

False Impressions: Contrasting Perceptions of Security as a Major Impediment to Achieving Survivable Systems

William Yurcik Aashish Sharma David Doss
Illinois State University
Department of Applied Computer Science
Survivability-Over-Security (SOS) Research Group
{wjyurci,ashish,dldoss}@ilstu.edu

Abstract: There is a distinct lack of basic understanding of user problems with current web technologies where the majority of electronic transactions occur at present. Our results show that a user's level of trust and risk are based on perceptions of website design that are significantly different based on prior knowledge. We report that corporations are already exploiting this result to maximize the use of superficial security cues that do not provide protection while minimizing investment in technological security solutions that do provide protection. Implications of this finding may help explain the measured increasing lack of Internet security and thus survivability of web-based information systems.

1.0 Introduction

Although a large proportion of users refuse to transact online due to their concerns about security, the actual source(s) of those concerns are not well understood. Marketing studies provide data on customers' opinions and preferences, but do not capture customers' actual thoughts and behaviors as they transact with sites. On the other hand, usability testing of websites does yield some data on users' behavior as they interact with sites, but there is little experimental control and the lessons learned from tests are rarely applied to general models of user behavior [7]. Despite the substantial expenditure by many companies in online security, there is very little published research on the specific factors that influence consumers' perceptions of the security of websites.

While security is only one aspect of a consumer's experience with a commercial website, it is an important one and may be a strong determinant of whether or not a user decides to begin or continue an online transaction. In order to ensure a positive user experience, it is therefore necessary to fully understand how different users perceive the risks associated with transacting online as well as how they perceive the various measures employed by sites to ensure secure transactions.

In this paper we have focused exclusively on website security since this is where the overwhelming majority of electronic transactions presently occur. The remainder of this paper is organized as follows: Sections 2 and summarize security evaluations by experts and novice users respectively. Section 4 details false security cues found among novice users. We conclude with a summary, conclusions, and future directions in Section 5.

2.0 Website Evaluation By Security Experts

In order to understand consumers' perceptions of the security of a website, it is necessary to first establish what website security techniques are available and what can be determined about the security of a specific website from inspection and interaction. Under a controlled setting we gathered information from Internet security experts to obtain a baseline measure of security metrics found across different sets of websites [8]. The expert group expressed that while there is a wide range of possible security techniques available, only a subset of these techniques will be employed by any single web site, not all techniques will be implemented properly, none of the techniques is completely foolproof, and increased security is a direct tradeoff with performance and usability. As a group these experts embodied the technical knowledge needed to determine if security vulnerabilities exist and the cues for their manifestation.

During initial evaluation, experts would conduct what is known as a "pre-attack". This pre-attack, which is also used by crackers in choosing potential targets, is an evaluation process to determine if a website's security vulnerabilities can be exploited:

- What is the operating system platform and web server software?

- Are both the operating system and web server the most current version with patches?
- Has the web site had an independent security assessment scan performed?

The experts also revealed that actual security requirements should be context dependent - the level of security on a site should be appropriate to the user's situation and goals [9]. The transfer of health or financial information (i.e., credit card number, social security number, etc.) requires the strongest security measures available while browsing for information required a lower levels of security.

Experts viewed security to be the partial responsibility of a user. The group felt that there are many things that users need to do to ensure their own security when transacting online. These included:

- being aware of one's surroundings if transacting online in a public place
- keeping browsers updated so that the highest encryption levels can be achieved
- session termination
- examination of verification certificates
- monitoring/controlling use of cookies by websites, especially in public places

These findings were not entirely unexpected: human error in the handling of passwords and other security measures are well-known human factors problems [2,5,6]. The experts also assigned partial responsibility to organizations for web site design and maintenance related to security. Security is an ongoing process - websites must always be up-to-date with all security measures and react quickly to vulnerabilities when they are uncovered.

As far as technical security metrics, experts identified encryption key length, certificates, cookies, performance and availability. While experts unanimously agreed that encryption is important, there was some debate about the actual level of encryption that is necessary. Experts also identified verification certificates from trusted third parties such as an important metric. The performance and availability of web sites was identified as an indicator of security. A site with repeated crashes reflected poor system implementation and therefore a site that may be more prone to attack.

