Two-factor Authentication in the Digital Age

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

James Keith

December 2, 2024

Abstract

Two-factor authentication (2FA) is a potent yet intricate tool, as it aims to fortify individual digital accounts with an additional layer of security. However, its implementation depends on assessing whether the benefits outweigh the costs, ultimately impacting the online user experience. When organizations implement 2FA, several critical aspects, particularly security, demand careful consideration. The primary objective of 2FA is to thwart potential attackers from gaining access to consumers' information through compromised passwords.

Moreover, businesses derive tangible financial benefits from 2FA, as it mitigates the likelihood of breaches and reduces the risk of lawsuits. While businesses wholeheartedly support the implementation of 2FA, consumers tend to be less enthusiastic about it. This is primarily because most 2FA applications need more user-friendliness, making the enrollment and utilization process arduous for a significant portion of the population. In conclusion, the implementation of 2FA is crucial to consumers and businesses. Therefore, a comprehensive understanding of its intricacies is essential for effective implementation.

Keywords: Two-factor Authentication, 2FA, Multi-factor Authentication, Cybersecurity, Economics, Psychology, Information Security

As a student pursuing a cybersecurity degree, I am learning about the complexities of cybersecurity. Whether it involves the cryptographic methods used to encrypt data or the frameworks and regulations governing the industry, cybersecurity is rapidly evolving. One cybersecurity tool familiar to anyone using online banking or social media is two-factor authentication (2FA). 2FA is a critical mechanism that prevents unauthorized access to one's online account by requiring an additional verification method. However, many companies do not require 2FA due to the cost of implementing such technology and its impact on user experience. With the threat of online attacks rising, technologies such as 2FA are more essential than ever for maintaining data security; therefore, implementing this crucial tool is increasingly vital.

I took an interdisciplinary approach to implementing two-factor authentication (2FA) to investigate how different disciplines perceive it. To develop a comprehensive understanding, I examined the fields of cybersecurity, information security, economics, and psychology to gain insights into how 2FA is regarded. I found that all parties concur that 2FA is essential; however, improvements can be made to enhance this crucial technology's ability to mitigate fraudulent activity and make it more user-friendly.

One point of view on 2FA comes from the cybersecurity perspective, which views multiple layers of account authentication as necessary. Cybersecurity is all about protecting the sensitive information stored in the digital world. Without protection, most would view cell phones and the internet as dangerous places where information is vulnerable to hacking. Cybersecurity aims to prevent this mentality by providing multiple layers of security architecture around an individual's and a business's data. 2FA is a strong example of this approach. Stanislav emphasizes this by stating, "Two-factor authentication is an ever-increasing necessity in information technology as the threats facing end-user security become more intense and

powerful. As criminals continue to improve their techniques to steal user credentials and otherwise circumvent traditional, single-factor authentication security mechanisms, there's a pressing need for individuals and organisations to understand their options better when it comes to authentication." According to Berrios et al., "2FA works by enabling a second factor of verification during the login process" (1). Stanislav also explains 2FA in a non-technical manner, stating, "However, if you've used an ATM or bought something with a debit card, you've actually engaged in using two-factor authentication. By possessing the debit card (what you have) and typing a PIN (what you know), you've utilized two factor classes for one authentication process." In essence, 2FA is designed to serve as a second line of defense if a password is compromised and an unknown source tries to access an individual's account. Without it, hackers would have free rein to steal one's data without the account owner ever knowing.

While cybersecurity views 2FA as essential, information security considers 2FA to be a vital layer of defense against data breaches and identity theft. Tsai and Su state, "numerous banks have adopted technical countermeasures, such as two-factor or multi-factor authentication, to prevent cyberattacks, online fraud, and unauthorized access to bank accounts" (1). Information security regards 2FA as a proven method to secure digital assets and reduce the number of account takeovers by threat actors. Although potential issues may arise if the integration with existing systems is conducted poorly, 2FA has been proven to help keep assets secure.

Though cybersecurity and information security support the implementation of 2FA into online accounts, the economic aspect depends on the associated costs. According to Bohme, "Organizations need to pay attention to the economic viability of IS investments. They have to find the balance between the risks of threats on one side and the possibility to mitigate the risks

and the costs thereof on the other side" (26). From a business standpoint, the bottom line is critical when making financial decisions. Although 2FA reduces the likelihood of a costly data breach, its deployment involves significant technological, personnel, and user training investments. Smaller businesses find this cost prohibitive, which typically results in underinvestment in security measures.

Conversely, the financial impact of cyberattacks far outweighs the cost of implementing robust security systems. Estimates indicate that companies could lose billions of dollars due to cybercrimes, which makes the cost of implementing 2FA economically feasible. Furthermore, reduced cyber-insurance premiums for utilizing 2FA technologies encourage the increased implementation of 2FA.

