Chapter 7
The Role of Psychology in Understanding Online Trust

Helen S. Jones
University of Dundee, UK

Wendy Moncur
University of Dundee, UK

ABSTRACT

Across many online contexts, internet users are required to make judgments of trustworthiness in the systems or other users that they are connecting with. But how can a user know that the interactions they engage in are legitimate? In cases where trust is manipulated, there can be severe consequences for the user both economically and psychologically. In this chapter, the authors outline key psychological literature to date that has addressed the question of how trust develops in online environments. Specifically, three use cases in which trust relationships emerge are discussed: crowdfunding, online health forums, and online dating. By including examples of different types of online interaction, the authors aim to demonstrate the need for advanced security measures that ensure valid trust judgments and minimise the risk of fraud victimisation.

INTRODUCTION

As our lives transition further into the digital world, the role of trust in day-to-day interactions is transforming. Internet users are required to make judgments about others without any of the emotional and behavioural cues that would be available in a face-to-face interaction (Rocco, 1998; Cheshire, 2011; Hancock & Guillory, 2015). Where interactions involve risk, through the disclosure of personal or financial information, a need for trust in other users and systems emerges. Although the development of trusting relationships online can benefit the user, both economically and personally, anonymity and the lack of accountability on the internet (Friedman, Kahn, & Howe, 2000) mean that this trust can also be manipulated more readily.

In cases where trust is misplaced or manipulated, users can suffer both financial loss and psychological trauma, depending on the nature of the relationship. Online fraud costs the UK almost £11 billion

DOI: 10.4018/978-1-5225-4053-3.ch007

per year (Action Fraud, 2016), and often results from abuse of a user's natural inclination to trust others. Examples include the theft of money through online transactions where the item never arrives or, on a more personal level, romance fraud where a user is manipulated into sending money to a fraudster posing as a potential romantic partner in need of financial assistance. In extreme cases, misplaced trust online may lead to physical harm, for example if a user makes the decision to meet with someone from a dating website whose motives turn out to be malicious. At the same time, legitimate organisations are impeded by a lack of trust from users who are overcautious and unwilling to divulge information online (Wang & Emurian, 2005). This means that withholding trust where it is warranted can result in missed opportunities for both the user and the organisations that are losing custom (Friedman, Khan, & Howe, 2000). It is therefore crucial that an optimal balance is reached to encourage users to make effective and accurate trust judgments online.

In this chapter, the authors will consider existing models of trust behaviour alongside insights from psychology and information systems that inform our understanding of the formation of trust beliefs and influence behaviour. The chapter will go on to consider three specific online scenarios in which trust is a prerequisite to successful interaction: crowdfunding, health forums, and online dating. These three scenarios cover a range of relationship types, from business-like investments through crowdfunding platforms, to personal and intimate relationship building through online dating. The commonality between all three though is that they emphasise a current trend towards a collaborative society and economy. Moving away from a need for institutional trust, these examples emphasise the need to understand how trust dynamics work between users and how social information can influence trust. By choosing to focus on these varying scenarios, the authors hope to demonstrate the diversity of risk faced online, whilst highlighting fairly underexplored examples of peer-to-peer interactions that are rapidly becoming the cornerstone to our digital lives.

There are parallels that can be drawn between crowdfunding and more traditional e-commerce transactions online, although the lack of legal regulation around crowdfunding means that this is an inherently riskier form of transaction. As an investment, rather than purchase, the funder has no guarantee that the product or organisation will be delivered as advertised. Similarly, engagement with health forums and online dating sites may be compared to traditional chat forum conversations in that they are computer mediated interactions between strangers. However, the personal and often intimate nature of these conversations means that users are likely to divulge information that can leave them in a more vulnerable position. As such there is an even more crucial need to ensure that the information people are sharing in such scenarios online is done so in a secure manner, and only with individuals who warrant trust. The potential to manipulate trust in these scenarios will be discussed, providing an overview of the central issues to be addressed in future research and security tools that are designed to encourage secure online connectivity.

BACKGROUND

What Is Trust?

Trust is an essential construct to the maintenance of a functioning society (Rotter, 1980). Without it, friendships and relationships would not exist, whilst organisations would not be able to establish and maintain a customer following. As such, definitions of trust are widespread and vary across disciplines,

including psychology, economics, and information systems. However, across these disciplines, there is consistency in the emphasis on risk and uncertainty as underlying prerequisites for the development of trust (Cheshire, 2011). In relation to online behaviour, this risk may be created by a request to divulge personal or financial information to an unknown website, or through interaction with strangers whose intentions are unverified. An appropriate definition of trust is often dependent on the type of relationship being described, for example definitions may differ across interpersonal, societal, or systems-based interactions. One definition that encapsulates the positions taken across disciplines suggests that "trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviours of another" (Rousseau, Sitkin, Burt, & Camerer, 1998). In this sense, trust exists alongside risk, where a person accepts that the other party may or may not act in the expected manner, but believes that their intentions are good.

As well as understanding *what* trust is on a conceptual level, much research has considered *how* this develops. This is crucial to understanding situations where trust is misplaced, or when distrust in another person or system is displayed. Some propose that a disposition to trust exists as a static trait that differs between people and is maintained across contexts (Gurtman, 1992; Sorrentino, Holmes, Hanna, & Sharp, 1995). In particular, this trait is thought to encapsulate trust decisions in novel scenarios, when interacting with a stranger or when there is little additional information available to inform behaviour. Rotter (1980) suggests that a predisposition to trust builds from early childhood experiences relating to trust that result in generalised beliefs about other people and the honesty of their intentions. However, trust is a complex construct and later explanations combine this predisposition into more substantial models that take into account factors specific to a given situation, as discussed in more detail below.

Modelling Trust Behaviour

Mayer, Davis, and Schoorman (1995) provide a comprehensive model of trust with three core beliefs that are incorporated into many later definitions and explanations: ability, benevolence, and integrity. *Ability* refers to the perceived skills and knowledge of the trustee, based on available information or prior knowledge about them. If a person believes someone to be highly capable of completing the task in question, they will likely be more willing to disclose information to this person (Gillespie, 2003). *Benevolence* accounts for the extent to which a person perceives the intentions of another to be positive and good-natured. Finally, *integrity* refers to the perceived adherence to personal and moral principles on the part of the trustee. These latter two constructs are thought to influence a person's willingness to rely on the trustee, which in turn informs decisions about trust related behaviours such as co-operation and business transactions (Gillespie, 2003).

Models such as that proposed by Mayer, Davis, and Schoorman (1995), which are commonly used across the trust literature, were proposed in relation to interpersonal or organisational trust in an offline capacity, before the emergence of the internet as a platform for social interaction and e-commerce, amongst other activities. Therefore, it is necessary to consider how such explanations translate into an online environment, and whether these are in fact still applicable. The core beliefs outlined for human interaction may still hold in the online environment (Lankton & McKnight, 2011), but there are a number of additional factors to consider that may hinder trust development, such as anonymity and lack of accountability online, unknown vulnerabilities, and lack of regulations in place to provide assurance in case of harm (Friedman, Kahn, & Howe, 2000). Interactions with online systems, rather than other users, may again be considered differently. Cheshire (2011) argues that there are fundamental differences

in the mechanisms underlying interactions between humans and systems, and that in many cases the need for trust is overridden by the security assurances available online, such as privacy icons. In these cases, the uncertainty and risk that underpins the need for trust is eradicated. Although this has potential positive consequences for secure behaviour, it does limit the potential for developing on-going trusting relationships. Cheshire (2011) does conclude though that the perceived humanness of some computer systems may blur the distinction between interpersonal and systems-based interactions.

Similarly, Lankton, McKnight, and Tripp (2015) suggest that different technologies elicit a different level of perceived humanness based on the social presence and affordances of a given system. Existing trust models, such as that proposed by Mayer, Davis, and Schoorman (1995) have been adapted to reflect the differing nature of interactions between a human user and a system, compared to interacting with another human. Functionality, helpfulness, and reliability replace ability, benevolence, and integrity, as the core beliefs associated with trust behaviour (McKnight, Carter, Thatcher, & Harrison, 2011). In some cases though there may be an interaction between the two sets of beliefs, for example in social networking sites where users display trust in the platform itself, as well as in the other users they are interacting with through the site. This is demonstrated in a study looking at trust on Facebook where the two sets of belief constructs were shown to conceptually relate (ability-functionality, benevolence-helpfulness, and integrity-reliability) in a model that outperformed either distinct set of beliefs in explaining trust attribution (Lankton & McKnight, 2011).