Although expert analysis focused on web site inspection, there was correlation between perceived security and company reputation. This was made clear with the role of customer service, or *accountability*, as part of security best practices. Other examples that stand out:

- password changing/delivery - use of postal mail is more secure than Email or telephone
- immediate access to customer service 24 hours a day, 7 days a week
- multiple methods for contacting customer service (email, phone, snail mail)

Equally important to recognizing superior security protection is discriminating cues that have little or no security value. Some examples of "illegitimate" security cues include:

- web site "look and feel"- navigation, layout, graphics, etc.
- download times (except if bugs or crashes are suspected)
- written policies on security
- company symbols- the presence of the symbols themselves means nothing

3.0 Novice User Perceptions of Websites

We have also studied, in a controlled setting, novice users' attitudes towards security, recognition and perception of various security indicators, and feelings about company reputation [8]. Our objective is to determine cues that non-expert users use to determine the security of a website before making a transaction decision as well as incongruities with cues identified by experts. The ultimate goal is to make recommendations for the effective presentation of security features on websites to bolster at least one part of the user experience. Our initial hypotheses were novice users: (1) feel strongly about the security of websites, but (2) do not fully understand or fail to perceive the security cues on the sites with which they transact. Unlike the expert group, some of our novice users indicated that security is not an issue and assumed that the responsibility was being adequately handled by the websites with which they transact. Some participants explained that they were concerned about security, but only when money was involved.

Novice user perception of their own responsibilities for security were mixed. While users had a general awareness of robust password procedures, most admitted that they did not follow procedures in practice. Novice users had a positive reaction to the presence of security challenge questions but their awareness of good criteria for

these questions was mixed.¹

There was little or no recognition of genuine security features among novice users. Even given the lack of knowledge about technical security metrics, most did indicate approval of a website explicitly stating its security measures even if they did not understand it. Counter intuitively; we identified a subset of valid security measures that may actually lead to negative perceptions of site security. For example, Paypal employs a “random number generator” to provides assurance that information is sent securely.² A majority of novice users concurred with security experts that site performance and availability can be a viable determinant of site security. The use of cookies prompted a mixed reaction - while most novice users’ recognized and knew a little about their functions, only a minority expressed concern about their use on sites labeling them a “necessary evil”.

Perhaps the single most important factor in a novice user’s perceptions of web site security was the brand and reputation of the company. Even though novice users’ were specifically asked to respond based only on the visible aspects and interactions, they continually returned to the company reputation. Most also explained that if a site is owned by a company that they know well and trust in general, then they are not concerned about the security of the site.³ In a twist on this theme, consumers perceptions also extended to indirect affiliations or ratings provided by trusted parties. While the expert group seemed to agree that an actual physical brick-and-mortar presence might be a factor in indicating the security of a web site, some consumers said it made no difference to them if a company only existed “virtually” as long as the reputation and positive experiences were there. For instance, more than one novice user claimed that they trust the booksellers Barnes&Noble and Amazon to the same degree because of their reputations, even though Amazon lacks a physical storefront.

4.0 False Security Cues

Given a set of cues found on websites that experts have identified as valid indicators of the level of security protection, we set out to determine if indeed, novice users’ could be “fooled” by these invalid cues.

When queried about **download times** on sites, novice user stated that long waiting times would make them worry about the security of the site. One novice user stated: “If the site is slow, they may not be spending enough money on their servers.” However, this waiting time can often be the result of a strong encryption implementation such as Secure Sockets Layer (SSL) exchanging keys. Some sites previously protected with SSL have even gone as far as using intermediate SSL proxy servers to decrease response time with the result being the introduction of new security vulnerabilities between the web site and the proxy. SSL itself is not foolproof; there have been documented cases of flaws due to weak encryption, accidental divulging of passwords or session cookies, and spoofing. Studies of user tolerance for response time delay indicates that it can be managed with cues to set expectations [1].

We found that half of our novice users’ viewed the **look-and-feel** of a website as having a direct impact on the security of the site. Comments such as “This site looks professional, so its obvious its not fly-by-night” and “Too many ads makes me worry about security” exemplify the strength with which simple visual aspects of a site can affect perceptions of the site as a whole.

While experts were wary of the **security policy statements**, explaining that what a website states and what it actually does may be very different, our consumer group seemed to place a great amount of trust in these words. Almost all novice users’ mentioned at some point that clearly posted security statements made them feel positive about a web site’s security. In fact, more than one novice user stated that even though they would never actually read the security statements, they felt better just knowing they were there. While security statement may sound comforting, the assurances are often vague and incomplete. For example, industry standard encryption only applies to the transmission of data – just as important but overlooked is how a website stores user data often dangerously on an Internet-accessible server which is preferred hacker target. A web site security policy should be clear that information is encrypted on all servers especially shopping carts.

