Problematic effects of hacking circumventing Multifactor Authentication prompts

Kaschiefe Higgins

College of Technology

Davenport University

CAPS 795: Capstone

Instructor: Dr Lonnie Decker

November 02, 2025

Table of Contents

Abstract

Multifactor authentication (MFA) is an essential tool that provides security for a variety of users as it provides enhanced security for identity theft protection and account hijacking. Due to the increasing evolving threats that exist it is very important that individuals are cautious whenever there is an MFA prompt. Multi-factor authentication allows an individual to access a website or a specific application with additional prompts that will allow easier access. Over the last decade many hackers have formulated methods to access users' vital information. This research will explore the effects that hacking can have circumventing MFA prompts as well as assessing the legitimacy of MFA prompts. This research provides insight into the methods of how hackers will attempt to evade or persuade users to provide key information to access their accounts. In addition, giving details on how different organizations utilize MFA to provide that extra layer of security.

Chapter 1

Introduction

The research conducted provides details on the legitimacy of Multifactor Authentication prompts and problematic effects of hacking circumventing Multifactor Authentication. Security is of utmost importance in any sector of society, hence the reason why I decided to conduct this research is that it will provide some insight that not all Multifactor authentication (MFA) prompts are legitimate. The research focuses on individuals employed in various sectors in society within the age range of 25-65. To eliminate losing data, users must be cognizant of the different threats that exist in the cyber realm from nefarious individuals, MFA is a mechanism that has been formulated to hinder hackers from exploiting users. However, there are loopholes that have been found which is why it is important to validate any prompts from MFA sources, especially from text or email.

Due to the second layer of protection that is provided by MFA, number of individuals tend to believe that it is 100% safe and cannot be breached because of the mechanism that exists within the operation of what is needed for this layer of protection. Which is the reason why all end users should be caution and not become complacent when responding to prompts initiated from an MFA source.

Problem Statement

Multi-factor authentication is a very important mechanism in ensuring that end-users data is protected. It allows an individual to access a website or a specific application with additional prompts that will allow easier access. Over the last decade many hackers have formulated

methods to access users' vital information. This research will explore what methodology does end- users in the workplace use to assess the legitimacy of MFA prompts.

Thesis Statement

Multifactor Authentication in the workplace can be reliable when prompts are legitimate. If MFA is not utilized properly there is a probability that personal data will be stolen. Clicking on spurious multifactor authentication will limit the layers of protection for access.

Questions that will be addressed in the study are:

1. Can hackers mimic applications to replicate MFA sources?
2. Does MFA guarantee 100% security from hackers?
3. What are the methods used for MFA prompts
4. What are the protocols at your workplace for MFA with devices?
5. Is it safe to use MFA as another layer of security.
6. How would you describe your expertise in MFA technology?

Chapter 2

Literature Review

Multifactor Authentication is a methodology that has been added as a second layer for protection for users that utilize technology. Users will react to prompt via text or email to provide a specific code for full access to their personal information, social media, work email/personal email or application software. Senior Editor at PC Magazine Eric Griffith mentions in his article that in a world where major security breaches happen every day and scammers lurk around every corner, what's the average internet user to do? Unfortunately, simply using strong passwords isn't enough anymore. Even complex and hard-to-guess passwords aren't a bulletproof form of security because they can be scooped up easily by a variety of methods. Instead, what you really need is a second way to verify yourself. That's why many internet services (some of which have felt the pinch of being hacked or breached) offer multi-factor authentication (MFA). (Griffith,2024). On reviewing his article Griffith indicates that due to the high surge in security breaches, the decision was made to implement an addition mechanism to protect the end user's personal information. In addition, he further highlighted the fact that passwords are not always safe and can be easily bypassed.

Although MFA is an ideal mechanism to protect your data. Hackers have formulated a variety of ways to acquire relevant information from users. Hence, it is vital that the end user, especially individuals in the workplace, concentrate on the legitimacy of the prompt that are received. Methods such as incorrect account settings for MFA, Malware that steals data from users' systems, MFA fatigue which is also called MFA push spam as well as over confidence from the user are few ways that MFA can become susceptible to hackers. Technology expert Al Lakhani states that it is important we take a step back and understand some of the inherent

weaknesses of your typical MFA solution. He further mentioned that there are ways that MFAs can be bypassed with the use of Adversary in the Middle (AitM) that captures session cookies from users at the point of authentication another method is phishing. MFA can sometimes be phishing resistant but not phishing proof (Lakhani,2024). After reviewing his article, the author captures a wholesome amount of information circumventing some weaknesses of MFA which are very important for users to understand ways that this safety mechanism can be circumvented.

Comparison of research question

From the research question. I used several sources to acquire the relevant information that would provide sufficient information for my research. The first author that mentioned aspects of my research question was Alex Vakulov experienced editor at Forbes magazine and cybersecurity expert. It turns out that multifactor authentication is not a foolproof solution, even for cybersecurity companies, let alone regular users. Hackers can bypass MFA. In fact, there are many techniques that have proven successful (Vakulov, 2024).

Hence the importance of identifying that mechanism to identify the legitimacy of MFA prompts. This will establish a more secure methodology of dealing with potential hacking of technological systems. The other author that has similar stances to Vakulov, is Danny Palmer who is the Senior Writer at ZDNET magazine. In his article, he outlines the intricacies of using Multifactor Authentication. He stated that there was a surge in cyber-attacks which aim to dodge MFA security. According to Microsoft, in just one campaign 10,000 organizations have been targeted in this way during the last year. One option for hackers who want to get around MFA is to use so-called adversary-in-the-middle (AiTM) attack which combined a phishing attack with a proxy server between the victim and the website they're trying to login to.

(Palmer,2022) maintained his stance regarding the vulnerabilities that may arise with MFA. He further stated that although MFA adds an extra layer of security they are not considered as a silver bullet to protect against phishing attacks, with the use of advanced phishing kits and other clever evasion techniques this mechanism can have loopholes where hackers exploit. Other Authors who believe that MFA is crucial in cyber security in any sector and how impactful it is.

(Yugoslavskiy, 2020) mentions in an article that adversary-in-the-middle may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware. Adversaries may also manipulate DNS and leverage their position to intercept user credentials, including access tokens (Steal Application Access Token) and session cookies (Steal Web Session Cookie). Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure.

