Abstract—This paper is a review of existing literature on the topic of user-friendliness in online banking security systems. The research presented herein seeks to promote critical thought on finding the most effective immediate steps online banks can take to better protect their customers, given what is currently understood about how users perceive and interact with online security systems.

Keywords: banking; security; user experience; human-computer interaction

I. INTRODUCTION

Online banking has quickly grown in importance in the past two decades. Online banking via banks’ own public-facing websites has been commonplace since as early as the year 2000, and both the number of banks offering online services and the number of customers using those services have skyrocketed in the following years. As the adoption of online banking has grown, so too have the dangers associated with banking electronically – and in particular, the dangers to the customers. Online banking fraud and theft have become a constant global problem, but the security measures that online banks have put in place in response, such as requiring longer passwords or various security questions, have not significantly stymied this widespread financial abuse. Ultimately, as attacks have become more sophisticated, the end users of online banking systems have suffered the increased responsibility of security; and this trend will continue unless there is an industry shift away from burdening online banking customers with security and instead toward implementing more user-friendly, human-centric security measures. This article intends to explain the results of four studies relevant to the problem of addressing the customer perspective on online banking security systems; and further, to pose the question: what are the most effective immediate steps that online banks can take to better protect their customers’ private information, given what is currently understood about how people interact with online banking systems and security measures? In answering this question, we must necessarily place usable (practical) security before theoretical security.

II. DISCUSSION

To discuss the usability problems with modern online banking, it is necessary to understand the current state of online banking interfaces and the security trends they follow. A comprehensive study produced by Kiljan et al. looked at a diverse sample of 80 online banks from 5 continents and assessed and compared the security of their services [1]. The study, conducted in 2015, is broken primarily into two sections discussing “customer to bank authentication” [p. 9] and “bank to customer authentication and communications security” [p. 21]. Some clear trends in customer-to-bank authentication were made immediately apparent by this study, such as the striking difference in adoption of multi-factor authentication in North America versus in Europe, South America and Oceania. Of the 35 online banks surveyed in the latter three regions, only four did not offer multi-factor authentication as a user authentication option – an adoption rate of 89% – contrasted with the one out of six North American online banks which offered multi-factor authentication, a minuscule 17% [p. 11]. As noted by the authors, this fact seems to follow the trend of North America’s late adoption of security enhancements to electronic funds; in the words of the authors, “the United States [had] only recently started to widely implement smart card-based payment cards that require a PIN” [p. 11].

In theory, requiring more factors from the user to authenticate them increases security by “increasing the amount of effort required by an adversary to commit successful identity fraud” [p. 10]. This is dependent, however, on the entropy of the factor provided and, importantly, on the difficulty the user experiences in producing the factor. For example, requiring the user to memorize a 16-character password of their own creation will most likely lead them to use common English words or personally meaningful information in their password, making it easier to remember but reducing its entropy. Likewise, if prompted to create a memorable PIN number, the average user will tend to enter a year or date that they will be able to recall, again reducing their security. Thus, the presence of multi-factor authentication alone does not necessarily lead to an improvement in security; the factors must play to the strengths of the user in order to seem acceptable and be repeatable. The
topic of user receptiveness to single- and multi-factor authentication was studied by Gunson et al. in 2011 [2]. In their research, the authors set up a controlled experiment in which participants were provided with fictitious credentials and directed to interact with an automated telephone banking service [p. 208]. In the experiment, half of the 62 participants were instructed simply to provide two of six preselected digits in order to authenticate, whereas the other half were to additionally provide a readout of a one-time password generated by a “keyfob” in their possession [p. 211]. The researchers found that, while "the two-factor process... took significantly longer," the participants "valued the extra security provided by the two-factor service," despite the added inconvenience [p. 217]. Undoubtedly, the extra inconvenience was acceptable because it relayed no additional cognitive load to the user – they needed simply to read off digits from a keyfob. Simple implementations of multi-factor authentication such as this, which add minimal burden to the user but which add reliable entropy, should be greatly preferred over ineffective approaches like requiring passwords to be longer or not to contain repeat characters.