In light of the above security statement findings, it was somewhat surprising the degree to which novice users’ discounted **visual security icons** found on sites as having nothing to do with security. When queried about credit card symbols, none of the participants said that these affected their sense of security. The same result was found

¹ Some realized information like “mother’s maiden name” could easily be obtained while others saw no problem with any questions.

² Users did not understand the function of the generator, which led to confusion and negative feelings about the website in general.

³ Explanations expressed the feeling that large or well-known companies will invest responsibly in security protection.

with graphic symbols representing third-party verification parties (such as TrustE) with most novice users' making statements such as "Anyone can put a symbol like that on their site." However, unlike the credit card symbols, many of these graphics were actually links to an actual third party site. This is a ripe area for research, the authors are aware of only one research publication in this area which identified the following criteria for effective security icons: intuitive, flexible in size and color, hidden until needed, and performance sensitive [4].

Another unexpected finding was that unlike the expert group, most of the novice users' focused more on **insurance** if the security of a website was breached rather than what a website does to prevent a breach from occurring in the first place. For example, novice users focused much attention on website information concerning theft and fraud insurance offered by the sites. They explained that they wanted to be sure they were covered in case something happened on the site resulting in a monetary loss. Novice users, in many cases, were more concerned with mechanisms for recovery after a loss rather than proactive measures to prevent it in the first place.

5.0 Lessons Learned

Perception management has always been a part of security [3]. Examples include concealment, camouflage, indirection, and deception. The appearance of strong security, maybe even more important than actual level of protection, may deter or reduce the frequency and intensity of attacks. We found the difference in perception of web site security cues between experts and novice users was very clear. While both groups agreed that a company's reputation and practices is a determinant of website security perception, novice users were less adept at differentiating between valid and false technical security cues. Based on these findings, we can make some general recommendations to enhance consumer perception of web site security.

There are certain perceptive cues that, while having nothing to do with actual security, nonetheless have a powerful effect on the novice user perception of website security. Corporate websites are aware of these cues as inexpensive steps to make novice users perceive a website as secure but this has often come at the expense of investment in technical security mechanisms (equipment, processes, and personnel). The result is an increasingly worst-case scenario: insecure websites that novice users perceive as secure. Anecdotal evidence suggests that some organizations even make the explicit financial decision that losses due to insecurity (theft, fraud) are less than the necessary investment in security. This is not new, however, but the use of human cognition cues to give novice users' the opposite impression is new.

We have only outlined only a small segment of the problems related to the security implications of human interaction with software. While we summarize state-of-the-art results, we realize that novice users are becoming more security conscious and perceptions will change. Future research in this area is vital to reconcile incentives for good security engineering matched with valid novice user perceptions.

References:

- [1] Bouch, A., A. Kuchinsky, and N. Bjatti, "Quality is in the Eye of the Beholder: Meeting Users' Requirements for Internet Quality of Service," *CHI 2000*, Hague Netherlands, pp. 297-304.
- [2] Carstens, D., P. McCauley-Bell, and L. Malone. "Development of a Model for Determining the Impact of Password Authentication Practices on Information Security," *Human Factors and Ergonomics Society (HFES) Congress*, San Diego, CA, July 2000, pp. 342-345.
- [3] Cohen, F. "A Note on the Role of Deception in Information Protection," *Computers & Society*, Vol. 17 No. 6, pp. 483-506.
- [4] Hosmer, H. "Visualizing Risks: Icons for Information Attack Scenarios," *23rd National Information Systems Security Conference (NISSC)*, Baltimore MD, Oct. 2000.
- [5] McCauley-Bell, P. and L. Crumpton. "The Human Factors Issues in Information Security: What Are They and Do They Matter?" *Human Factors and Ergonomics Society (HFES)*, 1998, pp. 439-443.
- [6] Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. John Wiley, 2000.
- [7] Turner, C. "Validating and Refining User Models of E-Commerce Customers With Usability Test Data," *9th Intl. Conf. on Human-Computer Interaction*, New Orleans LA, Aug. 2001.
- [8] Turner, C., M. Zavod, and W. Yurcik. "Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites," *Intl. Conf. on E-Commerce Research (ICECR)*, 2001, Vol. 2, pp. 628-636.
- [9] Wolf, G., and A. Pfitzmann. "Properties of Protection Goals and Their Integration Into a User Interface," *Computer Networks*, 32, pp. 685-699.