Title: Motivating Multifactor Authentication Use Among Millennial End-Users

Purpose:

The purpose of this study is to better understand how to motivate millennial end-users to voluntarily enable multi-factor authentication (MFA) on their online accounts. Online account takeover by malicious actors is a real, tangible, and prevalent cyber security threat. The consequences of such intrusions can be severe. For example, the FBI estimates that account takeovers related to Business Email Compromises (BEC) have resulted in over $3 billion in victim losses. Outside of the corporate environment, account takeovers can also result in other crimes such as loss of personally identifying information (PII) for use in identity theft, loss of intellectual property, or public exposure of photographs and communications of a personal nature. Fortunately, readily available (and oftentimes free) MFA technologies and services can greatly reduce or eliminate the threat of unauthorized account access and takeovers even if an end-user has lost control of their account passwords. Although widely available, it is up to individual end-users to configure capable online accounts to use MFA, and this is rarely done. For example, it is estimated that < 7% of all Google Gmail users have activate MFA, and that number drops down to 2-5% when including other online accounts. In this study, a sample population of millennial college students that use Gmail for their school email have just recently (January 2017) been authorized to use MFA for their school accounts, on a strictly opt-in basis. The goal of the study is to motivate greater use of MFA among the population for not only their school Gmail account, but other capable online accounts as well.

Design/methodology/approach:

This study uses a two-phased experimental design with three groups. In the first phase of the study, the first (control) group is presented a video with a basic fear-appeal that highlights the perils of account takeovers and then introduces and encourages the voluntary use of a MFA as a free, easy-to-use solution to this problem. Participants are informed that their school Gmail account is capable of MFA and that they are strongly encouraged to set up this security protection. The second group (intervention group #1) is presented a similar video that describes the threat and consequences of account takeover, but also includes a real-time walkthrough of configuring MFA on their school Gmail using SMS/text messaging as the second authentication factor. SMS/text message was chosen for this intervention group based upon a pilot study with a group of 22 millennials that identified SMS/text messages as the most accessible and comfortable MFA option. The third group (intervention group #2) gets the same fear-appeal as the other groups, but instead includes a real-time walkthrough of configuring MFA on their school Gmail using the “Google Prompt” service as the second authentication factor. The Google Prompt service greatly simplifies the ongoing MFA authorizations with a simple Yes/No style button for the user to push on their smartphone (Android or iPhone). However, the initial setup for using Google Prompt is more involved for iPhone users, which could be a confounding factor in adoption of this technology. All three groups then answer a series of survey questions about their intention to use MFA services 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 (from all three 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 will run from February through April 2017 at a small private university in the Midwest United States. The goal is to have at least 100 participants per group complete both phases of the study. 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 components of different behavioral models if sufficient sample size is achieved. Initial analysis will be presented at the April 2017 conference (if accepted).

Research limitations/implications (if applicable):
The expectation of this research is two-fold. First, the desired end-state is a notable increase in the use of MFA by participants in this study, not only for their school Gmail accounts, but other capable online services as well. The study will also capture participant justifications if they decide not to use MFA in order to improve the threat message in future studies. Second, the different control and intervention groups are expected to provide insight into the behavioral factors that contribute most strongly to MFA adoption, which can lead to more refined behavioral models for this specific security threat and demographic.

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 account takeover as addressed by the use of MFA services. Additional research examining other security threats and related actions is needed.

Practical implications (if applicable) :
This research has the potential for some substantial practical implications. The first significant impact could come to organizational Security Education Training and Awareness (SETA) programs and for the general population. The method used in this study represents a low-cost, lightweight approach to motivating voluntary security actions that significantly limit the chances of account takeover. Additionally, online account services that offer MFA solutions can benefit from this research by tailoring their tools and security settings presentation towards millennials to gain greater adoption.

Originality/value:
To the authors' knowledge, there is very little research published that specifically looks at

understanding and motivating security behaviors for this tangible security threat (account takeovers).