(Suleski, et al,2023) in their article stated that MFA security classification is an important field, and its impact on authentication security can improve frameworks against potential cyber threats. Mobile users face various cyber threats to their privacy in interconnect networks. Based on the information garnered from the authors, the article describes the overall impact that MFA can have on the health sector specifically. In recent years there have been some breaches with the health sector, which is why it is paramount that MFA are implemented as well as ensuring that there is legitimacy in the messages.

Problems that can occur while using MFA

Having security is the key in preventing any system from being hacked. After the inception of multifactor authentication, individuals with nefarious intentions have formulated new methodology to extract data from users. According to (Multi Factor Authentication Security

Risks,2021) mentions that as companies increase their security requirements, hackers are also adapting their attacks. There have been recent attacks that were able to bypass security systems, including some MFA requirements. For the SolarWinds Orion compromise, for example, attackers stole the single sign-on (SSO) private keys, which allowed them to bypass the MFA checks entirely. As indicated in the article, companies have been experiencing hacking although MFA has already been implemented.

Roger Grimes network security expert, MFA and biometrics mentioned in his article methods that people use to convince users of the legitimacy of an MFA prompt. In an example he states that network hijacking was utilized as an MFA hack. In the example he states that the hacker created a fake website similar to the original, the hacker then prompts the user to access the fabricated website, user then input their credentials which information which is given is then used by the hacker to then access the original website, the legitimate website sends back the legitimate token which the hacker then steals and take over user's session.

He also mentioned that in Iran phishers bypass the 2FA protection offered by yahoo and google mail. A fake google and yahoo security page was used to lure users to provide their credentials. The attacker would simultaneously enter credentials in a real login page, in the event targets were protected by 2FA, users would be redirected to a new page that requested a onetime code (Grimes,2019). The author of the article indicated that although MFA is very useful in enhancing security systems there are methods that are used to bypass or acquire data that can be used to cause havoc in individuals' lives.

Matt Novak, reporter from Gizmodo magazine, mentions in his article that the Federal Government warned the public that using text message as a methodology for MFA is not secure medium because text is not encrypted. Novak went on to state that a threat actor with access to a

telecommunication provider's network who intercepts these messages can read them. SMS MFA is not phishing-resistant and is therefore not strong authentication for accounts of highly targeted individuals. He further highlighted the fact that messaging applications such as Signal provided end-to- end encryption although it is not made impossible for hacking. In addition, CISA (Cybersecurity and Infrastructure Security Agency) recommends end-to-end encrypted messaging compatible with iPhone or Android Operating Systems to prevent the unsecure nature. (Novak,2024). Although the author mentioned an alternative (Signal app), it is very important that users pay keen attention to the prompts received via text to ensure that there is some legitimacy circumventing texts.

Another author that provided incite on the topic is Matt Kapko, a technology journalist who mentions that the recent spate of phishing attacks against identity-based authentication shows the extent to which MFA defenses can crumble, even under unsophisticated tactics. He also stated that Twilio's, a software company that widely uses two-factor authentication service was compromised in August after multiple employees were duped into providing their credentials to threat actors. The attack, part of a larger campaign that compromised at least 10,000 user credentials, spread to 163 Twilio customers, including Okta and Signal, and traveled downstream to many of their respective users' credentials (Kapko,2022). In this article Kapko mentions vulnerabilities that exist with MFA and how much impact it can have on user.

With the increase threat developing within the cyber realm, it is incumbent that as individuals working in the cyber realm realize that the threat is not going away soon. As I research on the topic of the authenticity of MFA prompts. (Odogwu,2023) mentions in his article that MFA prompt bombing attack is a process where cybercriminals send loads of malicious MFA requests to your system, hoping that you will approve them mistakenly. It's one of the chief

vulnerabilities of multi-factor authentication. Despite being a good system for enhancing cybersecurity with various user verification procedures, hackers use simple human error to beat it. As the author mentions in his article about the methodology used by hackers, users must be cognizant of such to better posture themselves from being bamboozled by these attempts.

Although using MFA can be an essential layer of security statistics have shown that there are loopholes that individuals can breach this layer of security. Mirren Mcdade senior writer and journalist at Expert insights magazine mentions that according to a report my M-Trends in 2024 Google's Mandiant threat intelligence team, threat actors are evolving new techniques such as Adversary-in-the-Middle (AiTM) attacks in attempts to bypass MFA. This shift emphasizes the importance of adopting phishing-resistant MFA methods. The MFA approach requires users to give additional proof that the user is who they say they are when Google detects a suspicious sign-in attempt. She further went on to state that in a report by Verizon in 2024 that found that 68% of breaches involved a non-malicious human error such as an individual falling victim to a social engineering attack or making an error. "Human element" can refer to a range of scenarios – ultimately, it comes down to humans being responsible for a vulnerability, either knowingly or unknowingly. This can include privilege misuse, stolen credentials, social engineering attacks, or genuine human error (McDade,2024). The author explains the significance of how human lapses in judgement can result in a system being hacked although multifactor authentication is established. With the constant evolution of threats, it is very important that keen attention is paid to MFA prompts.

(Flynn, 2023) in his article stated that Over 50% of people who receive phishing emails are tricked by them. A whopping 70% of people open their phishing emails, which is a considerably higher number than the meager 3% who open traditional spam emails.

The question remains: can hackers find loopholes and initiate prompts that will trick the user? Flynn further when on to say that yes hackers can beat MFA by utilizing various methodology to do so. He mentioned the use of exploited generated tokens which involves websites relying on authentication apps such as Microsoft and Google authenticators which can be temporarily accessed by hackers.

MFA usage is undeniably an effective way to properly poster your system security to fend off attempts by hackers to gain access to relevant information. However, it is vital that the best and most appropriate security be implemented to safeguard your data. According to (More than a Password: CISA, 2025) not all MFA methods give you the same level of protection. Some MFA types are better than others—phishing-resistant MFA is the standard all industry leaders should strive for, but any MFA is better than no MFA. You should still strive to implement a stronger MFA to avoid being hacked. From this article the author highlights the importance of MFA and that there are very many vulnerabilities that may exist with the type of MFA chosen. In conjunction with the information from CISA (Cybersecurity and Infrastructure Security Agency) (Hoffman, 2022) also mentioned in her article that former CISA director urged Americans to ask their online service providers to offer the MFA feature if the tool is not yet available as a security option for their accounts.

