
Elder-friendly Design's Effects on Acceptance of Novel Technologies

Zachary Schall-Zimmerman

Undergraduate Researcher
Indiana University
611 N Woodlawn Ave.
Bloomington, IN 47403
zschallz@indiana.edu

L Jean Camp

Associate Professor
Indiana University
901 E. 10th St.
Bloomington, IN 47403
ljcamp@indiana.edu

Abstract

In this paper we describe the effect elder-friendly design had on elder acceptance of a technology designed to enhance online security. This elder-friendly alternative interface was developed for an anti-phishing toolbar that was previously found usable by students but rejected as unfathomable by elders. We recruited five elders to use both the toolbar instantiation and the elder-friendly interface in their homes for three weeks. During that time we generated a phishing email attack. We then had third researcher interview all participants. No elders using either interface responded to the phishing attack. Interviews indicated that elders found the more transparent toolbar interaction unusable, while the elder-friendly interface was acceptable. Elders could identify and describe times that it assisted their decision-making, yet when asked to describe generic benefits they could not do so.

Keywords

Useable security, ambient interfaces, financial security, privacy, elder acceptance.

ACM Classification Keywords

H.5.2 [User Interfaces]: User-centered Design, Evaluation, K.4.1 [Public Policy Issues]: Privacy

Copyright is held by the author/owner(s).

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

General Terms

Human Factors, Security, Design

Introduction

There exist very few user-friendly mechanisms that communicate the risks involved with everyday Internet use. With this in mind, it is no surprise that non-expert users, who do not already possess well-developed means for performing the complex calculus of risk necessary for online safety, often fall prey to online scams such as phishing attacks. During a phishing attack, a malicious website masquerades as an entity that the victim trusts in order to gain sensitive information from the victim. During the first half of 2009, an average of 35,211 unique phishing websites were reported each month. [1] This problem becomes more profound as elders (individuals 65 and older), are rapidly becoming an increasing population among Internet users. Elders have been historically targeted by financial scams and are not commonly highly experienced computer users. Yet the population of elders and the percentage of elders online are both rapidly increasing. For example, 22% of America's elders used the Internet in 2004, which was a 47% increase from 2000. [2] This also has implications for e-commerce; 82% of Americans 65 of age and older do not feel comfortable giving their credit card information online. [3]

There are many technical solutions to mitigate phishing attacks, however the interactions of these tend to be deeply flawed. A common approach is the browser toolbar, yet these have been found to be ineffective. [4] In this paper we describe elders' responses to a user-centered toolbar with an interaction designed to be acceptable to non-experts, and an elder-friendly

alternative physical front-end interface to the toolbar's services.

Net Trust

Net Trust is a privacy-aware anti-phishing reputation mechanism for Mozilla Firefox (see figure 1). One goal in the design was to implement transparent data flows, so that there was not a trade-off between security and privacy. The reputation system leverages socially grounded trust mechanisms and on-screen risk communication in the form of a toolbar. This toolbar allows users to easily generate, share, and annotate website reputation ratings amongst themselves through a private social network. Reputation ratings for websites shown in Net Trust are generated based on explicit ratings they set on the user interface and implicit ratings on how often users and their peers visit websites. Net Trust allows users to automatically share this information in a way that is controlled by the data subject, limited, and resistant to reputation attacks such as Sybil attacks. Net Trust also indicates how long a website has been up and alerts the user with a negative reputation rating for the website if it has been up for less than two weeks, or does not have a domain name. Users can also choose to download reputation ratings from third party organizations such as the Better Business Bureau, the FDIC, and McAfee® "Site Advisor™". The cryptographic and communications protocols that power Net Trust are described in detail in an IBM Systems Journal article, "Privacy-Aware Architecture for Sharing Web Histories." [5]

In one user study, participants (aged 18-36) responded positively to the Net Trust toolbar. They particularly embraced the ability to share and receive website reputation ratings and comments in a private, self-

selected social network. [6] However, elder participants in a separate unpublished user study responded negatively to the Net Trust toolbar. The study was aborted, as the elders did not want to engage with the toolbar. They found the transparency of data confusing as opposed to empowering. Net Trust risk awareness appeared to be creating the risk, as opposed to



figure 1. Net Trust Toolbar displaying a negatively rated website.

