oct 7, 2016.

[91] James Stanier, Stephen Naicken, Anirban Basu, Jian Li, and Ian Wakeman. Can we use trust in online dating? *JoWUA*, 1, 2010.

[92] Scam statistics. `https://www.scamwatch.gov.au/about-scamwatch/scam-statistics`. 2019.

[93] Milica Stojmenoviæ and Robert Biddle. Hide-and-seek with website identity information. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–6. IEEE, 2018.

[94] Milica Stojmenović, Temitayo Oyelowo, Alisa Tkaczyk, and Robert Biddle. Building website certificate mental models. In *International Conference on Persuasive Technology*, pages 242–254. Springer, 2018.

[95] Milica Stojmenović, Eric Spero, Temitayo Oyelowo, and Robert Biddle. Website identity notification: Testing the simplest thing that could possibly work. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–7. IEEE, 2019.

[96] Tinder Application Support. How do i create a tinder account? `https://www.help.tinder.com/hc/en-us/articles/115003356706-How-do-I-create-a-Tinder-account-`.

[97] Patti Tilley, Joey F George, and Kent Marett. Gender differences in deception and its detection under varying electronic media conditions. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. IEEE, 2005.

[98] Catalina L Toma, Jeffrey T Hancock, and Nicole B Ellison. Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, 34, 2008.

[99] Kathleen L Valley, Joseph Moag, and Max H Bazerman. A matter of trust':: Effects of communication on the efficiency and distribution of outcomes. *Journal of Economic Behavior & Organization*, 34, 1998.

[100] Aldert Vrij. *Detecting lies and deceit: The psychology of lying and implications for professional practice*. Wiley, 2000.

[101] Aldert Vrij, Pär Anders Granhag, and Stephen Porter. Pitfalls and opportunities in nonverbal and verbal lie detection. *Psychological science in the public interest*, 11, 2010.

[102] Tara Whalen and Kori M Inkpen. Gathering evidence: use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, pages 137–144. Canadian Human-Computer Communications Society, 2005.

[103] Cathleen Wharton, Janice Bradford, Robin Jeffries, and Marita Franzke. Applying cognitive walkthroughs to more complex user interfaces: experiences, issues, and recommendations. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 381–388. ACM, 1992.

[104] Johannes Wheeldon and Jacqueline Faubert. Framing experience: Concept maps, mind maps, and data collection in qualitative research. *International journal of qualitative methods*, 8, 2009.

[105] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, pages 169–184, 1999.

[106] Barbara M Wildemuth. *Applications of social research methods to questions in information and library science*. ABC-CLIO, 2016.

[107] Emma J. Williams and Kate Muir. *A Model of Trust Manipulation: Exploiting Communication Mechanisms and Authenticity Cues to Deceive*, pages "249–265". "Springer International Publishing", "2019".

[108] Janine Willis and Alexander Todorov. First impressions: Making up your mind after a 100-ms exposure to a face. *Psychological science*, 17, 2006.

[109] Haidong Xia and José Carlos Brustoloni. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In *Proceedings of the 14th international conference on World Wide Web*, pages 489–498. ACM, 2005.

[110] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering*, 16, 2004.

[111] Giorgos Zacharia and Pattie Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14, 2000.

[112] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *2013 APWG eCrime Researchers Summit*, pages 1–11, Sep. 2013.

[113] Xudong Zheng. Hi! i'm xudong zheng! https://www.xudongz.com/. Johns Hopkins University.

[114] Xudong Zheng. Phishing with unicode domains. https://www.xudongz.com/blog/2017/idn-phishing/. April 14, 2017.

[115] Miron Zuckerman, Bella M DePaulo, and Robert Rosenthal. Verbal and nonverbal communication of deception. In *Advances in experimental social psychology*, volume 14. Elsevier, 1981.

Appendix A

Recruitment Materials for the First Study

In this we present the materials that we used to invite the participants to our study such as invitation email and the poster, as well as the materials that we used before and during out session such as the consent form, the interview questions, and the Tinder simulation profiles.

Carleton UNIVERSITY
Canada's Capital University

Research Consent Form

Name and Contact Information of Researchers:

Anis Ghazvinian, Carleton University, Department of Human Computer Interaction

Tel.: 613 770 8678

Email: anisghazvinian@cmail.carleton.ca

Supervisor and Contact Information:

Anil Somayaji, Carleton University, Department of Computer science

Email: soma@scs.carleton.ca

Project Title

The trust indicator factors of online dating applications.