(Multi-Factor Authentication Breach Prevention:7 MFA Vulnerabilities,2025) highlighted the fact that various methods attackers use to bypass MFA highlight the importance of a layered approach to security. Organizations must recognize that while MFA provides an additional layer of protection, it is not a silver bullet.

The 2023 MGM Resorts breach, which reportedly began with a social engineering attack against the company's service desk, illustrates how even large organizations with substantial security resources remain vulnerable when focusing too narrowly on technical controls without addressing human factors. This article shed some light on the fact although MFA is in place to prevent cyber-attacks the probability of humanistic errors will exist if individuals are not steadfast at understanding the issues that may arise from just clicking a MFA prompt that is not legitimate.

(Jones, 2024) in an article that mentioned that in 25% of cases, incident response specialists responded to fraudulent MFA push notifications sent by attackers, Cisco Talos found. In addition, "Nick Biasini, head of outreach at Cisco Talos, said via email. "Basic MFA with SMS based notification is the least secure, but better than no MFA at all". He then further stated that MFAs poorly configurated led to two of the biggest attack campaign last year involving a ransomware attack against Change Healthcare and dozens of attacks against Snowflakes customers. His viewpoint provided additional insight into the number of cases that individuals have pushed notification ignorant of the fact that these notifications are fake, cementing the claim that not all MFA prompts are legitimate.

David Braue, award winning journalist, mentions in his article that last year's breach of Uber was due to a mechanism utilized by hackers. He further explained that the attacker found a way to bypass MFA or exploit a vulnerability in its code, but because he knew enough about how it worked that he could weaponize it against a hapless Uber employee.

Having already stolen the employee's username and password, analysis has shown, the attacker wrote a script that automatically attempted to log into Uber's systems — knowing that each logon would generate a new alert on the user's smartphone, demanding that the logon be approved or denied. Each time the user tapped "Deny," the script would try to logon again — flooding the target for more than an hour with a string of notifications that became so annoying that, by the time the attacker contacted the employee on WhatsApp claiming to be an Uber technical support officer, the victim was ready to tap "Approve" just to make it all go away (Braue, 2023). This author explained how MFA fatigue is used as a hacker's weapon to cause frustration and havoc on their targets.

(Doyle,2025) provided some of her insight on how criminals often exploit humans who can be susceptible to their methods to acquire useful data. Doyle further went on to mention that cybercriminals are clever. Exploiting weaknesses is the name of their game, and they are strategic about when to launch MFA fatigue attacks. Late at night or during busy periods, when users are less alert, distracted, or likely to prioritize convenience over caution, are prime times for these attacks.

Another author that shared highlighted areas where individuals can be swayed into click a prompt that is not legitimate is (McKee, 2024) who mentioned that common tactic for threat groups such as Storm-1167, known for crafting fake Microsoft authentication pages to harvest credentials. They also create a second phishing page miming the MFA step of the Microsoft login process, prompting the victim to enter their MFA code and grant the attacker access. From there, they gain access to a legitimate email account and can use it as a platform for a multi-stage phishing attack. Although MFA is an essential tool to enhance security, there can be issues that may arise with this implementation. With MFA there is a drawback of losing access to a specific

account that is vital with the user's assessment of the MFA prompt. (Klivan et al ,2023). Multi-Factor Authentication is intended to strengthen the security of password-based authentication by adding another factor, such as hardware tokens or one-time passwords using mobile Apps. However, this increased authentication security comes with potential drawbacks that can lead to accounting and asset loss. If users lose access to their additional authentication factors for any reason, they will be locked out of their accounts. Consequently, services that provide Multi-Factor Authentication.

Chapter 3

Methods used to gather information

The research methodology utilized interviews involving subject matter experts in the technology field to aid the data collection aspect of the research. The researcher conducted face-to-face interviews that allowed data collection. According to (Siedlecki,2022) interviewing skills are paramount in acquiring the appropriate data for specific research which includes a precise plan on the details of the interview such as time and type of questions etc. The research will focus on individuals employed in various sectors in society within the age range of 25-65, to eliminate losing data users must be cognizant of the different threats that exist in the cyber realm from nefarious individuals.

Data collection procedures and analysis

Data was gathered from interviews conducted with three industry technology experts. These interviews took place in an area convenient for the interviewee. The researcher notated all the answers given from the researcher to acquire the needed data to analyze for the research. Once data is collected it was analyzed, using charts and graphs to represent data as well as verbal interpretation which will be followed by findings and conclusions Overall, I believe this method will yield the best results based on the topic that is being researched. In addition, all ethical considerations will be addressed as to avoid any ethical issues that may arise. Participants will be given the required information about the research to facilitate an understanding of the main idea. Once data is collected it will be analyzed, which will be followed by findings and conclusions.

Chapter 4

Results

A total of six questions were asked to three computer industrial technology experts to gather their viewpoint on the topic.

