# The Effect of Trust in Authentication Methods on Risk Perceptions and Security Concerns when using Mobile Devices

*Research in Progress*

**Jordan B. Barlow**
University of St. Thomas (Minnesota)

**Sinjini Mitra**
California State University, Fullerton

## ABSTRACT

This research in progress study examines how perceptions of authentication methods on mobile devices, both biometric- and non-biometric-based, can in turn affect risk perceptions, security concerns, and intentions when completing sensitive actions on a mobile device. We conducted an initial small-scale scenario-method survey study with 62 graduate and undergraduate students to test how their perceptions (trust, usefulness, ease of use, and convenience) of authentication methods would affect their perceptions of various sensitive actions (e.g., banking, health) on a mobile device that uses a given authentication method. We found that trust in an authentication method affects risk perceptions and security concerns. In turn, such risk perceptions and security concerns affect intentions to complete such actions on that device. The effect was fully mediated. We also find that convenience, usefulness, and ease of use of an authentication method have no significant effect on risk perceptions and security concerns, and that the effect is not significantly different between biometric-based and non-biometric-based methods. This research is in progress; based on workshop feedback we plan to collect additional data to further refine our study.

## KEYWORDS

Mobile devices; trust; risk; security concerns; authentication

## INTRODUCTION

The use of authentication methods to protect mobile devices such as smartphones and tablets is now ubiquitous. While traditional authentication relied on methods such as PINs, passcodes, or passwords, industry surveys indicate that more advanced authentication methods, such as biometric-based methods (e.g., fingerprint, face recognition, etc.), are rapidly increasing in popularity in the general population (Deloitte 2018).

One open question is how the use of various authentication methods on mobile devices affects users' perceptions and behaviors when using those devices. Most research on authentication methods, particularly biometric-based methods, has focused on acceptance and adoption of those methods (Alhussain and Drew 2012; Miltgen et al. 2013) or simply comparing perceptions between various authentication methods without developing a larger nomological network (Bhagavatula et al. 2015; Guerra-Casanova et al. 2016; Khan et al. 2015; Rasnayaka and Sim 2018; Wang et al. 2019; Zimmermann and Gerber 2020). Few studies have examined how the use of these authentication methods on a mobile device affects perceptions and behaviors outside of the authentication method itself.

In this study, we examine how perceptions of various authentication methods, including trust, usefulness, convenience, and ease of use, affect the way users perceive risk and security concern when completing sensitive actions on a device, such as banking, health transactions, or other transactions with personally identifiable information. In other words, this study seeks to answer the following research question: *Do user perceptions of authentication methods on mobile devices affect the extent to which they are deterred by risk and security concerns to complete activities on their mobile device?*

# THEORY AND HYPOTHESIS DEVELOPMENT

## Theoretical Background

Much of the research to date on mobile authentication methods, particularly biometric-based methods, has been empirical in nature. These studies focus on comparing perceptions (e.g., convenience, ease of use, privacy concerns) and acceptance of authentication methods between different types of authentication methods (Bhagavatula et al. 2015; Guerra-Casanova et al. 2016; Khan et al. 2015; Rasnayaka and Sim 2018; Wang et al. 2019; Zimmermann and Gerber 2020). These studies have not examined the impact of such perceptions on mobile device behavior nor on the perceptions of risk or security concerns.

Those papers that have studied authentication methods from a theoretical standpoint have mostly focused on acceptance or adoption as the dependent variable. For example, Miltgen et al. (2013) combined elements from the Technology Acceptance Model (TAM) and its successors, as well as theory on privacy and trust, to predict the intention to accept biometric-based authentication methods. Alhussain and Drew (2012) used a qualitative methodology and a grounded theory approach to develop a theory predicting acceptance of biometric authentication based on user, organization, and system aspects.

One notable recent study theorized and tested biometric mobile authentication to examine its effects on security concerns, convenience, perceived usefulness, trust, and willingness to purchase in an online store (Ogbanufe and Kim 2018). We build on this previous work (Alhussain and Drew 2012; Miltgen et al. 2013; Ogbanufe and Kim 2018), continuing to use theories and literature of trust, security concern, risk perception, usefulness, ease of use, and convenience to examine how perceptions of an authentication method will affect perceptions and intentions regarding sensitive actions on mobile devices.

## Hypothesis Development

Multiple studies have examined whether users want to adopt authentication methods on their mobile devices based on several key constructs such as perceived usefulness and perceived ease of use (from TAM) as well as their trust in them and the convenience they offer. However, no studies have examined how such perceptions affect the willingness of users to engage in activities on their mobile devices based on their risk perceptions. We propose a mediated model where we examine not only how perceptions of authentication methods affect perceived risk and security concern, but also how those perceptions and concerns in turn affect behavior on mobile devices. In line with previous literature on risk perceptions and security concerns (Bélanger and Carter 2008; Chiu et al. 2014; Park et al. 2015; Pavlou 2003), we hypothesize that when a user perceives a potential action to have more risk or security concerns, they will be less likely to engage in that action.

*H1: When completing activities with sensitive information on mobile devices using authentication, (a) risk perceptions and (b) security concerns will be negatively related to a participant's willingness to engage in such activities.*

In turn, the remainder of our hypotheses predict that perceptions about the authentication method on a mobile device will affect risk perceptions and security concerns. Unlike previous research that has measured risk perceptions or security concerns regarding the authentication method itself (Bhagavatula et al. 2015; Guerra-Casanova et al. 2016; Khan et al. 2015; Miltgen et al. 2013; Wang et al. 2019; Zimmermann and Gerber 2020), we examine the perceptions regarding completing sensitive actions (e.g., banking, health, etc.) on the mobile device.

First, we examine the effect of perceived usefulness. Ogbanufe and Kim (2018) found that biometric-based authentication methods led to higher perceived usefulness than other methods. Miltgen et al. (2013) found that the perceived usefulness of an authentication method would lead to its acceptance. No studies have examined whether usefulness predicts how users perceive risk and security in taking sensitive actions. If a user finds an authentication method to be useful, that indicates that the user believes it works for its intended purpose, which should lead the user to feel less risk and security concern in performing sensitive actions on a device that uses that authentication method.

