Hacking Multifactor Authentication

Rajeshwari Reddy Pokal

Master of Science in Technology, Pittsburg State University

GRT-714-01: Network Admin Concepts

Dr. Derrel Fincher

December 03, 2023

# What is Hacking Multifactor Authentication?

Multifactor authentication (MFA) Is a security system to verify the user's identity for logins. It is a two-step verification for the systems to protect from hackers. Now-a-days protecting our data and personal information is more crucial for us, so the use of Multi Factor Authentication (MFA) is a powerful safeguard against any unwanted access. In this paper hacking methods and techniques are covered, and shows the difficulties and dangers associated with MFA. Strengthening our digital data against cyber threats is also discussed.

Cyber-attacks cause many risks to the user’s personal details. Because of increasing use of digital gadgets and social media, so much of the information is out through the internet that it can be easy for hackers to get the information. It is important to have high level knowledge about cyber security awareness to the users and individuals, so that they can easily overcome the trap. The information also has several types like email addresses, phone number, financial information, and social engineering frauds like SIM swapping, biometric forgery, and social media (Palmer, 2022).

# Implementation Of Hacking Multifactor Authentication in Workplace

Implementing multifactor authentication in the workplace is important for cybersecurity to protect the data and prevent unauthorized access. MFA is especially important in the workplace to improve the security of the company's data; it is an additional lock for digital data. Usually, we will enter password to get into our accounts, but MFA will make it some more advanced method to protect like special code like OTP, fingerprints or facial lock. Nowadays companies are relying on cloud applications to increase their productivity and to work remotely with teams. This has become even more crucial in the COVID-19 pandemic for many remote collaborations for successful business. According to Verizon's 2020 data breach investigations report most of the data breach reasons are compromised accounts and stolen credentials. It is most important for organizations to secure their accounts by using MFA. By training the employees in the company to secure their credentials, it will be easy for them to face any situations and secure their data. By using single sign-on (SSO) which helps by the identity and access management system, and gives users access to all their accounts with a single set of login credentials (Witts, 2023).

# Types of Multifactor Authentication in Workplace

## SMS-Based MFA

The several types of MFA used in the workplace are email code, text and call one-time passwords, biometric verification, physical key, and authenticator app. Whenever the user logs into their account a one-time code is sent to their phone number via SMS. It will be a brief period and they need to complete their authentication process along with their password. SMS-based MFA provides an extra layer of security to protect their sensitive data. It might be weak to SIM swapping and interception. Compared to other MFA methods, SMS messaging can be misdirected, making them less secure. SMS-based multifactor authentication is used when advanced methods might not be possible. Companies improve security by encouraging customers to activate the MFA techniques that instruct users on how to secure their mobile devices and personal information (Mindanao, 2022).

## Token-Based MFA

To improve user's authentication procedures, token-based MFA has been developed and it is a strong security technique. Through mobile apps users obtain virtual tokens, using time-based one-time password technique this token gives codes to the users while login through their accounts to complete their process. This type of MFA is successful because frequently the codes are changing, while these tokens are accessed through mobile devices and physical hardware token. In organizations they may face difficulties while transferring money, so using the token-based method they may not face any difficulties because it gives new code every time while transferring (Mindanao, 2022).

## Biometric Authentication

Biometric authentication is a unique security technique that uses physical features to confirm users' identities. By using fingerprints, facial expressions, iris recognition, and voice recognition these methods give more protection than passwords. This process has two steps; the first step is enrollment, in which the user's biometric information is collected from the users and stored safely. Another step is authentication; in this stage the system verifies the biometric information of the users and matches the recorded data, this makes the biometric MFA more secure. For example, every person has a unique fingerprint scan, iris scan has a unique design of the eyes, while facial features some people have same face, but there will be a little bit of difference in them. Every person has their unique identity to recognize their face, iris, and fingerprints. Biometric technology has more advancement to making the authentication more secure and user friendly (Mindanao, 2022).

# Methods Of Hacking

## SIM Swapping

Through the fraud technique of SIM swapping criminals can obtain victim`s phone numbers through mobile network operators to replace the SIM card linked with a new one. This gives the opportunity to the hackers to monitor messages, calls, and other information, the hackers can have access to the internet accounts through the victim's phone number. In 2021, FBI report says that SIM-swapping incidents were increased. Compared from January 2018 to December 2020, the FBI reported 320 complaints and $12 million loss, in addition in 2021 there were 1,611 complaints and losses were exceeded to $68 million worth of documents (Tung, 2022).