Carleton University Project Clearance

Clearance #: 109951 Date of Clearance: April 30, 2019

Invitation

You are invited to take part in a research project if you are between 18 – 59 years old and you have experience using online dating apps namely Tinder. The information in this form is intended to help you understand what we are asking of you so that you can decide whether you agree to participate in this study. Your participation in this study is voluntary, and a decision not to participate will not be used against you in any way. As you read this form, and decide whether to participate, please ask all the questions you might have, take whatever time you need, and consult with others as you wish.

What is the purpose of the study?

This study is going to find out what factors do dating site users use to determine whether a profile is legitimate or not, find out the influence of the verification badges on the users, and design a trust indicator based on those factors.

What will I be asked to do?

If you agree to take part in the study, we will ask you to have a 30 minutes semi structured interview with the researcher and doing a 10 minutes activity which is not require any physical activities. As part of this, you will be asked to evaluate aspects of simulated dating profiles. Please note that the interview and the activity will audio recorded to transcribe. This study will take place in the Carleton Clockware Security Lab, located on 5th floor of Herzberg Building at Carleton University.

Carleton UNIVERSITY
Canada's Capital University

Risks and Inconveniences

We do not anticipate any physical harm; however, there are risks of recalling unpleasant memories in this study. Therefore, you are allowed to stop the study or your participation in the study as soon as you feel anxious or distress.

Possible Benefits

You may not receive any direct benefit from your participation in this study. However, your participation may allow researchers to better understand what factors do dating site users use to determine whether a profile is legitimate or not, find out the influence of the verification badges on the users, and design a trust indicator based on those factors.

Compensation/Incentives

The participants will be compensated with a $10 Starbucks gift card in this study.

No waiver of your rights

By signing this form, you are not waiving any rights or releasing the researchers from any liability.

Withdrawing from the study

If you withdraw your consent during the course of the study, all information collected from you before your withdrawal will be discarded.

After the study, you may request that your data be removed from the study and deleted by notice given to the Anis Ghazvinian until 30th April, 2019.

Please note that if you withdraw your participating in the study right away before finishing the study, or if you decide to withdraw later (till 30th April, 2019), you can keep the gift card.

Confidentiality

We won't ask you any identifying information in this study and the interview participants will be assigned a random code; however, the researcher will have a confidential list (master list) of participants just in case. The list will include the participants' name, email and the random code which will be assigned to each participant. The list will be kept in a locked cabinet in the Carleton Computer Security Lab (CCSL) in the 5th floor of Herzberg Building at Carleton University which has a very limited and swipe card access, but separately from all the collected data.

We will treat your personal information as confidential, although absolute privacy cannot be guaranteed. No information that discloses your identity will be released or published without your specific consent. However, research records identifying you may be accessed by the Carleton University Research Ethics Board to monitor the research. All data will be kept confidential, unless release is required by law (e.g. child abuse, harm to self or others).

The results of this study may be published or presented at an academic conference or meeting, but the data will be presented so that it will not be possible to identify any participants unless you give your express consent.

We will password protect any research data that we store or transfer.

Data Retention

After finalizing the whole project, the audio files will be destroyed by the end of upcoming summer (2019) semester. Transcribed data (audio transcription) and analysed data will be saved and kept in encrypted files on CCSL lab systems located in 5th floor of Herzberg building, for 5 years and then they will be deleted.

New information during the study

In the event that any changes could affect your decision to continue participating in this study, you will be promptly informed.

Ethics review

This project was reviewed and cleared by the Carleton University Research Ethics Board B. If you have any ethical concerns with the study, please contact Dr. Bernadette Campbell, Chair, Carleton University Research Ethics Board (by phone at 613-520-2600 ext. 4085 or by email at ethics@carleton.ca).

Statement of consent – print and sign name

I voluntarily agree to participate in this study. ___Yes ___No

I agree to be audio recorded ___Yes ___No

(If you are not agreed to audio recording, we appreciate your decision, but we cannot let you be part of the study.)