*H2: Perceived usefulness of an authentication method will be negatively related to the (a) risk perceptions and (b) security concerns of completing an activity with sensitive information on a mobile device that incorporates that authentication method.*

Next, we examine trust. Trust has been linked to perceptions of risk and security concerns in previous literature (Bélanger and Carter 2008). When users trust in technology, they perceive less risk and security concern because they feel they can rely on the technology to protect them. Miltgen et al. (2013) theorized a link between trust in authentication methods and general perceptions of risk. They found no significant effect; however, that study examined general risk perceptions of the authentication method, whereas we examine the risk, and security concern, of performing sensitive actions. We believe that while users may not link their trust to riskiness of an authentication method, they should link their trust in the authentication method to situations where sensitive data are involved.

*H3: Trust in an authentication method will be negatively related to the (a) risk perceptions and (b) security concerns of completing an activity with sensitive information on a mobile device that incorporates that authentication method.*

There is a tradeoff in most people's minds between security/risk on one hand, and usability on the other hand; this has been demonstrated in the context of authentication methods (Allen and Komandur 2019; Gunson et al. 2011). This theoretical tradeoff leads us to argue that the perceived ease of use and the convenience of an authentication method may actually lead users to perceive that such authentication methods are not as strong and will increase risk perceptions when using these authentication methods.

*H4: Perceived ease of use of an authentication method will be positively related to the (a) risk perceptions and (b) security concerns of completing an activity with sensitive information on a mobile device that incorporates that authentication method.*

*H5: Convenience of an authentication method will be positively related to the (a) risk perceptions and (b) security concerns of completing an activity with sensitive information on a mobile device that incorporates that authentication method.*

Our hypotheses are summarized in Figure 1 below.

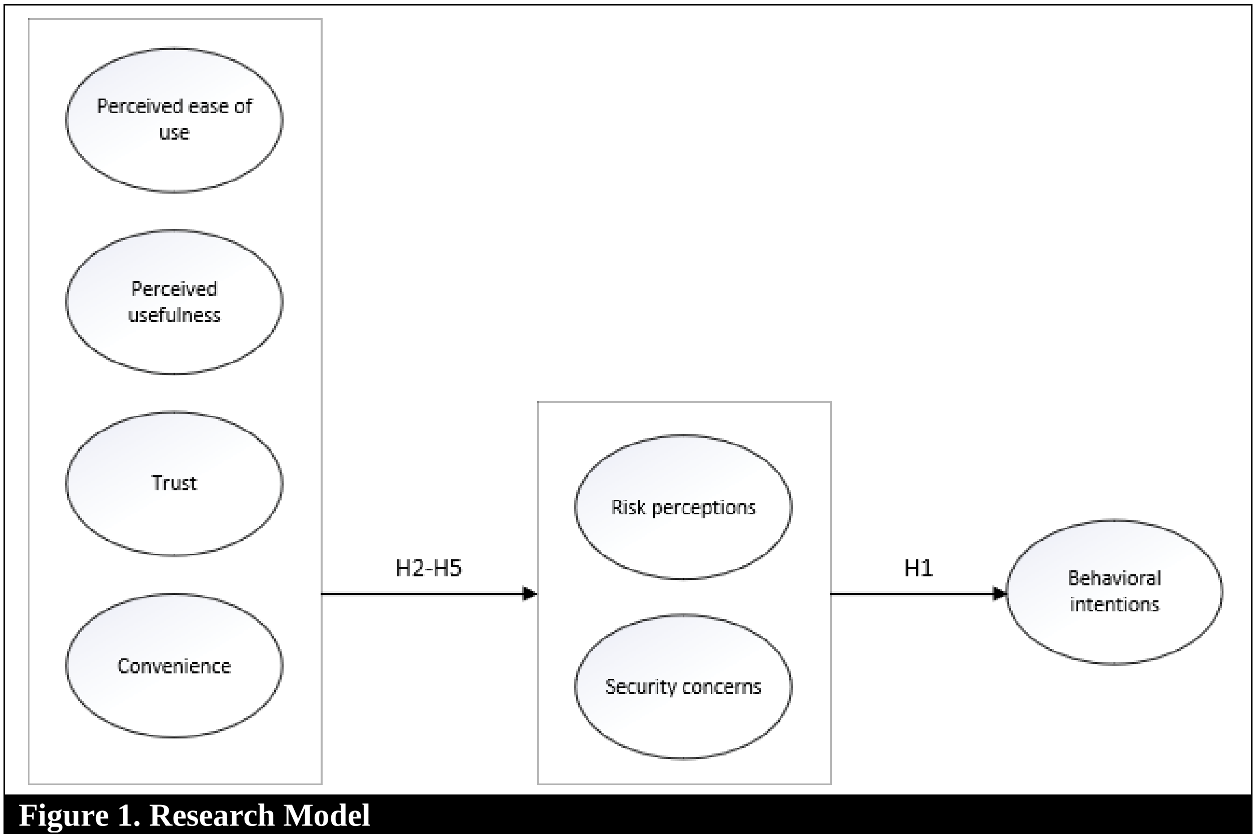

**Figure 1. Research Model**

## METHOD

### Participants

Participants were undergraduate and graduate students at a large public university in the United States. Students received a small token extra credit for participating in the study. 62 out of a total of 98 students who received the survey invitation participated in the survey (response rate of 63.3%): 45.9% were male; the average age of participants was 24.1.

### Treatments and Scenarios

A scenario method was used in the survey to prevent social desirability bias in the responses. During the survey, each participant viewed three versions of a scenario. Each scenario presented a fictional character who uses a mobile device set up with a particular authentication method. It then states that the fictional character decides to use the mobile device to complete a specific action. The survey then asks the participants how likely they would be to complete that same action, and also asks their perceptions of risk and security concerns regarding such an action. The versions of the scenario varied on two factors: (1) the type of authentication method on the fictional character's device; and (2) the sensitive action that was completed by the fictional character.

There were seven different types of authentication method that could appear in any version of the scenario: (1) PIN or passcode; (2) password; (3) hand geometry; (4) fingerprint; (5) face recognition; (6) voice recognition; and (7) retina or iris (eye) scan. We consider the first two to be "traditional" authentication methods and the latter five to be "biometric" authentication methods. Each participant was randomly assigned to one of these seven authentication methods. All scenarios that a participant viewed included the same authentication method on the fictional character's device.

There were three different actions that could appear in any version of the scenario: (1) "completing an online banking transaction on a mobile device"; (2) "using an app with personal health information on a mobile device"; and (3) "using an app that contains personally identifiable information (e.g., social security number) on a mobile device". Each participant viewed and responded to three versions of the scenario—each one containing one of these three actions, but always with the same authentication method.