Hackers frequently use the customer care department of mobile network operators to obtain new SIM cards to execute SIM swapping. Through these SIM swapping methods hackers can be successful by accessing email, social media accounts, and bank accounts by requesting them by forgotten password or account recovery using the hacked phone number. This technique is extremely dangerous for bitcoin users who frequently rely on SMS-based two-factor authentication to secure their accounts. To reduce the SIM swapping risks, FBI suggests avoiding phone-based account verification unknown person, providing financial information on social media, be aware of providing personal information through online, and use unique passwords for social media accounts. Companies also encourage to consider using MFA apps which are safer compared to SMS-based authentication (Tung, 2022).

## Biometric Forgery

The present security is led by biometric technology, which has physiological and social factors for identity verification. Even though it has high security, the systems are exposed to forgeries. The main reason for the forgery method is artificial intelligence and machine learning, these techniques pose a serious threat to the security of biometric authentication. These technologies cause a serious threat to biometric authentication by making it to create artificial biometric data that resembles real identity like facial features, fingerprints, and voice patterns. Biometric database is another data theft for the biometric forgeries hackers obtain the unauthorized access to the stolen biometric data, due to that security identity verification. For example, the use of deepfake technology in facial recognition systems can be a threat, deepfakes use AI algorithms to create realistic images and videos that perfectly match the look and mannerisms of a person. Deepfake technology can fool the facial recognition software to a fake image of a person if they use it for identification (Pandya, 2019).

The Federal Trade Commission (FTC) has raised some concerns regarding the use of biometric data like fingerprints and facial expressions. FBI has focused on putting an end to the false claims related to biometric information and wants companies who use this technology to follow the law. FTC also recommends companies improve the efficiency of their biometric technology, and they need to examine whether an organization’s users of this technology is unfair if it fails to access the possible risks to users and does not train properly. The federal trade commission wants to make sure that these technologies are used properly and do not negatively impact on consumers (Ritchie et al, 2023).

## Social Media Hacking

The threat of hacking has increased on social media, which is an essential part of our daily life. Even though we download security software like Virtual Private Networks (VPN) to secure our devices while browsing and downloading we are still facing cyberattacks. Hackers focus on big platforms in which users are large, such as Facebook, Instagram, Twitter, and WhatsApp, commonly called Meta platform. The consequences of social media will be identity theft, online harassment, and financial frauds, so cybercriminals find these platforms to target easily for illegal activities and billions of users give their personal data to them. Cyberattacks use a variety of strategies to hack social media accounts by taking advantage of user`s weakness. One popular type is phishing technique, in which the attackers send harmful code messages or links through emails and direct messages. When users click on these links, the virus may enter their device and the user's information is stolen. Another thing is hackers also focus on Bluetooth and public WIFI networks for entering social media accounts without authorization. Due to data breaches, account security is in danger because of the leaked information from previous security incidents and it is used for illegal activities (Castro, 2022).

To reduce the risk caused by social media hacking, users need to set up strong security methods. It is necessary to set up strong password policies like creating different passwords for every account and changing them regularly. Users to authenticate their identity by using second method I.e., 2 Factor Authentication (2FA) it adds extra layer to the security. By setting up alarm for new device logins to secure the identity and they can take appropriate action for unauthorized access. Users are recommended to use VPN while connecting to the public WIFI and beware of phishing attacks and avoid clicking suspicious links (Iwugo, 2023).

# Hacking Techniques

## Phishing Attack

Phishing attacks, in which cybercriminals send anonymous messages to users and trick them to share their information, are becoming more common and complicated. Over 225 million phishing attacks were examined over 6 months by message security provider Slash Next which found that 61% increase in phishing compared to 2021. in which 50% attacks were on mobile devices, as the attackers were focused on mobile communication sector. Business email compromise attacks are the subset of phishing to get money, the hackers are following new methods by disturbing cryptocurrency and geopolitical developments. This is the best approach to get the money these types of attacks were increased. Spear phishing is another approach to attack people when the holiday season starts hackers try to trick the customers related to tax schemes and shopping deals (Violino, 2023).

To protect from phishing attacks people are advised to use warnings when sharing personal information, particularly when sharing unexpected requests. While clicking on any links in the email verify the sender's credibility and examine the links toughly. Use different methods to confirm the validity of any messages you receive from the mail and direct messages. To improve the security of the device use multi factor authentication, anti-phishing software, and stay up to date on the most recent techniques.