(Optional) I agree to be contacted for follow up research ___Yes ___No

_____ _____

Signature of participant Date

Research team member who interacted with the subject

I have explained the study to the participant and answered any and all of their questions. The participant appeared to understand and agree. I provided a copy of the consent form to the participant for their reference.

_____ _____

Signature of researcher Date

Carleton UNIVERSITY
Canada's Capital University

Subject: Invitation to participate in a research project on **Trust indicator in Online Dating**

Dear Sir / Madam,

Thank you for inquiring about our study. My name is Anis Ghazvinian and I am a master's student in the Human Computer Interaction at Carleton University. I am working on a research project under the supervision of Prof. Anil Somayaji. This email is going to give you more information about our study.

"Trust indicator in Online Dating" is the title of our study and it aims to explore the trust indicators and the influence of verification badges on users of online dating applications.

The requirements to participate in this study are: being an adult between 18 - 59, having experience using online dating applications (preferably Tinder) over a month, having experience going on at least one date through online dating applications, and being comfortable with English.

This study involves one 30 minutes interview that will take place in the Carleton Computer Security Lab (CCSL) located in room 5145 of the Herzberg Building at Carleton University. With your consent, interviews will be audio recorded. Once the recording has been transcribed, the audio recording will be destroyed.

While this project does not involve professional and physical risks, care will be taken to protect your identity and prevent privacy-related and psychological risks. This will be done by keeping all responses confidential and allowing you to request that certain responses not be included in the final project. Please note that this study may involve recalling unpleasant memories related to online dating, even though we will not ask you any direct questions about your past experiences.

You will have the right to end your participation in the study at any time (including in the middle of a session), for any reason, up until the 30th April, 2019. If you choose to withdraw, all the information you have provided will be destroyed.

As a token of appreciation, I will be providing you with refreshments during the interview and you will receive a $10 Starbucks gift card. You can keep the gift card if you withdraw from the study, even in the middle of the session.

All research data, including audio recordings, notes, and transcripts, will be stored securely. Any physical copies of data (including any handwritten notes or USB keys) will be kept in a locked cabinet in the CCSL, which has limited access. Data on computers will be stored in encrypted form. Research data will thus only be accessible by the researcher and her research supervisor.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. (Clearance # 109951, Clearance expires on: 30/04/2019)

CUREB-B:
If you have any ethical concerns with the study, please contact Dr. Bernadette Campbell, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

If you would like to participate in this research project, or have any questions, please contact me at (613

770 8678) or (anis.ghazvinian@carleton.ca).

Sincerely,

Anis Ghazvinian

Carleton UNIVERSITY

Trust Indicators In Online Dating

We are looking for volunteers for a ressearch study which is going to explore the trust indicators and the influence of the verification badges on the users on online dating applications.

If you are interested to participate in this study and you are:

1. An adult between 18 - 59
2. Have experience using online dating app (preferably Tinder) over a month
3. Have experience going on at least a date through the app
4. comfortable with English

Please send an email to Anis.ghazvinian@carleton.ca

Participants will be compensated with a $10 Starbucks gift card.

This research has been cleared by the Carleton University Research Ethics Board (CUREB-B), REB clearance # 109951

Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca
Anis.ghazvinian@carleton.ca

Study 1 - Part 1:

Tinder Questions:

General questions:

1. Are you currently using Tinder?
2. Can you briefly explain why are you using/ left Tinder?
3. Did/ Do you use free version of Tinder or the paid version of that?
4. How long have you been/ were you on Tinder?
5. Can you tell me a little about your experience using Tinder?
6. Can you tell me about any concern (if any) that you have using Tinder?
7. Do you have concerns about fake profiles on Tinder?

Profile making questions:

8. When you want to make a profile on Tinder, are you agree to give the application your real name and age?
9. How many pictures are you willing to share in your Tinder profile?
10. If Tinder ask you to take picture in special poses but promise you to not share those pictures with anyone else, are you willing to do that?
11. How much personal information are you willing to share with Tinder application? If Tinder promise you to not share those with anyone, are you willing to share more personal information?

Selection (swiping) and texting questions:

12. What factors determine whether you swipe right or left on a person?!
13. What are some obvious factors that make you think a profile is fake?

14. Do the number of pictures play a rule to find weather a profile is fake or not? How about the description of a profile? Can the person's location show the profile is fake?
15. Before you start chatting with a person, what factors convince you to send text/reply a person?!
16. After chatting with a person for a while (short term) what factors persuade you to continue talking or even convince you to meet that person?