## Procedures

The survey was completed online. Students received the link to complete the survey from their instructor. Students completed the survey anonymously and received credit by sharing a screenshot of the completion page to the instructor. Following the informed consent statement, the survey started with questions asking about participants' general privacy concerns when dealing with information on the Internet.

The following section of the survey introduced the seven authentication methods available to secure data on mobile devices. For each of these seven authentication methods, we asked participants their level of familiarity and experience. The next section of the survey asked questions regarding self-efficacy – specifically, how confident participants would feel using a new authentication method on their device that they had not used before.

For the remainder of the survey, each participant was asked questions regarding only one of the seven authentication methods, to reduce survey fatigue. The randomization tool in Qualtrics was used to randomly select which of the seven methods any given participant would see in both the scenarios and other sections of the survey. Before the scenarios, the survey asked participants about perceived trust, convenience, ease of use, and usefulness for the given authentication method that was assigned to them. Participants were then presented with the three scenarios and the corresponding scenario questions. The survey ended with a solicitation of demographic information.

## Variables and Measurement

All item wording is shown in full in Appendix A. Unless noted otherwise, all items used five-point Likert scales.

*Dependent Variable.* The outcome variable in this study is a user's intentions to complete a potentially sensitive action on a mobile device. *Intentions* was measured using a four-item scale adapted from Barlow et al. (2018). These items ask participants the likelihood that they would complete the action that the fictional character in the scenario completed. Thus, the intentions scale was completed three times by each participant—once per scenario.

*Mediating Variables. Risk perceptions* were measured using a three-item scale adapted from Pavlou (2003). *Security concerns* were measured using a three-item scale adapted from Ogbanufe and Kim (2018). Both risk perceptions and security concerns were measured three times—once for each of the three scenarios that a participant viewed.

*Independent Variables. Trusting intentions* was measured using a four-item scale adapted from McKnight et al. (2002). *Convenience* was measured using a three-item scale adapted from Ogbanufe and Kim (2018). *Perceived ease of use* and *perceived usefulness* were each measured using a six-item scale adapted from Davis (1989). All four of these constructs were adapted to the context by including language about the authentication method (e.g., "Learning to use *this authentication method* would be easy for me.").

*Authentication Method Control Variables.* Because each participant was randomly assigned to one specific authentication method, several variables were included in the analysis to control for which authentication method the participant saw. *Authentication method type* was a binary variable equal to 1 if the participant saw scenarios and questions involving a biometric authentication method (i.e., fingerprint, hand geometry, eye scan, voice recognition, or face recognition) and 0 if the participant saw scenarios and questions involving a traditional authentication method (i.e., PIN or passcode, password). *History with authentication method* was measured using a scale developed by the authors which asked how familiar the participant was with the authentication method. *Authentication method self-efficacy* was measured by adapting the 12-item computer self-efficacy scale (Compeau and Higgins 1995).

*General Control Variables*. We controlled for general *innovativeness in IT* using a three-item scale adapted from Yi et al. (2006). We measured general *privacy concerns* using a seven-item scaled adapted from Dinev and Hart (2004). We also collected the following demographic information as control variables: *age* (in years), legal *gender* (male, female, prefer not to answer), *experience using mobile devices* (in years), and highest level of *education* completed.

## ANALYSIS AND RESULTS

### Primary Analysis

To test our hypotheses, we ran a series of multiple linear regression models using SPSS. In our main analysis, we combined the items across all three scenarios to provide a more generalizable measure of risk perceptions, security concerns, and behavioral intentions regarding actions on a mobile phone for a specific authentication method. Thus, our final sample size was *n* = 62 (one record per subject). As a robustness check, Appendices B - D provide separate analyses for each of the three scenarios separately. To test H1 (and any potential direct—i.e., non-mediated—effects of the independent variables), we ran a model with behavioral intentions as the dependent variable. Results are shown below in Table 1.

These results show that users are less likely to complete a sensitive action on a mobile device when they perceive there is risk or security concern associated with the situation. These results support H1a and H1b.

To test H2a/H3a/H4a/H5a, we ran a model with risk perceptions as the dependent variable. Results are shown below in Table 2.

**Table 1. Linear Regression with Behavioral Intentions as DV**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 4.964 | .445 | | 11.164 | .000 |
| Perceived Usefulness | .114 | .077 | .176 | 1.487 | .144 |
| Trusting Intentions | -.011 | .069 | -.018 | -.162 | .872 |
| Ease of Use | -.046 | .073 | -.059 | -.632 | .531 |
| Convenience | .095 | .062 | .153 | 1.519 | .136 |
| **Gender *** | **-.157** | **.076** | **-.125** | **-2.070** | **.044** |
| Age | -.005 | .010 | -.038 | -.445 | .659 |
| Mobile device experience | -.004 | .014 | -.017 | -.254 | .801 |
| Education | .122 | .073 | .133 | 1.678 | .100 |
| Innovativeness in IT | -.009 | .040 | -.013 | -.218 | .829 |
| AuthMethod HistExp | -.010 | .031 | -.021 | -.324 | .748 |
| AuthMethod Type | .019 | .085 | .014 | .224 | .824 |
| Privacy Concerns | .008 | .046 | .012 | .184 | .855 |
| Computer Self-efficacy | -.028 | .051 | -.035 | -.540 | .592 |
| **Risk Perceptions **** | **-.312** | **.104** | **-.313** | **-2.986** | **.005** |
| **Security Concerns ***** | **-.512** | **.094** | **-.591** | **-5.470** | **.000** |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

These results show that if a user trusts the authentication method on a mobile device, they will be less likely to perceive risk or security concerns in performing sensitive actions on a device with that authentication method. This supports H3a. Perceived usefulness, ease of use, and convenience of an authentication method did not have a significant effect. Thus, H2a, H4a, and H5a are not supported.

To test H2b/H3b/H4b/H5b, we ran a model with security concerns as the dependent variable. Results are shown below in Table 3.

These results show that, just as with risk perceptions, trust in the authentication method leads a user to have fewer security concerns when completing sensitive actions on a mobile phone with that authentication method. This provides support for H3b. H2b, H4b, and H5b were not supported.

