Applied Ergonomics 45 (2014) 1337–1342

Contents lists available at ScienceDirect

Applied Ergonomics

journal homepage: www.elsevier.com/locate/apergo

# Reducing online identity disclosure using warnings

Sandra Carpenter[a],[*], Feng Zhu[b], Swapna Kolimi[b]

[a] Department of Psychology, The University of Alabama in Huntsville, 301 Sparkman Drive, Huntsville, AL 35899, USA
[b] Department of Computer Science, The University of Alabama in Huntsville, 301 Sparkman Drive, Huntsville, AL 35899, USA

ARTICLE INFO

*Article history:*
Received 1 October 2012
Accepted 7 October 2013

*Keywords:*
Warnings
Cybersecurity
Identity protection

ABSTRACT

In an experimental design, we tested whether written warnings can reduce the amount of identity information exposure online. A psychological attack on information privacy that has been shown to be effective in previous research was launched. This attack took advantage of the fact that people respond to certain types of requests in a relatively automatic, or mindless, fashion. The experiment manipulated the word that was used in the alert header: “warning”, “caution”, or “hazard”. All warnings proved to be effective in reducing disclosure, but “hazard” proved to be most effective. Also warnings were more effective in reducing disclosure of driver’s license numbers than email addresses. The discussion (a) provides tentative conclusions why these patterns were obtained, (b) suggests how to design warnings in cyber-environments, and (c) addresses future possibilities for research on this topic.

In 2008, the Bureau of Justice Statistics reported that 11.7 million people in the U.S. experienced at least one attempted or successful incident of identity theft in the past 2 years (Office of Justice Programs, 2011). These attacks exploit psychology at least as often as technology, especially attacks used by professional attackers. Psychological attacks are strategies that use psychological principles to influence people to disclose information that they would prefer to keep private. The weakest link in security and privacy is people, many of whom fall victim to psychological attacks each year. Research done in our cybersecurity lab has empirically demonstrated the effectiveness of psychological attacks on privacy (Zhu et al., 2011a,b, 2013). The research described in this article shows that warnings can provide substantive mitigation of such attacks.

Every year in the UK, 3.2 million people are victims to scams and collectively lose £3.5 billion (Lea and Fischer, 2009). The mere combination of zip code, birth date, and gender can uniquely identify 87% individuals in the U.S. (Sweeney, 2000), and identity information links personal preferences, behaviors, and health conditions to individuals. People may fall prey to a wide range of identity exposure threats. Besides identity theft, over the last three decades, many service providers (e.g., retailers, factories, and medical clinics) have routinely collected identity information, with some service providers collecting as many as 100 identity elements from a user (Sweeney, 2002). Over 90% of U.S. commercial websites collect identity information (Culnan, 2000), and most websites that provide health information on the Internet collect health-related information (Sheehan, 2005). Third-party service providers such as *DoubleClick* (one of the largest Internet advertising service providers) have specialized in collecting, compiling, and analyzing users’ information (Solove et al., 2006).

Most people indicate that they want to keep their sensitive identity information private, but their identity exposure behaviors often do not match their attitudes (Ackerman et al., 1999; Consolvo et al., 2005; Spiekermann et al., 2001). More recently, our own research studied people’s attitudes toward keeping 26 identity elements (i.e., specific pieces of personal information) private and confirmed that most people exposed identity information that they had indicated that they wanted to keep private (Zhu et al., 2009). People tend to have a sense of personal immunity to common hazards and find it difficult to make decisions about safety under conditions of uncertainty (Bettman et al., 1987). Unfortunately, uncertainty occurs frequently in privacy exposure situations (Acquisti and Grossklags, 2005). If people cannot directly or easily perceive risks that might derive from their identity exposure, they may fall victim to psychological attacks. Rational choice models of decision-making generally understate problems that individuals have with drawing on appropriate cognitive calculation mechanisms in risky situations (March, 1994). People may therefore be unlikely to use controlled, effortful, and rational strategies for making decisions about risk and about revealing private information (Lea and Fischer, 2009). Instead, they may be more likely to use heuristic strategies for decision-making, which can reduce cognitive effort and time taken to reach a decision, but can lead to poor decisions.

[*] Corresponding author. Tel.: +1 256 824 2319; fax: +1 256 824 6949.
*E-mail addresses:* Sandra.Carpenter@uah.edu, carpens@uah.edu (S. Carpenter).

0003-6870/$ – see front matter © 2013 Elsevier Ltd and The Ergonomics Society. All rights reserved.
http://dx.doi.org/10.1016/j.apergo.2013.10.005

