Chapter 2
 Foreground Trust as a Security Paradigm: Turning Users into Strong Links

Stephen Marsh  
University of Ontario, Canada

Natasha Dwyer  
Victoria University, Australia

Anirban Basu  
KDDI R&D Laboratories, Japan

Tim Storer  
University of Glasgow, UK

Karen Renaud  
University of Glasgow, UK

Khalil El-Khatib  
University of Ontario, Canada

Babak Esfandiari  
Carleton University, Canada

Sylvie Noël  
University of Trento, Italy

Mehmet Vefa Bicakci  
Carleton University, Canada

ABSTRACT

Security is an interesting area, one in which we may well be guilty of misunderstanding the very people we are working for whilst trying to protect them. It is often said that people (users) are a weak link in the security chain. This may be true, but there are nuances. In this chapter, the authors discuss some of the work they have done and are doing to help users understand their information and device security and make informed, guided, and responsible decisions. This includes Device Comfort, Annoying Technologies, and Ten Commandments for designers and implementers of security and trust systems. This work is exploratory and unfinished (it should in fact never be finished), and this chapter presents a step along the way to better security users.

INTRODUCTION

Security involves difficult decisions. They are difficult because security is a process, one in which there are continuous updates, alterations, considerations and adjustments to settings, requirements, and a myriad of different profiles and patterns. Security is also a relationship between the person actually using the system we are trying to make secure, and the things they have no control over or understanding of, like the system itself (see for example Flink, 2002).

DOI: 10.4018/978-1-4666-6158-5.ch002
Often, we hear that users are the weakest link in the security chain. A simple web search will reinforce that view. For example: “You can implement rock solid network security; enforce strong, complex passwords; and install the best anti-malware tools available. Most security experts agree, however, that there is no security in the world that can guard against human error.” (Techhive, 2012). Of course, there are studies that address this, particularly where passwords are concerned, such as Notoatmodjo and Thomborson (2009), Yan et al. (2004) and Adams and Sasse (1999). There are also approaches from HCI that directly counter that view (Sasse et al, 2001). As well, there is a nascent understanding of the different aspects of users that affect IS (cf. Frangopoulos et al, 2013). In general however, it is accepted wisdom that educating users in their own defence is needed.

Today, the decisions we must make about security of many kinds occupy an important place. Whilst security has always been paramount, the difference now is the tools we use. Computers, either on desktop, laptop, or in our pockets, help us to do things more quickly. They can also help put us into difficult situations more quickly. Information – private, heretofore shared only with a chosen few, can be exposed to the many. Protecting information, devices, and people, is the task of information security.

We conjecture that, if a system is not compromised already it most certainly can be. Attacks are more sophisticated, targeted and widespread. We pour more and more intellectual capital into defences against the adversaries. But to what end? Systems now not compromised can be, and many are, with or without our knowledge whilst their own complexity increases. This ultimately results in more frustration at the very least on the part of the users we are trying to defend, and we arrive at a challenging confusion: the system is broken.

Enhanced security mechanisms such as more complex login procedures or systems that put more demands on users do not ultimately help the user engage with the security process – at the least they encourage the user to rebel (Norman, 2010). As an aside, this also appears to be the case for the very developers we depend on (Bodden et al, 2013). In our work we aim to provide systems that leverage human social norms, in particular, in our work, trust and comfort, and their darker siblings distrust and discomfort. These are tools that have been used by humans for millennia in situations of risk. The paradigm that most interests us in this instance is what Dwyer (2011) calls Foreground Trust. Foreground Trust is a toolset to allow devices to present information to users in order to allow them to make their own trust (and hence security)-focused decisions. Our most recent work in this area has been concerned with integrating comfort and trust reasoning techniques into mobile devices, which we call Device Comfort, and which is examined below.

Security experts understand of course, the power of crowdsourced security – not least, there is an understanding that engaging people in the process of personal security in public places (‘If you see something, say something’) has potential not only to increase security but also to increase awareness of security.

We are beginning the journey of designing and creating systems, models, and interfaces for, whilst thinking of, the Turing Complete User (Lialina, 2012) – the user who employs devices and applications to do many different things, sometimes all at once; the user who understands that there are different ways to do the same thing, and that individual applications for different tasks may or may not be the way in which they want to accomplish their tasks. Given their inherent understanding of ‘how they do things,’ these users deserve to be brought into the security relationship. Moreover, since, we believe, everyone can be engaged in processes that concern them, we aim to make real users into real Strong Links in the process – understanding, engaged, and responsive.

This chapter explores some of the work we have been doing with the ultimate goal of being able to engage users in the process of security,