**Table 2. Linear Regression with Risk Perceptions as DV**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 4.229 | .868 | | 4.872 | .000 |
| Perceived Usefulness | .304 | .177 | .466 | 1.717 | .093 |
| **Trusting Intentions *** | **-.339** | **.156** | **-.528** | **-2.165** | **.035** |
| Ease of Use | -.230 | .171 | -.296 | -1.344 | .185 |
| Convenience | -.095 | .147 | -.153 | -.645 | .522 |
| Gender | -.183 | .180 | -.144 | -1.015 | .315 |
| Age | .009 | .025 | .070 | .341 | .735 |
| Mobile device experience | -.031 | .033 | -.148 | -.940 | .352 |
| Education | -.099 | .174 | -.107 | -.567 | .574 |
| Innovativeness in IT | .036 | .095 | .053 | .378 | .707 |
| AuthMethod HistExp | .047 | .072 | .099 | .651 | .518 |
| AuthMethod Type | .094 | .203 | .068 | .461 | .647 |
| Privacy Concerns | -.006 | .106 | -.008 | -.052 | .959 |
| Computer Self-efficacy | .055 | .123 | .069 | .448 | .657 |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

**Table 3. Linear Regression with Security Concerns as DV**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | T | Sig. |
| (Constant) | 4.134 | .968 | | 4.272 | .000 |
| Perceived Usefulness | .378 | .198 | .504 | 1.915 | .062 |
| **Trusting Intentions *** | **-.415** | **.174** | **-.562** | **-2.379** | **.021** |
| Ease of Use | -.157 | .191 | -.176 | -.824 | .414 |
| Convenience | -.192 | .164 | -.269 | -1.170 | .248 |
| Gender | -.128 | .201 | -.088 | -.636 | .528 |
| Age | .016 | .028 | .112 | .566 | .574 |
| Mobile device experience | -.037 | .037 | -.152 | -.999 | .323 |
| Education | -.113 | .194 | -.106 | -.582 | .564 |
| Innovativeness in IT | -.047 | .106 | -.060 | -.440 | .662 |
| AuthMethod HistExp | -.015 | .081 | -.027 | -.186 | .853 |
| AuthMethod Type | .035 | .226 | .022 | .155 | .878 |
| Privacy Concerns | .125 | .118 | .157 | 1.061 | .294 |
| Computer Self-efficacy | .074 | .137 | .082 | .542 | .590 |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

In all models, the results did not differ whether the authentication method was biometric-based or traditional.

We tested the mediation effects in our model following the procedures of Baron and Kenny (1986), along with the Sobel (1982) test. The first step was to check the direct effects of trust, PEOU, PU, and convenience on behavioral intentions (to see if there is an effect that is mediated). This model is equivalent to that shown in Table 1, with the exception of omitting the mediators from the analysis. The results of this model are shown below in Table 4.

**Table 4. Linear Regression with Behavioral Intentions as DV and No Mediators**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 1.529 | .814 | | 1.879 | .066 |
| Perceived Usefulness | -.174 | .166 | -.269 | -1.050 | .299 |
| **Trusting Intentions *** | **.307** | **.147** | **.480** | **2.093** | **.042** |
| Ease of Use | .106 | .161 | .137 | .662 | .511 |
| Convenience | .223 | .138 | .360 | 1.614 | .113 |
| Gender | -.035 | .169 | -.028 | -.206 | .837 |
| Age | -.015 | .023 | -.127 | -.656 | .515 |
| Mobile device experience | .025 | .031 | .119 | .807 | .424 |
| Education | .211 | .163 | .229 | 1.292 | .203 |
| Innovativeness in IT | .004 | .089 | .006 | .044 | .965 |
| AuthMethod HistExp | -.017 | .068 | -.036 | -.250 | .804 |
| AuthMethod Type | -.028 | .190 | -.020 | -.148 | .883 |
| Privacy Concerns | -.054 | .099 | -.078 | -.544 | .589 |
| Computer Self-efficacy | -.083 | .115 | -.105 | -.720 | .475 |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

The results in Table 4 show that trust in an authentication method does affect intentions of users to perform sensitive actions on mobile devices using that authentication method. The second step of mediation analysis is to show an effect of the mediator on the dependent variable; as shown in Table 1, the mediators (risk perceptions and security concerns) have a significant effect on behavioral intentions. The third step is demonstrating an effect of the independent variable on the mediator; trusting intentions has a significant effect on both mediators (see Tables 2 and 3). The final step is to check whether the independent variable influences the dependent variable after controlling for the mediator. Trusting intentions have no direct effect on behavioral intentions when controlling for the mediators (see Table 1). This is confirmed by the Sobel tests: (for risk perceptions: test-statistic = 1.760, *p* = 0.078; for security concerns: test-statistic = 2.185, *p* = 0.029). Thus, the effect is fully mediated.

## DISCUSSION

There are three main findings from our study. First, we found that trust in a mobile device's authentication method influences the level to which users perceive risk and security concerns in the actions they would take on that mobile device, which in turn influences users' intentions to complete certain actions on that device. The effect was fully mediated, meaning that even though trust in an authentication method has no direct effect on which actions users intend to complete on their mobile devices, there is an indirect effect. The behavior of a user is only affected by perceptions of the authentication method through risk and security perceptions of actions being affected by trust in the authentication.

Next, we found no significant effect for usefulness, ease of use, and convenience of the authentication method. While previous literature indicates that these variables do have an effect on whether users adopt them, we found that these perceptions did not ultimately affect how users perceived or intended to behave in regard to mobile device actions with sensitive data.

Third, while not explicitly hypothesized, we found that there was no significant difference between biometric-based and non-biometric-based authentication methods in regard to perceived risk, security concerns, or intentions. While users may perceive these authentication methods differently, the difference between them ultimately does not affect how users perceive certain actions on a mobile device.

## Limitations

The main limitation of the study is a relatively smaller sample size. Although the size was reasonable for valid statistical inference ($n > 30$), a larger sample may have implied better generalization of our results to a bigger population. We hence expect to continue collecting data for a future study outside of the university and conduct more rigorous analysis using the current results as a baseline. Second, our sample consisted of students, both graduate and undergraduate, enrolled in a large public university. Although the participants came from diverse demographic backgrounds, we believe that a better representative sample of the general population that includes people of varying ages would lead to more general conclusions as perceptions tend to vary by this demographic to a certain extent.

Another limitation is the focus of authentication methods only at the device level. This study did not consider the effects of authentication built into the actual application (e.g., banking app, health information app). We hope to address this issue and incorporate it into our scenario method before collecting additional data.

## Theoretical Contributions

We believe this research makes several theoretical contributions. First, this study is one of the first to examine perceptions of biometric-based and non-biometric-based authentication methods outside of the perspective of simply adopting such methods. Our study is the first to examine how such methods impact the perceived risk and security concern of other actions on mobile devices.