Kiljan et al. [1] define their usage of the term “multi-factor” to refer to the requirement of two or more authentication “factors,” which they reasonably title “knowledge,” “possession” and “biometrics” in reference to the more common mnemonic of something you know, something you have, and something you are [p. 10]. However, they further break down these categories based on the technologies involved in storing and processing them. One interesting subcategory of the “possession” factor they detail is the “One-Time Password”, often distributed via SMS message but occasionally given out in person as text written on physical cards or tokens [pp. 13-14]. One-time passwords are a simple avenue of multi-factor authentication that are also often user-friendly, since copying text from a text message or notecard to a desktop or mobile text field is trivial for the user. While adoption of one-time passwords exists among different subsets of the 80 banks – from passwords stored on physical cards and tokens, to those sent via SMS, to those stored inside installed client software – the implementations themselves are widely varied and never represent a majority of the online banking industry [p. 20].

In fact, a lack of standardization plagues just about every aspect of online banking security measures. A study produced by Subsorn and Limwiriyanakul of Suan Dusit Rajabhat University, Bangkok [3] corroborated the findings of Kiljan et al.; that the security systems put in place by various online banks – even from the same region – vary wildly and differ greatly in requirements and features [pp. 265-267]. Subsorn and Limwiriyanakul's work brings to light a lack of standards not just a lack of standardization in the design decisions of various online banking systems, but also in the versions of software being run to keep user-bank electronic communication confidential and to preserve data integrity [p. 269]. The authors found that six of 12 surveyed Thai online banks “[had] deployed 128-bit encryption but indicated 256-bit encryption on their websites” [p. 269]. Further, the two found that “[a]lmost half of the selected Thai commercial banks (six out of 12 [sic]) have employed extended validation SSL certificates whereas the other remaining seven banks only used standard validation” [p. 267]. By using extended validation (EV) SSL certificates in their web hosting, banks and companies establish a higher level of trust in the user since their certificate and identity have been vouched for by a Certificate Authority (such as VeriSign). Practically speaking, lacking an EV certificate will cause many popular browsers like Safari and Chrome not to display the company or bank's name in a green “trusted” box at the top of the browser, which reduces the users' trust in the security and competence of the online banking portal, and makes it more feasible for an attacker to redirect a customer to a malicious site without their knowledge as no change to the URL bar will occur. In order to combat the dangerous absence of security standards in the user-facing portions of online banking, more reports like Subsord and Limwiriyakul's, that aggregate the complicated and inconsistent practices of online banks, will be necessary to understand the state of things.

In addition to all the well-known security devices such as passwords and client-side applications, there still exist many alternatives that are either just beginning to see adoption or that are still theoretical. Among these new approaches, the most popular and recognizable is probably biometric authentication, which includes the use of fingerprints or even iris or face scans to confirm the identity of a user. Tassabehji and Kamala, in their 2012 case study, evaluated the user-friendliness of various methods of biometric authentication [4], asking 116 participants both about their “practical familiarity” with the tools and processes presented to them and their opinions of the “suitability” of said tools and processes [pp. 491-493]. Presented with fingerprint scanning, iris scanning, facial recognition and voice recognition [p. 493], the participants “unanimously approved” fingerprint scanning as the most suitable to online banking [p. 494]. Quite telling was Tassabehji and Kamala's finding that the participants' experiences with biometric authentication mechanisms was largely “limited to individual devices,” and that such experience most often occurred in dedicated physical locations such as in “immigration control at airports” [p. 493]. This interesting observation hints at a fear, prevalent in the security industry, of trying and failing to securely manage users' biometric information; unlike passwords, static biometric details such as fingerprints cannot be revoked. Still, biometrics offer greater usability than knowledge-based factors, and research into properly utilizing biometrics is still ongoing.

III. CONCLUSION

These studies expose the fact that, while banks have attempted to make using their online services simple for their
customers, there are still two interrelated problems: that the burden of security is still being placed heavily on the customer; and that, while more human-friendly approaches to the user-facing aspects of online banking security exist, those alternatives are often either explored as fallbacks or as auxiliary to the traditional, less-usable primary security measures [1]. Further, although many online banks employ a variety of security measures to prevent unauthorized entry into customer accounts, and to keep the process of logging in simple and relatively easy for the customer, there is a huge lack of global standardization on what measures are most effective or even required. Several promising advances have been made in the area of human-friendly security system, both in theory and in practice, but full adoption of these improvements has been slow. Ultimately, if online banks intend to address this problem – by picking the most usable and effective security measures available as immediately as possible – they will need to learn from their peers, standardize on effective solutions, and otherwise keep up to date with incremental improvements to all other systems.

ACKNOWLEDGMENT

I would like to thank Professor Keeling for his prompt and insightful feedback throughout the process of drafting this literature review, as well as the dedicated efforts of those researchers in the computer security field whose work I was fortunate enough to read.

REFERENCES


