Perceptions of Risk and Security Concerns with Mobile Devices using Biometric vs Traditional Authentication Methods

Sinjini Mitra
California State University, Fullerton, smitra@fullerton.edu

Jordan B. Barlow
University of St. Thomas, jordan.barlow@stthomas.edu

Perceptions of Risk and Security Concerns with Mobile Devices using Biometric vs Traditional Authentication Methods

Completed Research

Sinjini Mitra
California State University, Fullerton
smitra@fullerton.edu

Jordan B. Barlow
University of St. Thomas
jordan.barlow@stthomas.edu

Abstract

Authentication methods on mobile devices provide an important layer of security. Many types of authentication methods exist, some traditional and some biometric-based. In this study, we use a survey method to examine whether the presence and type of an authentication method affect perceptions of risk and security concerns around three specific types of mobile device actions: banking, health, and activities with personally identifiable information (PII). We also survey users' general perceptions of trust, usefulness, convenience, and ease of use toward authentication methods, both traditional and biometric. We find that users' perceptions of risk and security concerns change when users consider the type of authentication method present on a device. While traditional methods are still more familiar to most users, we also find that perceptions of biometric-based methods are more similar to perceptions of traditional methods than in the past.

Keywords

Authentication, biometrics, risk, security concern.

Introduction

With mobile devices now ubiquitous in today's world, there is an ever-present need to secure such mobile devices. One key element of keeping information on mobile devices private and secure is to enable authentication methods. Traditional authentication methods, which are still commonly in use, require a user to remember a particular piece of information, such as a personal identification numbers (PIN), passcode (number or shape), or password.

The use of biometric authentication for mobile devices is becoming increasingly common in the general population. Biometric authentication involves physiological methods to identify users. These methods include hand geometry (i.e., hand shape recognition), fingerprint identification, eye (iris or retina) scans, facial recognition, and voice recognition, among others. Users are becoming more familiar and comfortable with using such methods on their personal devices (Deloitte 2018).

Little behavioral research exists on biometric authentication, yet new research into user perceptions and behaviors surrounding biometric authentication is needed as the technical environment changes, biometric methods become more usable, and user acceptance increases. Early behavioral research on biometric authentication more than a decade ago found that most people were either unaware of biometric authentication methods (Kowalski and Goldstein 2006) or hoped that the usability and security features of biometric methods would improve (Heckle et al. 2007; Karatzouni et al. 2007).

More recently, research has examined users' understanding of the term "biometrics" and has found that more users understand the term, but are still only familiar with some of the available biometric-based methods (Buckley and Nurse 2019).

A few research studies have developed or adapted theory to understand the acceptance of biometric authentication methods (Alhussain and Drew 2012; Miltgen et al. 2013; Ogbanufe and Kim 2018). Others have examined the perceived tradeoff between usability and security (Allen and Komandur 2019; Gunson et al. 2011).

Much of the remaining existing behavioral research around biometric-based authentication methods has focused on surveying users' perceptions of usability, security, and intentions to accept the method (Bhagavatula et al. 2015; Guerra-Casanova et al. 2016; Khan et al. 2015; Rasnayaka and Sim 2018; Wang et al. 2019; Wolf et al. 2018; Zimmermann and Gerber 2020). These papers compare perceptions regarding various authentication methods, including biometrics. However, these studies focused exclusively on the authentication method itself. That is, none of these studies examined how users perceive the risk and/or security concerns of users when completing certain actions (e.g., banking, health, etc.) on a mobile device. Authentication methods do not exist in a vacuum, but rather are used as a layer of protection for users who perform various types of actions on their devices. How do users perceive actions on mobile devices differently based on the authentication layer of that mobile device? In other words, we seek to understand not only the current perceptions of users toward the various authentication methods themselves, but also how actions taken on mobile devices using these authentication methods are perceived.

Specifically, we examine risk perceptions and security concerns in this study. Whether or not a risk is real, the perception of a risk changes human behavior (Jiang and Klein 1999; Park et al. 2015). *Risk perceptions* have been defined as a "subjective expectation of suffering a loss in pursuit of a desired outcome" (Bélanger and Carter 2008; Warkentin et al. 2002). Risk is complex and multi-dimensional, but one key component of risk that we focus on is privacy risk, the potential loss of personal information or control over that information (Chiu et al. 2014; Pavlou 2003).