Next, we believe this research contributes to the literature by being one of the first to examine security aspects of actions taken on a mobile device by not only considering the action itself, but also considering other aspects of the mobile device. While many studies have examined the use of banking, health, and other apps including sensitive data, we are not aware of any study that has gone beyond perceptions of that action or app to also include how other security settings on the mobile device (e.g., authentication) could affect those behaviors.

Finally, as many earlier papers on perceptions of biometrics were in the early development stages of biometric-based methods, this study also contributes by showing the changing attitudes of users. In this study, we found no significant difference between biometric-based and non-biometric-based methods in how they affected users' perceptions of risk, security concerns, and willingness to complete actions on a mobile device.

## Implications for Practice

The main implication for practice is that designers of mobile devices should be aware that authentication methods available on the device influence users' perceptions (and ultimately behavior) around the riskiness and security concerns of completing actions on those devices. The perceived risk and security concerns around any given action are influenced not only by the action itself, but also by additional security measures available on the phone (i.e., authentication). App designers should also consider the impact that technical aspects of users' devices including authentication might have on how users ultimately choose to view and use those apps.

## Next Steps and Goals for Workshop

This study is a work in progress. We completed a small-scale data collection with undergraduate and graduate students. We plan to collect additional data after presenting our work at the workshop. Further, we hope to enrich our theory and hypothesis development with additional literature and fine-tuning of our theoretical background. We also plan to expand our Discussion section with more insights for both theory and practice. We look forward to discussing these additional plans as we present our work.

# REFERENCES

Alhussain, T., and Drew, S. 2012. "Developing a Theoretical Framework for the Adoption of Biometrics in M-Government Applications Using Grounded Theory," in: *Security Enhanced Applications for Information Systems*, C. Kalloniatis (ed.), InTech, pp. 183-208.

Allen, C. G., and Komandur, S. 2019. "The Relationship Between Usability and Biometric Authentication in Mobile Phones," *International Conference on Human-Computer Interaction*, pp. 183-189.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. 2018. "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance," *Journal of the Association for Information Systems* (19:8), p. 3.

Baron, R. M., and Kenny, D. A. 1986. "The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," *Journal of personality and social psychology* (51:6), p. 1173.

Bélanger, F., and Carter, L. 2008. "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems* (17:2), pp. 165-176.

Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., and Savvides, M. 2015. "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," *Internet Society Usable Security (USEC)*.

Chiu, C. M., Wang, E. T., Fang, Y. H., and Huang, H. Y. 2014. "Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk," *Information Systems Journal* (24:1), pp. 85-114.

Compeau, D. R., and Higgins, C. A. 1995. "Computer self-efficacy: Development of a measure and initial test," *MIS quarterly*), pp. 189-211.

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly*), pp. 319-340.

Deloitte 2018. "Biometric authentication is gaining trust--but is it foolproof?" Retrieved from https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/biometric-authentication-future-applications.html.

Dinev, T., and Hart, P. 2004. "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behaviour & Information Technology* (23:6), pp. 413-422.

Guerra-Casanova, J., Ríos-Sánchez, B., Viana-Matesanz, M., Bailador, G., Sánchez-Ávila, C., and De Giles, M. J. M. 2016. "Comfort and security perception of biometrics in mobile phones with widespread sensors," *2016 IEEE 35th symposium on reliable distributed systems workshops (SRDSW)*, pp. 13-18.

Gunson, N., Marshall, D., Morton, H., and Jack, M. 2011. "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security* (30:4), pp. 208-220.

Khan, H., Hengartner, U., and Vogel, D. 2015. "Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying," *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pp. 225-239.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and validating trust measures for e-commerce: An integrative typology," *Information systems research* (13:3), pp. 334-359.

Miltgen, C. L., Popovič, A., and Oliveira, T. 2013. "Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context," *Decision Support Systems* (56), pp. 103-114.

Ogbanufe, O., and Kim, D. J. 2018. "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decision Support Systems* (106), pp. 1-14.

Park, I., Sharman, R., and Rao, H. R. 2015. "Disaster experience and hospital information systems: an examination of perceived information assurance, risk, resilience, and his usefulness," *Mis Quarterly* (39:2), pp. 317-344.

Pavlou, P. A. 2003. "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International journal of electronic commerce* (7:3), pp. 101-134.

Rasnayaka, S., and Sim, T. 2018. "Who wants Continuous Authentication on Mobile Devices?," *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1-9.

Sobel, M. E. 1982. "Asymptotic confidence intervals for indirect effects in structural equation models," *Sociological methodology* (13), pp. 290-312.

Wang, K., Zhou, L., and Zhang, D. 2019. "User Preferences and Situational Needs of Mobile User Authentication Methods," *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 18-23.

Yi, M. Y., Jackson, J. D., Park, J. S., and Probst, J. C. 2006. "Understanding information technology acceptance by individual professionals: Toward an integrative view," *Information & Management* (43:3), pp. 350-363.

Zimmermann, V., and Gerber, N. 2020. "The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes," *International Journal of Human-Computer Studies* (133), pp. 26-44.

## APPENDIX A. SURVEY ITEMS

| Construct | Item Ref | Items (5 point Disagree/Agree scales unless otherwise noted) | Source |
|---|---|---|---|
| Behavioral Intentions | INT-01 | In this situation, I would do the same as Joe. | Barlow et al. (2018) (adapted) |
| | INT-02 | If I were Joe, I would have also used my smartphone with this level of authentication to complete this action. | |
| | INT-03 | I think I would do what Joe did. | |
| | INT-04 | I think others would do the same if they were Joe. | |
| Risk perceptions | RP01 | How would you characterize the decsion to complete this action on a mobile device? [1-Insignificant risk / 5-Significant risk] | Pavlou (2003) (adapted) |
| | RP02-R | How would you characterize the decsion to complete this action on a mobile device? [1-Very negative / 5-Very positive (R)] | |
| | RP03-R | How would you characterize the decsion to complete this action on a mobile device? [1-High potential for loss / 5-High potential for gain (R)] | |
| Security concern | SECCON1-R | I feel that completing this action on a mobile device would be: [1-Unsafe / 5-Safe (R)] | Ogbanufe and Kim (2018) (adapted) |
| | SECCON2-R | I feel that completing this action on a mobile device would be: [1-Not secure / 5-Secure (R)] | |
| | SECCON3 | I feel that completing this action on a mobile device would be: [1-Protected / 5-Unprotected] | |
| Perceived usefulness | PU1 | Using this authentication method would enable me to securely accomplish tasks more quickly. | Davis (1989) (adapted) |
| | PU2 | Using this authentication method would improve my ability to securely accomplish tasks. | |
| | PU3 | Using this authentication method would increase my ability to be productive in a safe environment. | |
| | PU4 | Using this authentication method would enhance my effectiveness in securely completing tasks. | |
| | PU5 | Using this authentication method would make it easier to securely accomplish tasks. | |
| | PU6 | I would find this authentication method useful to securely accomplish tasks. | |
| Trusting intentions | TRUST1 | On mobile devices where I complete a task that needs to be secure, I would feel comfortable depending on this authentication method. | McKnight et al. (2002) (adapted) |
| | TRUST2 | I can always rely on this authentication method when I use a mobile device to complete a task that needs to be secure. | |
| | TRUST3 | I feel that I can count on this authentication method to help when I use a mobile device to complete a task that needs to be secure. | |
| | TRUST4 | On mobile devices where I complete tasks that need to be secure, I would use this authentication method. | |
| Convenience | CONV1 | I feel that this method of authentication is: [1-Difficult / 5-Easy] | Ogbanufe and Kim (2018) (adapted) |
| | CONV2 | I feel that this method of authentication is: [1-Inconvenient / | |