Verified badges question:

17. Have you ever seen a profile with verified badges on Tinder?
18. Do you know how the verified badge works on Tinder?
19. If a person has a verified badge on Tinder, what would you think about that person?

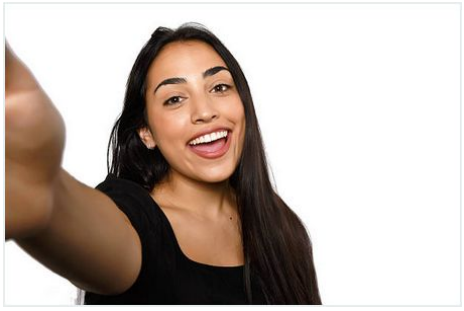
Other Online Dating Questions:

20. Is Tinder the only app you use? If not, what are the others?
21. Can you briefly compare your experience using other applications with your experience on Tinder?
22. What does the verified badge mean to you in general?
23. Ideally, what would you want the verified badge means?

Emma, 21

3 kilometers away

French/ English
Looking for someone to watch Bob Ross videos with
PSW. Gym. Music. Photography.



Jenine, 24

15 kilometers away

Trish, 32

City of Ottawa

Algonquin College

34 kilometers away

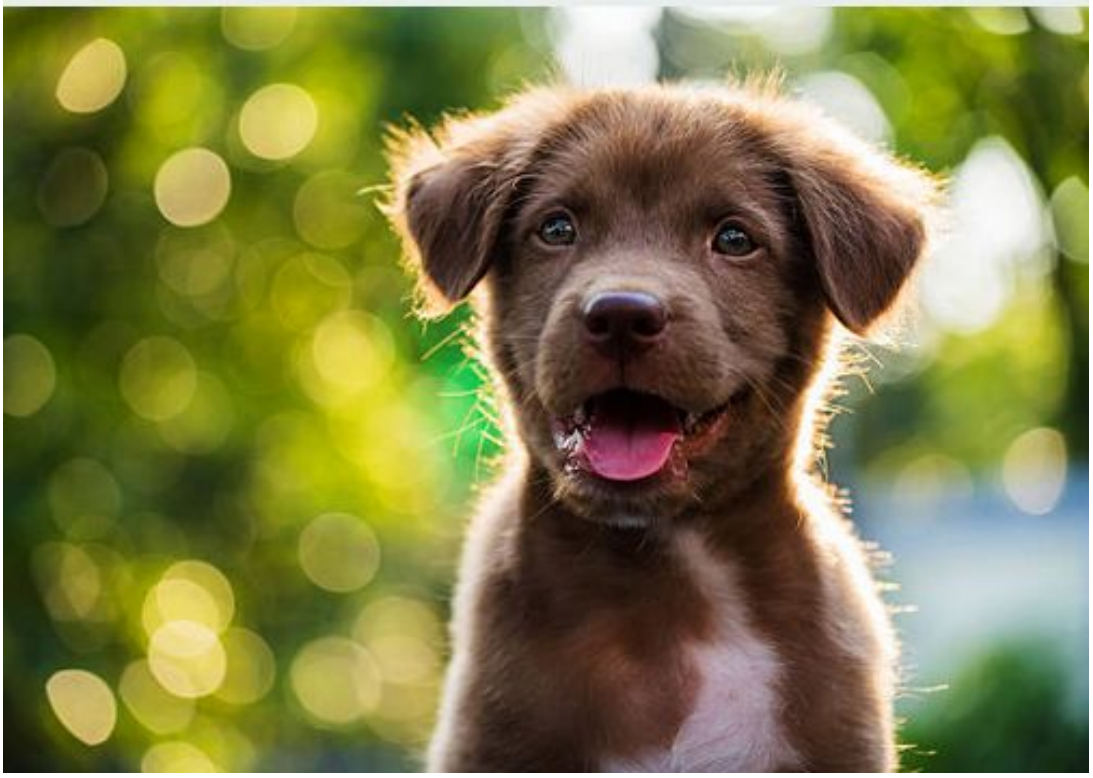
Looking to connect with someone and see where it goes.

