Familiarity Breeds Con-victims: Why We Need More Effective Trust Signaling

M. Angela Sasse and Iacovos Kirlappos

Department of Computer Science, University College London, UK
a.sasse@cs.ucl.ac.uk

1 Introduction

The past 10 years have seen a plethora of research on trust in online interactions. In the late 90s, the issue was whether people would be willing to trust the Internet enough to order and enter their credit card details online. Most of the academic research and commercial advice published then focused on 'how to increase user trust online' by making websites 'user friendly' and having a 'personal touch' e.g. in the form of photos of company staff. Unfortunately, much this advice on how to make your Internet presence trustworthy is now being used by perpetrators of phishing scams, who are using the latest 'trustworthy UI design techniques' to trick users into revealing authentication credentials and other personal data. A key trust issue that has emerged with the huge popularity of social networking is users' voluntary (and sometimes ill-judged) disclosure of personal information, and accidental sharing of that data by applications and other users.

Whilst many new applications and services have emerged, little progress has been made in helping ordinary users to work out who they can trust online, and who they can't. Trust is only required when risk and uncertainty are present. Since it serves as a shortcut for a full risk-benefit analysis and mechanisms to assure that a transaction partner delivers what is being promised, there are significant economic benefits to trust-based environments [1]. In online transactions, uncertainty is increased because transactions partners are separated in space, and – unless delivery is instant (e.g. when buying a music track) - in time.

2 The Importance of Trust Signaling

When deciding whether to trust, user look for signals of trustworthiness – cues about the transaction partner's ability and motivation to deliver their side of the transaction, rather than 'taking the money and run' [4]. In real-world transactions, first-time interactions are regarded as more risky, whilst a past history of interactions allow the trustor to form a reasonable expectation of the trustee's behaviour. Users transfer this behaviour to online transactions: they will trust website that they have used in the past, or rather – any site that looks, feels or sounds like one they have used successfully in the past – not realising that in online environments, attackers can more easily mimic the appearance and behavior of genuine transaction partners.

I. Wakeman et al. (Eds.): IFIPTM 2011, IFIP AICT 358, pp. 9–12, 2011.

In a recent study, we had participants buying music festival tickets under conditions of risk and uncertainty. We found that people use the following as indicator of trustworthiness:

1. **Previous experience with the website.** Users will trust websites they have used before – or rather: websites they think they have used before – and those that look or feel familiar. Small differences in appearance or behavior usually won't raise suspicion, nor do certificate warnings, because users have been de-sensitised by too many false positives.
2. **Logos and certifications.** Most of the websites display some form of trust logo, and many users them as symbols of trust. We found, however, that none of our participants could explain though what these logo signify, and why a website is secure if it has this logo. Very few participants checked whether the logo was a clickable link and what information about the merchant it was providing.
3. **Reference to other names the participants could recognize.** Websites that had affiliate programs which included known venues around the country created a feeling of trust in participants. The inclusion of the *Oxfam* charity name in a website (www.gigantic.com), and mentioning that they give 10% of their profits to it, made participants think that it cannot be fake - even though there was no way to verify whether the claims of that website were true, since no links existed that confirmed.
4. **Advertising.** Participants had mixed reactions on the presence of advertisements on websites. Adverts of well-known companies induced a feeling of trust for 14% of participants. Their main argument was "*why would a company pay them to include advertisements in their website if they were scammers*?" On the other hand, 11% of participants said that if they have a lot of advertisements, then they can be scams, and they preferred to buy from sites that displayed fewer of these.
5. **Social Networking references.** Inclusion of links to *Facebook* and *Twitter* pages can significantly affect the level of trust in a site. 19% of participants mentioned that if a retailer has a *Facebook* Page or a *Twitter* site, then they cannot be fraudulent, as their victims could post negative comments on those sites after they were scammed, deterring other people from using them. In addition, the inclusion of other user feedback in the website can also contribute in the creation of a feeling of trust and received positive comments by 11% of participants. This was strongly present in the case of a website which included pictures of the people that left feedback for its services, or other members of the website that are planning to attend an event, concurring with findings that richer media representations could lead to a positive trust bias.
6. **Amount of information provided.** The amount of information the website included on the particular event influenced 17% of participants. Although all websites included information on the event (gate opening times, facilities, instructions how to get to the venue etc), those that had that information viewable on the main event page seemed to attract the participants more. Inclusion of visual artifacts like maps increased the level of trust and made them appear more persuasive and real.

7. **Website Layout.** 19% of participants mentioned that the structure of the website design was something that looked familiar to them from other websites they are using, which are known to be legitimate. So the websites they have chosen to trust are possibly genuine as the layout is similar. Indication that a site sells tickets for a variety of events was also critical, as participants did not perceive it as a scam aiming to target a particular event audience.
8. **Company Information.** The type of information the website provided on the company behind it also affected decisions. 14% of participants mentioned that the presence of the registration number of the company, VAT numbers, direct telephone numbers, ticket delivery information and claims that they are official ticket outlets seemed to be trusted more. As with the logos (see 2), however, none of the participants knew how to verify this information though.

Our results show that trust signalling in online interactions is currently dysfunctional. Attackers have an easy game - techniques that are successfully employed in the real world are currently even cheaper and easier to online (a point elaborated by Stajano & Wilson [3]).

Information about ability and motivation of a trustee to fulfil can be inferred from signals of trust-warranting properties [2]. There are two main types of signals for trustworthiness:

- **Symbols of trustworthiness.** Symbols have an arbitrarily assigned meaning - they are specifically created to signify the presence of trust-warranting properties. Examples of symbols for such properties are e-commerce trust seals. Symbols can be protected by making them very difficult to forge, or by threatening sanctions in the case of misuse. They are a common way of signaling trustworthiness, but their usability is often limited. Because they are created for specific settings, the trustor has to know about their existence and how to decode them. At the same time, trustees need to invest in emitting them and in getting them known.
- **Symptoms of trustworthiness.** Symptoms are not specifically created to signal trust-warranting properties; rather, they are by-products of the activities of trustworthy actors. As an example, a steady gaze and firm voice may not require much effort when telling the truth, but may require some training to maintain while lying. Therefore, exhibiting symptoms of trust incurs no cost for trustworthy actors, whereas untrustworthy actors would have to invest some effort to engage in effective mimicry.

Our currently online environment has very much relied on trust symbols; but the results of our study illustrate why they do not work in an online environment – they are cheap to mimic, and users cannot tell the difference between genuine and mimicked ones. The presentation will argue that we need to shift our design efforts to supporting trust symptoms, which are impossible or expensive for attackers to forge, and provide user with richer cues that are embedded in the specific transactions.

References

1. Gefen, D.: E-Commerce: The Role of Familiarity and Trust. Omega: International Journal of Management Science 28(6), 725–737
2. Riegelsberger, J., Sasse, M.A., McCarthy, J.D.: The mechanics of trust: a framework for research and design. International Journal of Human-Computer Studies 62(3), 381–422 (2005)
3. Stajano, F., Wilson, P.: Understanding scam victims: seven principles for systems security. In: Technical Report 754. University of Cambridge (2009)
4. Twyman, M., Harvey, N., Harries, C.: Trust in motives, trust in competence: Separate factors determining the effectiveness of risk communication. Judgment and Decision Making 3, 111–112 (2008)