Volume 25 | Issue 4 | November 25, 2025

BCSI Investigations Inc.

The Investigator Newsletter

AI Data Poisoning

How cybercriminals manipulate AI algorithms to mislead or commit fraud.

About Us

Since 2000, BCSI Investigations Inc. has performed thousands of successful investigations. Our integrated team of investigators and support services ensure

Data Poisoning & AI Manipulation.
How cybercriminals manipulate AI algorithms to mislead or commit fraud.

AI data poisoning occurs when the learning model used by the AI software is altered to produce incorrect output. This can be something as simple as the AI model incorrectly stating 1+1=3, or something as complex as a self-driving car misinterpreting green lights as stop signs and red lights as go signs. There can be major impacts if this is not caught early on.

It is essential to recognize the signs of data poisoning and address them as early as possible. These signs include:

that the investigations are conducted promptly with leading-edge techniques.

With over 40 years of combined experience, BCSI Investigations Inc. is the platinum standard for private investigations.

Contact us at 604-922-6572 or visit our website at www.picanada.ca to learn more.

Visit our Website

- The performance of the model deteriorates
- AI starts giving random results that don't make sense
- Increase false positives/false negatives

There are different types of data poisoning to look for:

- **Backdoor attacks:** a hidden trigger is put into the dataset that can be used to bypass security if the correct pattern is put into the model
- **Data Injection:** data is added to the training dataset to confuse the model
- **Mislabeling attack:** modifies the dataset to confuse labels
- **Deletion attacks:** data is removed from the dataset

The best ways to avoid data poisoning are to implement robust security policies and perform regular data sanitization. It's essential to regularly review the datasets to ensure there is no unwanted or missing data.

Thank you for trusting **BCSI Investigations Inc.** to keep you informed and protected.

Services | Firm Profile | Contact Us | Email

STAY CONNECTED