Question 1

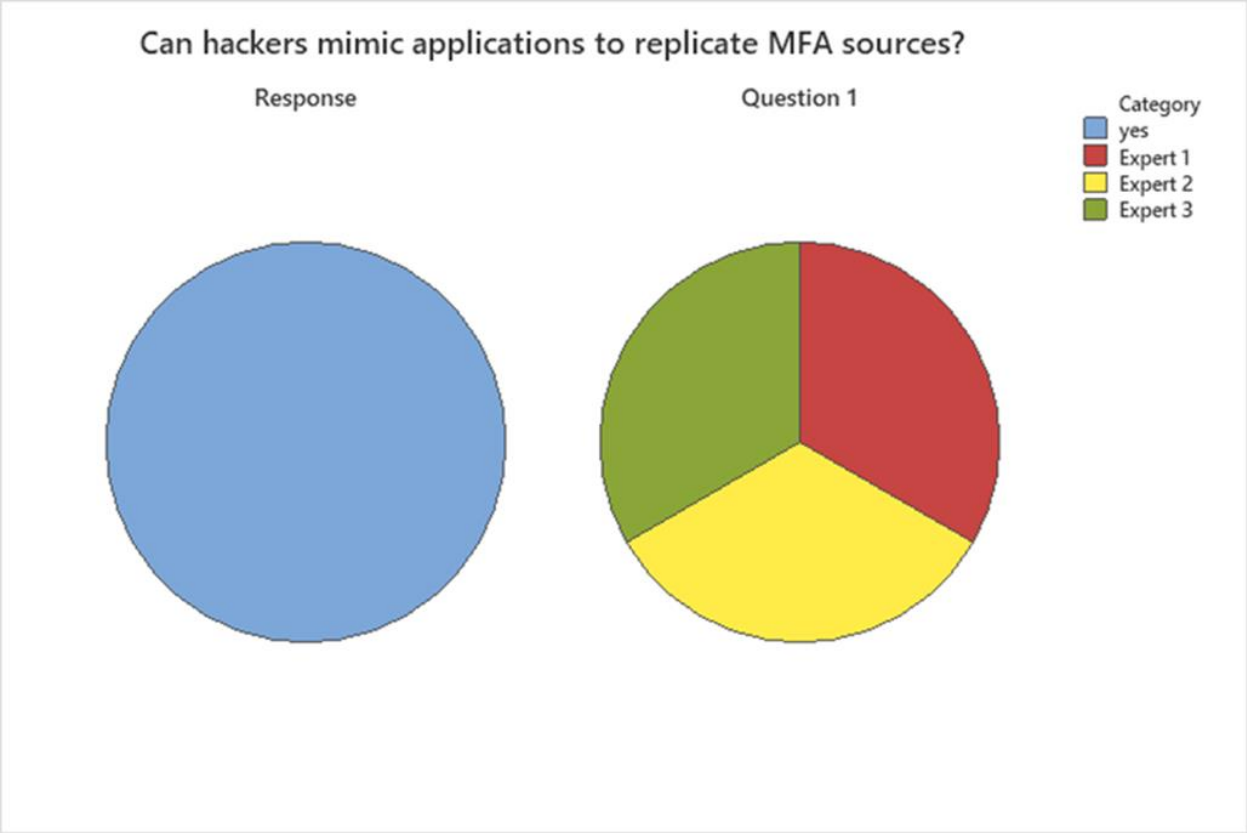

Figure 1

Can hackers mimic applications to replicate MFA sources?

Figure 1 above illustrates the results from this question all the interviewees mentioned that hackers can mimic application to replicate MFA sources. This is vital as it highlights the need for developing a better understanding of multifactor authentication, especially in society. Which further proves the point that nefarious individuals can use varied methods to acquire users' data. However, as technology develops and grows society should become aware of these threats and properly posture themselves to detect attempts. It is best to create an atmosphere where all

employees are fully cognizant of the hackers and their ability to create pages like the original page that would need the credentials from the MFA source. As K. Hunter, personal communication, September 17,2025) mentions that Hackers can create similar landing pages to actual vendors and have victims enter credentials, prompts to install private/unofficial apps then redirect the victim to official sites to repeat action. Apps loaded on personal devices can run in background capture screen, grab web services and keystrokes. In that way both hackers and victims have access to resources. It is vital that security personnel create an atmosphere where all employees are fully cognizant of the hackers and their ability to create pages like the original page that would need the credentials from the MFA source. With the increase in technology, hackers have developed multiple methods to acquire data, and it is our responsibility to become aware of threats that exist. (K. Osullivan, personal communication, September 20, 2025) mentioned that majority of these methods used to replicate MFA sources would fall under social engineering.

Question 2

Figure 2

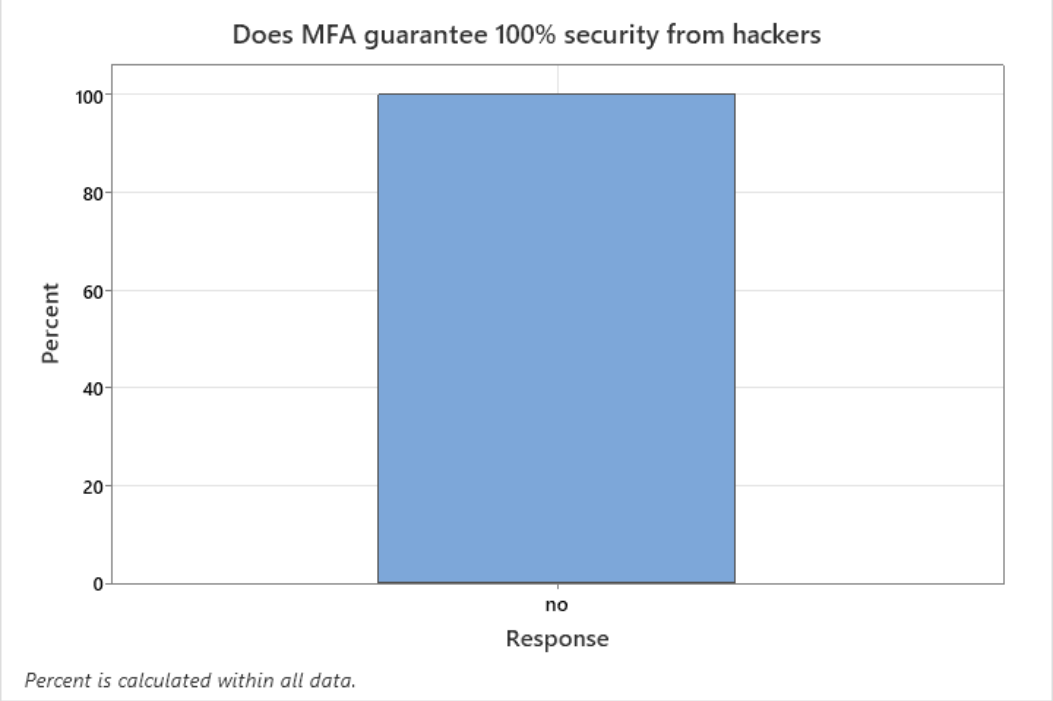

Figure 2.1

Does MFA guarantee 100% security from hackers?

Figure 2 and Figure 2.1 above illustrates the results from this question does MFA guarantee 100% security from hackers. From the viewpoint of Industrial experts who utilize this method, it states that it can be very effective in detecting any unauthorized access to a user account. Although there is not 100 percent guarantee as shown in the results. It is evident that although MFA provides a level of security measures for data access, there are loopholes that can have negative effect on the overall security of a user's data. (K. Osullivan, personal communication, September 20, 2025) states that although MFA is a layer of security that users should have, there is not a 100 percent guarantee of security from hackers. Overall, this methodology is vital in securing data. However, all users should ensure that they have other cyber protective mechanisms to face any threats that may arise.