As for the psychological aspect of implementing two-factor authentication into cybersecurity, I examined why the general population needs 2FA. Most individuals prefer to avoid 2FA due to the comprehensive setup process and the additional steps involved in using it. Marky states that "2FA mechanisms usually exhibit user experience issues that create user friction and even lead to poor acceptance, hampering the wider spread of 2FA" (1). Since user accessibility is not a strong suit of 2FA, many individuals decline to use it because they do not want to deal with a program that glitches or partially functions. Furthermore, the setup process can be time-consuming, thereby deterring people whose time is valuable. Even though 2FA apps have been developed and are considerably more user-friendly, many still hesitate to use the technology due to its reputation.

With 2FA not viewed favorably by the population, one may ask why they should care about it. The answer can be traced to the continued rise of phishing attacks. Phishing scams arise from attackers sending emails or links to individuals that appear to be from a reputable source

but are, in fact, malicious. Once an individual clicks the link or opens the email, malware is downloaded onto their device in the background without their knowledge. Most phishing scams download keystroke loggers onto an individual's device, sending the attacker every keystroke that the individual makes on that device. Attackers can then compile passwords, credit card numbers, social security numbers, and addresses that can be used to impersonate individuals fraudulently.

Since phishing attacks are on the rise, one may wonder why people need to recognize these scams for what they are. The answer to this question is surprising. According to research conducted by Zheng, "Online scams typically use social engineering techniques that exploit people's "psychological weaknesses" to manipulate recipients into believing and doing things they would normally not" (20). Essentially, people desire to trust and believe what they view, even when it may not be accurate or truthful. Zheng also states, "People may not recognize phishing scams because most individuals do not create phishing themselves" (5). The research indicates that people struggle to identify phishing content because they want to believe the link is safe, even when it isn't. Another misconception is that technology and spam blockers will adequately filter phishing emails and links, which is false, as many programs fail to identify such threats.

Given that phishing scams victimizing individuals occur daily, coupled with the challenges of user-friendliness associated with two-factor authentication (2FA) and the financial considerations involved in its implementation, it becomes evident why the adoption of 2FA has not proceeded at the necessary pace. Though cybersecurity and information system disciplines view 2FA as an essential step in keeping user information secure, the cost of implementing it into a company's system and its poor reputation among the population have resulted in a slow rollout.

However, there are methods to improve 2FA's reputation and increase its implementation across more online accounts. The first step is streamlining the consumer setup process through help guides and videos. Creating step-by-step videos and guides helps consumers understand the process and minimizes confusion. Encouraging users to download 2FA applications on mobile phones and laptops is the next step in broadening the use of 2FA. Though security keys are the most secure method of 2FA, they are challenging to set up and expensive to purchase. Instead, mobile 2FA applications are free to install and use, making them the ideal option for companies. Further, companies looking to implement 2FA should gradually roll out the technology to select users on a trial basis. By trialing the release, the company can obtain user feedback and make improvements before releasing it to all users.

2FA implementation has been slow throughout the past decade, but the rise of phishing attacks and threat actors hijacking passwords has pushed businesses to implement the technology more swiftly. By making the technology more user-friendly and incentivizing it for businesses in exchange for reduced cyber-insurance premiums, 2FA can be integrated throughout the digital world. Once implemented, fraudulent activity will be reduced, and account takeovers will be harder to achieve, as an extra layer of security will protect users' accounts. Trialing the implementation of 2FA with a select user base will also help companies understand where improvements can be made and facilitate a smoother, more user-friendly transition.

2FA is necessary to keep digital accounts secure from both seen and unseen threats. However, implementing this technology is a process that requires time and feedback from users to be completed successfully. When viewed from a singular discipline, the implementation of 2FA will continue to fall short of what is necessary, as user issues and costs hinder its ability to expand. However, from an interdisciplinary standpoint, one can formulate a comprehensive plan

that considers cybersecurity, information security, economics, and psychology perspectives, allowing for the structural implementation of 2FA. While threats to online accounts will continue to evolve with the rise of generative artificial intelligence and quantum computing, 2FA will remain at the forefront of the battle to keep online accounts secure and digital information safe.

References

Berrios, J., Mosher, E., Benzo, S., Grajeda, C., & Baggili, I. (2023). Factorizing 2FA: Forensic analysis of two-factor authentication applications. *Forensic Science International. Digital Investigation (Online)*, *45*, 301569. https://doi.org/10.1016/j.fsidi.2023.301569

Bohme, R. (2013). *The Economics of Information Security and Privacy* (2013.). Springer Berlin / Heidelberg. https://doi.org/10.1007/978-3-642-39498-0

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., Eghtebas, C., & Kunze, K. (2022). "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Transactions on Computer-Human Interaction*, *29*(5), 1–32. https://doi.org/10.1145/3503514

Stanislav, M. (2015). *Two-Factor Authentication [electronic resource]* (1st edition.). https://learning.oreilly.com/library/view/two-factor-authentication/9781849287333/xhtml/preface.html

Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information Systems and E-Business Management*, *19*(1), 77–105. https://doi.org/10.1007/s10257-020-00481-5

Zheng, S. Y. (2024). *Online Scam Detection Using Human Psychology: Toward Usable Cybersecurity*. ProQuest Dissertations & Theses. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/online-scam-detection-using-human-psychology/docview/2917539656/se-2?accountid=12967