The research discussed in this chapter demonstrates the underlying constructs that support the development of trust in both interpersonal and systems based interactions. As mentioned above, an element of risk and uncertainty is a precursor for trust, as is the case in many online interactions where we are unfamiliar with the user or organisation we are interacting with. In the scope of this chapter, the authors are interested in understanding situations where trust is misplaced and the intentions of the 'other' turn out to be malicious. In order to do this, psychological mechanisms that inform beliefs about ability, benevolence, and integrity, in turn influencing trust behaviour, are considered.

Psychological Mechanisms in Trust Behaviour Online

Trust is recognised as a fundamental construct underpinning stability within society (Rotter, 1980), yet there is a disparity of literature drawing upon the psychology underlying trust behaviour (Dunning, Anderson, Schlösser, Ehlebracht, & Fetchenhauer, 2014). However, there are a number of constructs and mechanisms from the field of psychology that show clear relevance to the development of relationships through online interaction, and which may act as pre-cursors to the trust beliefs discussed above (ability, benevolence, and integrity). These fit into two main areas: the psychology of persuasion, which considers the role of social influences in trust development; and individual differences between users, which include cognitive and personality traits that may impact trust behaviour. Each of these will be discussed in more detail below.

Psychology of Persuasion

Literature on the psychology of persuasion and social influence outlines core factors that can elicit behaviour change. Cialdini (2001) outlines six principles of influence: reciprocation, commitment and consistency, social proof, liking, authority, and scarcity. A number of these can be linked to patterns of online behaviour (Guadagno & Cialdini, 2005), and demonstrate potential vulnerabilities that might be

manipulated by fraudsters trying to deceptively gain the trust of users online for personal gain. Social proof, which provides insight on how to act in a given situation based on the behaviour of others and a desire to be liked, has been show to influence compliance online (Guadagno, Muscanell, Rice, & Roberts, 2013). Although compliance suggests only a surface-level change in behaviour, rather than a permanent attitude change (Turner, 1991), this is enough to have severe consequences for a user if they divulge security-related information as a result. Pee (2012) also demonstrated the influence of the majority in the context of social media, suggesting that the behaviour of others has a greater effect on willingness to trust in false information online than the information quality or source credibility does.

Reciprocation, another of Cialdini's principles, and one of the fundamental norms of human society, suggests an obligation to repay the good will of others. In this sense, by giving through an act of kindness, a person is assured that the recipient will return the favour at some point in the future. There is potential for this perceived obligation to be used as a bargaining tool against a person, and thus be used to manipulate behaviour. The notion of reciprocation is amplified when there is a shared sense of social identity between those involved, as the distinction between personal and group welfare is blurred (Abrams & Hogg, 2010). Shared identities often develop in online environments, and so it is possible that the notion of reciprocation could be used to persuade a user to engage unwillingly in a financial transaction as a return favour, for example, putting them at risk of fraud victimisation.

Aside from the notion of reciprocation, social identity alone may influence behaviour as a result of compliance with the norms of the group (Reynolds, Subašić, & Tindall, 2014), for fear of rejection or social out-casting. Originally developed to explore intergroup conflict and harmony (Tajfel & Turner, 1979), social identity theory is now commonly cited in understanding how group consensus on appropriate behaviour in a given situation can overcome uncertainty (Abrams & Hogg, 2010). In relation to trust, to which uncertainty is a precursor, people may rely on factors such as shared social identity to inform beliefs about ability and integrity during an interaction. There is a consensus that people have multiple social identities, and a specific context will influence which of these prevails (Turner, Hogg, Oakes, Reicher, & Wetherell, 1987). In addition, Goffman (1959) likens social identity to a theatrical performance, whereby the audience in a given scenario influences the character portrayed. In line with social proof, social identity theory implies that behaviour and beliefs are influenced by the actions and expectations of others, in particular those with whom we share a common identity. This human inclination to comply with the norms of a group may be used to manipulate behaviour by making a person feel obligated to act in a given way or divulge certain information that they may not otherwise do.

Within the context of a social group with a shared identity, a set of norms is established that orient the behaviour of group members (Neville, 2015). These arise through interaction and relationship building within the group (Turner, 1991), and often result from a compromise between the personal or alternate social norms of those in the group. Although there is some speculation on the exact process by which norms influence behaviour change (Reynolds, Subašić, & Tindall, 2014), it is acknowledged that social identity and norms interact to govern how a person should feel and act in a given situation (Turner et al., 1987). For example, a person who identifies as a football supporter may act in a rowdy manner at a match, but they would be unlikely to act this way in the workplace, where instead they adopt the identity of a reliable employee. There has also been some speculation on the motivations of compliance with social norms, with some arguing that this is purely a tactic employed to enhance personal self-image and give the impression of a moral lifestyle (Krueger, Massey, & DiDonato, 2008). Alternate research though has demonstrated that the adoption of social norms and associated group identity can result in long-term attitude change (Newcomb, 1943). Despite their importance in maintaining an orderly society

(Turner, 1991), social norms have been shown to lead to an excess of trust, which has clear consequences in light of cyber security threats, such as those associated with the example scenarios that are discussed later in this chapter. One example of such an impact comes from a study on privacy concerns in social networking sites, which demonstrated that perception of social norms about what data should be visible to others influenced security behaviour (Utz & Krämer, 2009). Dunning et al. (2014) suggest that fear of the negative consequences associated with disobeying social norms, such as guilt and anxiety, can lead people to comply and behave in ways that leave them vulnerable to the malicious intentions of others through unwarranted trust.

Individual Differences

Alternative accounts of behaviour online suggest that individual differences between users may be influential. Although the empirical evidence to support this is less convincing than that of social identity and social norms theories, it should be noted none the less in providing a comprehensive overview of the perspectives that psychology offers. In the broad context of trust behaviour, gender studies show that men are more trusting than women (Buchan, Croson, & Solnick, 2008), whilst women are viewed as more trustworthy (Dollar et al., 2001). Whilst these findings are replicated in relation to online shopping behaviour (Garbarino & Strahilevitz, 2004; Van Slyke, Comunale, & Belanger, 2002), the authors are unaware of any evidence to indicate that this is the case in online interpersonal interactions such as those described later in the chapter. That is not to say that these differences do not exist, simply that there is a dearth in literature to support this currently. Similarly, whilst there is a common conception that older users are more vulnerable online, the evidence for this is not clear cut, and in any case research in relation to the examples outlined below is lacking.

Kaptein and Eckles (2012) report findings that the success of persuasion techniques in an online context can be partially explained by individual differences in personality constructs, such as the need for cognition (i.e. the inclination to engage more rational cognitive processing techniques), and that this was consistent across multiple trials. In this sense, they propose that these differences are static rather than transient traits, and imply that some users are more susceptible to persuasion than others. The exact individual differences are not outlined though, and instead a broad heterogeneity in response between users is reported. More research would be necessary to establish if there are specific constructs that influence response to persuasion techniques in order to understand the nature and implications of these findings.

The notion of individual differences does link with a disposition to trust, discussed above, which may act as a static trait between users making some more likely to trust than others. Roghanizad and Neufeld (2015) on the other hand propose that trust behaviour is situation specific. This work taps in to dual-process theories of reasoning, which suggest that individual differences (Kyllonen & Christal, 1990; Markovits, Doyon, & Simoneau, 2002) or situational factors (Stanovich, 1999; Kahneman, 2000; Evans, 2003) might influence engagement in either rational or intuitive processing. When processing rationally, a person takes in all aspects of the information available to them in order to make an informed decision about how to behave or respond. Intuitive responses on the other hand rely on surface level information and pre-existing heuristics. When faced with risk, such as the requirement to disclose personal information online, Roghanizad and Neufeld (2015) propose that users rely on intuitive responses rather than engaging in rational contemplation about the trustworthiness of a given website or user.

The mechanisms discussed in this section have all been shown to influence behaviour in social situations, and by analogy relate to how users interact with one another online, and how relationships develop. Decisions surrounding the three beliefs associated with trust behaviour (ability, benevolence, and integrity) are likely to be informed by these mechanisms. By outlining the factors that influence and inform trust decisions and behaviour, the authors are also highlighting a number of vulnerabilities that might be used to manipulate impressions of trustworthiness made in an online environment, and thus deceive a user by eliciting trust where it is not warranted. This provides insight when considering fraud victimisation, and demonstrates core considerations in the development of tools to tackle cyber security issues surrounding human vulnerability.

