Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Int. J. Human-Computer Studies 62 (2005) 759–783
International Journal of Human-Computer Studies
www.elsevier.com/locate/ijhcs

Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices?

Chris Wright*, Peter Ayton

Department of Psychology, City University, Northampton Square, London, EC1V 0HB, UK

Received 1 October 2004; received in revised form 12 January 2005; accepted 4 March 2005
Available online 20 April 2005
Communicated by C.M. Karat

Abstract

A longitudinal study tested whether a regret-based intervention could persuade computer users to make more security-conscious choices in relation to backing up their work and internet security. Computing science students reported their attitudes and behaviour in relation to the two issues at three timepoints (baseline, intervention and follow-up phases) over a 12-week period. In the intervention phase, students imagined themselves in a scenario where, had they chosen to act differently, they could have avoided a negative outcome. They then considered how regretful they would feel in that situation. The results showed that, for backing up, students showed more positive attitudes and data-protective behavioural choices immediately after the intervention and at follow-up, compared to their baseline measures. The second scenario was less effective at changing participants' attitudes and behaviour in relation to disabling active scripting. Possible reasons for the difference in effectiveness of the intervention for the two targeted issues are discussed.

Keywords: Regret; Choice; Decision-making; Computing; Backing-up; Internet security

*Corresponding author. Present address: Department of Mental Health Sciences, Royal Free and University College Medical School, Hampstead Campus, Rowland Hill Street, London, NW3 2PF, UK.
E-mail addresses: c.wright@medsch.ucl.ac.uk (C. Wright), P.Ayton@city.ac.uk (P. Ayton).

1071-5819/$ - see front matter
doi:10.1016/j.ijhcs.2005.03.001

1. Introduction

In recent years it has been recognized that, when assessing the reliability and security of computer systems, one should not focus exclusively on technical issues; one should also consider human factors—that is, the people who use the system (Anderson, 2001, pp. 8–9). Weirich and Sasse (2001) agree that human behaviour can play a role in computer security failure. Having a security policy is not, in itself, sufficient to guarantee system security. For example, in relation to password mechanisms, there is evidence to suggest that a large number of computer system users "consistently behave in a manner that undermines the security of the systems they are using" (Weirich and Sasse, 2001, p. 137)—by sharing passwords, writing passwords down or choosing cryptographically weak passwords. This behaviour need not necessarily result from a lack of education or awareness about the security risk or the security policy. It appears that, unless they are sufficiently motivated, system users will cut corners to avoid the extra effort that compliance with security policies requires—particularly if the recommended practices are perceived as obstacles that stop them getting on with their job.

Weirich and Sasse (2001) argue that researchers should explore methods of persuading system users that the investment of time and effort to comply with security policies is worthwhile. They also note that conventional fear appeals are unlikely to be effective in persuading all system users to behave in a security-conscious way, since many individuals have belief systems that render them "immune" to this type of communication. For example, many users did not expect that they would personally suffer any negative consequences as a result of their non-compliance with password policy and viewed *not* sharing passwords as a sign of not being a "team player", not trusting your colleagues or being a "nerd". However, interviews with system users also revealed that some individuals did make the effort to follow policies most of the time and Weirich and Sasse (2001) suggest that the attitudes and beliefs expressed by these individuals might guide the design of effective persuasion messages. For example, some of the users who chose to adhere to the password policy said that they did this in order to avoid personal embarrassment or being blamed by others. If there was a breach of system security, they felt it would be hard to justify behaviour that was contrary to the established security policy. It therefore seems that, at least in part, these system users were considering the emotional consequences of a security breach as part of their decision-making.

Psychological research and theory has begun to explore the ways in which emotions can influence human choice and judgement (Schwarz, 2000). Rather than disrupting cognitive processes as was once believed, it now appears that emotions may actually be *essential* for effective decision-making (Damasio, 1994, 2003). According to one theory, our memory for previous experiences includes the emotions associated with the events and these "somatic markers" may guide our future decision-making, either consciously or sub-consciously—if an event has a negative affective tag, the individual will avoid similar events in the future (Damasio, 1994). Finucane et al. (2000) also argue that individuals may—in certain