Lisa, 21

6 kilometers away

Student
A little shy
Just out of a relationship, just looking to meet new people.
In Ottawa

If we match, say hi. ;)



Kara, 24

Costco
UBC
16 kilometers away

New to Ottawa.

If you think you know me from this profile; you're wrong.

Ben, 27

3 kilometers away

I love spending time in the outdoors. I really like food and cooking, Brooklyn nine-nine, and a good beer.

Originally from the US...PS sorry about our president, I didn’t vote for him

Justin, 34

15 kilometers away

Paul, 32

City of Ottawa

Algonquin College

34 kilometers away

Looking to connect with someone and see where it goes.

Jack, 37

6 kilometers away

I’m obsessed with the countryside;
Woods, forests, fields, lakes and mountains
I live my life as if it were a folk song.
I’m 6’5, my specialty is the top shelf.

Liam, 22

Analyst at public services

16 kilometers away

Analyst by day.
Interest: family, fashion, and fitness.
I believe beauty attracts the eyes but personality captures the heart.

Appendix B

Recruitment Materials for the Second Study

In this appendix we present materials related to our second study, the one on online services. We include the materials used for inviting the participants to our study, including a sample invitation email to participants who voluntarily indicated their interest to be contacted for a follow-up study and a sample invitation email for new participants. We also include the materials that we used before and during the study sessions such as the consent form, our study test plan, and the synthetic profiles we showed participants.

Carleton UNIVERSITY
Canada's Capital University

Research Consent Form

Name and Contact Information of Researchers:

Anis Ghazvinian, Carleton University, Department of Human Computer Interaction

Tel.: 613 770 8678

Email: anisghazvinian@cmail.carleton.ca

Supervisor and Contact Information:

Anil Somayaji, Carleton University, Department of Computer science

Email: soma@scs.carleton.ca

Project Title

Human Patterns in Trustworthy Internet Navigation

Carleton University Project Clearance

Clearance #: 111234

Invitation

You are invited to take part in a research project if you are between 18 – 59 years old and you have experience using social networking platforms (Facebook, Instagram, LinkedIn, etc.), online banking, online shopping, and email services. Your participation in this study is voluntary, and a decision not to participate will not be used against you in any way. As you read this form, and decide whether to participate, please ask all the questions you might have, take whatever time you need, and consult with others as you wish.

What is the purpose of the study?

Users of online services often get phished, or tricked, into using untrustworthy services, causing them to disclose confidential information such as email addresses, passwords, and credit card numbers to attackers. Most people know such information is sensitive and anecdotally people do attempt to determine whether they are accessing trustworthy services. In this study we are attempting to learn the strategies people use to evaluate the trustworthiness of online services. Our hope is that if we can better understand these behaviours, it will be possible to develop mechanisms to help people make more reliable trust decisions.

What will I be asked to do?

If you agreed to take part in the study, we will have six tasks and after each task the facilitator will ask you some questions regarding the task. You will be interacting with specific web services for email, social media, and e-commerce. Please note that you will not be asked to login or provide your password to any sites at any time.

Carleton UNIVERSITY
Canada's Capital University

Risks and Inconveniences

We do not anticipate any physical or psychological harm; however, you are allowed to cease your participation in the study if you feel anxious or distressed.

Possible Benefits

You may not receive any direct benefit from your participation in this study. However, you may learn techniques for determining whether you are accessing legitimate online services. Also, your participation may help in the development of tools that would allow users to better determine whether Internet services are legitimate.

Compensation/Incentives

Participants will be compensated with a $10 Starbucks gift card for participation in this study.

No waiver of your rights

By signing this form, you are not waiving any rights or releasing the researchers from any liability.

Withdrawing from the study

If you withdraw your consent during the course of the study, all information collected from you before your withdrawal will be discarded.

After the study, you may request that your data be removed from the study and deleted by notice given to the Anis Ghazvinian until September 30th, 2019.

Please note that if you withdraw your participating in the study right away before finishing the study, or if you decide to withdraw later (till September 30th, 2019), you can keep the gift card.

Confidentiality

We won't ask you any identifying information in the study and you will be assigned a code; however, the researcher will have a confidential list (master list) of participants just in case if any of the participants would like to withdraw from the study later, before September 30th. The list will include the participants' name, email and the random code which will be assigned to each participant. The list will be kept in a locked cabinet in the Carleton Computer Security Lab (CCSL) in the 5th floor of Herzberg Building at Carleton University which has very limited access via swipe card, separate from the rest of the collected data. This master list will be discarded on September 30th, 2019.