Information Systems Approaches to Trust Behaviour Online

Although this chapter will focus predominantly on the human factors influencing the development of trust between users, it is worth also mentioning a complimentary approach, which considers the relationship between the user and the system they are engaging with. In both unidirectional and bidirectional interactions online, the platform on which these take place can have an important role in how the user perceives the trustworthiness of a site, but also of the other users that they might interact with on that site. Lindgaard, Fernandes, Dudek, and Brown (2006) suggest that people form an opinion about the visual appeal of a website within the first 50ms, and this may have a crucial impact on perceived trustworthiness (Lindgaard, Dudek, Sen, Sumegi, & Noonan, 2011). Factors such as errors making the site look unprofessional, the colour scheme adopted (Cyr, Head, & Larios, 2010), and the design of the site can have a crucial impact. The influence of these systems-based factors may depend on the type of site though, with ease of navigation viewed as important to informational sites (including online communities) whilst the presence and strength of brand placement is deemed more influential on sites with which the user is highly invested, such as financial services (Bart, Shankar, Sultan, & Urban, 2005).

Security assurances are regularly incorporated within web pages, although empirical data on the value of these is varied, with some suggesting that these have a positive impact on trust development (Odom, Kumar, & Saunders, 2002; Rifon, LaRose, & Choi, 2005; Wu, Hu, & Wu, 2010), whilst others report no effect (Hui, Teo, & Lee, 2007; McKnight, Kacmar, & Choudhury, 2004). The presence of security cues may contribute to the normative appearance of a website though, and in turn reflect whether information is presented as the user would expect it to be. This expectation of normality can act as a precursor to trusting beliefs about the authenticity of a web site (Li, Hess, & Valacich, 2008). The impact of these assurance cues may also be dependent of the level of risk involved in the interaction, with objective assessments such as these playing more of a role in trust development under low risk (Raghanizad & Neufeld, 2015).

Contrary to Cheshire's (2011) opinion that trust cannot exist between a human and a system, this research suggests that the assurances provided by the presence or absence of certain cues on a website can provide insight at least into the initial trustworthiness of an organisation or group. However, the development of ongoing relationships is reliant on more than this. In combination with interpersonal trust, these approaches seem to work together in explaining how users can decide which sites/platforms to interact with. They may then engage only with those perceived most trustworthy to develop on going relationships and interactions, which most often become reliant on interpersonal trust to succeed long term.

APPLIED ONLINE SCENARIOS

In this section, the authors explore the existing literature around user decision-making across three different example scenarios. As discussed above, these examples provide insight into a range of interaction types, from the business-like transaction of crowdfunding investment, to the intimate relationship building through online dating platforms. These highlight interesting new areas of interest in terms of trust in peer-to-peer interactions, which have perhaps been less extensively explored than more traditional business-to-peer scenarios such as e-commerce. It is hoped that this section highlights the valuable opportunities, and need to consider these three scenarios in the design of security solutions to protect users.

Crowdfunding

Crowdfunding acts as an alternative source of funding for small businesses that may be unable to gain financial backing through traditional means, such as bank loans and venture capital (Gerber & Hui, 2013). This inability to attain backing is often due to poor financial history, or simply because the business is new and therefore does not have the financial record to warrant support from corporate investors (Song & van Boeschoten, 2015). Crowdfunding platforms, such as Kickstarter and IndieGoGo, allow creators and business owners to design a campaign and collect money through small pledges made by funders. Two common models of crowdfunding are outlined here, although it should be recognised that these are not the only models in existence – with others including peer-to-peer lending, and charitable donations. The first to be discussed though – *reward-based* – generally generates smaller pledges, and provides funders with some form of non-monetary reward for their contribution (Belleflamme & Lambert, 2014; Lukkarinen, Teich, Wallenius, & Wallenius, 2016). Rewards range from an acknowledgement in the credits of a film being produced from the funding, to a discounted pre-order version of a product being launched as a result of the campaign (Mollick, 2014). The second model to consider is *equity-based*, whereby funders receive partial equity in the business they are supporting, and as such their contribution is acknowledged through on-going financial recuperation (Rakesh, Choo, & Reddy, 2015; Beier & Wagner, 2016). In addition to different campaign models, there are also two distinct investment structures for crowdfunding (as described in Gerber, Hui, & Kuo, 2012). The 'all-or-nothing' approach, adopted by Kickstarter, means that if a project does not reach its funding target, the investments are returned to the funders. The alternative is the 'all-and-more' approach, as employed by IndieGoGo, whereby the creator receives all of the contributions given to the campaign, regardless of whether the target sum is reached. The nature of these approaches means that 'all-or-more' generates higher risk for the funder, as they may lose their money and not receive any form of reward, financial or otherwise, if the project does not progress due to lack of funding.

The alternative forms of fundraising elicit differing theoretical approaches in terms of considering funder motivations and decisions to support a campaign, and as such, to place trust in the creator. Uncertainty and risk are at the core of participation in crowdfunding, given the lack of legal regulation in place, meaning that there is no guarantee a product will be delivered, or promise of financial security if a business fails to succeed (Kim, Shaw, Zhang, & Gerber, 2017). Although the lack of regulation is consistent across all types of crowdfunding, this has greater consequences in equity-based investments, as funders often put forward larger sums of money, and are reliant on the ongoing success of a business. As well as cases where the creators successfully launch a product, but this is not well received by the public, there are also situations where creators may be fraudulently collecting money, with no intention

of giving back to the funders. These creators develop a misleading campaign, collecting money from funders for a non-existent concept or business. Given the evident risk factors and uncertainty involved in crowdfunding, it is important to understand how funders make decisions about which projects to support, in order to reduce risk of financial loss and potential fraud victimisation.

Aside from the financial benefits, creators on crowdfunding platforms report being motivated by the increased awareness they raise for their product or business, the community that develops from the support of numerous funders sharing their knowledge and experience, and the ability to maintain control over their business. For the funders, key motivators across campaign types include a sense of online philanthropy and becoming part of a community of supporters. On the other hand, participation is deterred by a lack of trust in how the creators will spend the money, as well as the potential downfalls in success as a result of creators' limited business experience (Gerber & Hui, 2013).

A majority of the research in the field of crowdfunding has focused on investment patterns and trends in the success of campaigns. Within reward-based campaigns, there is a trend for an inverted bell curve pattern of funding behaviour, whereby support peaks at the beginning of the campaign and rapidly declines until the deadline approaches, when a surge in funding activity occurs in successful campaigns (Kuppuswamy & Bayus, 2013; Beier & Wagner, 2016; Agrawal, Catalini, & Goldfarb, 2014). The initial peak in funding at the early stages of the campaign often comes from friends and family of the creator (Horvát, Uparna, & Uzzi, 2015), which is evidenced by geographical patterns in the location of funders (Agrawal, Goldfarb, & Catalini, 2011). Although funding from friends and family is not of interest here, given our aim of understanding how trust develops between strangers, it *is* of interest that this initial peak in funding is shown to predict overall campaign success, by encouraging additional funders in the latter stages (Colombo, Franzoni, & Rossi-Lamastra, 2015). The lull in funding activity in the central period may be explained by a diffusion of responsibility, whereby funders are less inclined to support the project as it already has support, so they make an assumption that other investors will continue to contribute (Kuppuswamy & Bayus, 2013; Fischer et al., 2011). The increase in activity as a project nears its closing date may indicate a deadline effect, something which has been acknowledged by researchers considering bidding in online auctions (Ariely & Simonson, 2003). Alternative explanations consider that risk averse funders wait until later in the campaign as they can identify whether a project will meet its funding target (Beier & Wagner, 2016), or that funders feel contributions at this stage are more meaningful, as they are pushing the campaign closer to its target, enhancing the philanthropic nature of their support (Kuppuswamy & Bayus, 2017).

Equity-based campaigns demonstrate a different pattern of support, with evidence of herding behaviour amongst investors (Kuppuswamy & Bayus, 2013). The behaviour of other investors is considered information assurance, on the assumption that if others are doing something, it must be the rational thing to do (Cialdini, 2001). In peer-to-peer lending platforms, where peers fund each other on a loan basis and the money is repaid with interest, a similar pattern is seen, with investors basing decisions on those who have already contributed, in place of more traditional cues such as the credit rating score of the creator (Zhang & Lui, 2012). In particular, research has demonstrated that the identity of early investors as experts in product development or financial investment encourages less-expert funders to contribute at a later stage (Kim & Viswanathan, 2014). This is supported by Burtch, Ghose, and Wattal (2016), who demonstrated that masking the identity of the earlier funders, and the amounts given, made others less inclined to contribute to the campaign. This behaviour indicates a reliance on social proof, with funders basing decisions on the behaviour of other funders, in both types of crowdfunding and links in with the principles of persuasion outlined above (Cialdini, 2001). Herding behaviour may leave

funders at risk of fraud (Kuppuswamy & Bayus, 2013), as their funding decisions are being motivated by the behaviour of others (information about which may have been falsified; Wessel, Thies, & Benlian, 2016) rather than on the merit of the campaign itself. In extreme cases, where creators may have used fake accounts to exaggerate the apparent support for their campaign, funders may be falsely drawn into believing the worth of the project, and as such leave themselves in a vulnerable position if this is not successful. As mentioned earlier, a lack of legal regulation surrounding crowdfunding and the limited resolution resources available from crowdfunding platforms themselves make this an even greater risk.