Question 3

What are the methods used for MFA prompts

Participant	Count	Percent	Response	Count	Percent
Expert 1	3	42.86	Required- Common Access Card with a code	**(Expert 3)**1	14.29
Expert 2	2	28.57	Required- Magic Link	**(Expert 1)**1	14.29
Expert 3	2	28.57	Required- One-Time Password	**(Expert 1)**1	14.29
N=	7		Required- One-Time Password	**(Expert 2)**1	14.29
			Required-Application Push Notification	**(Expert 2)**1	14.29
			Required-Authenticator app	**(Expert 1)**1	14.29
			Required-Biometrics	**(Expert 3)**1	14.29
			N=	7	

Tally Table 1

What are the methods used for MFA prompts.

Table 1 highlights the results on the methods used to determine MFA prompts such as Common access card with a code, magic link, push notification, authenticator applications and one-time passwords. From the data, one-time password (OTP), magic link and authenticator applications are utilized together more than the other methodology used for MFA prompts. In choosing the specific MFA one must consider the scalability, security, cost and the ability to integrate with other systems. (Vazquez et al ,2018) mentions that usability, security and costs are the most used criteria for comparing and selecting authentication schemes, whereas the context is given an important remark as well.

Question 4

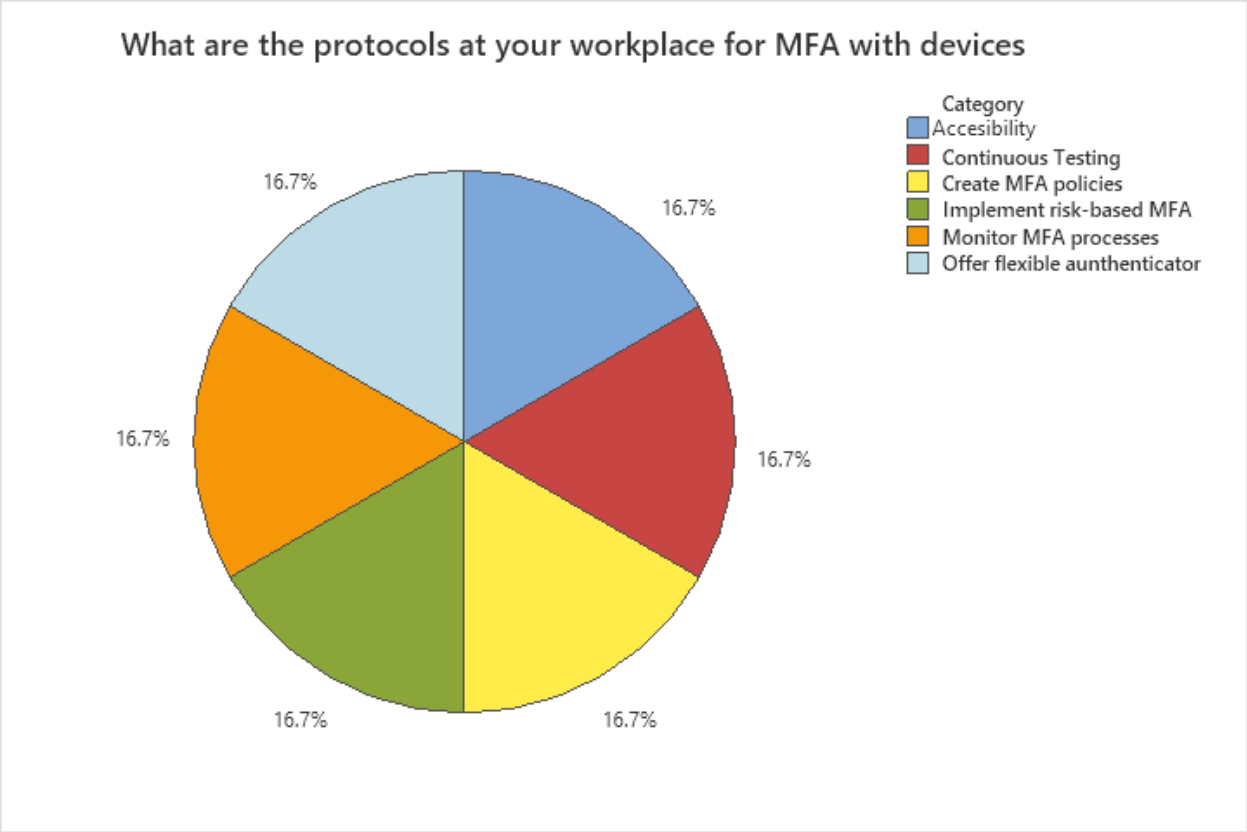

Figure 3

What are the protocols at your workplace for MFA with devices?

The experts from their organizations use Microsoft to implement MFA that is used in the workplace. (K. Hunter, personal communication, September 17,2025) mentioned that Microsoft 365 contains MFA options that are very helpful whenever they are to set MFA protocols for their workplace. (Fanti,2023) mentioned that these benefits include centralized user and group management, secure authentication, capabilities and the ability to enforce advanced security measures. The categories outlined in figure 3 are the protocols that are needed to make a successful implementation on devices used in the workplace. The advantage garnered when these are used will be added to the security and efficiency of the specific MFA that is chosen for the

company. With flexibility in the authenticator option will make the MFA effective and productive while it provides the type of security. Continuous testing provides a data repository for failed logins, friction points etc. Overall, these protocols will result in creating a safer atmosphere and better reliability on the MFA type that is utilized. In addition, the probability of getting hacked with an efficient MFA is very low.

