Title: Enhancing End-User Psychological Capital to Motivate Voluntary Security Actions

Purpose:
This study focuses on understanding the behavioral factors that motivate or inhibit end-users to take voluntary cyber security protective actions. Specifically, this paper investigates the use of password manager applications to combat the deleterious effects of inadequate account access controls by a subset of end-users, millennials. Current research in this field relies heavily upon the use of fear appeals to motivate end-user behavior, even though there is evidence that the use of fear to propel protection-related behaviors is not overly effective. An alternative approach that has not yet gained significant traction in the behavioral information security field is the use of positive psychology to motivate security behaviors. The form of positive psychology explored in this paper is known as Psychological Capital (PsyCap), a higher-order construct that is comprised of hope, optimism, resilience, and self-efficacy. This paper compares the results of testing two different behavioral models, one focused on fear appeals and the other that includes attempts to build the recipient's PsyCap, to determine which is more effective at engendering the voluntary use of password managers.

Design/methodology/approach:
This study uses a two-phased experimental design with two groups. In the first phase of the study, the first (control) group is presented a video with a fear-appeal that highlights the consequences of poor account management (weak passwords, password reuse, etc.) and then introduces and encourages the voluntary use of a password manager application as a free, easy-to-use solution to this problem. The second (PsyCap intervention) group is presented a similar video that describes the threat and consequences of poor password management, but also includes a modified message designed to enhance the participants' PsyCap towards using a password manager. Both groups then answer a series of survey questions about their intention to use a password manager application in the future as well as items related to constructs from protection motivation theory (PMT) and psychological capital. The second phase of the data collection is conducted approximately one week after completing the first phase survey. Participants (from both groups) are presented the same survey that collects objective data on whether they adopted the use of a password manager, subjective reasons for adoption/non-adoption, and future adoption intentions. This study measures both intentions and actual security behaviors.

Findings:
Data collection is complete and analyses is in progress. There were 356 participants in the control group and 197 participants in the PsyCap intervention group. Initial results show that the PsyCap intervention provided a statistically significant increase in actual security behavior over the control group. Control group (fear-appeal) password manager adoption was 13.5% (48 of 356) whereas PsyCap intervention group adoption was 28.4% (56 of 197). Future analysis includes conduct of Covariance Based Structural Equation Modeling (CBSEM) to test the components of the two behavioral models (PMT and PsyCap). The bulk of the analysis will be complete and able to be presented at the April 2017 conference (if accepted).

Research limitations/implications (if applicable):
The major implication of this research is that it challenges the strong focus of behavioral security researchers to use fear/PMT-related theories to explain voluntary security actions. The PMT is a foundational theory used in numerous recent IS-basket journals to explain or predict security behaviors. This study supports a move towards research that motivates voluntary security behaviors through the use of positive psychological motivators, such as captured by PsyCap.

There are numerous limitations to this study. This research focuses on a specific subset of end-users - millennials. There is evidence to suggest that results of security behavior research conducted on millennials is not generalizable to other demographics and age groups. The goal of future research will be to expand the population frame. Additionally, the participants in this study are from a single university in the Midwest United States. Although the population of the sample is approximately 20% international, future research in different geographic and cultural environments is required. Also, this study looks at the very specific security threat of poor account access management addressed by password manager applications. Additional research examining other security threats and related actions is needed.

Practical implications (if applicable) :
This research has the potential for several substantial practical implications. The first significant impact could come to organizational Security Education Training and Awareness (SETA) programs and for the general population. This study offers evidence that more emphasis should be placed upon building up the psychological capital of end-users to take appropriate security actions instead of focusing more on building a stronger feeling of fear about security threats. Additionally, the messages used in this study were short videos (7-8 minutes long) that can be presented to end-users and employees in the same manner as a Public Service Announcement (PSA) related to good security hygiene. This is a low-cost, lightweight approach to improving overall account management practices. Commercial providers of security tools and services can also benefit from this research by tailoring their marketing efforts towards millennials with messages meant to strengthen the positive psychological benefits of their products.

Originality/value:
The PsyCap construct is relatively new to the literature (circa 2005). To the authors' knowledge, only one study in behavioral information security has examined the PsyCap construct in a behavioral model (Burns et al., 2017). The Burns et al. (2017) paper models PsyCap as an antecedent contributor to the PMT sub-constructs, whereas the present study examines PsyCap as a potential alternative to fear-focused behavioral models like the PMT. Additionally, much of the behavioral security literature, including Burns et al. (2017), examines "general" security behavior intentions, whereas the present paper measures both intentions and actual behaviors for a specific security threat and related mitigating action. This paper should contribute to both the broader scholarly community and the general population of end-users by comparing and contrasting two fundamentally different behavioral models applied to an important and accessible voluntary security action.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Computers in Human Behavior, 68, 190-209.