Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Justifying Breaking the Glass: How Accountability Can Deter Unauthorized Access

David Eargle
Brigham Young University - Utah

Anthony Osborn Vance
Brigham Young University - Utah, anthony@vance.name

Gove Allen
Brigham Young University - Utah

Daniel Barrick
Brigham Young University - Utah

Tyson Bearnson
Brigham Young University - Utah

See next page for additional authors

Authors
David Eargle, Anthony Osborn Vance, Gove Allen, Daniel Barrick, Tyson Bearnson, and Tim Tialin

Justifying Breaking the Glass: How Accountability Can Deter Unauthorized Access

David Eargle
Anthony Vance[1]
Gove Allen
Daniel Barrick
Tyson Bearnson
Tim Tialin
Marriott School of Management, Brigham Young University,
Provo, Utah, USA

ABSTRACT

This research-in-progress study examines how accountability—the expectation that one will be required to answer for one's actions, and justification—the requirement to give reasons for performing an action—can reduce instances of break-the-glass violations—can encourage compliance with data access policies. We examine whether justification can embolden users to break the glass in warranted situations, and deter users in inappropriate situations. We propose a series of lab experiments to test our hypotheses. We expect that our results will have implications for research on information security policy (ISP) compliance and practice.

Keywords: Unauthorized access, privilege escalation, information security policy violation, accountability, justification.

INTRODUCTION

Unauthorized access abuses by users of medical records systems are distressingly frequent to hospital administrators (Cooper et al. 2008; Rubenstein 2008). However, if the potential for abuse of private information is so great, why aren't these systems more tightly controlled? One reason is practical necessity. In many domains such as health care, for example, the need for flexibility in accessing critical information trumps access control (Zhao et al. 2010).

[1] Corresponding author. anthony@vance.name +1 801 361 2531

According to one hospital administrator, the problem is stated as follows: "There are just thousands of people who have access—and need to have access—to confidential information, and to try to change their behavior is a challenge" (Rubenstein 2008, p. D1). In some organizational contexts, such as healthcare and banking, users are permitted to temporarily escalate their user privileges in critical situations using a technique called "breaking the glass" (Johnson et al. 2011; Zhao et al. 2010). However, with privilege escalation comes potential for abuse.

BACKGROUND AND THEORY

One promising means for modifying the behaviors of users with broad access privileges is through accountability, which is "the implicit or explicit pressure to justify one's beliefs and actions to others" (Tadmor et al. 2009, p. 8; Vance et al. Forthcoming 2013). The construct of accountability has been examined in a variety fields, including psychology and organizational behavior (Lerner et al. 1999; Sedikides et al. 2002).

An important submanipulation of accountability is justification, or reason-giving (Lerner et al. 1999). Justification suggests that a person may behave differently if he/she is required to first give reasons for the actions he/she is about to take. Reason-giving has been shown to cause a change in intended behavior when it is required of individuals before an action or process has taken place (e.g., Simonson et al. 2000), whereas if it is required afterwards, it tends to lead to confirmation bias (Huber et al. 2001). It has been suggested that reason-giving "functions in the service of rhetorical ethos", giving the individual a chance to portray himself as "human, with human autonomy and agency" (Cheng et al. 2002, p. 417). Justification is different from rationalizations that people use to violate social norms (Siponen et al. 2010). Whereas rationalizations are kept private and typically go unverbalized, justification or reason-giving is explicitly stated and is given to another audience. Thus, justification causes one to critically examine one's motivations, whereas as rationalization does not. However, despite this compelling evidence, to date no research has examined the potential of accountability and justification on break-the-glass violations and compliance. Prior research has consistently found that a person's expectation that he/she will be held accountable reduces the likelihood the person will behave in socially unacceptable ways (Gelfand et al. 1999). At the same time, accountability and justification have been used to encourage prosocial behaviors and decision making (Mero et al. 1995). We therefore propose the following research questions:

RQ1: Can justification features in the user interface be designed to increase users' perception of accountability within the system, and thereby **discourage** users from committing break-the-glass violations?

