Persuasion, Social Graces, and Computer Security

Elizabeth Stobert[1], Sonia Chiasson[2], Robert Biddle[2]

[1]Department of Psychology, [2]School of Computer Science
Carleton University, Ottawa, Canada
estobert@connect.carleton.ca, chiasson@scs.carleton.ca, robert_biddle@carleton.ca

Abstract. Although computer users want to behave securely, they often lack the motivation and confidence to protect themselves and their computers. In this paper, we propose a framework that harnesses aspects of social interaction and the *Media Equation* for designing a novel approach to persuasive technology for computer security. We then apply this framework to anti-virus software, and show how this social support addresses the current weaknesses, and thus might help users in better managing their computer security.

1 Introduction

Computer security is a universally acknowledged concern, but for users it is typically not their primary focus when interacting with a computer. This creates an opportunity for persuasive technology in helping people keep their computers secure. Anti-virus software is one area particularly in need of persuasive technology. Computer users are often lax about installing and updating anti-virus software, although these simple actions can protect them from a variety of computer problems. In this paper, we propose a new framework that harnesses social interaction for designing persuasive technology for computer security, and show its applicability to an anti-virus program.

2 Background

The design of our framework draws from main three areas; these are briefly introduced in this section.

Computer Security Usable security is concerned with increasing the usability of computer security systems, while still maintaining the security they support [1]. Supporting the user creates challenges for design, since security is often a secondary task for users.

Persuasion for Security The potential applications of persuasive technology to usable security are plentiful. Users want their computers to be secure, but they are often unaware of, or unwilling to take, the necessary steps. Previous work in applying persuasion to computer security has focused on improving people's attitudes [2] and improving security behaviour, such as password choices [3].

The Media Equation We are particularly interested in the aspects of persuasive technology that deal with computers as social actors. We observe that most people have a strong desire to behave securely and some understanding that they should be behaving more securely. However, it seems that they face the experience alone and uncertain. We speculate that a social approach to persuasion for computer security will be most effective. One of the foundations of Fogg's persuasive technology was his earlier involvement with Reeves and Nass's work on the *Media Equation* [4]. It is defined by Reeves and Nass as "Media equals real life". This means that humans tend to behave as though the computer system with which they are interacting is an actual person. Studies have shown that people treat computers according to the rules of everyday human interaction and respond to politeness, flattery and generosity from a computer the way they might to another person.

3 A Social Graces Framework

Our framework draws on components of both Fogg's persuasive technology and the media equation that specifically address the kind of social support we believe will be helpful in persuading users to behave securely. These are: flattery, politeness, reciprocity, and interpersonal distance.

Flattery The media equation suggests that people will react to flattery from a computer similarly to how they react to flattery from another person. Fogg and Nass [5] found that people responded to flattery from a computer in the same way they responded to flattery from other humans. The implications for flattery in design are numerous. Computers should offer praise, even when it is not fully justified. It makes users feel happier, both with themselves and with the computer [4]. For security, this means reorienting the focus to highlighting and praising secure behaviour, rather than criticizing users for insecure behaviour.

Politeness Many rules go into the art of being polite, but in its most basic form, politeness is about trying to make people happy [4]. People show politeness toward computers when evaluating a computer's performance, and react positively to politeness from computers. In informing the user about security, computers should display politeness informing the user about security. The program should greet the user, and give the impression that since the user is paying attention to security matters, the security software is attending to the user.

Reciprocity The norm of reciprocity is at work when people respond with similar kinds of behaviour to that which they are shown. Hence, positive overtures lead to cooperation with others [6]. Reciprocity can also go the other way — if others are rude or unhelpful, people are likely to behave similarly in response. According to the results of a study by Fogg and Nass [7], humans reciprocate to computers similarly to how they reciprocate to other people. By their nature, security programs are helpful to users, but the program should put effort into making the user aware that the security program is working to help them.

Interpersonal Distance Interpersonal distance refers to the relationship between people and others while speaking. While the rules and customs of inter-

personal distance vary by culture, everyone uses distance to convey information about their stance on a situation. If a computer program is going to use a character with an image and face, care should be taken in how the face is presented. For security, user's attention should be grabbed at key moments, but contact should be minimized at less crucial times.