Aside from the funding patterns observed most commonly in crowdfunding, researchers have considered alternative factors that may also influence funding behaviour, many of which relate to the social engagement of the creator. As a campaign progresses, funding is increased when the creator provides valuable updates (Hornuf & Schwienbacher, 2015; Kuppuswamy & Bayus, 2013), reassuring a potential funder that the project is progressing, and the creator is engaged in the fundraising process. In equity-based crowdfunding, project updates are particularly influential when they relate to new business developments and information about additional promotional campaigns being run by the creator (Block, Hornuf, & Moritz, 2016). Openness about prior financial history (Lukkarinen, Teich, Wallenius, & Wallenius, 2016) and linking social media accounts (Vismara, 2016) also encourages funders, as they likely feel that the creator has nothing to hide. In addition, the availability of social media information may elicit support through funders who feel they have a shared social identity with the creator (Kromidha & Robson, 2016). This openness to share as much information as possible with potential funders and demonstrate a robust social identity may also act as a reassurance that the creator did not just set up an account yesterday for the purpose of fraudulently gathering money. The extent and mechanisms by which wider online behaviour elicits trust in a creator is yet to be explored in the academic literature though.

A reliance on social information is further demonstrated through the influence of prior social capital gained on the crowdfunding platform. Creators who have established social capital through funding prior projects, completing successful projects in the past, and contributing to the crowdfunding community are more likely to receive funding in the early stages of a project, and more likely to reach their funding target (Colombo, Franzoni, & Rossi-Lamastra, 2014; Zvilichovsky, Inbar, & Barzilay, 2015). This demonstrates the importance of reciprocation (Cialdini, 2001) to trust behaviour in crowdfunding. Prior behaviour on the platform generates a community spirit amongst funders and creators, which often crosses over to external social networking sites (Skirnevskiy, Bendig, & Brettel, 2017; Rakesh, Choo, & Reddy, 2015). The positive impact of this on campaign success seems to link to social identity theory, discussed earlier, whereby a shared identity as a fellow crowdfunder or successful creator, encourages the development of trusting relationships between platform users.

However, there is potential for a fraudster to manipulate this reliance on social identity in order to attract funders to a campaign. By giving a sense of community and shared identity through the information published via the campaign, trust may develop under false pretences. Additional social information may be manipulated to attract further funders, as demonstrated by Wessel, Thies, and Benlian (2016) who report that 1.6 per cent of campaigns analysed incorporated a faked Facebook 'like' count. The effect of this fake information was an initial spike in funding, followed by a sharp decline, which was put down to the lack of actual social media coverage for the campaign, as the majority of this was faked, so genuine distribution was minimal. In an 'all-or-more' campaign, this means that initial investors who were tricked by fake social information will lose their money due to the consequential lack of funding later in the campaign. Although the intentions of the creator in this case may not be fraudulent, misleading

the funder through false information remains unethical and highlights additional concerns for funders to consider when they are making decisions about campaign funding.

In outlining the key motivators and influential factors for crowdfunding campaigns, this section also highlights mechanisms that might be manipulated by a fraudster to elicit trust from a potential funder and falsely encourage their participation. Social behaviours, such as herding and reliance on demonstration of shared identity as an indicator of trustworthiness, leave the funder vulnerable. The lack of quality cues available to funders, when a product is yet to be manufactured and a business is in its infancy, makes it difficult to engage rational decision-making. This emphasises a need for solutions that provide validated assurances about creator legitimacy to encourage secure online behaviour and reduce fraud victimisation in this domain.

Health Forums

Engagement with online health information continues to increase, with estimates of between 50 (Office for National Statistics, 2016) and 70 (Gandhi, & Wang, 2015) per cent of people using the internet as a source of medical advice in 2015-16. One element of the search for information online involves connecting with online health forums, where users come together to discuss their own personal experiences (Rozmovits, & Ziebland, 2004; Zhao, Abrahamson, Anderson, Ha, & Widdows, 2013), to develop friendships (Leitner, Wolkerstorfer, & Tscheligi, 2008), and form support networks with others experiencing the same health issues (Kummervold et al., 2002; Zhao et al., 2013). The internet provides an opportunity for forum users to anonymously disclose information that they might otherwise be too embarrassed to share (Jones et al., 2011; Coulson, 2005; Kummervold et al., 2002). Such interactions can lead to reduced fear and isolation (Rozmovits, & Ziebland, 2004), and a more effective adaptive response to diagnosis that has in some cases improved patient quality of life as well as increasing survival time (Coulson, 2005). At the same time, reports demonstrate that users of online health information still have a higher level of trust in medical professionals than they do in online information (Li, James, & McKibben, 2016), suggesting that they are not influenced solely by the subjective contributions of other users.

On the other hand, there are two core concerns associated with forum use that will be discussed here: the quality of information provided in these, and the authenticity of the group members engaging in conversation. Although there is evidence that overall, users still trust medical advice from their doctors, this is not to say that the contributions of forum users do not also have some level of influence. There are movements in existence that have formed and continue to be promoted through online groups that actually advise against common medical practise. For example, the 'pro-anorexia' movement that supports the disease, and discourages recovery efforts (Fox, Ward, & O'Rourke, 2005), or a network of chronic fatigue sufferers who promote rest and inactivity, contrary to typical medical advice (Wright, Partridge, & Williams, 2000). The social power behind such movements poses a risk to the health of those that become invested in it, if they are following advice based on social proof from peers, rather than scientific evidence.

Anonymity in online forums is viewed by many as a positive factor, allowing users to disclose information more freely without being embarrassed. However, this also makes it more difficult to assess the credibility of another user (Lederman, Fan, Smith, & Chang, 2014), with a lack of verifiable social information to base this judgment on. Without any measures in place to validate the medical information provided, users may be left reliant on inaccurate advice that in extreme cases may be dangerous to their health (Coulson, 2005; Sudau et al., 2014). Sudau and colleagues (2014) conducted analyses on user

posts from a Multiple Sclerosis forum online to establish the quality of external links provided. This demonstrated that across 8628 posts analysed, only 31 contained links to scientific publication about the topic in question, whilst 2829 contained links to social media sources, such as YouTube and Facebook. This reliance on unverified and subjective information, especially in relation to health information with many users suffering from serious illnesses, raises concern for the risks associated with engaging in online health forums.

In order to reach a stage where the benefits outweigh the potential costs in these forums, some have called for systems to be put in place that can verify the claims made by other users (Lederman, Fan, Smith, & Chang, 2014) or allow for authentication of another user's credibility to provide information through mutual rating systems (Zhao, Ha, & Widdows, 2013). Alongside the risk of misinformation being communicated amongst forum users, there is a threat of emotional exploitation in cases where fraudulent accounts are used to spread fake stories (Lederman, Fan, Smith, & Chang, 2014). Cases of Munchausen's by Internet are well reported, whereby somebody extensively researches the symptoms and associated consequences of a condition, in order to give a convincing fake account of being a sufferer in an online forum (Feldman, 2000). The motivations behind this are not transparent, but a lot of the time this seems to stem from a desire for attention. Regardless of the intention, the consequences of such behaviour can damage the trusting relationships between members of a forum group. Once one person is outed as being a liar, the bond between other members rapidly declines, as they no longer know who to believe (Pulman & Taylor, 2012). This type of trolling behaviour is also used to provoke emotional arguments between users, as another way of disrupting the group dynamic. There are reported cases of users abusing such forum groups for financial gain as well, generating donation from sympathetic others. In order to address the issues highlighted here and ensure that users are able to safely engage with health forums online, the authors note that understanding how these communities develop and the factors that lead users to disclose personal information or act on advice that may put them at risk is important.