RQ2: Can justification features in the user interface be designed to increase users' perception of accountability within the system, and thereby **encourage** users to break the glass *in warranted situations* (e.g., break the glass compliance)?

METHOD

To investigate our research question, we propose a series of laboratory experiments involving off-limits content on the Web in a university context. In these experiments, we plan to experimentally vary whether users are required to give reasons (justify themselves) before breaking the glass to view off-limits content on the Web.

Experiment 1 – Discouraging Break-the-Glass Violations

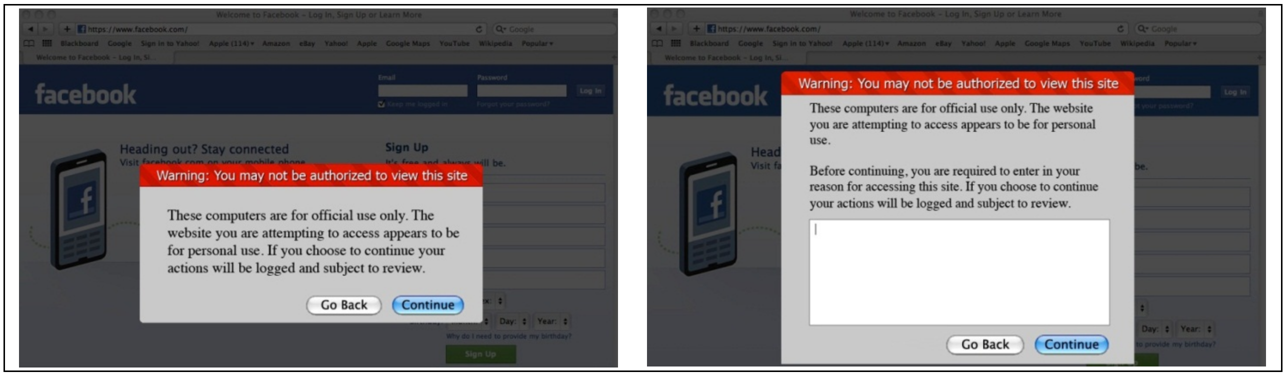
Experiment 1 will test whether justification mechanisms in the user interface can deter participants from accessing non-work related websites during an experimental task. Deception will be used so that participants will believe that the goal of the study is to complete a Web-based survey unrelated to the topic of breaking the glass. However, partway through the survey, the server hosting the survey will ostensibly crash, forcing the participants to wait while the researchers leave the room to resolve the problem with the survey server. Participants will be left on their own for approximately 15 minutes, at which time the researchers will return and dismiss the subjects.

One policy of the experimental lab is that its computers may only be used for experimental purposes. Any non-work related browsing of the Web may result in loss of compensation (in the form of extra credit or money) and future participation in the experimental lab. However, with cell phones and other devices previously confiscated for the duration of the experiment, participants will be tempted to use the Web to while away the experimental session.

When a non-study related website is accessed, a break-the-glass screen is raised warning the user that the website is off-limits, and prompting the user to choose whether he/she wants to proceed anyway. In the control treatment, no prompt for a justification for why one is about to break the glass is given (Figure 1, left-hand side). In the experimental treatment, users must offer an explanation for why they are choosing to break the glass (Figure 1, right-hand side). The dependent variable will be the number of off-limit sites that participants in each group accesses.

Experiment 2 – Encouraging Warranted Access of Off-limits Content

For Experiment 2, we will test whether justification will encourage participants to access off-limits websites when warranted as part of the experimental task. Participants will be required to complete a time-limited experimental task designed to induce participants to access off-limits content. Visiting off-limits sites will trigger the presentation of a warning to the participant similar to the ones shown in Figure 1, which will notify the participant that the website is off-limits, and that if they continue to the site, then their access to it will be logged and subject to review by campus administrators. At this point, the participant must decide whether to continue the experimental task and risk review by campus administrators, or abandon their current task and visit a different website, thus wasting precious experimental time.



Warning: You may not be authorized to view this site

These computers are for official use only. The website you are attempting to access appears to be for personal use. If you choose to continue your actions will be logged and subject to review.