4 Case Study: Anti-Virus Programs

Anti-virus software is responsible for checking the user's computer for malicious programs and preventing malware from being installed. However, the user is still responsible for installing the anti-virus software on their computer, for updating it, and for running regular scans to check for computer viruses. Applying persuasion to anti-virus programs is important because it allows the users to learn and develop necessary skills for dealing with malware. In this section, we will attempt to apply the aspects of our social graces framework discussed above to a hypothetical anti-virus program.

Flattery An anti-virus program that used flattery would take the trouble to tell the user they were doing a good job, even when the user was not behaving especially well. When the user updated the software or scanned their hard drive for viruses, the computer might give them a message such as "You're good at keeping your computer virus-free!" Another opportunity for the use of flattery would arise when the results of the user's actions resulted in a virus being caught or removed. While the anti-virus program technically found and repaired the problem, messages such as "Good job freeing your computer from viruses!" would help the user feel good about their role in catching viruses, and more powerful in their ability to keep their computer safe. Users would also be more likely to think that the anti-virus program was doing a good job. Praise need not necessarily be flamboyant or even verbal/textual to be effective. Anecdotal evidence suggests that users like seeing "positive" icons and will complete tasks to restore these to a positive state. For example, to have a green or smiling icon in the system tray as opposed to a red or frowning icon.

Politeness Anti-virus programs are brief and make no effort to be kind even when sharing bad news. If programs were polite to its user, the user might well be more polite in return: considering its requests more seriously, and taking its advice more frequently. One simple way for an anti-virus program to be polite would be to add greetings and good-byes to the program. When the user opens the program, the program should greet them with a cheerful "Hello!" or perhaps "Welcome back! No viruses detected". Anti-virus programs can be polite in more subtle ways that may also positively impact users' perception. They should wait until the computer is idle to perform background scans, and should not interrupt users to restart their system (and should certainly not restart without consent).

Reciprocity The relationship between the user and the anti-virus program is mutually beneficial: if the user downloads updates and runs the virus scan, the computer finds and fixes infected files. Leveraging reciprocity in an anti-virus

program would probably involve making the user aware of the complex task being performed by the anti-virus program in finding and removing viruses from the program. The computer might remind the user of ways to help the anti-virus software, using dialogues such as "In order to check your computer for viruses, the program needs to be updated. Could you help me out by downloading the latest updates?"

Interpersonal Distance Current anti-virus programs tend to be impersonal. Interaction is fairly superficial and mechanical, making them fairly unmemorable and easy to ignore. To be more persuasive, an anti-virus program might include an on-screen character to interact with the user. For example, "Anti-virus Veronica" might be a computer security expert, who needs help from the user in order to do her job. Veronica's framing in the window might be related to the intensity of her message. When not communicating, she might be visible at a distance, in perhaps a full-body view. But when Veronica had a specific message to share, she might walk toward the window to deliver her message, seemingly growing larger for the user. As the intensity or importance of the message increased, so might the relative size of her face.

5 Conclusion

Designing for usable security can be difficult and often involves helping users help themselves. While users want their computers to be secure, they typically do not attend very closely to matters of security. Persuasive technology based on social strategies can bring new insight to designing for usable security. In particular, we suggest that social factors are critical to designing for usable security, and we have identified a framework involving social responses to flattery, politeness, reciprocity, and interpersonal distance.

References

1. Cranor, L.F., Garfinkel, S., eds.: Security and Usability: Designing Secure Systems That People Can Use. O'Reilly Media, Inc (2005)
2. Weirich, D., Sasse, M.A.: Pretty Good Persuasion: A first step towards effective password security in the real world. In: New Security Paradigms. (2001) 137–143
3. Forget, A., Chiasson, S., Biddle, R., van Oorschot, P.C.: Persuasion as education for computer security. In: AACE E-Learn Conference. (October 2007)
4. Reeves, B., Nass, C.: The Media Equation: How People Treat Computers, Television and New Media Like Real People and Places. Cambridge Univ. Press (1996)
5. Fogg, B.J., Nass, C.: Silicon sycophants: the effects of computers that flatter. International Journal of Human-Computer Studies **46** (1997) 551–561
6. Aronson, E., Wilson, T.D., Akert, R.M., Fehr, B.: Social Psychology: 3rd Canadian Edition. Pearson Prentice Hall (2007)
7. Fogg, B.J., Nass, C.: How users reciprocate to computers: An experiment that demonstrates behavior change. Technical report, Stanford University (1997)