The sense of trust that often develops between users within patient communities can lead relationships to progress from anonymous interactions to the disclosure of personal information. This can leave the user vulnerable to a number of security threats, predominantly identity theft, and endanger their personal safety as a result if details such as location are disclosed. Ongoing interactions rely on continued exchange of such information though, and can lead users to share more information than they possibly should, in an effort to maintain the relationship. In order to prevent trust being misplaced and confidential information disclosed as a result, it is important to understand where this trust originates from in the development of communities. As mentioned above, anonymity online makes it difficult for users to assess the credibility of those providing information. However, users are often reliant on warrants, such as the quality of source information and evidence of a user's credentials to provide assurance for the trustworthiness of the person posting content, and the information provided (Richardson, 2003; Mun, Yoon, Davis, & Lee, 2013). Trust can also be influenced by the response rates of a user, with research suggesting that the more regularly a person posts in the group, the more trustworthy they are perceived (Ridings, Gefen, & Arinze, 2002). Once trust has been established, this then positively predicts the development of empathic relationships and likelihood that a user will share health information and their own personal experiences, and take on board that of others within the community (Zhao, Abrahamson, Anderson, Ha, & Widdows, 2013).

The development of empathy between users in online health forums may also be predicted by the presence of a shared social identity (Zhao, Ha, & Widdows, 2013; Zhao et al., 2013). Given the importance of personal experiences and ability to exchange knowledge, users report feeling a connection

with those who are similar to them (Sillence & Briggs, 2015), with 41% of Americans who seek online health information reporting that they wanted to interact with someone like them (Fox & Jones, 2009). There is little research considering the specific aspects of social identity that users wish to relate to in the context of health forums and communities. In many scenarios it may be the case that the similarity extends no further than suffering from the same condtiion, but this is an interesting avenue for further exploration. Before engaging with a community, potential new users may utilise archived forum discussions to establish whether they share the same basic norms and beliefs as the community (Erickson, 1997).

In line with the other use cases outlined here, there is a clear link between the development of trusting relationships and social identity, which in turn can lead to increased information sharing and potential vulnerability, when anonymous community members turn out to be malicious. Other factors, such as reciprocation, may also influence behaviour within the forum. For example, if a user has received useful advice, they may feel the need to repay the favour, say if someone is raising money for treatment. In situations like this, there is potential for the strong bonds created between users to be manipulated by a fraudster. This highlights an on-going challenge to detect malicious intentions within group members, thus protecting other users from harm, but whilst also attempting to maintain the trust dynamic that benefits so many users on a day-to-day basis.

Online Dating

The use of online dating sites is now the second most common way to meet a new partner, preceded only by introduction through friends (Hagen-Rochester, 2012). Recent statistics suggest that around 40% of Americans use online dating, with 7% of marriages in 2015 resulting from relationships started through this medium (Thottam, 2017). The stigma associated with online dating is also decreasing, with a 15% increase between 2005 and 2013 in the number of people who view it as a good way to meet new people and potential partners (Thottam, 2017). Although these data come from one of the largest dating sites (www.eHarmony.com), and thus might be biased, acceptance of online dating is evident in daily society, with people talking more openly about their experiences. These sites provide unique opportunities, allowing people who may never previously have crossed paths to meet one another, and also allowing interaction in a novel social environment (Whitty, 2008), which may benefit certain users, for example those who are more introverted. Although users of traditional online dating sites find it difficult to judge personality over the internet (Zytko, Freeman, Grandhi, Herring, & Jones, 2015), chatting socially online has been shown to elicit similar levels of trust as a face-to-face meeting (Zheng, Veinott, Bos, Olson, & Olson, 2002). As such, the extent to which trust builds through dating sites may be considered comparable to that established in an offline meeting.

However, as with most interactions online, there are risks involved with online dating. The most heavily reported in research is the misrepresentation of personal attributes, such as weight and height statistics. Over half of online daters report feeling that someone they interacted with has seriously misrepresented themselves in their profile (Smith & Duggan, 2013). It seems that women are more prolific liars in this sense than men (Lo, Hsieh, & Chiu, 2013), and that this most often involves misrepresentation of physical appearance, whilst men more often misrepresent information about marital status, relationship goals, and height (Schmitz, Zillmann, & Blossfeld, 2013). As a result, many users report that they are concerned with the veracity of information given on a dating profile (Norcie, de Cristofaro, & Bellotti, 2013; Couch, Liamputtong, & Pitts, 2012). These misrepresentations often relate to minor, and seemingly superficial, concerns that the user may be exaggerating in order to attract a partner. While this may

cause confusion or annoyance when meeting the person offline for the first time, the long-term impact is likely to be minimal. In some cases this falsification can be taken to the extreme though, with the use of photos and information taken from another person's profile to intentionally deceive another. Also know as 'catfishing', this behaviour usually stems from a lack of self-confidence and desire to portray a more attractive individual, or from a malicious motive to take revenge on someone by convincing them of a potential love interest, only to humiliate them later on.

There are also many cases of financial loss in relation to online dating though, with £39 million lost to online romance fraud in the UK alone in 2016 (Cacciottolo & Rees, 2017). This is an occurrence that is becoming increasingly common, with an increase of 33% in the number of instances reported between 2013 and 2014 (Action Fraud, 2015). In cases of fraud, the criminals will engage with a potential partner and develop a relationship with them, often declaring love early on in the encounter. They then progress to procure money from the victim, often with a cover story of a personal crisis or a lack of money to visit the partner. In some cases, victimisation can progress to sexual abuse, where the user is persuaded to engage in cyber sexual activities, such as sending naked photographs to the fraudster. This can leave them in a vulnerable position, if they have sent sensitive media to the perpetrator that can then be used against them (Whitty, 2015). One possible consequence is blackmail, which may lead not only to financial loss on the part of the victim, but also to emotional trauma. This emotional distress is seen to be more prominent with those who are particularly lonely (Buchanan & Whitty, 2014).

There are also risks involved at the point when relationships are taken offline and users agree to meet for the first time. Users themselves report feeling concern surrounding sexual risk (such as unplanned pregnancy, sexually transmitted diseases, and violence), emotional trauma, and the risk of encountering dangerous individuals when meeting up offline (Couch, Liamputtong, & Pitts, 2012). Although it is difficult to authenticate the attributes a user reports on their profile without meeting them offline (Zykto et al., 2015), a user is putting their personal safety at risk by choosing to do this. It is therefore essential for research to progress from considering how users misrepresent superficial information such as their height and income data, to focus on methods for combatting malicious behaviour. This could help to reduce instances of misplaced trust that result in financial fraud or physical abuse.

There are some newly developed apps that are designed to provide assurance about a user's identity before any interpersonal interaction has even begun. For example, Tinder requires users to login through Facebook as a way to authenticate identity. However, whilst this allows for common interests and mutual friends to be used as an indication of a shared normative identity (Duguay, 2017), there is potential for this to be manipulated, as a user can generate a fake Facebook account in the moment to access Tinder. An alternative example, Happn (https://www.happn.com/), uses location features to monitor the number of times you have crossed physical paths with a user, and showing the last location where this occurred. Users report that this gives them a perception of similarity with the other user, if they spend a lot of time going to the same types of places (Ma, Sun, & Naaman, 2017). In a sense, this demonstrates the importance of a shared social identity between two users before they have even begun to interact. So, it is apparent that across these apps there are elements of shared identity that influence the decision-making process at the point where the user is deciding whether to engage with a potential partner.

At the point where two users begin to interact, there are a number of additional uncertainty reduction strategies that may be employed to assess the trustworthiness of a potential partner. Users report asking specific questions, checking consistency in information across conversations, and even Googling the information that another user gives about themselves (Gibbs, Ellison, & Lai, 2011). Engagement with these types of strategic assessments is predicted by how concerned a user is about three issues: their

personal safety, the likelihood of another user providing misrepresentative information, and fear of recognition by people they know (Gibbs, Ellison, & Lai, 2011). Further to this, concern about issues such as personal safety may depend upon the user's motivation for using the dating site in the first place. For example, Lutz and Ranzini (2017) report that Tinder users who are only interested in casual hook-ups are likely to be less concerned about their personal safety than users who are looking for friendship, or self-validation. This highlights not only a need to consider how security tools might help to protect the user, but also how to educate users of the need to conduct such due diligence in the realm of online dating.

