Bulletin from The Atrium 06/19/2024

How can generative AI be used for fraud?

Generative AI is capable of producing realistic text and images, and can even mimic faces and voices. These capabilities can equip fraudsters with tools to create convincing but misleading information that could deceive anyone. Here are some examples of how generative AI can be used by fraudsters:

- **Deepfake.** A deepfake uses generative AI to copy the appearance and voice of a person. Deepfake videos can be convincing, usually showing the person saying things they've never said. For example, fraudsters can use the likeness of a celebrity to promote fake products or services.

- **Enhanced email phishing.** Fraudsters can use generative AI to create more sophisticated phishing emails without spelling mistakes and errors, and even copy the voice and tone of trusted people or businesses. This could make phishing emails harder to spot.

- **Voice spoofing.** Voice spoofing (or voice cloning) uses generative AI to copy a person's voice. This technology could help fraudsters to improve their scams. For example, attaching a voice message to a phishing email could make the email look more convincing if the copied voice is from a trusted person.

How can I protect myself against generative AI fraud?

- **Verify information.** Always verify emails, messages, or phone calls that seem unusual or unexpectedly ask for personal information. Contact the sender directly through known and verified channels to confirm the legitimacy of the request. Avoid clicking links, downloading attachments, or calling numbers that you don't recognize or trust.

- **Be cautious.** Question investment opportunities that promise returns that are too good to be true. Before investing, ask for more information and do your research. Determine the legitimacy and motives of those promoting the offer before making any investment decisions.

- **Pay attention to the detail.** Keep an eye out for inconsistencies in facial expressions, unnatural movements, or audio not syncing with lip movements, which are all signs of a deepfake.

- **Stay informed.** Learn how AI technologies work and educate yourself on the latest trends in AI fraud, so you can better recognize potential threats.
- **Report suspicious content.** Report anything unusual to the **Canadian Anti-Fraud Centre** online or by phone at 1-888-495-8501. Your actions could help prevent others from being deceived. If something doesn’t feel right, it probably isn’t.

By following these tips, you can reduce the risk of falling victim to generative AI fraud and help create a safer online environment for everyone.