## Password Sharing

In this digital world password security is very crucial to everyone to secure their data. To protect our sensitive data, we need to stop unwanted access to the systems. To strengthen our passwords, we need to use password management procedures to reduce cybersecurity threats. The 2023 state of the phishing report from Proofpoint contains unexpected data like 31% of working adults created unique passwords for every account they have, and 8% of them have revealed their passwords to threat situations. The several types of password cracking are brute-force attack, dictionary attack, credential stuffing, and rainbow table attacks. Organizations can defeat the treats by implementing strict password policies, regularly updating passwords, and adding MFA. (Gleeson, 2023)

To secure the system users without depending only on password-based credentials they should use password less authentication techniques like biometric, time-based one-time password (TOTP), and push notifications these techniques help the users to increase the security. Proofpoint provides some solutions to provide security like TAP account takeover, which is made to protect from various threats like phishing, business email compromise, and brute force attack. These solutions help the organization to deal with challenges that they face.

# Real-life Example of Hacking Multifactor Authentication

This happened to me in 2022 my Instagram was hacked by cyberattacks. While using Instagram I got the message in the message box that I need to change the password and update the Instagram, then I clicked the link that I got to my phone. After that I changed my Instagram password and updated it. After some time, I logged in to Instagram it showed the wrong password, and my Instagram is not working and got hacked. Later my friends called me and asked that I have messaged them that I need money and send the money to the given account, then I said that my account is hacked. Finally, the hacker asked many of my friends, then I immediately acted to that and informed the cybercrime police to deal with it. This experience made me more cautious to messages and emails.

# Conclusion

In conclusion, safeguarding our personal data against cyberhackers is important. By turning on the MFA, updating, and checking regularly for any unauthorized access it makes our data more secure. MFA strategies are crucial to secure our digital data from hackers. There are several users falling for cyber-attacks despite having so many solutions. Several attacks have human involvement as a primary cause and in addition it has technology. Even though the users may ignore the important mails and consider it as suspicious, everyone should have the training for not to click the fraud links.

The implementation of multifactor authentication (MFA) provides strong protection to the user's data in this digital world. This paper explained how MFA is implemented in the workplace using different techniques to protect our data from cybercriminals. MFA security is growing more in businesses for cloud apps and remote collaboration. We need to learn some hacking techniques, so that we can tackle the situation in a better way and our data will be secured. My personal experience that I shared highlights the need for individual awareness and quick reaction in the situations of an attack. To reduce these threats, we need to strength our digital platform, apply MFA, and keep on updating your security.

# References

Castro, C. (2022, September 30). *Social media hacking: How to protect your account against intruders.* TechRadar. <https://www.techradar.com/how-to/social-media-hacking-how-to-protect-your-account-against-intruders>

Gleeson, B. (2023, September 13). *5 password cracking techniques used in cyber attacks*. Proofpoint. <https://www.proofpoint.com/us/blog/information-protection/password-cracking-techniques-used-in-cyber-attacks>

James, G. K. (2021, October 19). *Rise of ransomware attacks on the education sector during the COVID-19 pandemic.* ISACA. <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic>

Iwugo, D. (2023, June 6). *How hackers attack social media accounts – and how to defend against them.* freeCodeCamp.org. <https://www.freecodecamp.org/news/how-to-protect-social-media-accounts-from-attackers/>

Mindanao, K. (2022, February 28). *What are the types of MFA? (& the best MFA for your business).* Intelligent Technical Solutions. <https://www.itsasap.com/blog/types-of-mfa>

Palmer, D. (2022, August 16). *Hackers are finding ways around multi-factor authentication. Here is what to watch for.* ZDNET. [https://www.zdnet.com/article/hackers-are-finding-ways-around-multi-factor-authentication-heres-what-to-watch-for/](https://www.zdnet.com/article/hackers-are-finding-ways-around-multi-factor-authentication-heres-what-to-watch-for/%20)

Pandya, J. (2019, April 17). *Hacking our identity: The emerging threats from biometric technology*. Forbes. <https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/?sh=6bea68a25682>

Ritchie, J. N. & A., & Jones, N. (2023, May 18). *FTC warns about misuses of biometric information and harm to consumers*. Federal Trade Commission. <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers>

Tung, L. (2022, February 9). *FBI warns: Sim-swapping attacks are rocketing, don’t brag about your crypto online*. ZDNET. <https://www.zdnet.com/finance/blockchain/fbi-warns-sim-swapping-attacks-are-rocketing-dont-brag-about-your-crypto-online/>

Violino, B. (2023, January 10). *Phishing attacks are increasing and getting more sophisticated. Here’s how to avoid them.* CNBC. <https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html>

Witts, J. (2023, March 28). *What is multi-factor authentication, how does it work, and should your organization be using it?* Expert Insights. <https://expertinsights.com/insights/what-is-multi-factor-authentication-how-does-it-work-and-should-your-organization-be-using-it/>