Question 5

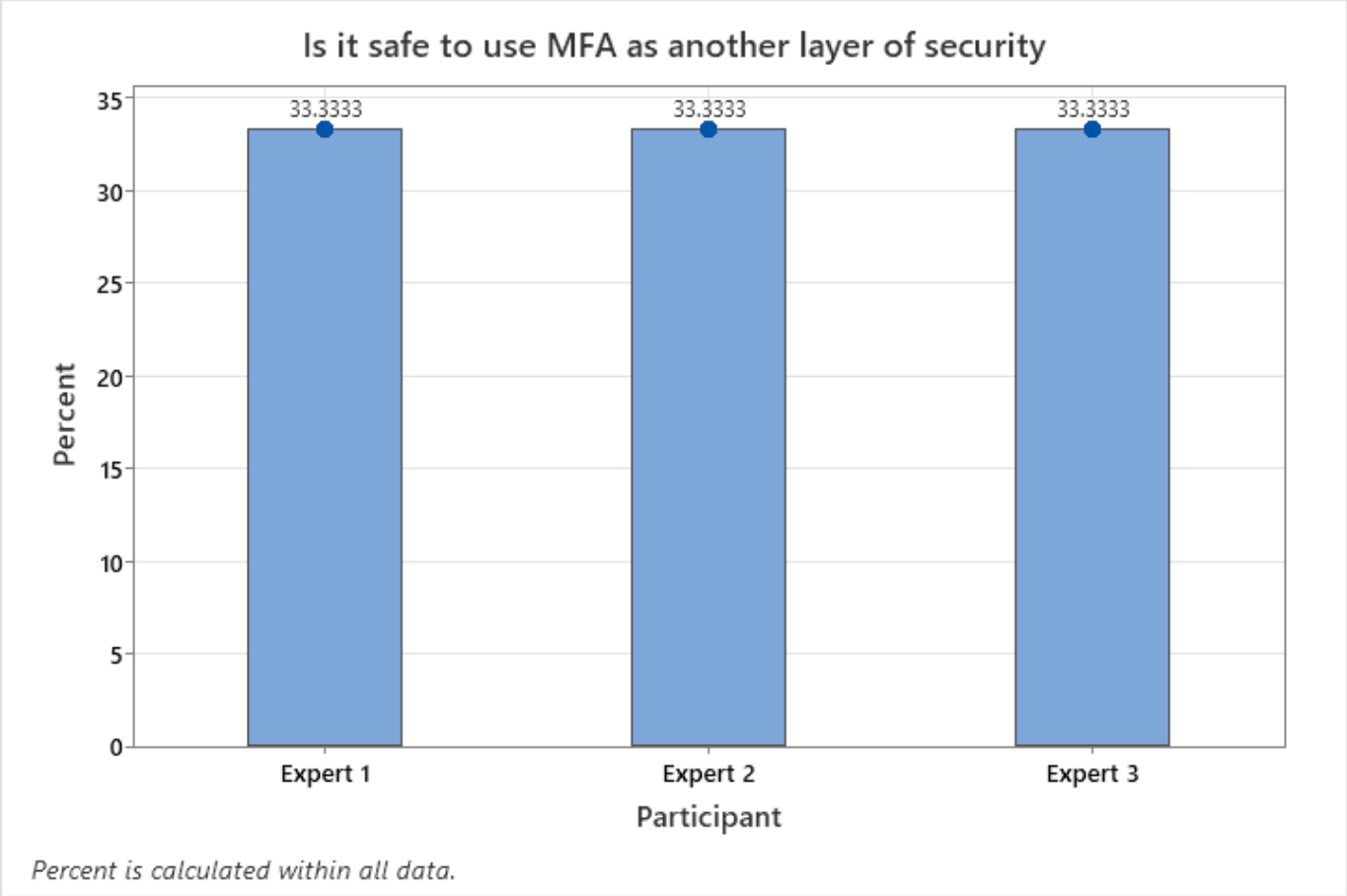

Figure 4

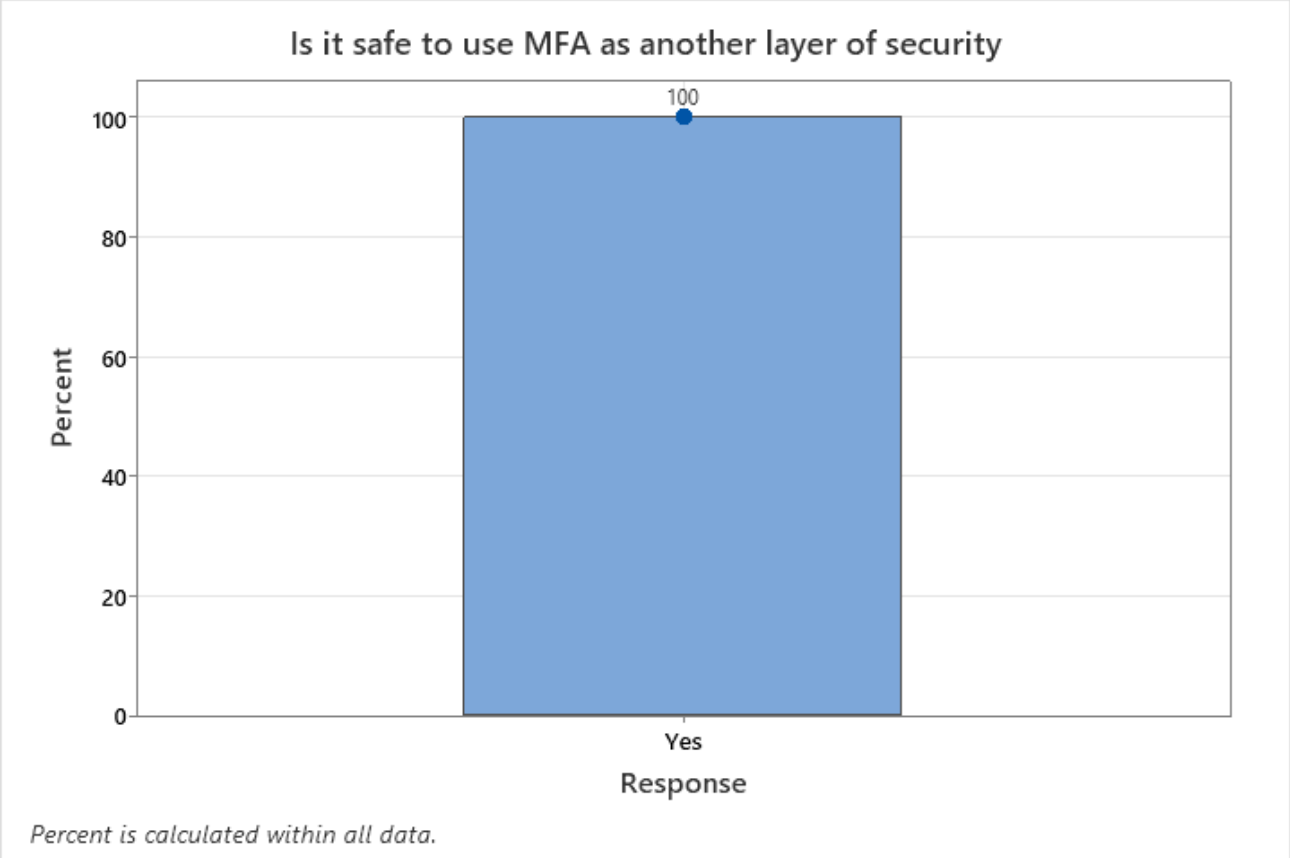

Figure 4.1

Is it safe to use MFA as another layer of security?