We will treat your personal information as confidential, although absolute privacy cannot be guaranteed. No information that discloses your identity will be released or published without your specific consent. However, research records identifying you may be accessed by the Carleton University Research Ethics Board to monitor the research. All data will be kept confidential unless release is required by law (e.g. child abuse, harm to self or others).

The results of this study may be published or presented at an academic conference or meeting, but the data will be presented so that it will not be possible to identify any participants unless you give your express consent.

Carleton UNIVERSITY
Canada's Capital University

We will password protect any research data that we store or transfer.

Data Retention

After finalizing the whole project, the audio files will be destroyed by the end of the Summer 2019 semester. Transcribed data (audio transcription) and analysed data will be saved and kept in encrypted files on CCSL lab systems located in 5th floor of Herzberg building for 5 years and then they will be deleted.

New information during the study

In the event that any changes could affect your decision to continue participating in this study, you will be promptly informed.

Ethics review

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

Statement of consent – print and sign name

I voluntarily agree to participate in this study. ___Yes___No

I agree to be audio recorded ___Yes___No

(If you are not agreed to audio recording, we appreciate your decision, but we cannot let you be part of the study.)

_____ _____

Signature of participant Date

Research team member who interacted with the subject

I have explained the study to the participant and answered any and all of their questions. The participant appeared to understand and agree. I provided a copy of the consent form to the participant for their reference.

_____ _____

Signature of researcher Date

Carleton UNIVERSITY
Canada's Capital University

Subject: Invitation to Participate in a Study on **Human Patterns in Trustworthy Internet Navigation**

Dear Sir / Madam,

Thank you for inquiring about our study. My name is Anis Ghazvinian and I am a master's student in Human Computer Interaction at Carleton University. I am working on a research project under the supervision of Prof. Anil Somayaji. This email is going to give you more information about our study.

"Human Patterns in Trustworthy Internet Navigation" is the title of our study and it aims to learn the strategies people use to evaluate the trustworthiness of websites since users of online services often get phished, or tricked, into using untrustworthy services, causing them to disclose confidential information such as email addresses, passwords, and credit card numbers to attackers. Most people know such information is sensitive and anecdotally people do attempt to determine whether they are accessing a trustworthy service. Our hope is that if we can better understand these behaviours, it will be possible to develop mechanisms to help people make more reliable trust decisions.

The requirements to participate in this study are: being an adult between 18 - 59, having experience using online banking, shopping, social media / networking mediums, and email services, and being comfortable with English.

This study involves one 40 minute session to complete six tasks and answer some questions following each task. The study will take place in the Carleton Computer Security Lab (CCSL) located in room 5145 of the Herzberg Building at Carleton University. With your consent, interviews will be audio recorded. Once the recording has been transcribed, the audio recording will be destroyed.

While this project does not involve professional and physical risks, care will be taken to protect your identity and prevent privacy-related and psychological risks. This will be done by keeping all responses confidential and allowing you to request that certain responses not be included in the final project.

You will have the right to end your participation in the study at any time (including in the middle of a session), for any reason, up until the September 30th, 2019. If you choose to withdraw, all the information you have provided will be destroyed.

As a token of appreciation, I will be providing you with refreshments during the interview and you will receive a $10 Starbucks gift card. You can keep the gift card if you withdraw from the study, even in the middle of the session.

All research data, including audio recordings, notes, and transcripts, will be stored securely. Any physical copies of data (including any handwritten notes or USB keys) will be kept in a locked cabinet in the CCSL, which has limited access. Data on computers will be stored in encrypted form. Research data will thus only be accessible by the researcher and her research supervisor.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. (Clearance # 111234)

CUREB-B:

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

If you would like to participate in this research project, or have any questions, please contact me at (613 770 8678) or (anis.ghazvinian@carleton.ca).