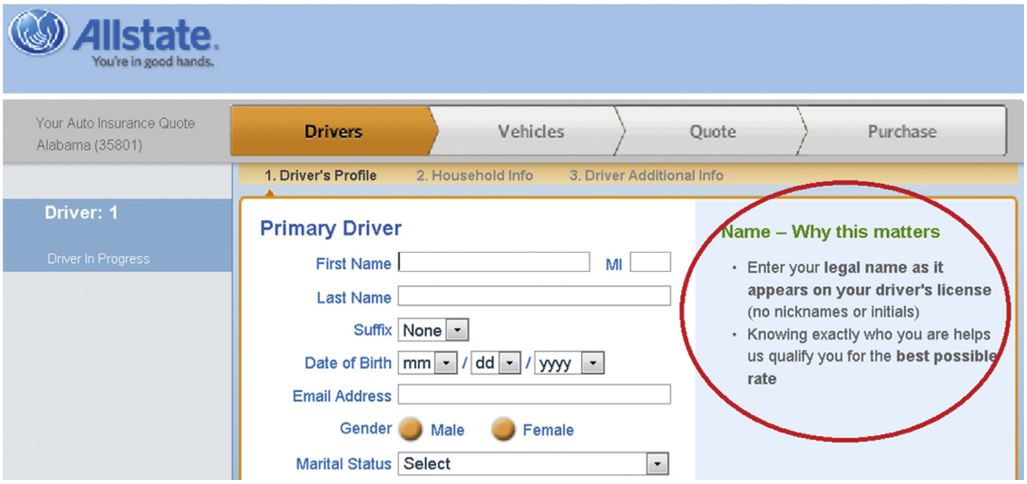
We propose that warnings presented to users via their computing devices can reduce the impact of psychological cyber-attacks on identity exposure. We have formulated this hypothesis on the basis of the extensive research on warnings in other domains (e.g., chemicals, medicines, equipment). Warnings, however, must be tested in the context in which they will be delivered to consumers (Wogalter, 2006a) because the same information in different formats can lead to different decisions (Bettman et al., 1987). Research specific to the effectiveness of computer-mediated countermeasures to psychological cyber-attacks on privacy is therefore necessary. In our research, we test the effectiveness of computer-mediated warnings in reducing people's disclosure behavior under online attack conditions.

People tend to be cognitive misers (Fiske and Taylor, 1991), using cognitive resources sparingly and typically for only important processing functions. Thus, rather than using controlled, rational strategies, they may use quick, and potentially automatic, heuristics for making decisions. There are numerous heuristics (i.e., rules of thumb) that, as psychological attacks, can lead to poor decisions about identity exposure. Our own previous research (Zhu et al., 2011b, 2013) has focused on psychological heuristic attacks (i.e., reciprocity and mindlessness).

The prevalence of heuristic, automatic compliance to a request is known as *mindlessness* (Langer, 1992). In a state of mindlessness, people rely on old categories of information to inform current decisions or behavior. Familiarity with a certain task can lead people to be confident in their ability to repeat the task (Langer, 1991). People think that they can perform the task more than adequately, which leads to the task being done in a mindless way. Most people, for example, give their phone numbers or zip codes at store check-out counters without considering how and when the information might be used. They seem to use a heuristic rule that they need to provide information when it is requested. Mindlessness has been successfully used to perpetrate scams through email, via advertisements on websites, and via cell phone messages (Lea and Fischer, 2009). These attacks are effective because the form of the request seems veridical to the victims. Fig. 1 shows that mindlessness attacks are already being used online and might elicit (unnecessary) private information from people. In this case, the information requested by the company is not necessary for an auto insurance quote, but is requested in the context of a mindless justification. That is, the online quote system will not actually take into consideration “exactly who you are” in citing the quote. The goal of the current research is to test the effectiveness of computer-mediated warnings under such mindlessness attack conditions, alerting users to potential risk of identity exposure, hopefully encouraging them to engage in controlled processing.

Controlled processing refers to the focused and logical treatment of information. Theorists and researchers have proposed complementary models for increasing the likelihood that people will use controlled (rational), rather than heuristic processing. The elaboration likelihood model (Petty and Cacioppo, 1986), for example, identifies conditions under which people will be likely to elaborate on information (i.e., focus attention and cognitive resources). Moreover, this model indicates the types of information that will be most persuasive (i.e., motivating) when people are engaged in controlled processing. In our context these types of information would include source credibility, message strength, and information about the severity of the hazard, among others. Research also indicates that people must have the motivation and the ability to resist persuasion attempts (McGuire and Papageorgis, 1961). An important step in reducing the disclosure of private information is to make the riskiness of disclosure more salient, presenting warnings with bright colors, with left-justified text, and with borders (Rousseau and Wogalter, 2006); text appearing in mixed case and including a good amount of white space (Wogalter, 2006a,b); and language that is simple, brief, and explicit (Young and Lovvoll, 1999).

Research in the associated area of providing warnings about phishing attacks can be instructive. *Phishing* refers to encouraging people to disclose personal information by directing them via email to a fraudulent website that requests the information. Schechter et al. (2007) provided participants with three types of clues that a website constituted a phishing attack: removal of https indicators, removal of site authentication images, and presenting a full screen warning page. Unfortunately, 36% of participants *using their own account* logged in to the phishing site even after receiving the most effective full page warning. These warning strategies were clearly not adequately effective. Egelman et al. (2008) tested the effectiveness of existing web browser phishing warnings (e.g., Firefox). They found active warnings (i.e., those interrupting the user's primary task) to be more effective than passive warnings (i.e., those not blocking users' ability to continue their tasks). These types of warnings, however, would be unlikely to be activated on legitimate websites, which is the focus of our research. Wu et al. (2006) evaluated the impact of three types of security toolbars in reducing people's compliance to phishing attacks. None of the security warnings, however, were successful in successfully preventing phishing attacks. From these three examples of research on phishing warnings it is clear that reducing disclosure on phishing



First Name MI
Last Name
Suffix None
Date of Birth mm / dd / yyyy
Email Address
Gender ● Male ● Female
Marital Status Select

Name – Why this matters

- Enter your **legal name as it appears on your driver's license** (no nicknames or initials)
- Knowing exactly who you are helps us qualify you for the **best possible rate**

**Fig. 1.** A screenshot of an Allstate automobile insurance website from 2011.