Security concerns are perceptions that a user feels unprotected against a potential security threat when using a system (Ogbanufe and Kim 2018). Thus, risk perceptions are perceptions regarding potential loss, and security concerns are perceptions regarding the amount of protection one feels when using a technology.

Thus, this study seeks to answer the following research question: *How does the type of authentication method used on a mobile device affect user perceptions of risk and security concerns when using that device for various activities?*

Hypothesis Development

Users complete many types of activities on mobile devices. In this study, we focus on activities that involve sensitive, private information. Specifically, we identified three types of information that users often protect: (1) financial/banking information, (2) personal health information, and (3) personally identifiable information (PII). When users complete activities that use these types of sensitive information, they rely on security features of their mobile device to ensure that such information remains private and secure. Thus, we consider users' perceptions of completing activities on a mobile device that involve these types of information.

In this study, we consider users' perceptions of risk and security concerns around these three situations, and how those perceptions change (or do not change) depending on which type of authentication method is being used on the device.

Both risk perceptions and security concerns are complex phenomena that can be predicted by behavioral, environmental, and technical factors around the system being used (Ogbanufe and Kim 2018; Pavlou 2003). We propose that the perceived risk and security concerns one feels when using a mobile device are influenced not only by the situation itself, but also by related technology factors such as the type of authentication being used in a system. Specifically:

H1*: General baseline perceptions of risk toward completing* [*(a) a banking activity / (b) a health-related activity / (c) an activity that uses personally identifiable information*] *on a mobile device will differ from perceptions of risk toward completing that activity on a mobile device with a specific named authentication method.*

H2*: General baseline security concerns toward completing* [*(a) a banking activity / (b) a health-related activity / (c) an activity that uses personally identifiable information*] *on a mobile device will differ* *from security concerns toward completing that activity on a mobile device with a specific named authentication method.*

While the previous hypotheses concern the difference between baseline perceptions and the inclusion of an authentication method, we are also interested in differing perceptions based on the type of authentication method (biometric vs. traditional). Because users often perceive that biometric-based authentication methods are more secure than traditional methods (Rasnayaka and Sim 2018), they may perceive less risk and security concerns in these situations when there is a biometric-based authentication method being used on the device. This would indicate that the risk or security concerns a user feels in a situation is dependent not only on the situation, but also on the authentication method on the device. However, the null hypothesis (no difference in these perceptions based on traditional vs. biometric authentication) would also be interesting because it would indicate that the specific type of authentication method on a device would not affect users' perceptions of risk and security concerns when completing actions with sensitive information. Thus:

***H3**: Perceptions of risk toward completing* [*(a) a banking activity / (b) a health-related activity / (c) an activity that uses personally identifiable information*] *on a mobile device will differ depending on the type of authentication method used on that device.*

***H4**: Security concerns toward completing* [*(a) a banking activity / (b) a health-related activity / (c) an activity that uses personally identifiable information*] *on a mobile device will differ depending on the type of authentication method used on that device.*

In addition to the above hypotheses examining authentication methods in specific scenarios, we also hypothesize differences between traditional and biometric-based methods on perceptions of usefulness, trust, ease of use, and convenience. Multiple previous studies surveyed user perceptions of these constructs (Bhagavatula et al. 2015; Guerra-Casanova et al. 2016; Khan et al. 2015; Rasnayaka and Sim 2018; Wang et al. 2019; Wolf et al. 2018; Zimmermann and Gerber 2020). However, because authentication methods are still being developed, and perceptions of them are rapidly changing, we believe it is valuable to report such perceptions on a regular basis.

***H5**: Perceptions of* [*(a) usefulness / (b) trust / (c) ease of use / (d) convenience*] *toward an authentication method will differ depending on the type of authentication method—traditional or biometrics.*

Finally, even though use of biometrics is increasing, the rapidly changing environment leads us to propose that, currently, users' familiarity, use, and experience with biometric-based methods is still low compared to traditional authentication methods.