From the data shown in Figure 4 and 4.1 all the experts express the fact that using MFA is a safe methodology to use as a second layer of security. Having MFA implemented is an added layer of security that will aid any organization in protecting its data from hackers. According to (Hendricks & Kettani, 2019). the methods of MFA can be used in combination to successfully secure data and provide adequate authentication practices. Multi-factor authentication will easily increase security due to the different steps that are required to gain access to specific information, once the MFA prompt is not met with the correct response no access will be granted. Although it adds a layer of security there is always existing threats from hackers utilizing a variety of methods to access data.

Question 6

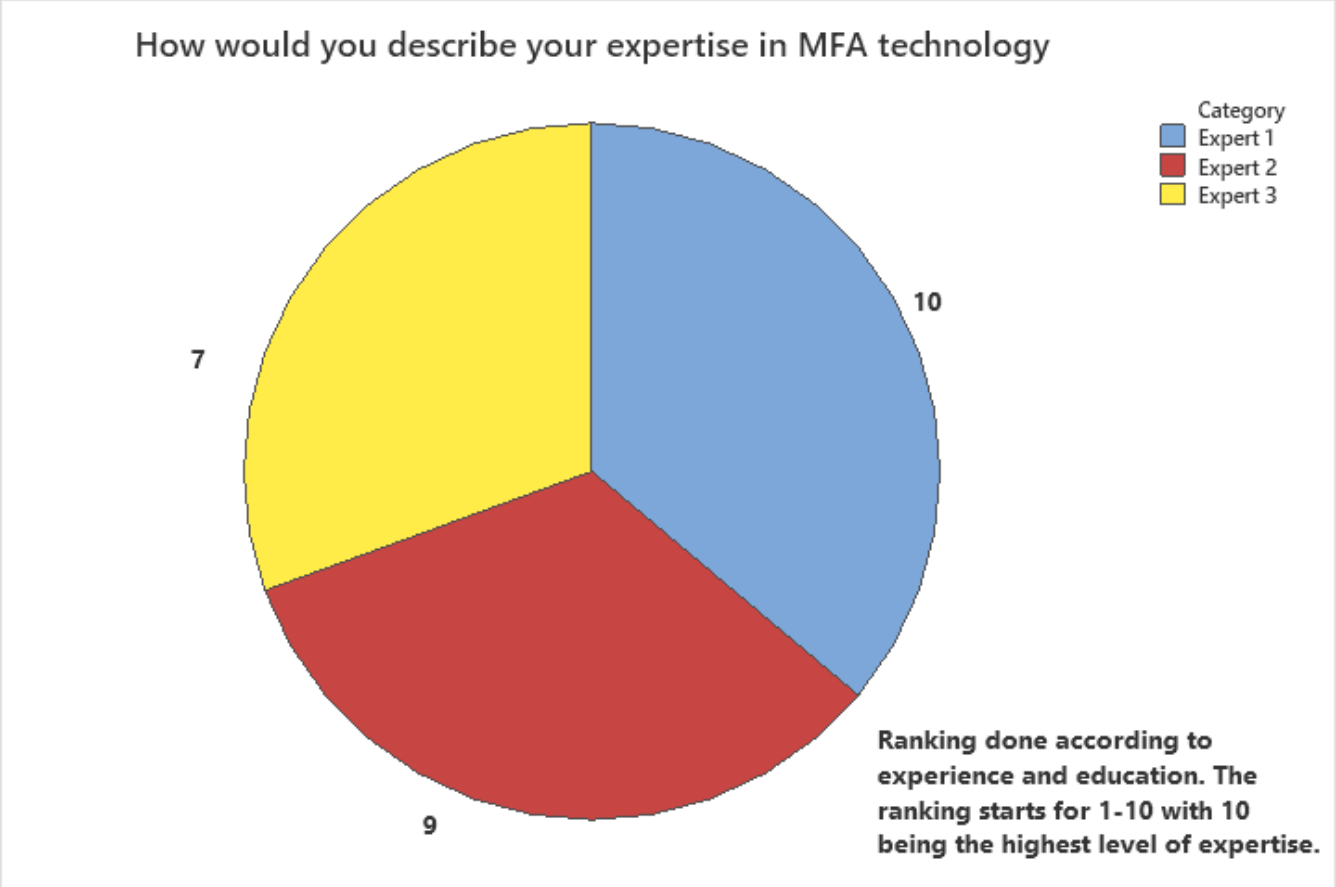

Figure 5

How would you describe your expertise in MFA technology?

The experts in the research provided there incite from their subject matter expertise on the matter. Expert number one had a plethora of information to provide that proved to be very important in understanding the impact of MFA. The other experts also provided a wholesome amount of information as well which ensured that this research was successful.

Discussion

The data analyzed suggests that multifactor authentication is very important in providing the necessary security. However, users should be mindful of the threats that exist although MFA is implemented in the daily security function for data access. The viewpoint from technological experts suggests that having MFA takes care of various aspects regarding safety and on the hand provides the public with ideal information. Although this can be used as another layer of security, users must be cognizant of their role in assessing legitimacy as well as ensuring their data is protected.

Can hackers mimic applications to replicate MFA sources?

Hacking has become more prevalent in society with more unique methodology to acquire data from nefarious sources. The data garnered from the research suggests that hackers can replicate MFA sources using a variety of methods such as creating landing pages for users to input their credentials, MFA push spam notification, and Sim card swapping. Overall, majority of the techniques used by hackers would be social engineering as this is a common method utilized.

Does MFA guarantee 100% security from hackers?

Having multifactor authentication does not guarantee 100 percent security from hackers. MFA provides some type of security as it allows users to provide a response to a prompt. Experts who utilize this method mention the effective in detecting any unauthorized access to a user account.

Is it safe to use MFA as another layer of security? Yes, with this added security features

It makes access to the intended party more credible. Using one's own personal devices

for biometric or other personal private information, the means to gain access.

What are the methods used for MFA prompts

MFA prompts are vital for the users to access their personal accounts whether through application or email. From the research OTP, magic link and common access card with a code, magic link, biometrics and authenticator applications are the methodology commonly used in the industry. Of these methods OTP, push notifications and authenticator applications are mostly used when compared to the other methods utilized. MFA prompts assist users in authenticating logins from independent sources, which is a key component in the layered security.

