AI Fraud up 300% in 2023: Key Tips by Mano Bank to Protect Your Money

Voice, video, and email scams using AI are spreading rapidly causing victims to lose billions of dollars. People have to learn how to identify and protect themselves against the attacks, claim financial fraud prevention experts at Mano Bank.

Vilnius, Lithuania Oct 5, 2024 (Issuewire.com**)** - Mano Bank, an international bank that offers innovative payment and creative financing solutions, is taking the lead in offering advice on how to prevent AI fraud.

As AI technology progresses, fraudsters utilize it on a large scale to defraud unaware users by exploiting vulnerabilities existing in the financial system and platforms.

For example, Americans lost 10 billion dollars related to various AI-generated fraud schemes in 2023.

However, the issue is not only a US phenomenon - various AI video, email, and phone schemes have been reported around the globe.

“With the aid of AI, scammers will only become more proficient in their deception techniques, which are already quite complex. It is more difficult now than ever to distinguish between real people and AI interactions, especially when those involve well-developed deepfakes and voice manipulation. While the targets of scammers are often senior citizens who have not mastered modern technologies and are not aware of new ways of scam, no one is protected from these AI-driven attacks,” said Andrius Popovas, Chief Risk Officer at Mano Bank.

The Irish Police Fraud Department claimed that in 2022, victims lost €13.5 million when criminals used AI to impersonate people and organizations to win their trust. Sophisticated emails and voices were produced by artificial intelligence that managed to persuade victims to send money or divulge passwords or personal information by impersonating family members or reputable financial institutions.

Similarly, con artists in Australia utilized artificial intelligence (AI) that mimics the voices of family members, elected officials, or employees of respectable businesses to obtain financial and personal data. According to a recent study, 20 billion spam calls were placed globally in just the first half of 2024, many of which were AI-deepfake frauds that made use of voice cloning technology produced by artificial intelligence.

“As the cases where AI is used for fraud will only increase, we need to have relevant information on how to protect ourselves from these types of fraud. We need to stay proactive and be more vigilant to identify red flags, which will help us not to fall victim to these frauds. I will share some tips that will help us,” continued Popovas.

1. Automated phishing attacks. The latest AI tools and technologies allow fraudsters to create highly persuasive mass mailings. In the past, texts sent by scammers were easy to recognize due to the many language errors. Unfortunately, the development of AI is being exploited by criminals. Their messages look increasingly professional now.

- You need to scrutinize suspicious messages, even if the email you received looks legitimate. Always double-check the sender’s details, including email addresses and phone numbers.

- Avoid clicking links in unsolicited messages, and access important accounts, such as your bank directly through official websites, and not through the links provided in those messages.

- Enable two-factor authentication as it will add an extra layer of security to your accounts and make it harder for scammers to gain access to them, even if they might steal your login details. Typically, two-step authentication involves logging in using a user code and password, and then verifying your identity by other means, such as email. signature, Smart ID login, Microsoft or Google Authenticator, and other methods.

2. Social engineering and identity theft. Using AI, fraudsters can collect and analyze large amounts of information. They can automate password selection processes and thus "guess" how you tend to log in.

To keep your passwords safe enough, follow a few rules.

- Use strong and unique passwords. Most organizations that use sensitive personal data encourage users to create passwords of at least 8-16 characters, use a combination of upper and lower case letters and numbers, and other characters. Special password managers can help you create and store complex passwords. A strong password can be a long, but easy-to-remember text with embedded characters - a favorite phrase, a fragment of a poem or another longer sentence consisting of a sufficiently long sequence of characters. For example, it can be a famous person's phrase ".well.done,Ist.bet2ter.than.well,Said" (Benjamin Franklin's phrase), or a quote from the book ".the, Answer.to.the.ultimate.question.of.life. the.universe.and.everything,Ist,42" (a catchphrase from Douglas Adams' book The Hitchhiker's Guide to the Galaxy).

Both of these passwords are long, and have all the standard password requirements, but are also very easy to remember. However, the main advantage of such passwords is not only that they are easy to remember - they are currently uncrackable by brute-force attacks. Also, although it seems easier to guess in the way of social engineering, it is very safe due to the additional characters, mixing of German and English, and the choice of upper and lower case letters.

- Always be critical if you are asked to disclose personal information. Don't be in a hurry to provide information about yourself; it's better to verify whether the people you're communicating with are really who they claim to be.

3. Fake videos. By using AI, it is possible to create highly evocative video and audio recordings that mimic real people - employees, representatives of institutions, and even family members. In this way, fraudsters try to create trust. Even if a video or audio looks realistic, do the following first.

- Check the source of the video. Contact the desired person directly and using official contacts. For example, you can always offer to call back on officially published phone numbers or by visiting the institution's official website.

- Always beware of unusual or rushed requests. If the video asks you to make a payment as soon as possible, to provide sensitive personal data, be especially careful, because it is the rush or encouragement that is usually the main sign of fraud. True, there may be real-life situations where you have to make hasty decisions, especially when it involves loved ones, but remember that a video or audio recording is rarely the first message you receive.

- Analyze the video and involve people with expertise if you can. Watch the video many times. Watch for unnatural movements, synchronization errors (such as mismatched spoken words and lip movements), and whether the recording is "stuck together" from several fragments.

4. Extra tips

- Stay informed about fraud schemes fraudsters use, and follow information provided by well-known banks and other reliable sources.

- Use two-step authentication when connecting to banks or other important accounts.

- Use antivirus programs and firewalls to protect your devices from malware.

- Before taking any action on the message or call you receive, check the information directly with the

bank or other official source.

“The development of AI is very fast, and as these technologies improve, so will the strategies that cybercriminals employ. We are headed where we haven’t been before, and to prevent financial losses, everyone must learn how to navigate this new environment and spot threats before it's too late. We must invest time to learn more about these new risks, handle personal data carefully, and put best practices for cybersecurity into action,” concluded Popovas.

ABOUT MANO BANK

Mano Bank is a financial institution dedicated to serving businesses and private clients across Europe with strong attention and personalized care. As the first bank in Lithuania to receive a specialized banking license in 2018, Mano Bank has been dedicated to providing business loans and payment services. By integrating digital technology with a cost-efficient approach, Mano Bank enables partners to save time and resources, allowing them to thrive in today's business environment.

Media Contact

Sensus PR

info@sensuspr.com

Source : Mano Bank

See on IssueWire