***H6**: Users'* [*(a) familiarity / (b) current use / (c) previous experience*] *with biometric-based authentication is lower than with traditional authentication methods.*

Method

Participants and Procedures

We recruited 181 graduate and undergraduate business students from two large US universities—one private university in the Midwestern United States and one public university in the West Coast of the United States. 43.4% had completed a high school education; 47.2% had completed an undergraduate education; 9.4% had completed a graduate degree (i.e., were in process of completing a second master's). Students received extra credit for participation, which entailed completing an online survey. To retain anonymity, students were asked to upload a screenshot of the survey completion page on the course website to receive credit. 44.4% of the participants were female and 54.4% were male. The average age was 24.77 years (standard deviation 6.12), and the average number of years working with a mobile device was 10.62 (standard deviation 3.82).

The first set of questions asked about general security concerns and perceived risk regarding each one of the three sensitive actions listed above (i.e., banking, health, personally identifiable information). These questions were asked prior to mentioning any authentication methods, to ascertain participants' baseline risk and security perceptions regarding these general situations. We asked participants their level of familiarity, use, and experience with each of seven authentication methods; however, to reduce potential survey fatigue, we asked participants questions regarding only one of the seven authentication methods for the remainder of the survey. We used randomization to assign which of the seven methods any given participant would see in both the scenarios and other questions. Before the scenarios, we asked participants their perceptions of trust, convenience, ease of use, and usefulness for the given authentication method that was assigned to them. Participants then read each of the three scenarios and a set of questions corresponding to each scenario, asking the perceptions of risk and security concerns for that given scenario. Additional procedural detail about the survey is listed at https://www.jordanbarlow.net/amcis-2022.html.

Scenarios and treatments

We used a scenario method in the survey to prevent social desirability bias. Specifically, each participant read three different versions of a scenario. Each one of the scenarios described a fictional character using a mobile device with a specific authentication method. The scenario also says that the character decides to use the device to complete a specific action involving sensitive information. We asked participants their perceptions surrounding the risk and security concerns of the action completed by the character. The scenarios varied on two factors: (1) the action that the character completed on the mobile device; and (2) the type of authentication method on the device.

Any given version of the scenario included one of the following three actions: (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 three versions of the scenario, i.e., one scenario with each of these three potential actions.

Each participant always saw the same authentication method. In other words, the participant viewed three scenarios with three different actions, each of them completed on a device with the same authentication method. Seven authentication methods could appear in the scenarios, and which of the seven a participant viewed was randomly assigned: (1) PIN or passcode; (2) password; (3) hand geometry; (4) fingerprint; (5) face recognition; (6) voice recognition; and (7) eye (retina or iris) scan. The first two are "traditional" authentication methods and the latter five are "biometric" authentication methods. Thus, the design was mixed factorial, with authentication type as a *between* factor and action completed as a *within* factor.

Measurement items

Unless noted otherwise, all items used five-point Likert scales. *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 four times—once as a baseline and then once for each of the three scenarios that a participant viewed.

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, eye scan, voice recognition, hand geometry, or face recognition) and 0 if the participant saw scenarios and questions involving a traditional authentication method (i.e., PIN or passcode, password). *Familiarity*, *use*, and *experience* with an authentication method were each measured using a scale developed by the authors.

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.").

We also collected the following demographic information: *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

Tests of hypotheses

To test H1 and H2, we asked each participant their base level perceptions of the risk and security concerns involved in three situations (banking, health, PII). We also asked each participant their perceptions of the risk and security concerns involved in these same three situations when using one specific named authentication method.

Using paired t-tests, we tested the differences between the baseline risk perceptions and perceptions of the risk involved in these same three situations afterwards. Results are shown below in Table 1(a).

For all three scenarios, as well as in the combined data, perceptions of risk decreased in the scenarios as compared to the baseline perceptions. We completed a similar analysis to compare security concerns between baseline and scenarios where a specific authentication method was named. Results are shown below in Table 1(b). A discussion of these and all results is given below in the Discussion section.