| | | | |
|---|---|---|---|
| | | 5-Convenient] | |
| | CONV3 | I feel that this method of authentication is: [1-Time-consuming / 5-Fast] | |
| Ease of use | PEOU1 | Learning to use this authentication method would be easy for me. | Davis (1989) (adapted) |
| | PEOU2 | I would find it easy to get this authentication method to do what I want it to do. | |
| | PEOU3 | My interaction with this authentication method would be clear and understandable. | |
| | PEOU4 | I would find this authentication method to be flexible to interact with. | |
| | PEOU5 | It would be easy for me to become skillful at using this authentication method. | |
| | PEOU6 | I would find this authentication method easy to use. | |
| Auth Method History | AMH-01 | Authentication methods are used to secure data on mobile devices (e.g., smartphone, tablet). How familiar are you with each of the following authentication methods? [5-point familiar/unfamiliar] | (original) |
| Privacy concerns | PC-01 | I am concerned that the information I submit on the Internet could be misused. | Dinev and Hart (2004) (adapted) |
| | PC-02 | I am concerned that credit card information can be stolen while being trasferred on the Internet. | |
| | PC-03 | I am concerned about submitting information on the Internet, because of what others might do with it. | |
| | PC-04 | I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee. | |
| | PC-05 | When I am online, I have the feeling of being watched. | |
| | PC-06 | When I am online, I have the feeling that all my actions are being tracked and monitored. | |
| | PC-07 | I am concerned that a person can find out personal information about me when I am online. | |
| Authentication method self-efficacy | CSE-Intro | Imagine you were given a new authentication method to use on your mobile device - one that you have never used before. The following questions ask you to indicate whether you could use this unfamiliar authentication method under a variety of conditions. For each condition, please rate your confidence regarding whether you think you would be able to successfully use the authentication method. | Compeau and Higgins (1995) (adapted from computer self-efficacy scale) |
| | CSE-Intro | I could successfully use the authentication method on my device…   [1-Not Confident / 5-Confident] | |
| | CSE01 | … if there was no one around to tell me what to do as I go. | |
| | CSE02 | … if I had never used a method like it before. | |
| | CSE03 | … if I had only a manual for reference. | |
| | CSE04 | … if I had seen someone else using it before trying it myself. | |
| | CSE05 | … if I could call someone for help if I got stuck. | |
| | CSE06 | … if someone else had helped me get started. | |

| | | | |
|---|---|---|---|
| | CSE07 | … if I had a lot of time to complete the task on the device where it was used. | |
| | CSE08 | … if I had just the built-in help facility for assistance. | |
| | CSE09 | … if someone showed me how to do it first. | |
| | CSE10 | … if I had used similar methods before this one to do the same job. | |
| Innovativeness in IT | INN1 | If I heard about a new information technology, I would look for ways to experiment with it. | Yi et al. (2006) |
| | INN2 | Among my peers, I am usually the first to try out new information technologies. | |
| | INN3 | I like to experiment with new information technologies. | |
| Gender | Gender | I am legally… [Male/Female/Prefer not to answer] | - |
| Age | Age | My age is… [open numerical field] | - |
| Mobile Experience | Mobile Experience | Number of years (approximate) that I've used a mobile device (e.g., smartphone, tablet). [open numerical field] | - |
| Education | Education | Highest level of education completed: [High School / Undergraduate degree / Graduate degree] | - |

## APPENDIX B. ANALYSIS ON BANKING SCENARIO

To test our hypotheses on each of the three separate sensitive actions (i.e., banking, health, personally identifiable information), we replicated our main analyses on these three subsets of data. This appendix reports the results for the banking scenario. Specifically, participants were asked about risk perceptions, security concerns, and behavioral intentions in a scenario where the fictional character "electronically deposit[s] a check into his personal checking account". Table B1 is analogous to Table 1 in the main text, Table B2 is analogous to Table 2, and Table B3 is analogous to Table 3. This appendix does not show the full detail of mediation testing, but the results match those of the main analysis. Because each participant completed all three versions of the scenario, the sample size is the same for all scenarios (N = 62). Results (see tables below) are the same as the main results.

**Table B1. Behavioral Intention as DV for Banking Scenario**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 4.579 | .687 | | 6.665 | .000 |
| Perceived Usefulness | .170 | .123 | .228 | 1.385 | .173 |
| Trusting Intentions | -.049 | .113 | -.067 | -.434 | .666 |
| Ease of Use | .070 | .116 | .078 | .600 | .552 |
| Convenience | .009 | .102 | .013 | .087 | .931 |
| Gender | -.093 | .124 | -.064 | -.747 | .459 |
| Age | -.009 | .017 | -.063 | -.518 | .607 |
| Mobile device experience | .006 | .023 | .025 | .268 | .790 |
| Education | .115 | .118 | .109 | .971 | .337 |
| Innovativeness in IT | -.117 | .066 | -.152 | -1.777 | .082 |
| AuthMethod_HistExp | .010 | .049 | .018 | .204 | .839 |
| AuthMethod_Type | .065 | .138 | .041 | .468 | .642 |
| Privacy Concerns | .013 | .072 | .017 | .183 | .856 |
| Computer Self-efficacy | -.112 | .083 | -.124 | -1.347 | .185 |
| **Security Concern **** | **-.329** | **.098** | **-.466** | **-3.372** | **.002** |
| **Risk Perceptions *** | **-.273** | **.119** | **-.333** | **-2.297** | **.026** |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