Sincerely,

Anis Ghazvinian

Carleton UNIVERSITY
Canada's Capital University

Subject: Invitation to Participate in a Study on **Human Patterns in Trustworthy Internet Navigation**
Dear (Name of the person),

Thank you for participating in my previous study, Trust Indicators In Online Dating. Previously you indicated you were willing to participate in follow-up research studies. As a result, I am writing to you today to invite you to participate in such a follow-up study pertaining to Human Patterns in Trustworthy Internet Navigation. The aim of this study is to find out the strategies people use to evaluate the trustworthiness of websites since users of online services often get phished, or tricked, into using untrustworthy services, causing them to disclose confidential information such as email addresses, passwords, and credit card numbers to attackers. Most people know such information is sensitive and anecdotally people do attempt to determine whether they are accessing a trustworthy service. Our hope is that if we can better understand these behaviours, it will be possible to develop mechanisms to help people make more reliable trust decisions.

This study involves one 40 minute session to complete six tasks and answer questions following each task. The study will take place in the Carleton Computer Security Lab (CCSL) located in room 5145 of the Herzberg Building at Carleton University. With your consent, the session will be audio recorded. Once the recording has been transcribed, the audio recording will be destroyed.

While this project does not involve professional and physical risks, care will be taken to protect your identity and prevent privacy-related and psychological risks. This will be done by keeping all responses confidential and allowing you to request that certain responses not be included in the final project.

You will have the right to end your participation in the study at any time (including in the middle of a session), for any reason, up until the September 30th, 2019. If you choose to withdraw, all the information you have provided will be destroyed.

As a token of appreciation, I will be providing you with refreshments during the interview and you will receive a $10 Starbucks gift card. You can keep the gift card if you withdraw from the study, even in the middle of the session.

All research data, including audio recordings, notes, and transcripts, will be stored securely. Any physical copies of data (including any handwritten notes or USB keys) will be kept in a locked cabinet in the CCSL, which has limited access. Data on computers will be stored in encrypted form. Research data will thus only be accessible by the researcher and her research supervisor.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. (Clearance # 111234)

CUREB-B:
Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

If you would like to participate in this research project, or have any questions, please contact me at (613 770 8678) or (anis.ghazvinian@carleton.ca).

Sincerely,

Anis Ghazvinian

Second User Study – Test Plan:

Research Question:

How do users ensure they access legitimate versions of online services such as email, social media, and financial services? Specifically:

- What are the processes people use to access online services?
- To what extent are these processes generally used, and to what extent are they task-specific?
- Are these processes vulnerable to attack (are they trustworthy), and do users perceive them as trustworthy?
- To what extent do existing interfaces and services support the processes of users?

Task 1: Email Platforms

I will open Google home page on one of the CCSL's systems and ask the participant to go to his/her email platform. **Please note that I will stop the participant from entering his/her username and password.**

Scenario:

Imagine today is Saturday. You just woke up and you want to check your email.

1. Do you normally use a web browser or an application (such as Outlook or a mobile app) to check your email?
2. Please show me how would you log in to your email account using a web browser. (Think aloud method)
3. Are you sure you have reached the correct sign-in page for your Email platform?
4. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your email sign-in page?
5. Do you normally only use your own machine to check your email? Or, are you okay using other computers (such as a friend's laptop or a library computer) to check your email?
6. You almost just used an unfamiliar machine to check your email. Do you think this machine is trustworthy? Why?
7. Would you want some other method to verify that you are connecting to your email provider securely? If so, what sort of method would you prefer?
8. How satisfied are you with your current process for accessing your email, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?

Task 2: Online Banking

I will offer the participants one of the CCSL's machines and I will open Google page and ask them to go to their bank website. **Please note that I will stop them from entering their username and password.**

Scenario:

Imaging while you are checking your email, you will see that you have received an email from your bank. How would you get to your online banking account?

1. Do you normally use a web browser or an application (such as the RBC mobile app) to check your online banking account?
2. Imagine there is a link in that email. Please show me how would you log in to your bank account using a web browser. (Think aloud method)
3. Are you sure you have reached the correct sign-in page for your bank platform?
4. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your online banking sign-in page?
5. Imaging there is NOT any link in that email, please show me how would you log in to your bank account using a web browser. (think aloud method)
6. Are you sure you have reached the correct sign-in page for your bank platform?
7. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your online banking sign-in page?
8. Are you normally just use your own machine to log into your bank account or are you okay using other public or your friends' laptop for example to sign into your online bank?
9. You almost just used an unfamiliar machine to log in to your bank account. Do you think this machine is trustworthy? Why?
10. Would you want some other method to verify that you are connecting to your online bank provider securely? If so, what sort of method would you prefer?
11. How satisfied are you with your current process for accessing your online bank account, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?