	(a) Risk Perceptions			(b) Security Concerns		
	Baseline	Scenario with Authentication Method	p-value	Baseline	Scenario with Authentication Method	p-value
Banking	2.891	2.624	<0.0001	2.582	2.446	0.102
Health	2.698	2.567	0.034	2.621	2.398	0.004
PII	3.735	3.447	<0.0001	3.309	3.416	0.196
Overall	3.108	2.880	<0.0001	2.837	2.753	0.177

Table 1. Differences in (a) Risk Perceptions and (b) Security Concerns

For all three scenarios, participants' security concerns decreased when an authentication method was stated to be used on a device. However, this effect was only statistically significant in the health scenario. Overall security concerns were not significantly different between the general baseline questions and the questions asked for a scenario with a specific named authentication method.

To test H3 and H4, we first validated that the baseline perceptions of risk (p=0.684) and security concerns (p=0.224) between the randomly selected groups were not significantly different. Then, we performed ANOVA to compare perceptions of risk and security concerns between traditional and biometric-based methods for each of the three types of activities. Results are shown in Table 2.

	(a) Risk Perceptions			(b) Security Concerns		
	Traditional	Biometric	p-value	Traditional	Biometric	p-value
Banking	2.37	2.73	0.012	2.14	2.57	0.010
Health	2.42	2.63	0.095	2.10	2.52	0.006
PII	3.49	3.43	0.703	3.32	3.46	0.471
Overall	2.76	2.96	0.096	2.52	2.85	0.010

Table 2. (a) Risk Perceptions and (b) Security Concerns between Types

Interestingly, the means for risk perceptions and security concerns were *higher* for the biometric-based methods than for traditional. This suggests that, overall, users are actually more confident in traditional than biometric-based authentication methods. H3 and H4 are supported (i.e., there is a significant difference), but the direction of the effect is unexpected.

To test H5, we also analyzed general differences in perceptions across different authentication methods. These findings supplement previous findings that surveyed user perceptions of these constructs. No significant differences for convenience were found based on the type of authentication method, as reported in Table 3 below. It is surprising to note that people generally placed *more* trust in traditional methods than in biometrics, which are expected to be more secure. Participants also view them as more useful. This finding may be a result of less familiarity or experience with biometrics-based methods for most of the survey participants or a sense of distrust toward companies collecting biometric data. The perception of higher levels of ease of use for traditional methods is, however, consistent with expectations.

Finally, in testing H6, our analysis showed that participants' baseline level of familiarity, use, and experience with traditional mobile authentication methods were significantly higher than those with biometric-based methods, as shown below in Table 3. The most commonly used biometric is fingerprint, and the least used is iris/retina scan. Passwords are the most common traditional method used.

	Traditional	Biometric	p-value
Usefulness	3.72	3.31	0.009
Trust	3.95	3.22	<0.0001
Ease of use	4.31	3.95	0.005
Convenience	4.13	3.94	0.259
Familiarity	4.682	3.281	< 0.0001
Current Use	95.0%	88.4%	0.011
Experience	4.215	2.338	< 0.0001

Table 3. Differences of Perceptions, Familiarity, Use, and Experience between Authentication Types

Additional analysis

In addition to the main analyses testing H1 and H2, we examined each of them for traditional methods (n=54) and biometric-based methods (n=127) separately. These analyses are shown in Tables 4-5 below.

	(a) Risk Perceptions			(b) Security Concerns		
	Baseline	Scenario with Authentication Method	p-value	Baseline	Scenario with Authentication Method	p-value
Banking	2.784	2.370	0.001	2.475	2.142	0.012
Health	2.562	2.420	0.181	2.457	2.105	0.005
PII	3.796	3488	0.017	3.284	3.321	0.801
Overall	3.047	2.759	<0.0001	2.739	2.523	0.034

Table 4. Differences in (a) Risk Perceptions and (b) Security Concerns: Traditional

	(a) Risk Perceptions			(b) Security Concerns		
	Baseline	Scenario with Authentication Method	p-value	Baseline	Scenario with Authentication Method	p-value
Banking	2.937	2.732	0.018	2.627	2.575	0.616
Health	2.756	2.630	0.095	2.690	2.522	0.080
PII	3.709	3.430	0.001	3.320	3.457	0.173
Overall	3.134	2.931	0.002	2.879	2.851	0.718

