# Challenges to multifactor authentication in the era of AI



In the evolving landscape of cybersecurity, multifactor authentication (MFA) has long been heralded as a crucial measure for protecting organisational information systems. It appears, however, that its effectiveness is facing new challenges as cybercriminals increasingly exploit vulnerabilities, particularly through the use of artificial intelligence (AI). The implications of this trend are drawing attention from various sectors including risk management, cyber insurance, and cybersecurity law.

Recent reports indicate that malicious actors are utilising AI-generated deepfake technology to circumvent traditional MFA protocols aimed at preventing account fraud. According to an article in Forbes, these criminals harness a series of AI tools available on the dark web to create convincing synthetic identities. The process generally involves generating a fake photograph, fabricating identification documents, and subsequently producing a deepfake video that meets the criteria of facial recognition systems. This method is particularly concerning as it allows attackers to successfully imitate a legitimate user’s identity, thus facilitating unauthorised access to sensitive accounts.

The report outlined the sequence of steps typically employed in these fraudulent activities:

1. Criminals create a fake image using generative AI websites.
2. They synthesize a fraudulent passport or government ID incorporating this image.
3. A deepfake video is generated, showcasing the fabricated identity in motion to deceive facial recognition technology.
4. Subsequently, the attackers register for a new account, upload the falsified credentials, and engage with verification systems that fall victim to the deepfake.

The use of AI is not the only area of concern when it comes to MFA weaknesses. The Cybersecurity & Infrastructure Security Agency (CISA) issued guidance suggesting that SMS should not be used as a second factor for authentication. This recommendation primarily arises from the inherent vulnerabilities of SMS, including its lack of encryption and susceptibility to interception by threat actors with access to telecommunications networks. The FBI has reported over 1,000 investigations related to "SIM swapping," a technique whereby criminals employ social engineering to hijack a victim’s phone number, further undermining the reliability of SMS-based MFA.

Moreover, a December report from Infosecurity Magazine highlighted additional vulnerabilities associated with MFA, reinforcing the notion that while MFA is a valuable security layer, it is not infallible. The increasing sophistication of AI-based tools employed by cybercriminals necessitates a more vigilant approach to information security.

Cybersecurity experts emphasise the importance of having a comprehensive information security program, ideally documented in a written information security plan (WISP). This program should maintain constant scrutiny of both existing and emerging technologies to counteract potential threats. As threats evolve, organisations are called upon to adapt their security measures accordingly, further emphasising that no single solution guarantees absolute protection against cyber threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.zerofox.com/blog/flash-report-deepfake-attacks-pose-a-growing-threat-to-mfa/> - This article explains how AI-based deepfake technology is used to bypass MFA systems that rely on biometric or behavioral data, and how attackers use social engineering to collect data for generating realistic audio and video content.
2. <https://natlawreview.com/article/ai-versus-mfa> - This article discusses how threat actors leverage AI deepfake tools from the dark web to bypass biometric systems and MFA strategies, particularly in preventing new account fraud.
3. <https://www.jdsupra.com/legalnews/ai-versus-mfa-8509321/> - This article details the process used by threat actors to create synthetic identities using AI-generated deepfakes to deceive facial recognition systems and bypass MFA.
4. <https://siliconangle.com/2024/03/25/new-solution-nametag-targets-ai-generated-deepfake-security-threats/> - This article introduces Nametag Autopilot, a solution designed to prevent AI-generated deepfake attacks and other social engineering tactics that exploit MFA vulnerabilities.
5. <https://www.zerofox.com/blog/flash-report-deepfake-attacks-pose-a-growing-threat-to-mfa/> - This article highlights the use of social engineering techniques, such as phishing and vishing, to collect data for generating deepfakes that can deceive MFA systems.
6. <https://natlawreview.com/article/ai-versus-mfa> - This article mentions the critical industries like financial services and telecommunications that are affected by AI-generated deepfakes in bypassing MFA and 'Know Your Customer' procedures.
7. <https://www.jdsupra.com/legalnews/ai-versus-mfa-8509321/> - This article explains the sequence of steps used by attackers to create and use deepfakes, including generating fake images, synthesizing identification documents, and producing deepfake videos.
8. <https://www.zerofox.com/blog/flash-report-deepfake-attacks-pose-a-growing-threat-to-mfa/> - This article discusses the evolving sophistication of cyber attacks and how AI and machine learning techniques allow threat actors to bypass MFA mechanisms.
9. <https://siliconangle.com/2024/03/25/new-solution-nametag-targets-ai-generated-deepfake-security-threats/> - This article emphasizes the need for advanced solutions like Nametag Autopilot to counter AI-generated deepfake attacks and other vulnerabilities in MFA systems.
10. <https://www.jdsupra.com/legalnews/ai-versus-mfa-8509321/> - This article underscores the importance of adapting security measures as threats evolve, highlighting the limitations of traditional MFA methods against AI-based attacks.
11. <https://natlawreview.com/article/ai-versus-mfa> - This article mentions the role of government agencies and cybersecurity experts in emphasizing the need for robust security measures beyond traditional MFA to protect against evolving threats.
12. <https://www.lexblog.com/2025/01/09/ai-versus-mfa/> - Please view link - unable to able to access data