Unlike the other use cases outlined here, the development of trust in online dating has a greater likelihood of progressing a relationship to the offline world, where the couple make the decision to meet in person. The addition of physical risk to the user and their wellbeing accentuates the need for accurate trust judgments to be made within the context of online dating. Whilst individual uncertainty reduction strategies go some way to reducing this threat, these are still subjective judgments for the most part and do not by any means provide a fool proof mechanism for the user to ensure the interactions and behaviour they engage in are secure. The research to date indicates a level of naivety in some users who are confident in meeting strangers without consideration of the risks. On the other hand, it highlights a number of users who want to gather further information as reassurance, but are reliant on Google or social media, where there is a distinct lack of due diligence provided from the dating platforms themselves.

CONCLUSION

In this chapter, the authors have highlighted the importance of accurate trust judgements in online interactions. Across the three example scenarios outlined, there are evident security threats that exist as a result of trust being misplaced or manipulated during interpersonal interactions with strangers. This supports the need to understand the underlying mechanisms that elicit such trust. As more and more day-to-day activities begin to transition into the digital world, the opportunities for malicious users to take advantage of the human inclination to trust others will only escalate. Statistics show year on year that instances of cybercrime and online fraud are increasing, with an 8% increase seen in 2016 (BBC News, 2017).

Whilst insights from existing theoretical perspectives provide some initial steps towards understanding trust in online contexts, it is evident that there is a need for much more comprehensive and explicit research in this area. Research has begun to demonstrate the importance of social psychological factors across the use cases outlined, including identity and shared norms. Human interaction is at the core of many online activities, in addition to those discussed, and it is therefore crucial that user-centric security tools are designed to address the existing vulnerabilities experienced by users. A solid theoretical grounding to explain how relationships develop through interaction across a range of online contexts would provide the building blocks that are necessary to enhance secure connectivity online and take important steps towards tackling the threats faced in an ever more digital age.

ACKNOWLEDGMENT

This research was supported by the EPSRC [grant reference: EP/N02799X/1].

REFERENCES

Abrams, D., & Hogg, M. A. (2010). Social identity and self categorization. In J. F. Dovidio, M. Hewstone, P. Glick, & V. M. Esses (Eds.), *The Sage handbook of prejudice, stereotyping and discrimination* (pp. 179–193). London: Sage. doi:10.4135/9781446200919.n11

Action Fraud. (2015). *Figures show online dating fraud is up by 33% last year*. Retrieved May 7, 2017, from http://www.actionfraud.police.uk/news/new-figures-show-online-dating-fraud-is-up-by-33per-cent-last-year-feb15

Action Fraud. (2016). *Fraud & cybercrime cost UK nearly £11bn in past year*. Retrieved May 5, 2017, from http://www.actionfraud.police.uk/news/fraud-and-cybercrime-cost-UK-nearly-11bn-in-past-year-oct16

Agrawal, A., Catalini, C., & Goldfarb, A. (2011). The geography of crowdfunding. *SSRN Electronic Journal.* Retrieved May 18, 2017, from http://ssrn.com/abstract=1692661

Agrawal, A., Catalini, C., & Goldfarb, A. (2014). Some simple economics of crowdfunding. *Innovation Policy and the Economy*, *14*(1), 63–97. doi:10.1086/674021

Ariely, D., & Simonson, I. (2003). Buying, bidding, playing, or competing? Value assessment and decision dynamics in online auctions. *Journal of Consumer Psychology*, *13*(1-2), 113–123. doi:10.1207/S15327663JCP13-1&2_10

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, *69*(4), 133–152. doi:10.1509/jmkg.2005.69.4.133

BBC News. (2017). *Cybercrime and fraud scales revealed in annual figures*. Retrieved May 11, 2017, from http://www.bbc.co.uk/news/uk-38675683

Beier, M., & Wagner, K. (2016). User Behavior in Crowdfunding Platforms--Exploratory Evidence from Switzerland. In *Proceedings from 49th Hawaii International Conference on System Sciences*. IEEE. doi:10.1109/HICSS.2016.448

Belleflamme, P., & Lambert, T. (2014). Crowdfunding: Some Empirical Findings and Microeconomic Underpinnings. *SSRN Electronic Journal*. Retrieved May 21, 2017, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437786

Block, J. H., Hornuf, L., & Moritz, A. (2016). Which updates during an equity crowdfunding campaign increase crowd participation? *SSRN Electronic Journal.* Retrieved June 1, 2017, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2781715

Buchan, N. R., Croson, R. T. A., & Solnick, S. (2008). Trust and gender: An examination of behavior and beliefs in the Investment Game. *Journal of Economic Behavior & Organization*, *68*(3-4), 466–476. doi:10.1016/j.jebo.2007.10.006

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283. doi:10.1080/1068316X.2013.772180

Burtch, G., Ghose, A., & Wattal, S. (2016). Secret Admirers: An Empirical Examination of Information Hiding and Contribution Dynamics in Online Crowdfunding. *Information Systems Research*, *27*(3), 478–496. doi:10.1287/isre.2016.0642

Cacciottolo, M., & Rees, N. (2017). Online dating fraud victim numbers at record high. *BBC News*. Retrieved May 5, 2017, from http://www.bbc.co.uk/news/uk-38678089

Cheshire, C. (2011). Online trust, trustworthiness, or assurance? *Daedalus*, *140*(4), 49–58. doi:10.1162/DAED_a_00114 PMID:22167913

Cialdini, R. B. (2001). The science of persuasion. *Scientific American*, *284*(2), 76–81. doi:10.1038/scientificamerican0201-76 PMID:11285825

Colombo, M. G., Franzoni, C., & Rossi-Lamastra, C. (2015). Internal social capital and the attraction of early contributions in crowdfunding. *Entrepreneurship Theory and Practice*, *39*(1), 75–100. doi:10.1111/etap.12118

Couch, D., Liamputtong, P., & Pitts, M. (2012). What are the real and perceived risks and dangers of online dating? Perspectives from online daters: Health risks in the media. *Health Risk & Society*, *14*(7-8), 697–714. doi:10.1080/13698575.2012.720964

Coulson, N. S. (2005). Receiving social support online: An analysis of a computer-mediated support group for individuals living with irritable bowel syndrome. *Cyberpsychology & Behavior*, *8*(6), 580–584. doi:10.1089/cpb.2005.8.580 PMID:16332169

Cyr, D., Head, M., & Larios, H. (2010). Colour appeal in website design within and across cultures: A multi-method evaluation. *International Journal of Human-Computer Studies*, *68*(1), 1–21. doi:10.1016/j.ijhcs.2009.08.005

Dollar, D., Fisman, R., & Gatti, R. (2001). Are women really the 'fairer' sex? Corruption and women in Government. *Journal of Economic Behavior & Organization*, *46*(4), 423–429. doi:10.1016/S0167-2681(01)00169-X

Duguay, S. (2017). Dressing up Tinderella: Interrogating authenticity claims on the mobile dating app Tinder. *Information Communication and Society*, *20*(3), 351–367. doi:10.1080/1369118X.2016.1168471

Dunning, D., Anderson, J. E., Schlösser, T., Ehlebracht, D., & Fetchenhauer, D. (2014). Trust at zero acquaintance: More a matter of respect than expectation of reward. *Journal of Personality and Social Psychology*, *107*(1), 122–141. doi:10.1037/a0036673 PMID:24819869

Erickson, T. (1997). Social interaction on the net: Virtual community as participatory genre. In *Proceedings of the Thirtieth Hawaii International Conference on System Sciences* (Vol. 6, pp. 13-21). IEEE. doi:10.1109/HICSS.1997.665480

Evans, J. B. T. (2003). In two minds: Dual-process accounts of reasoning. *Trends in Cognitive Sciences*, *7*(10), 454–459. doi:10.1016/j.tics.2003.08.012 PMID:14550493

Feldman, M. D. (2000). Munchausen by internet: Detecting factitious illness and crisis on the Internet. *Southern Medical Journal*, *93*(7), 669–672. doi:10.1097/00007611-200007000-00005 PMID:10923952

Fischer, P., Krueger, J. I., Greitemeyer, T., Vogrincic, C., Kastenmüller, A., Frey, D., & Kainbacher, M. (2011). The bystander-effect: A meta-analytic review on bystander intervention in dangerous and non-dangerous emergencies. *Psychological Bulletin*, *137*(4), 517–537. doi:10.1037/a0023304 PMID:21534650

Fox, N., Ward, K., & O'Rourke, A. (2005). Pro-anorexia, weight-loss drugs and the internet: An "anti-recovery" explanatory model of anorexia. *Sociology of Health & Illness*, *27*(7), 944–971. doi:10.1111/j.1467-9566.2005.00465.x PMID:16313524

Fox, S., & Jones, S. (2009). The social life of health information. *Pew Research Center*. Retrieved May 18, 2017, from http://www.pewinternet.org/2009/06/11/the-social-life-of-health-information/

Friedman, B., Khan, P. H. Jr, & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34–40. doi:10.1145/355112.355120

Gandhi, M., & Wang, T. (2015). Digital Health Consumer Adoption: 2015. *Rock Health*. Retrieved May 12, 2017, from https://rockhealth.com/reports/digital-health-consumer-adoption-2015/

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, *57*(7), 768–775. doi:10.1016/S0148-2963(02)00363-6

Gerber, E. M., & Hui, J. (2013). Crowdfunding: Motivations and deterrents for participation. *ACM Transactions on Computer-Human Interaction*, *20*(6), 34. doi:10.1145/2530540

Gerber, E. M., Hui, J. S., & Kuo, P. Y. (2012). Crowdfunding: Why people are motivated to post and fund projects on crowdfunding platforms. In *Proceedings of the International Workshop on Design, Influence, and Social Technologies: Techniques, Impacts and Ethics* (Vol. 2, p. 11). Academic Press.