**Table B2. Risk Perceptions as DV for Banking Scenario**

| Predictors | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | 4.821 | 1.164 | | 4.141 | .000 |
| Perceived Usefulness | .231 | .238 | .255 | .973 | .336 |
| **Trusting Intentions *** | **-.512** | **.210** | **-.574** | **-2.442** | **.018** |
| Ease of Use | .040 | .230 | .037 | .172 | .864 |
| Convenience | -.241 | .197 | -.280 | -1.223 | .227 |
| Gender | -.321 | .241 | -.183 | -1.332 | .189 |
| Age | -.023 | .034 | -.135 | -.684 | .498 |
| Mobile device experience | -.050 | .045 | -.168 | -1.107 | .274 |
| Education | -.072 | .233 | -.056 | -.308 | .760 |
| Innovativeness in IT | .186 | .127 | .199 | 1.462 | .150 |
| AuthMethod_HistExp | .065 | .097 | .097 | .664 | .510 |
| AuthMethod_Type | .048 | .272 | .025 | .177 | .860 |
| Privacy Concerns | -.055 | .142 | -.057 | -.385 | .702 |
| Computer Self-efficacy | .070 | .164 | .064 | .428 | .670 |

* $p$ < 0.05; ** $p$ < 0.01; *** $p$ < 0.001

**Table B3. Security Concerns as DV for Banking Scenario**

| Predictors | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | 4.352 | 1.418 | | 3.069 | .004 |
| Perceived Usefulness | .420 | .289 | .399 | 1.452 | .153 |
| **Trusting Intentions *** | **-.601** | **.256** | **-.579** | **-2.350** | **.023** |
| Ease of Use | .126 | .280 | .101 | .451 | .654 |
| Convenience | -.372 | .240 | -.371 | -1.546 | .129 |
| Gender | -.340 | .294 | -.167 | -1.158 | .253 |
| Age | -.019 | .041 | -.094 | -.453 | .653 |
| Mobile device experience | -.059 | .055 | -.172 | -1.080 | .286 |
| Education | -.004 | .284 | -.003 | -.014 | .989 |
| Innovativeness in IT | .153 | .155 | .141 | .988 | .328 |
| AuthMethod_HistExp | .082 | .118 | .106 | .689 | .494 |
| AuthMethod_Type | -.107 | .331 | -.048 | -.322 | .749 |
| Privacy Concerns | .004 | .173 | .003 | .022 | .983 |
| Computer Self-efficacy | .030 | .200 | .024 | .152 | .880 |

* $p$ < 0.05; ** $p$ < 0.01; *** $p$ < 0.001

## APPENDIX C. ANALYSIS ON HEALTH DATA SCENARIO

To test our hypotheses on each of the three separate sensitive actions (i.e., banking, health, personally identifiable information), we replicated our main analyses on these three subsets of data. This appendix reports the results for the health scenario. Specifically, participants were asked about risk perceptions, security concerns, and behavioral intentions in a scenario where the fictional character "update[s] information about his current health issues in a medical app". Table C1 is analogous to Table 1 in the main text, Table C2 is analogous to Table 2, and Table C3 is analogous to Table 3. Because each participant completed all three versions of the scenario, the sample size is the same for all scenarios (N = 62).

For this particular scenario, risk perceptions and security concerns still significantly affected behavioral intentions (H1), but trust in the authentication method did not affect risk perceptions or security concerns of working with health data on a mobile device with that authentication method. Rather, ease of use of the authentication method had a significant effect on these mediating variables.

**Table C1. Behavioral Intention as DV for Health Scenario**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 4.462 | .614 | | 7.268 | .000 |
| Perceived Usefulness | .020 | .122 | .025 | .166 | .869 |
| Trusting Intentions | .121 | .107 | .150 | 1.129 | .265 |
| Ease of Use | -.010 | .125 | -.011 | -.083 | .934 |
| Convenience | .164 | .101 | .211 | 1.631 | .110 |
| Gender | -.128 | .122 | -.081 | -1.049 | .300 |
| Age | -.007 | .017 | -.046 | -.411 | .683 |
| Mobile device experience | .007 | .023 | .026 | .308 | .760 |
| Education | .154 | .118 | .133 | 1.299 | .200 |
| Innovativeness in IT | -.037 | .067 | -.043 | -.548 | .586 |
| AuthMethod_HistExp | .014 | .051 | .023 | .272 | .787 |

| | | | | | |
|---|---:|---:|---:|---:|---:|
| AuthMethod_Type | .066 | .138 | .038 | .477 | .636 |
| Privacy Concerns | -.028 | .076 | -.032 | -.373 | .711 |
| Computer Self-efficacy | -.109 | .084 | -.110 | -1.292 | .203 |
| **Security Concern **** | **-.384** | **.122** | **-.465** | **-3.149** | **.003** |
| **Risk Perceptions *** | **-.303** | **.134** | **-.319** | **-2.266** | **.028** |
| * *p* < 0.05; ** *p* < 0.01; *** *p* < 0.001 | | | | | |

**Table C2. Risk Perceptions as DV for Health Scenario**

| Predictors | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---:|---:|---:|---:|---:|
| | B | Std. Error | Beta | | |
| (Constant) | 1.938 | 1.097 | | 1.768 | .084 |
| Perceived Usefulness | .235 | .224 | .272 | 1.048 | .300 |
| Trusting Intentions | -.206 | .198 | -.243 | -1.042 | .303 |
| **Ease of Use *** | **-.593** | **.216** | **-.577** | **-2.742** | **.009** |
| Convenience | .144 | .186 | .176 | .775 | .442 |
| Gender | -.066 | .227 | -.040 | -.291 | .772 |
| Age | .037 | .032 | .227 | 1.158 | .253 |
| Mobile device experience | -.025 | .042 | -.088 | -.589 | .559 |
| Education | .114 | .220 | .094 | .520 | .605 |
| Innovativeness in IT | .041 | .120 | .046 | .341 | .735 |
| AuthMethod_HistExp | .003 | .092 | .005 | .035 | .972 |
| AuthMethod_Type | -.063 | .256 | -.035 | -.247 | .806 |
| Privacy Concerns | .171 | .134 | .187 | 1.283 | .206 |
| Computer Self-efficacy | .164 | .155 | .157 | 1.062 | .294 |
| * *p* < 0.05; ** *p* < 0.01; *** *p* < 0.001 | | | | | |

