# Kaspersky warns AI-generated passwords leave users vulnerable to hacking



In the age of cyber threats and sophisticated hacking techniques, the advent of artificial intelligence has introduced both innovative tools and new vulnerabilities. On World Password Day, Alexey Antonov, Data Science Team Lead at Kaspersky, issued a crucial warning against the use of AI-generated passwords, emphasising that the very technology designed to enhance security may inadvertently expose users to higher risks.

Antonov’s analysis involved generating 1,000 passwords using large language models (LLMs) such as ChatGPT, Llama, and DeepSeek. What he discovered was alarming: despite the apparent complexity suggested by these models, a significant number of their generated passwords displayed predictable patterns that are easily exploited by cybercriminals. He noted, “All of the models are aware that a good password consists of at least 12 characters, including uppercase and lowercase letters, numbers, and symbols.”

However, many of the passwords produced were not as secure as they should be. Instances included common dictionary words and typical character substitutions, such as “P@ssw0rd” or numeric representations of letters in words. The findings revealed that nearly 60% of generated passwords could be cracked within an hour using modern GPUs or cloud-based cracking tools. Remarkably, 88% of passwords generated by DeepSeek and 87% produced by Llama failed Kaspersky's security tests, a stark contrast to ChatGPT, where only 33% did not meet adequacy for protection against attacks.

Kaspersky is not alone in expressing concerns about the security of AI-generated passwords. Recent studies show a spike in cyber-attacks targeting user credentials, particularly in gaming and AI platforms. Over the past three years, Kaspersky's Digital Footprint Intelligence division uncovered more than 36 million compromised accounts, with a staggering 33-fold increase in stolen OpenAI user credentials reported in 2023 alone. This illustrates the critical need for robust security measures when using popular AI tools.

To protect oneself against these vulnerabilities, Antonov recommends using reputable password managers instead of relying on AI for password generation. These tools create random, highly unpredictable passwords that are difficult for attackers to crack, employing cryptographic algorithms for secure generation. Additionally, password managers store credentials in a secure vault, accessible through a single master password, and often offer functionalities like auto-fill and synchronisation across devices.

In a digital landscape where convenience often compromises security, it's advisable for users to remain vigilant. Rather than falling back on generated passwords that may seem strong, prioritising password security through established methods and dedicated tools can significantly diminish the risk of cyber threats. As cybercriminals become increasingly adept at exploiting weaknesses in AI, the importance of traditional security measures cannot be overstated.

In conclusion, while the allure of AI-generated passwords is undeniable, the potential risks associated with them far outweigh the perceived benefits. As Kaspersky's findings highlight, the key to robust online security lies not in the promises of AI, but in the time-tested strategies of careful password management and vigilance against evolving cyber threats.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraphs 1, 2, 3
3. Paragraphs 6
4. Paragraphs 1, 2, 4, 5
5. Paragraphs 6
6. Paragraph 2
7. Paragraph 2

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

## Bibliography

* <https://futurecio.tech/kaspersky-warns-against-ai-password-generation/> - Please view link - unable to able to access data
* <https://itbrief.asia/story/kaspersky-warns-ai-generated-passwords-expose-users-to-attacks> - Kaspersky has issued a warning regarding the use of large language models (LLMs) such as ChatGPT, Llama, and DeepSeek for password generation, citing unpredictable security weaknesses that could make users vulnerable to cyberattacks. Alexey Antonov, Data Science Team Lead at Kaspersky, examined passwords produced by these models and discovered notable patterns that could compromise their integrity. He found that almost 60% of passwords can be cracked in under an hour using modern GPUs or cloud-based cracking tools. Kaspersky recommends individuals and organizations use dedicated password management software instead of relying on LLMs.
* <https://www.kaspersky.com/about/press-releases/kaspersky-more-than-36-million-ai-gaming-credentials-compromised-by-infostealers-in-3-years> - Kaspersky Digital Footprint Intelligence experts discovered over 36 million compromised AI and gaming credentials over the past three years. The credentials were stolen using infostealers, specialized malware designed to steal user logins and passwords. Notably, in 2023, the number of OpenAI users' stolen credentials increased 33-fold compared to the previous year, as 664,000 records with logins and passwords, including those for ChatGPT, were posted on the dark web. Kaspersky emphasizes the need for robust security measures to protect against such threats.
* <https://businesscafe.lk/business-news/technology/item/17847-on-world-password-day-kaspersky-warns-against-ai-password-generation> - On World Password Day, Kaspersky's Alexey Antonov cautioned against using large language models (LLMs) like ChatGPT, Llama, and DeepSeek for password generation. He found that these models often produce passwords with predictable patterns, such as substituting letters with numbers or generating common words like 'password'. Antonov developed a machine learning algorithm in 2024 that revealed almost 60% of passwords could be cracked in under an hour using modern GPUs or cloud-based cracking tools. Kaspersky advises users to use dedicated password management software instead of relying on AI for password creation.
* <https://www.kaspersky.co.uk/about/press-releases/gipy-malware-steals-passwords-under-the-guise-of-ai-application> - Kaspersky discovered a new malware campaign named Gipy that exploits the popularity of AI tools by disguising itself as an AI voice generator. The malware uses GitHub to store password-protected archives containing various types of malware, enabling cybercriminals to steal data, mine cryptocurrency, and download additional malicious software. Gipy has been active since mid-2023, targeting users worldwide, with the top five affected countries being Russia, Taiwan, the US, Spain, and Germany. Kaspersky emphasizes the need for vigilance against such threats.
* <https://www.33rdsquare.com/ai-can-crack-most-passwords-how-to-protect-your-passwords-from-an-ai-attack/> - The article discusses how AI can crack most passwords and provides tips to protect your passwords from AI attacks. It emphasizes the importance of using long, complex, and unique passwords for each account. The article also highlights the role of password managers in generating and storing strong passwords, and the necessity of securing your password manager with a strong master password and two-factor authentication. Regularly updating passwords and avoiding common patterns are also recommended to enhance security.
* <https://usa.kaspersky.com/blog/make-your-passwords-stronger-with-kaspersky-password-manager/24923/> - Kaspersky Password Manager not only stores passwords but also checks their strength, analyzes reuse, and assesses vulnerability. It can generate strong, random passwords and store them securely. The article provides guidance on setting a strong master password and using the password manager to its fullest to enhance password security.