Gibbs, J. L., Ellison, N. B., & Lai, C. H. (2011). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, *38*(1), 70–100.

Gillespie, N. (2003). Measuring trust in working relationships: The behavioral trust inventory. *Proceedings from Academy of Management Conference*.

Goffman, E. (1959). The moral career of the mental patient. *Psychiatry*, *22*(2), 123–142. doi:10.1080/00332747.1959.11023166 PMID:13658281

Guadagno, R. E., & Cialdini, R. B. (2005). Online persuasion and compliance: Social influence on the Internet and beyond. In Y. Amichai-Hamburger (Ed.), *The social net: The social psychology of the Internet* (pp. 91–113). New York: Oxford University Press.

Guadagno, R. E., Muscanell, N. L., Rice, L. M., & Roberts, N. (2013). Social influence online: The impact of social validation and likability on compliance. *Psychology of Popular Media Culture*, *2*(1), 51–60. doi:10.1037/a0030592

Gurtman, M. B. (1992). Trust, distrust, and interpersonal problems: A circumplex analysis. *Journal of Personality and Social Psychology*, *62*(6), 989–1002. doi:10.1037/0022-3514.62.6.989 PMID:1619552

Hagen-Rochester. (2012). Online dating dumps the stigma. *Futurity*. Retrieved June 1, 2017, from http://www.futurity.org/online-dating-dumps-the-stigma/

Hancock, J., & Guillory, J. (2015). Deception with technology. In S. Sundar (Ed.), *The handbook of the psychology of communication technology* (pp. 270–289). Malden, MA: Wiley-Blackwell.

Hornuf, L., & Schwienbacher, A. (2015). Portal Design and Funding Dynamics in Crowdinvesting. *SSRN Electronic Journal*. Retrieved June 2, 2017, from http://ssrn.com/abstract=2612998

Horvát, E. Á., Uparna, J., & Uzzi, B. (2015). Network vs market relations: The effect of friends in crowdfunding. In *Proceedings from 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 226-233). IEEE.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Management Information Systems Quarterly*, 19–33.

Jones, R., Sharkey, S., Ford, T., Emmens, T., Hewis, E., Smithson, J., & Owens, C. (2011). Online discussion forums for young people who self-harm: User views. *The Psychiatrist*, *35*(10), 364–368. doi:10.1192/pb.bp.110.033449

Kahneman, D. (2000). A psychological point of view: Violations of rational rules as a diagnostic of mental processes. *Behavioral and Brain Sciences*, *23*(5), 681–683. doi:10.1017/S0140525X00403432

Kaptein, M., & Eckles, D. (2012). Heterogeneity in the effects of online persuasion. *Journal of Interactive Marketing*, *26*(3), 176–188. doi:10.1016/j.intmar.2012.02.002

Kim, K., & Viswanathan, S. (2014). *The Experts in the Crowd: The Role of Reputable Investors in a Crowdfunding Market*. Retrieved May 16, 2017, from https://accounting.eller.arizona.edu/sites/mis/files/ssrn-id2258243.pdf

Kim, Y., Shaw, A., Zhang, H., & Gerber, E. (2017). Understanding Trust amid Delays in Crowdfunding. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 1982-1996). ACM.

Kromidha, E., & Robson, P. (2016). Social identity and signalling success factors in online crowdfunding. *Entrepreneurship and Regional Development*, *28*(9-10), 605–629. doi:10.1080/08985626.2016.1198425

Krueger, J. I., Massey, A. L., & DiDonato, T. E. (2008). A matter of trust: From social preferences to the strategic adherence to social norms. *Negotiation and Conflict Management Research*, *1*(1), 31–52. doi:10.1111/j.1750-4716.2007.00003.x

Kummervold, P. E., Gammon, D., Bergvik, S., Johnsen, J. A. K., Hasvold, T., & Rosenvinge, J. H. (2002). Social support in a wired world: Use of online mental health forums in Norway. *Nordic Journal of Psychiatry*, *56*(1), 59–65. doi:10.1080/08039480252803945 PMID:11869468

Kuppuswamy, V., & Bayus, B. L. (2013). Crowdfunding creative ideas: The dynamics of project backers in Kickstarter. *SSRN Electronic Journal.* Retrieved May 18, 2017, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234765

Kyllonen, P. C., & Christal, R. E. (1990). Reasoning ability is (little more than) working-memory capacity?! *Intelligence*, *14*(4), 389–433. doi:10.1016/S0160-2896(05)80012-1

Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust Facebook?: Examining technology and interpersonal trust beliefs. *ACM SiGMiS Database*, *42*(2), 32–54. doi:10.1145/1989098.1989101

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 880.

Lederman, R., Fan, H., Smith, S., & Chang, S. (2014). Who can you trust? Credibility assessment in online health forums. *Health Policy and Technology*, *3*(1), 13–25. doi:10.1016/j.hlpt.2013.11.003

Leitner, M., Wolkerstorfer, P., & Tscheligi, M. (2008). How online communities support human values. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges* (pp. 503-506). ACM.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39–71. doi:10.1016/j.jsis.2008.01.001

Li, Y. B., James, L., & McKibben, J. (2016). Trust between physicians and patients in the e-health era. *Technology in Society*, *46*, 28–34. doi:10.1016/j.techsoc.2016.02.004

Lindgaard, G., Dudek, C., Sen, D., Sumegi, L., & Noonan, P. (2011). An exploration of relations between visual appeal, trustworthiness and perceived usability of homepages. *ACM Transactions on Computer-Human Interaction*, *18*(1), 1–30. doi:10.1145/1959022.1959023

Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! *Behaviour & Information Technology*, *25*(2), 115–126. doi:10.1080/01449290500330448

Lo, S. K., Hsieh, A. Y., & Chiu, Y. P. (2013). Contradictory deceptive behavior in online dating. *Computers in Human Behavior*, *29*(4), 1755–1762. doi:10.1016/j.chb.2013.02.010

Lukkarinen, A., Teich, J. E., Wallenius, H., & Wallenius, J. (2016). Success drivers of online equity crowdfunding campaigns. *Decision Support Systems*, *87*, 26–38. doi:10.1016/j.dss.2016.04.006

Lutz, C., & Ranzini, G. (2017). Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Social Media and Society, 3*(1).

Ma, X., Sun, E., & Naaman, M. (2017). What Happens in happn: The Warranting Powers of Location History in Online Dating. In *Proceedings of ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 41-50). ACM. doi:10.1145/2998181.2998241

Markovits, H., Doyon, C., & Simoneau, M. (2002). Individual differences in working memory and conditional reasoning with concrete and abstract content. *Thinking & Reasoning*, *8*(2), 97–107. doi:10.1080/13546780143000143

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2), 12. doi:10.1145/1985347.1985353

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A two-stage model of initial trust in a web business. *Electronic Markets*, *14*(3), 252–266. doi:10.1080/1019678042000245263

Mollick, E. (2014). The dynamics of crowdfunding: An exploratory study. *Journal of Business Venturing*, *29*(1), 1–16. doi:10.1016/j.jbusvent.2013.06.005

Mun, Y. Y., Yoon, J. J., Davis, J. M., & Lee, T. (2013). Untangling the antecedents of initial trust in Web-based health information: The roles of argument quality, source expertise, and user perceptions of information quality and risk. *Decision Support Systems*, *55*(1), 284–295. doi:10.1016/j.dss.2013.01.029

Neville, F. (2015). Preventing violence through changing social norms. In P. D. Donnelly & C. L. Ward (Eds.), *Oxford textbook of violence prevention: Epidemiology, evidence, and policy* (pp. 239–244). Oxford University Press.

