Singtel

The growing threat of AI hacking

In a short time span, AI has made a substantial impact on automation, productivity, and efficiency. But this advanced technology can be used for malicious purposes, such as figuring out passwords in mere minutes or even seconds. We explore the many advantages of AI and how bad actors are abusing it for illicit purposes, including AI-powered credential cracking.

A look at AI

AI or artificial intelligence is an interdisciplinary field that simulates human intelligence such as decision-making and problem-solving processes via software-coded heuristics.[1]

Several industries are making the most of AI technologies to innovate, drive change, and improve processes and cyberspace security:[2]

Healthcare

AI is being used to carry out personalised treatment plans for patients, speed up drug research and discovery, improve disease detection times and accuracy.

Finance

Fraud detection, credit scoring, risk assessment, and algorithmic trading tasks can benefit from AI's accurate and efficient calculations and trades.

Manufacturing

AI's advanced algorithms can enable manufacturing companies to detect defective products before they get shipped out and use robotics to increase productivity.

Energy

With AI, smart grid management, demand forecasting, renewable energy optimisation, and energy conservation systems are vastly improved.

Retail

Retail companies are using AI-powered apps and services to perform targeted marketing, intelligent inventory management, and integrating visual search technologies.

Customer service

The customer service industry uses AI for digital virtual assistants and chatbots, optimising call center operations, and sentiment analysis tasks.

Impressive AI numbers

AI is more than just a buzzword – it's a business gamechanger. The following noteworthy numbers highlight how impactful AI is to businesses worldwide:[3]

By **2030**, it's estimated that the global AI market will reach a value of **US$1.35 trillion**.

Companies using AI for product design, development, and production **save 30 times more than others.**

According to **94% of business leaders**, AI will be essential for business success in the next five years.

91% of top organisations are investing in AI activities.

Early adopters of AI-powered supply-chain management tools saved **15%** on logistics and increased inventory by **35%** and service levels by **65%**.

In **2023**, the global AI adoption rate reached 35%.

The abuse of AI technology

According to various cyber threat intelligence reports, cybercriminals are abusing AI's advanced technology to power their nefarious schemes and malicious attacks:

Deepfakes

Malicious actors use deepfake technology[4] to alter benign images, videos, and even audio files to use in impostor scams such as virtual kidnapping, a type of cybercrime that abuses AI to manipulate victims' decision-making processes.[5]

Improving malicious code

Cybercriminals use generative AI technology, such as ChatGPT, to quickly improve their malware's code or generate base code that they will later on refine.[6]

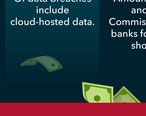
AI-powered hacking and password cracking

Malicious actors use AI and machine learning (ML) algorithms to guess passwords by making educated guesses based on a victim's personal information, publicly available data, and common or previously leaked password information.

In 2023, scientists have found that cybercriminals can use AI to guess passwords with more than 90% accuracy just by listening to the sound of keys being pressed.[8]

Phishing and social engineering techniques

Cybercriminals use AI to draft convincing and persuasive phishing emails that impersonate executives to trick victims into sending critical company information or large amounts of money.[7]



The true cost of stolen credentials[9]

US$4.45 million

Average cost of a data breach in 2023.

US$5.9 million

Amount finance firms lose per data breach, which is 28% higher than the global average.

82%

Of data breaches include cloud-hosted data.

US$2 billion

Amount the Securities and Exchange Commission (SEC) fined banks for cybersecurity shortcomings.

51%

Of organisations planned to increase their cybersecurity budgets in 2023.

Combat AI-powered hacking with Singtel SingVerify

SingVerify is an authentication solution that helps enterprises enhance their cybersecurity posture and reduce fraud. It's an effective tool to enhance existing authentication processes and mitigate the human risk in authentication.

SingVerify gives businesses access to a basket of APIs, allowing them to verify a customer's digital identity through real-time telco network data.

It also reduces the risk of cybercriminals hijacking the authentication process. In a traditional 2FA verification process, when 2FA details are encoded on a phishing site, an attacker can capture the details and use it to log in on the real site. Since **SingVerify performs authentication in the backend using real-time data**, it hinders attackers from proceeding to the app UI and encoding 2FA details.

Transform your business with Singtel.

Contact us

References

[1] Investopedia, Artificial Intelligence (AI): What It Is and How It Is Used, 2023.
[2] Forbes, 15 Amazing Real-World Applications Of AI Everyone Should Know About, 2023.
[3] Techopedia, 150+ Artificial Intelligence Statistics You Need to Know in 2024 – Who is Using It & How?, 2024.
[4] Thomson Reuters, Practice Innovations: Seeing is no longer believing – the rise of deepfakes, 2023.
[5] CNN, 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping, 2023.
[6] Trend Micro, Hype vs. Reality: AI in the Cybercriminal Underground, 2023.
[7] SC Magazine, AI abuse grows beyond phishing to multistage cyberattacks, 2023.
[8] The Guardian, AI can identify passwords by sound of keys being pressed, study suggests, 2023.
[9] IBM, Cost of a data breach 2023: Financial industry impacts, 2023.