**Table C3. Security Concerns as DV for Health Scenario**

| Predictors | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---:|---:|---:|---:|---:|
| | B | Std. Error | Beta | | |
| (Constant) | 2.470 | 1.203 | | 2.054 | .046 |
| Perceived Usefulness | .151 | .246 | .152 | .614 | .542 |
| Trusting Intentions | -.220 | .217 | -.225 | -1.013 | .316 |
| **Ease of Use *** | **-.501** | **.237** | **-.424** | **-2.111** | **.040** |
| Convenience | .051 | .204 | .054 | .252 | .802 |
| Gender | -.047 | .249 | -.024 | -.188 | .852 |
| Age | .042 | .035 | .225 | 1.204 | .235 |
| Mobile device experience | -.036 | .046 | -.112 | -.782 | .438 |
| Education | .069 | .241 | .049 | .288 | .774 |
| Innovativeness in IT | -.109 | .131 | -.107 | -.833 | .409 |
| AuthMethod_HistExp | -.097 | .100 | -.134 | -.968 | .338 |

| | | | | | |
|---|---|---|---|---|---|
| AuthMethod_Type | -.014 | .281 | -.007 | -.049 | .961 |
| **Privacy Concerns *** | **.319** | **.147** | **.303** | **2.177** | **.035** |
| Computer Self-efficacy | .190 | .170 | .158 | 1.118 | .269 |
| * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ | | | | | |

## APPENDIX D. ANALYSIS ON PERSONALLY IDENTIFIABLE INFORMATION SCENARIO

To test our hypotheses on each of the three separate sensitive actions (i.e., banking, health, personally identifiable information), we replicated our main analyses on these three subsets of data. This appendix reports the results for the personally identifiable information scenario. Specifically, participants were asked about risk perceptions, security concerns, and behavioral intentions in a scenario where the fictional character “complete[s] a tax form that includes his social security number”. Table D1 is analogous to Table 1 in the main text, Table D2 is analogous to Table 2, and Table D3 is analogous to Table 3. Because each participant completed all three versions of the scenario, the sample size is the same for all scenarios (N = 62). In this scenario, security concerns (but not risk perceptions) predicted behavioral intentions. None of the independent variables predicted risk perceptions nor security scenarios.

**Table D1. Behavioral Intention as DV for Personally Identifiable Info Scenario**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 4.212 | .889 | | 4.737 | .000 |
| Perceived Usefulness | .045 | .156 | .044 | .286 | .776 |
| Trusting Intentions | .046 | .137 | .045 | .333 | .741 |
| Ease of Use | -.140 | .147 | -.115 | -.952 | .346 |
| Convenience | .177 | .127 | .182 | 1.395 | .170 |
| Gender | -.134 | .156 | -.068 | -.861 | .394 |
| Age | .002 | .022 | .011 | .096 | .924 |

| | | | | | |
|---|---|---|---|---|---|
| Mobile device experience | -.005 | .029 | -.015 | -.172 | .864 |
| Education | .096 | .152 | .066 | .633 | .530 |
| Innovativeness in IT | .100 | .082 | .095 | 1.221 | .229 |
| AuthMethod_HistExp | -.079 | .064 | -.106 | -1.246 | .219 |
| AuthMethod_Type | -.078 | .176 | -.036 | -.447 | .657 |
| Privacy Concerns | .037 | .094 | .034 | .391 | .698 |
| Computer Self-efficacy | .119 | .105 | .096 | 1.130 | .264 |
| **Security Concern ***** | **-.681** | **.130** | **-.763** | **-5.240** | **.000** |
| Risk Perceptions | -.097 | .158 | -.090 | -.616 | .541 |
| * *p* < 0.05; ** *p* < 0.01; *** *p* < 0.001 | | | | | |

**Table D2. Risk Perceptions as DV for Personally Identifiable Info Scenario**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 5.929 | 1.330 | | 4.458 | .000 |
| Perceived Usefulness | .447 | .271 | .473 | 1.647 | .106 |
| Trusting Intentions | -.298 | .240 | -.321 | -1.243 | .220 |
| Ease of Use | -.137 | .263 | -.122 | -.523 | .604 |
| Convenience | -.187 | .226 | -.208 | -.830 | .411 |
| Gender | -.160 | .276 | -.088 | -.581 | .564 |
| Age | .012 | .038 | .067 | .311 | .757 |
| Mobile device experience | -.020 | .051 | -.064 | -.386 | .701 |
| Education | -.338 | .267 | -.253 | -1.269 | .211 |
| Innovativeness in IT | -.119 | .145 | -.122 | -.820 | .416 |
| AuthMethod_HistExp | .074 | .111 | .107 | .665 | .509 |
| AuthMethod_Type | .296 | .311 | .148 | .951 | .346 |
| Privacy Concerns | -.133 | .162 | -.133 | -.823 | .415 |
| Computer Self-efficacy | -.070 | .188 | -.061 | -.374 | .710 |
| * *p* < 0.05; ** *p* < 0.01; *** *p* < 0.001 | | | | | |

**Table D3. Security Concerns as DV for Personally Identifiable Info Scenario**

| | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| Predictors | B | Std. Error | Beta | t | Sig. |
| (Constant) | 5.581 | 1.613 | | 3.460 | .001 |
| Perceived Usefulness | .564 | .329 | .491 | 1.713 | .093 |
| Trusting Intentions | -.425 | .291 | -.376 | -1.461 | .151 |
| Ease of Use | -.097 | .318 | -.071 | -.306 | .761 |
| Convenience | -.256 | .273 | -.234 | -.935 | .354 |
| Gender | .004 | .334 | .002 | .013 | .990 |
| Age | .024 | .047 | .112 | .519 | .606 |

| | | | | | |
|---|---|---|---|---|---|
| Mobile device experience | -.017 | .062 | -.044 | -.266 | .791 |
| Education | -.404 | .323 | -.248 | -1.250 | .218 |
| Innovativeness in IT | -.183 | .176 | -.155 | -1.040 | .304 |
| AuthMethod_HistExp | -.029 | .135 | -.035 | -.218 | .828 |
| AuthMethod_Type | .226 | .377 | .093 | .599 | .552 |
| Privacy Concerns | .052 | .196 | .043 | .267 | .791 |
| Computer Self-efficacy | .002 | .228 | .001 | .008 | .994 |

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$