Newcomb, T. M. (1943). *Personality and social change: Attitude formation in a student community*. New York: Dryden.

Norcie, G., De Cristofaro, E., & Bellotti, V. (2013). Bootstrapping trust in online dating: Social verification of online dating profiles. In *Proceedings of International Conference on Financial Cryptography and Data Security* (pp. 149-163). Springer. doi:10.1007/978-3-642-41320-9_10

Odom, M. D., Kumar, A., & Saunders, L. (2002). Web assurance seals: How and why they influence consumers' decisions. *Journal of Information Systems*, *16*(2), 231–250. doi:10.2308/jis.2002.16.2.231

Office for National Statistics. (2016). *Internet access – households and individuals: 2016*. Retrieved May 21, 2017, from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016#activities-completed-on-the-internet

Pee, L. (2012). Trust of Information on Social Media: An Elaboration Likelihood Model. In *Proceedings of the International Conference on Information Resources Management (CONF-IRM)* (pp. 2-9). AIS.

Pulman, A., & Taylor, J. (2012). Munchausen by internet: Current research and future directions. *Journal of Medical Internet Research*, *14*(4), e115. doi:10.2196/jmir.2011 PMID:22914203

Rakesh, V., Choo, J., & Reddy, C. K. (2015). Project recommendation using heterogeneous traits in crowdfunding. *Proceedings of Ninth International Conference on Web and Social Media*, 337-346.

Reynolds, K. J., Subašić, E., & Tindall, K. (2015). The problem of behaviour change: From social norms to an ingroup focus. *Social and Personality Psychology Compass*, *9*(1), 45–56. doi:10.1111/spc3.12155

Richardson, K. (2003). Health risks on the internet: Establishing credibility on line. *Health Risk & Society*, *5*(2), 171–184. doi:10.1080/1369857031000123948

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems*, *11*(3), 271–295. doi:10.1016/S0963-8687(02)00021-5

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs*, *39*(2), 339–362. doi:10.1111/j.1745-6606.2005.00018.x

Rocco, E. (1998). Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 496-502). ACM Press. doi:10.1145/274644.274711

Roghanizad, M. M., & Neufeld, D. J. (2015). Intuition, risk, and the formation of online trust. *Computers in Human Behavior*, *50*, 489–498. doi:10.1016/j.chb.2015.04.025

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *The American Psychologist*, *35*(1), 1–7. doi:10.1037/0003-066X.35.1.1

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. doi:10.5465/AMR.1998.926617

Rozmovits, L., & Ziebland, S. (2004). What do patients with prostate or breast cancer want from an Internet site? A qualitative study of information needs. *Patient Education and Counseling*, *53*(1), 57–64. doi:10.1016/S0738-3991(03)00116-2 PMID:15062905

Schmitz, A., Zillmann, D., & Blossfeld, H. P. (2013). Do women pick up lies before men? The association between gender, deception patterns, and detection modes in online dating. *Online Journal of Communication and Media Technologies*, *3*(3), 52.

Sillence, E., & Briggs, P. (2015). Trust and engagement in online health a timeline approach. In S. S. Sundar (Ed.), *The Handbook of the Psychology of Communication Technology* (pp. 469–487). Malden, MA: Wiley Blackwell.

Skirnevskiy, V., Bendig, D., & Brettel, M. (2017). The influence of internal social capital on serial creators' success in crowdfunding. *Entrepreneurship Theory and Practice*, *41*(2), 209–236. doi:10.1111/etap.12272

Smith, A., & Duggan, M. (2013). *Online dating & relationships*. Pew Research Center. Retrieved May 16, 2017, from http://www.pewinternet.org/2013/10/21/online-dating-relationships/

Song, Y., & van Boeschoten, R. (2015). Success factors for Crowdfunding founders and funders. *Proceedings of the 5th International Conference on Collaborative Innovation Networks COINs15*.

Sorrentino, R. M., Holmes, J. G., Hanna, S. E., & Sharp, A. (1995). Uncertainty orientation and trust in close relationships: Individual differences in cognitive styles. *Journal of Personality and Social Psychology*, *68*(2), 314–327. doi:10.1037/0022-3514.68.2.314

Stanovich, K. E. (1999). *Who is rational? Studies of individual differences in reasoning*. Mahwah, NJ: Erlbaum.

Sudau, F., Friede, T., Grabowski, J., Koschack, J., Makedonski, P., & Himmel, W. (2014). Sources of information and behavioral patterns in online health forums: Observational study. *Journal of Medical Internet Research*, *16*(1), e10. doi:10.2196/jmir.2875 PMID:24425598

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. *The Social Psychology of Intergroup Relations, 33*(47), 74.

Thottam, I. (2017). 10 Online dating statistics you should know. *eHarmony*. Retrieved June 1, 2017, from http://www.eharmony.com/online-dating-statistics/

Turner, J. C. (1991). *Social influence*. Milton Keynes, UK: Open University Press.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Oxford, UK: Blackwell.

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology (Brno)*, *3*(2).

Van Slyke, C., Comunale, C. L., & Belanger, F. (2002). Gender differences in perceptions of web-based shopping. *Communications of the ACM*, *45*(7), 82–86. doi:10.1145/545151.545155

Vismara, S. (2016). Equity retention and social network theory in equity crowdfunding. *Small Business Economics*, *46*(4), 579–590. doi:10.1007/s11187-016-9710-4

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105–125. doi:10.1016/j.chb.2003.11.008

Wessel, M., Thies, F., & Benlian, A. (2016). The emergence and effects of fake social information: Evidence from crowdfunding. *Decision Support Systems*, *90*, 75–85. doi:10.1016/j.dss.2016.06.021

Whitty, M. T. (2008). Liberating or debilitating? An examination of romantic relationships, sexual relationships and friendships on the Net. *Computers in Human Behavior*, *24*(5), 1837–1850. doi:10.1016/j.chb.2008.02.009

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455. doi:10.1057/sj.2012.57

Wright, B., Partridge, I., & Williams, C. (2000). Management of chronic fatigue syndrome in children. *Advances in Psychiatric Treatment*, *6*(2), 145–152. doi:10.1192/apt.6.2.145

Wu, G., Hu, X., & Wu, Y. (2010). Effects of perceived interactivity, perceived web assurance and disposition to trust on initial online trust. *Journal of Computer-Mediated Communication*, *16*(1), 1–26. doi:10.1111/j.1083-6101.2010.01528.x

Zhang, J., & Liu, P. (2012). Rational herding in microloan markets. *Management Science*, *58*(5), 892–912. doi:10.1287/mnsc.1110.1459

Zhao, J., Abrahamson, K., Anderson, J. G., Ha, S., & Widdows, R. (2013). Trust, empathy, social identity, and contribution of knowledge within patient online communities. *Behaviour & Information Technology*, *32*(10), 1041–1048. doi:10.1080/0144929X.2013.819529

Zhao, J., Ha, S., & Widdows, R. (2013). Building trusting relationships in online health communities. *Cyberpsychology, Behavior, and Social Networking*, *16*(9), 650–657. doi:10.1089/cyber.2012.0348 PMID:23786170

Zheng, J., Veinott, E., Bos, N., Olson, J. S., & Olson, G. M. (2002, April). Trust without touch: jump-starting long-distance trust with initial social activities. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 141-146). ACM. doi:10.1145/503376.503402

Zvilichovsky, D., Inbar, Y., & Barzilay, O. (2015). Playing both sides of the market: Success and reciprocity on crowdfunding platforms. *SSRN Electronic Journal*. Retrieved May 8, 2017, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304101

Zytko, D., Freeman, G., Grandhi, S. A., Herring, S. C., & Jones, Q. G. (2015, February). Enhancing evaluation of potential dates online through paired collaborative activities. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing* (pp. 1849-1859). ACM. doi:10.1145/2675133.2675184

KEY TERMS AND DEFINITIONS

Crowdfunding: A campaign platform that allows creators and business owners to collect money for a project through small pledges made by funders.

Fraud: Deception for the purpose of personal of financial gain.

Health Forums: Discussion networks that support peer-to-peer discussion surrounding medical concerns as a source of information and community interaction.

Online Dating: Using sites and apps online as a way of meeting potential romantic partners.

Social Identity: The perception one has of their sense of belonging to certain societal groups.

Social Norms: An unwritten set of rules that inform how a person should behave in a certain social situation.

Trust: A belief in the good intentions of another under circumstances where a lack of knowledge or experience means that there is an element of risk and uncertainty in the interaction.