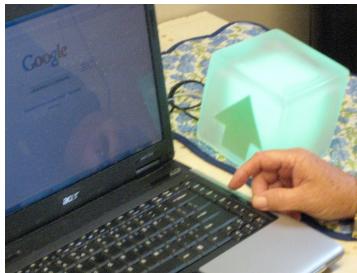


figure 2. Ambient Trust displaying a positively rated website.

Ambient Trust

Elder response to Net Trust prompted us to design an alternative interface to Net Trust focused specifically on the needs of the elderly. We call this interaction *Ambient Trust*. Ambient Trust is a cube with a color-coded light that displays reputation ratings from the Net Trust system. It externalizes Net Trust's reputation ratings by using color and animations. For example when a website was recently created¹, or has been reported to be a harmful website by a user's friend or a

¹ For the distinctive temporal characteristics of different types of malicious websites please see [7].

communicating how to mitigate it. Elders did not respond well to the social networking component of Net Trust, and the toolbar form factor. Elder participants particularly disliked the size of the ratings onscreen and were unfamiliar with the concepts of "friending" or online "buddies."

third party organization selected by the user the cube will pulse and glow different shades of red depending on the severity of the negative rating. If a website has no negative ratings from any source but has a positive rating the cube will glow different shades of green depending on the average positive rating of the website reported by Net Trust (see figure 2). If there is no data about the website from any sources and the website has been up for more than a week the cube will glow a steady yellow. Each time the user visits a new website the Ambient Display is updated with the rating from Net Trust.

To make it easier for elders to rate websites and share the ratings with their friends and family, touch sensors shaped like arrows were added to the sides of the cube. When a user touches the *up* arrow on the cube the rating of the domain of the currently displayed website will be increased, and similarly touching the downwards arrows results in a decreased rating.

Initial Evaluation: Focus Group

To explore whether or not this sort of device could be of use to elders, as part of a larger project, fifty elders

participated in multiple focus groups helping us address their conceptions of risks in daily (e.g. falls) and online activities (e.g. phishing) and using technology as a solution to these problems. These focus group participants provided guidance for the production-quality prototype used later in our in-home experiment. During the focus groups participants were shown how Ambient Trust works and were asked to discuss such as: "Do you want to share reputations of websites with your friends?", "Would you use Ambient Trust?", and "Do you fear for your safety online?"

All participants agreed that they did not mind sharing their website reputation ratings, so long as they were not personally identifiable. All but one participant said they would use Ambient Trust. One asked where he could purchase it.

During a closing discussion participants were asked what they liked and disliked about the Ambient Trust prototype. All of the participants agreed that they liked the immediate feedback on websites' reputations that they did not have to solicit from friends and family. Participants also liked the fact that the feedback was in a physical form that was easy to see and immediately understandable, rather than being small on a screen. One of the participants expressed concern about color-blind users being able to distinguish good websites from bad websites, which helped us formulate the idea of using a pulsing pattern of the with a red glow when a website with a negative rating is visited.

In-home Study

Five participants were recruited from a local retirement community to use Ambient Trust and the Net Trust

toolbar on their own computers for three weeks; three used Ambient Trust (with a hidden Net Trust backend), two used only the Net Trust toolbar. During the study, elders were asked to leave weekly comments on a study website about their experience with the device or toolbar and record the number of times they thought it was inaccurate in its display of ratings. During the last week of the study, participants were phished multiple times by the researchers posing as various local and national banks.

The phishing attack consisted of emails pretending to be from a bank, reminding the participant to update his or her information to avoid account suspension. The email included a link to a website we created and looked the same as the bank's online login page asking for their account number. Only the event of a form submission was recorded; no actual input was stored. Because this website had no domain name Ambient Trust would display a red pulsing color and the Net Trust toolbar would alert the user by displaying an instantiation of the ubiquitous pop-up message box.

