Does an individual's ethical preference impact their decision to take voluntary security actions?

Salvatore Aurigemma, University of Tulsa, USA
Thomas Mattson, University of Tulsa, USA
Lori Leonard, University of Tulsa, USA

Purpose

The purpose of this study is to better understand if an individual's ethical preference, measured against the duality of Ethics of Care or Ethics of Justice, has a direct or moderating effect on that person's intentions and actual voluntary security actions related to account access protections. Numerous academic studies and industry surveys indicate that people are, for the most part, aware of the threat due to poor account access management (such as the use of weak or reused passwords) and the recommended mitigating actions and technologies available to them to counter the threat. However, even in the face of the knowledge and sometimes personal experience with such threats, many people still do not take the voluntary security actions that can largely protect them against the most prevalent cybersecurity threats they face. For example, the 2016 Pew Internet Security Survey found that 64% of respondents personally experienced impact from a major data breach and yet often fail to take the minimum recommended actions to protect their accounts. The same study found that while a large majority of people (75%) know what a strong password is, almost 40% admit to using weak passwords or reusing the same password on all their accounts. Unfortunately, the reuse of passwords on personal and work accounts is a common problem that routinely leads to organizational data breaches. Given that there is widespread awareness and media reporting of cybersecurity threats facing the general population, failing to take basic security actions is not only a personal issue, but has potential widespread negative consequences for one's friends, family, and employers. In short, it is becoming a moral and ethical imperative for individuals to take known voluntary security actions. In this study, a sample population of millennial college students is presented with information regarding the impact of poor account management and provided guidance on using two different protective technologies, password manager applications and two factor authentication services. We capture ethical preferences of participants and measure intent to take these protective security actions as well as actual usage a week later.

Design/methodology/approach:

This study uses a two-phased experimental design. In the first phase of the study, participants are presented videos with a basic fear-appeal that highlights the perils of account takeovers and then introduces and encourages the voluntary use of (1) a password manger application, or (2) two-factor authentication (2FA) as free, easy-to-use solutions to this problem. All participants then answer a series of survey questions to ascertain their ethical preferences and their intention to use these cyber-protective technologies in the future as well as items related to constructs associated with a number of human behavioral models. The second phase of the data collection is conducted approximately one week after completing the first phase survey. Participants are asked to provide objective data on whether they adopted the use of a password manager or 2FA, subjective reasons for adoption/non-adoption, and future adoption intentions. This study measures both intentions and actual security behaviors.

Findings:

Data collection was completed in the Fall 2017 at a small private university in the Midwest United States with over 200 participants for both phases of the study. Data analysis will be conducted in the Spring

2018. Anticipated methods include group comparisons of intention and actual behavior using t-tests and ANOVA analyses, with potential Covariance Based Structural Equation Modeling (CBSEM) to test the direct and moderating effect of ethical preferences on intentions and actions. Initial analysis will be presented at the March 2018 conference.

Research limitations/implications (if applicable):

The expectation of this research is two-fold. First, it is important to empirically evaluate if ethical preferences have any correlation with voluntary security intentions and actions. Second, the study will also capture participant justifications if they decide not to use these cyber-protective technologies to qualitatively assess whether the participants recognize an ethical /moral impetus. This information may be useful in tailoring security messaging to individuals of different ethical preferences, providing more effective activation of moral impetus to take voluntary security actions.

There are numerous limitations to this study. This research focuses on a specific subset of endusers - 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.

Practical implications (if applicable) :

This research has the potential for some interesting practical implications. One significant impact could come to organizational Security Education Training and Awareness (SETA) programs and for cybersecurity PSA-type education for the general population. If ethical preferences do have a significant impact on voluntary security actions, this may provide an opportunity to tailor security messaging to activate the moral compass of the affected individuals and result in higher security participation and better overall hygiene.

Originality/value:

To the authors' knowledge, there is very little research published that specifically looks at the impact of ethical preferences on voluntary security actions. Research has looked at other aspects of cybersecurity behaviors, such as intent to commit computer abuses. However, exploring and improving voluntary security actions can have a broad and positive impact beyond the organizational boundaries.