Table 5. Differences in (a) Risk Perceptions and (b) Security Concerns: Biometrics

For the traditional methods (Table 4), we found that risk perceptions change for banking and PII scenarios, while security concerns change for banking and health scenarios. We found, when considering biometric-based methods (Table 5), that risk perceptions decrease from the general baseline to a scenario with a biometric-based method being mentioned, particularly for banking and PII scenarios. Security concerns, on the other hand, tend to decrease more for health scenarios than others when comparing baseline perceptions to perceptions of scenarios with the authentication method present.

We also analyzed differences in perceptions based on demographic variables. No statistically significant differences for any of the four variables representing user perceptions – usefulness, trusting intentions, ease of use, and convenience – were observed based on gender. Significant associations were observed with the level of education of participants, as shown in Table 6. Participants who had "high school" as their highest level of education completed felt higher levels of positive perceptions toward authentication methods in general, and those with an undergraduate degree had the lowest.

	High School	Undergrad	Grad	p-value
Usefulness	3.68	3.24	3.30	0.010
Trust	3.66	3.26	3.35	0.037
Ease of use	4.27	3.86	4.03	0.004
Convenience	4.34	3.69	3.86	<0.0001

Table 6. Perceptions based on Education

Discussion

Interpretation of findings

A summary of which hypotheses were supported is shown below in Table 7. The results of our study lead us to several findings. First, the way users perceive risk and security concerns of actions on mobile devices is affected by having an authentication method on that device. Analysis of H1 shows that users perceive less risk when completing a banking or action with personally identifiable information (and potentially also in health activities) when they know an authentication method is being used on the device.

Analysis of H2 shows that the security concerns users feel partially change when they are aware of authentication methods on a device, but not as significantly as with risk perceptions. Specifically, users feel less security concerns for health-related activities when they complete them on a device with an authentication method being used.

The second main finding of this study (H3 and H4) is that, overall, users perceive risk and security differently depending on the authentication type. Specifically, users tend to perceive more risk and security concerns regarding biometric methods. This is surprising, given that other previous research has found users to perceive biometrics to be more secure than traditional authentication. However, such studies have asked users directly about the risk and security concerns of the authentication methods themselves, not the perceptions of risk and security concerns regarding a specific type of action taken on a device with that method.

Third, we found that perceptions of convenience did not significantly differ between traditional and biometrics-based methods, but perceptions of usefulness, trust, and ease of use were significantly higher for traditional methods (H5).

Finally, we found that despite the increasing knowledge of and popularity of biometric-based methods, there currently remains a significant difference in familiarity, current use, and experience between traditional and biometric methods (H6). Taking together the results of H5 and H6, we find that biometric-based methods are still not as commonly used as traditional methods, and that perceptions remain persistent that such methods are not as useful, trustworthy, or easy to use as the traditional methods.

Hypothesis	Supported?
H1. Risk perceptions differ from baseline to scenario with authentication method	Yes (a, b, c)
H2. Security concerns differ from baseline to scenario with authentication method	Yes for health scenarios (b); No for others (a, c)
H3. Risk perceptions differ depending on the type of authentication method	Yes for banking and health (a, b); No for PII (c)
H4. Security concerns differ depending on the type of authentication method	Yes for banking and health (a, b); No for PII (c)
H5. Perceptions of an authentication method will differ depending on the type of method	Yes: usefulness (a), trust (b), ease of use (c); No: convenience (d)
H6. Users have more familiarity, current use, and previous experience with traditional methods than with biometrics	Yes

Table 7. Summary of Hypothesis Support

Limitations

Our findings should be interpreted considering the limitations of our research. First, the research was conducted with a student population. The restricted age range may affect the results of the age variable in our analysis. However, within the student population, there was a variety of work and life experience. We believe the results regarding perceptions of authentication methods would likely translate well to the general population. A general population data collection is planned for a larger extension of this study.

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).