What are the protocols at your workplace for MFA with devices

MFA Protocols are necessary to ensure that employees understand the severity of neglecting the usage of MFA as a means of security. Some important protocols implemented by companies for MFA implementations are MFA policies, which aid in providing an understanding for individuals to become assertive of potential dangers as well as expectation from all. Other important protocols are continuous training and flexible authenticators these will be advantageous to any organization as individuals will always be prepared while the flexibility adds to the variety of authentication based on the resources and type that will enable a potent MFA system with the knowledge of existing hacking threats.

Limitation

During the research I had difficulty scheduling the interviews as the individuals would often cancel the interview time slotted. This created some difficulty during the analysis of the data that was provided during the interview. The other challenge faced was the methodology chosen to acquire data. I utilized the interview mode, which however, turned out to be a challenge as I had to listen to the information provided and notate for data gathering. The location for the interview

posed an issue as there was noise distraction that influenced the responses. The sample size at times limited the statistical prowess as there were only three main industrial experts providing the data needed.

Future research

This research will be continuous as this is the first of two phases. This phase focuses on the problematic effects from hacking circumventing MFA prompts from an industrial expert viewpoint. The other will focus from the endpoint user's view.

Chapter 5

Conclusion and recommendations

This topic is vital in making individuals cognizant of threats that exist from hackers who strive to steal personal data for their use. MFA is paramount in adding a second layer of protection. Although it provides that security users must ensure that any prompts received are legitimate as one click can result in a loss of company files, secured data or even personal data. Data in the wrong hands does not matter, since the data was only intended to be used by individuals ordained to view or manipulate. Hence the importance of validating all MFA prompts prior to clicking which will eliminate the probability of being hacked. From the findings, MFA is utilized as a methodology to add security, and it provides the user with an option whenever there is a request to access their account. This research provides the wider public with relevant details on how hacking can influence the security of MFA prompt, with the limitations experienced during the research, in the second phase of my research other methods such as questionnaires will be utilized to acquire data.

Overall, having MFA adds an additional layer of security that allows protection of data. There are loopholes that exist with this mechanism, and this research will provide the necessary details to inform the wider public of threats that exist from nefarious individuals.

Reference

Braue, D. (2023). Multi-Factor Authentication Is (Not) 99 Percent Effective.Cybercrime Magazine.https://cybersecurityventures.com/multi-factor-authentication-is-not-99-percent-effective/

Doyle, K. (2023). Understanding MFA Fatigue: Why Cybercriminals Are Exploiting Human Behaviour.IT Security Guru.https://www.itsecurityguru.org/2025/02/25/understanding-mfa-fatigue-why-cybercriminals-are-exploiting-human-behaviour/

Fanti, M. (2023). Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA. Packt Publishing Ltd.

Flynn, J. (2023).17 Essential Multi-factor Authentication (MFA) Statistics [2023].Zippia. https://www.zippia.com/advice/mfa-statistics/

Griffith, E. (2024). How to Set Up Multi-Factor Authentication and Safeguard Your Online Accounts.PCMAG. https://www.pcmag.com/how-to/multi-factor-authentication-2fa-who-has-it-and-how-to-set-it-up

Grimes, R. (2019). Security. UCF Information Security.https://infosec.ucf.edu/security/

Henricks, A., & Kettani, H. (2019, October). On data protection using multi-factor authentication. In Proceedings of the 2019 International Conference on Information System and System Management (pp. 1-4).

Hoffman, M. (2022). CISA Director Jen Easterly: Americans Need 'More Than a Password' on Sensitive Online Accounts.https://executivegov.com/2022/06/cisa-urges-internet-users-to-implement-multifactor-authentication/

Jones, D. (2024). MFA plays a rising role in major attacks, research finds. Cybersecurity Dive. https://www.cybersecuritydive.com/news/mfa-multi-factor-authentication-cisco-talos-cyber/719254/

Kapko, M. (2022). Multifactor authentication is not all it's cracked up to be. Cybersecurity Dive. https://www.cybersecuritydive.com/news/multifactor-authentication-weaknesses/633399/

Klivan, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023, November). " We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 3138-3152).

Lakhani, A. (2024). Multi-factor authentication suffers from three major weaknesses. TechRadar. https://www.techradar.com/pro/multi-factor-authentication-suffers-from-three-major-weaknesses

Mcdade,M.(2025). Multi-Factor Authentication (MFA) Statistics You Need To Know In 2025. Expert Insights.https://expertinsights.com/user-auth/multi-factor-authentication-statistics

Mckee, J. (2024). 4 Ways Hackers use Social Engineering to Bypass MFA.Red Sky Alliance. https://redskyalliance.org/xindustry/4-ways-hackers-use-social-engineering-to-bypass-mfa

(More than a Password: CISA, 2025). https://www.cisa.gov/MFA

(Multi Factor Authentication Security Risks,2021). Identity Management Institute. https://identitymanagementinstitute.org/multi-factor-authentication-security-risks/

(Multi-Factor Authentication Breach Prevention:7 MFA Vulnerabilities,2025).Nevada .IT Solutions.https://nvits.com/ways-mfa-can-be-breached-password-protection-guide/

Novak, M. (2024). Feds Warn SMS Authentication Is Unsafe After 'Worst Hack in Our Nation's History'. Gizmodo.https://gizmodo.com/feds-warn-sms-authentication-is-unsafe-after-worst-hack-in-our-nations-history-2000541129

Odogwu, C. (2023). What Is a Multi-Factor Authentication Prompt Bombing Attack.MUO.https://www.makeuseof.com/multi-factor-authentication-prompt-bombing-attack/

Palmer, D. (2022). Hackers are finding ways around multi-factor authentication. Here's what to watch for. ZDNET.https://www.zdnet.com/article/hackers-are-finding-ways-around-multi-factor-authentication-heres-what-to-watch-for/

Siedlecki, S. L. (2022). Conducting interviews for qualitative research studies. Clinical Nurse Specialist, 36(2), 78-80.

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital health https://doi.org

Vakulov, A. (2024). How Hackers Bypass MFA, And What You Can Do About It.Forbes.https://www.forbes.com/sites/alexvakulov/2024/09/05/how-hackers-bypass-mfa-and-what-you-can-do-about-it/

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30-37.

Yugoslavskiy, D. (2020). Adversary-in-the-Middle.Mitre Attack. https://attack.mitre.org/techniques/T1557/