Go Back Continue

Warning: You may not be authorized to view this site

These computers are for official use only. The website you are attempting to access appears to be for personal use.

Before continuing, you are required to enter in your reason for accessing this site. If you choose to continue your actions will be logged and subject to review.

Go Back Continue

Figure 1. Break the Glass Screens with and without Justification

This situation mirrors organizational contexts such as healthcare in which employees are allowed to “break the glass” in special circumstances and temporarily escalate their access privileges. We hypothesize that those participants who are given the opportunity to enter a justification will be more likely to view the off-limits content than those who have no opportunity to explain their actions.

CONCLUSION

We expect our results to show that justification mechanisms in the user interface can encourage compliance with break-the-glass policies (i.e., breaking the glass when appropriate), while discouraging break-the-glass policy violations. This is predicted by accountability theory, which explains that accountability encourages prosocial behaviors and deters anti-social behaviors. By applying justification to the problem of break-the-glass privilege escalation, our findings have the potential to extend research on information security policy violations and to inform practice for those industries that employ break-the-glass mechanisms.

REFERENCES

Cheng, M. S., and Johnstone, B. 2002. "Reasons for Reason-giving in a Public-Opinion Survey," *Argumentation*, (16:4), November, pp. 401-420.

Cooper, H., and Grynbaum, M. 2008. "State Dept. to examine breach of passport files," *New York Times*. March (available at http://www.nytimes.com/2008/03/21/world/americas/21iht-passport.4.11324015.html).

Gelfand, M. J., and Realo, A. 1999. "Individualism-collectivism and accountability in intergroup negotiations," *Journal of Applied Psychology*, (84:5), October, pp. 721-736.

Huber, O., and Seiser, G. 2001. "Accounting and convincing: the effect of two types of justification on the decision process," *Journal of Behavioral Decision Making*, (14:1), January, pp. 69-85.

Johnson, M. E., and Willey, N. D. 2011. "Usability Failures and Healthcare Data Hemorrhages," *Security & Privacy, IEEE*, (9:2), March, pp. 35-42.

Lerner, J. S., and Tetlock, P. E. 1999. "Accounting for the effects of accountability," *Psychological bulletin*, (125:2), March, pp. 255-275.

Mero, N. P., and Motowidle, S. J. 1995. "Effects of rater accountability on the accuracy and the favorability of performance ratings," *Journal of Applied Psychology*, (80:4), August, pp. 517-524.

Rubenstein, S. 2008. "Are Your Medical Records at Risk?; Amid Spate of Security Lapses, Health-Care Industry Weighs Privacy Against Quality Care," *Wall Street Journal*. (available at http://online.wsj.com/article/SB120941048217350433.html).

Schmitt, E. 2011. "White House Upgrades Computer Safety," *New York Times*. October (available at http://www.nytimes.com/2011/10/07/us/politics/white-house-orders-new-computer-security-rules.html).

Sedikides, C., Herbst, K. C., Hardin, D. P., and Dardis, G. J. 2002. "Accountability as a deterrent to self-enhancement: the search for mechanisms," *Journal of Personality and Social Psychology*, (83:3), September, pp. 592-605.

Simonson, I., and Nowlis, S. M. 2000. "The Role of Explanations and Need for Uniqueness in Consumer Decision Making: Unconventional Choices Based on Reasons," Stanford University, Graduate School of Business.

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee systems security policy violations," *MIS Quarterly*, (34:3), September, pp. 487-502.

Tadmor, C., and Tetlock, P. E. 2009. "Accountability," in *The Cambridge dictionary of psychology,* D. R. Matsumoto (ed.), Cambridge University Press: Cambridge; New York, p. 8.

Vance, A., Lowry, P. B., and Egget, D. Forthcoming 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems*, (29:4), November.

Zhao, X., and Johnson, M. E. 2010. "Managing Information Access in Data-Rich Enterprises with Escalation and Incentives," *International Journal of Electronic Commerce*, (15:1), September, pp. 79-112.