Task 3: Social Media/ Networking

I will offer the participants one of the CCSL's machines, and open Google page and ask them to go to their bank website. **Please note that I will stop them from entering their username and password.**

Scenario:

After checking your email and your online banking account, now is time to check your social media/ networking accounts.

1. Which social media / networking mediums do you normally use?
2. Do you normally use a web browser or an application to check your social media / networking account?
3. Please show me how would you log in to your social media / networking account using a web browser. (think aloud method)
4. Are you sure you have reached the correct sign-in page for your social media / networking platform?
5. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your social media/ networking platform sign-in page?
9. Are you normally just use your own machine to log into your social media/ networking account or are you okay using other public or your friends' laptop for example to sign into your social media / networking account?
10. You almost just used an unfamiliar machine to log in to your social media/ networking account. Do you think this machine is trustworthy? Why?
11. Would you prefer some other method to verify that you are connecting to your social media/ networking platform provider securely? If so, what sort of method would you want?
12. How satisfied are you with your current process for accessing your social media/ networking account, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?

Task 4: Social Media/ Networking (Friend Request)

I will offer the participants one of the CCSL's machines, and open Google page and ask them to go to their bank website. **Please note that I will stop them from entering their username and password.**

Scenario:

While you are checking your social media/ networking account, you will get two notifications. The first one indicates that a random person sent you friend request.

1. How would you know that person is legitimate?

2. Is there any specific feature here that you can rely on to assure you that this person is trustworthiness or untrustworthiness?
3. Have you ever seen the trust indicators on the social networking / social media platforms?
4. Are you aware of how the trust indicators work?
5. Does seeing trust indicators have any impact on your decision of accepting the friend request of a stranger or not?
6. If you are able to introduce or demonstrate a way that verifies legitimate people from fake ones, what would that be?
7. Would you want some other method to verify that person is legitimate or not? If so, what sort of method would you prefer?
8. How satisfied are you with your current process for weather a person is legitimate or not, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?

Task 5: Online Shopping (for friend/ not familiar website)

I will offer the participants one of the CCSL's machines, and open Google page and ask them to go to their bank website. **Please note that I will stop them from entering their username and password.**

Scenario:

The second notification says that next week is your best friend's birthday. However, you are very busy and don't have time to go shopping. Therefore, you will decide to order something online. Your friend is really interested in a book/a travel mug, an electronic gadget/other. (please note that you should choose something that you have never ordered that before)

1. Do you normally use a web browser or an application (such as Amazon mobile app) to order something?
2. Please show me how you would order your good using a web browser. (think aloud method)
3. Are you sure you have reached the correct sign-in page for your bank platform?
4. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your online banking sign-in page?
5. When you are in the transaction page, how would you trust that page to share your credit card information?
6. You almost just used an unfamiliar processor to order your good. Do you think this processor is trustworthy? Why?
7. Would you prefer some other method to verify that you are connecting to legitimate online shop provider securely? If so, what sort of method would you prefer?

8. How satisfied are you with your current process of online shopping, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?

Task 6: Online Shopping (shopping from familiar website)

I will offer the participants one of the CCSL's machines, and open Google page and ask them to go to their bank website. **Please note that I will stop them from entering their username and password.**

Scenario:

After you ordered your friend's gift, you remember that something (something you already ordered it before) for yourself as well.

1. Do you normally use a web browser or an application (such as Amazon mobile app) to order something?
2. Please show me how you would order your good using a web browser. (think aloud method)
3. Are you sure you have reached the correct sign-in page for your bank platform?
4. Is there any specific feature here that you can rely on to assure you that you are on the correct page, rather than a malicious one that is designed to look like your online banking sign-in page?
5. When you are in the transaction page, how would you trust that page to share your credit card information?
6. You almost just used an unfamiliar processor to order your good. Do you think this processor is trustworthy? Why?
7. Would you prefer some other method to verify that you are connecting to legitimate online shop provider securely? If so, what sort of method would you prefer?
8. How satisfied are you with your current process of online shopping, on a scale from 1 to 5 (1 is very unsatisfied and 5 is very satisfied)?