Next, due to the randomization of authentication methods, some participants were asked questions regarding authentication methods with which they did not have personal experience. Although we find it important to measure general perceptions of all methods regardless of past use, this procedure in the survey could potentially bias some of the results. Future research should examine multiple methods per participant and control for which methods participants have personally used in the past. Further, our survey was perceptional and scenario-based and thus participants did not respond regarding their own devices.

Implications for research

Our research has several implications for research and leads to several questions that should be addressed in future research. First, our study is one of the first to examine the effect of authentication methods on perceptions of related activities on mobile devices. While previous research has examined perceptions about the authentication methods themselves, our research examined whether perceptions of risk and security concerns around completing certain activities on a mobile device would be affected by the presence and type of authentication method. This is one of the first studies to examine the effects authentication methods have in different specific contexts (e.g., banking, health). We encourage more research in examining not only authentication methods themselves, but also how they affect related perceptions of security.

A second, related, implication of this study is that researchers should consider the specific context and the specific authentication method available when examining behavior on a mobile device. Research around mobile device behavior should not omit the mention of authentication methods available because we have shown that knowledge of the authentication method affects user perceptions of the overall situation.

Third, we contribute to the ongoing studies examining user perceptions of usefulness, trust, convenience, and ease of use toward biometric-based authentication methods. Because these methods are still changing and becoming more common, perceptions around them are constantly changing. We call for additional research in the future to continue examining how these perceptions are changing over time. At the current time, we find that users are still significantly less likely to be using biometric-based methods, but we find that their perceptions are becoming more similar to perceptions of traditional authentication methods.

Implications for practice

Our research also has implications for practice. First, because we find that perceptions (e.g., usefulness, trust, etc.) about biometric-based methods are similar to perceptions around traditional authentication methods, we caution developers of biometric-based methods that even though the methods may be more secure from a technical standpoint, awareness of how users will perceive them is essential. More training for users may be necessary to teach how biometric-based methods may differ from traditional methods.

Second, for developers of mobile applications, we warn that users may perceive using apps as being less risky or more secure when they are actively using an authentication method on their device. Developers wanting to assure their users that using the app is safe should not only discuss security within the app, but also remind users to use authentication methods on their device.

Conclusion

In summary, our study found that users perceive actions on mobile devices differently when they are aware of authentication methods on the device. However, we also found that users do not perceive much difference in risk, security concern, trust, convenience, ease of use, and usefulness between biometric-based methods and more traditional methods. While we find traditional methods to still be more common, perceptions around authentication methods continue to evolve.

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.

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," *USEC 15: Workshop on Usable Security*.

Buckley, O., and Nurse, J. R. 2019. "The Language of Biometrics: Analysing Public Perceptions," *Journal of Information Security and Applications* (47), pp. 112-119.

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.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:1), 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.

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," *IEEE 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.

Heckle, R. R., Patrick, A. S., and Ozok, A. 2007. "Perception and Acceptance of Fingerprint Biometric Technology," *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pp. 153-154.

Jiang, J. J., and Klein, G. 1999. "Risks to Different Aspects of System Success," *Information & Management* (36:5), pp. 263-272.

Karatzouni, S., Furnell, S. M., Clarke, N. L., and Botha, R. A. 2007. "Perceptions of User Authentication on Mobile Devices," *Proceedings of the ISOneWorld Conference*, pp. 11-13.

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)*, pp. 225-239.

Kowalski, S., and Goldstein, M. 2006. "Consumers' Awareness of, Attitudes Towards and Adoption of Mobile Phone Security," *20th International Symposium on Human Factors in Telecommunication*, pp. 20-23.

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?," *IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1-9.

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

Warkentin, M., Gefen, D., Pavlou, P. A., and Rose, G. M. 2002. "Encouraging Citizen Adoption of e-Government by Building Trust," *Electronic Markets* (12:3), pp. 157-162.

Wolf, F., Kuber, R., and Aviv, A. J. 2018. "An Empirical Study Examining the Perceptions and Behaviours of Security-Conscious Users of Mobile Authentication," *Behaviour & Information Technology* (37:4), pp. 320-334.

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.