Study Outcome

During the study no participants responded to the multiple phishing attacks. Also, weekly reports from the participants suggested that Net Trust and Ambient Trust had been consistently accurate in its display of reputation ratings. To better understand this outcome, participants were asked to participate in semi-structured interviews focused on the phishing attacks and the device's effect on their use of the Internet.

Participants using only the Net Trust toolbar expressed criticisms about the toolbar during the interviews. One participant said, "I already have a search toolbar yet

here is another one. The extra space the toolbar takes on the screen makes it harder for me to read my email." He went on to say that because had no "instruction manual" he forgot how to use the toolbar soon after the researchers explained it to him. These comments confirm the findings of the initial elder user study of Net Trust where we found that elders particularly did not like the toolbar form factor. Perhaps because of this interface alone, elders did not enjoy using the technology and thus rejected it.

In comparison, participants using the Ambient Trust Cube, as in the previous focus group, responded positively to the elder-friendly interface. When asked what she liked about the cube, one participant said that she appreciated that it was easy to see and easy to use. One participant chose to keep the cube after the study, and another participant said that she would be willing to pay for a marketed version of the cube. These responses appear to indicate that the Cube was more accepted than the toolbar by elder users.

While the interviews indicated that the elder-friendly, physical interaction is more accepted than the on-screen toolbar, two participants asserted that they did not see any benefit to using the Cube and that it did not change the way they used the Internet. However, each participant was able to identify and describe multiple times in which the Cube helped inform their decision on whether to trust a website or not. One participant, while researching how to do her taxes online, stumbled upon a website that the cube rated very negatively. The participant said, "I immediately closed the website and I closed my browser." It seems that these users' perceived benefit of using Ambient Trust did not align with their actual benefit.

Conclusion

Security interactions that align with the perceptions and serve the needs of the more technologically practiced population are a challenge to design. Yet even when a security technology is designed that functions well for a younger, technologically adept population it may not work for other groups. In this work we have shown that elder-centered design, resulting in an ambient physical interaction, proved to be acceptable, usable, and useful. Elders used the technology, and it informed their decision-making. In this case, our elder participants accepted a novel technology when provided with an alternative ambient interface designed to address their needs. However, making novel technologies more elder-friendly is not necessarily enough to overcome elders' considerable barriers to adoption of new technologies as even those who could identify effective uses of the technology could not or did not care to enumerate the benefits.

Acknowledgements

We would like to thank Lesa Lorenzen-Huber and Celine Chhoa for their help with this paper. We would also like to acknowledge the contributions of the residents and staff of Meadowood Retirement Community in Bloomington, Indiana. This material is based upon work supported by the National Science Foundation under award number 0705676. This work was also supported in part by a gift from Google. Opinions, findings, conclusions, recommendations or points of view in this document are those of the authors and do not necessarily represent the official position of the National Science Foundation, Indiana University, Google, or any employers or affiliates of the authors.

References

- [1] APWG. "Phishing activity trends: First Half 2009." http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf.
- [2] Fox, Susannah. Older Americans and the Internet. Pew Internet & American Life. Washington D.C., 2004. http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Society_and_the_Internet/pew_internet_seniors_032504.pdf.
- [3] Horrigan, John B. Online Shopping - Internet Users Like the Convenience But Worry About the Security of Their Financial Information. PEW Internet & American Life Project. Washington D.C.: PEW, 2008. http://www.pewinternet.org/pdfs/pip_online%20shopping.pdf.
- [4] Wu, Min, Robert Miller, and Simon Garfinkel, "Do Security Toolbars Actually Prevent Phishing Attacks?"
- [5] Alex Tsow, Camilo Viecco, Camp, L. Jean, "A Privacy-Aware Architecture for Sharing Web Histories", *IBM Systems Journal* accepted.
- [6] Alex Tsow, Faraneh Asgarpour & L. Jean Camp Usability Analysis and User Trust Behaviors of a Social Networking Toolbar, APWG eCrime Researchers Summit (Pittsburgh, PA) 4 -5 Oct. 2007.
- [7] Tyler Moore and Richard Clayton, "The Impact of Incentives on Notice and Take-down", Seventh Workshop on the Economics of Information Security (WEIS 2008), June 25-28 2008.