



## Common AI-Related Investment Scams

By Wei Woo

Artificial Intelligence (AI) has revolutionized many aspects of our lives, including the financial sector. However, this technological advancement has also given rise to sophisticated investment scams that pose significant risks to investors. This article will explore common AI-related investment scams that you should work in partnership with your Investment Advisor to try to avoid.

### AI-Powered Romance Scams

AI technology has enhanced the capabilities of romance scammers, allowing them to create more convincing fake profiles and engage in more natural conversations. These scammers often use AI-generated content to build trust with their victims before eventually requesting money for fraudulent investment opportunities. This is especially common with single seniors who are divorced, widowed, or been single for a while. Seniors are in a loneliness epidemic, which is an ongoing trend of increasing social isolation and feelings of loneliness experienced by people across the globe. Over 50% of Canadian seniors struggle to some degree with loneliness, according to the Canadian Social 2023 Survey, with 30.1% stating they do not have people they can rely on when they have problems, and over 300,000 people report consistently feeling lonely over the past 10 years. The AI romance scams have been very successful on scamming seniors based on this trend.

### Deepfake Scams

Deepfake technology, powered by AI, allows scammers to create highly convincing video and audio impersonations of trusted figures. In a notable case, a finance clerk in Hong Kong was defrauded of \$25 million when scammers used deepfake technology to impersonate senior executives during a video call. In Edmonton, Alberta, over 15 victims with a loss of 1.9 million were scammed after believing Elon Musk and Justin Trudeau were endorsing an investment, due to deepfake technology. This technology can be used to manipulate investors into making hasty financial decisions based on false information.

## **AI-Powered Social Media Bots**

Sophisticated AI-powered bots can create and manage social media profiles that appear genuine, complete with realistic personal details and activity. These bots can engage in conversations, comment on posts, and even send direct messages, making it difficult for users to distinguish them from real people. Scammers use these bots to spread misinformation about investment opportunities and manipulate public opinion on certain stocks or cryptocurrencies. AI-powered social media bots are very popular on online dating websites and phone apps, as a way to create AI romance scams mentioned above.

## **AI-Driven Investment Scams**

Fraudsters are leveraging AI algorithms to create more convincing investment scams. These scams often target cryptocurrency and stock trading, using AI to:

1. Create fake social media profiles, forums, and websites that spread misinformation about investment opportunities.
2. Manipulate stock prices through tactics like astroturfing, where thousands of fake accounts flood the internet with coordinated messages to generate false hype or fear around a particular stock or cryptocurrency. Extremely popular in the Youtube comments section.
3. Simulate real-time trading activities on fraudulent investment platforms, making them appear legitimate.
4. Falsely promising they are using a highly successful and secretive AI software to do trading that are making people thousands of dollars per week, and that you are one of the few with access to it, but only if you act now!

## **AI-Enhanced Phishing Scams**

AI technology is being used to create more sophisticated phishing attempts. Scammers can use AI to generate personalized and convincing emails or messages that appear to be from legitimate financial institutions or investment advisors. These messages may prompt victims to reveal sensitive financial information or transfer funds to fraudulent accounts.

## **Working with your Investment Advisor**

Investors can work closely with their investment advisors to implement several strategies to protect their finances from AI-related scams.

### Education and Awareness

This includes:

1. Talking to your advisor about recent common financial scams and red flags to watch for.
2. Regularly communicating with your advisor about what may seem like interesting investment opportunities before acting on it, as it may be too good to be true.

### Enhanced Due Diligence

Advisors and clients should do thorough research of any investment opportunity before committing funds. This includes:

1. Verifying the credentials of individuals and companies involved in the investment.
2. Reviewing the investment's history and performance.
3. Checking with regulatory agencies to ensure the investment is legitimate.

### Implement Strong Security Measures

Investment advisors should work with their clients to implement robust security measures, such as:

1. Using multi-factor authentication for all financial accounts.
2. Regularly updating passwords and using strong, unique passwords for each account. I always tell clients it's important to update at least every 6 months, even if it is a hassle.
3. Being very cautious about sharing personal or financial information online or over the phone.
4. See my article on "[Protecting Online Investment Accounts](#)".

### Regular Account Monitoring

Advisors should encourage clients to regularly review their accounts for any suspicious activity. This includes:

1. Monitoring account statements for unauthorized transactions or sudden changes in investment holdings.
2. Promptly reporting any suspicious activity to the advisor and relevant authorities.

### Encourage Skepticism

Both Advisors and clients should foster a healthy sense of skepticism:

1. Be wary of unsolicited investment opportunities, especially those promising high returns with low risk.
2. Take time to make investment decisions and resist pressure tactics.
3. Seek second opinions on investment opportunities from trusted financial professionals.

## **Conclusion**

As AI technology continues to advance, so too will the sophistication of investment scams. By working closely with their investment advisors and implementing robust protective measures, investors can significantly reduce their risk of falling victim to these fraudulent schemes. Education, vigilance, and a proactive approach to security are key to safeguarding financial assets in an increasingly complex digital landscape.

If you want to explore post-retirement goals aimed at creating healthy and balanced financial strategies, please contact me at [wwoo@researchcapital.com](mailto:wwoo@researchcapital.com).

## **Wei Woo, CIM, EPC**

Investment Advisor

Research Capital Corporation

3481 Allan Dr. SW

Edmonton, AB, T6W - 3G9

Office: 780 - 460 - 6628

Cell: 780 - 299 - 0760

*Research Capital is a national investment firm with offices in Vancouver, Calgary, Edmonton, Regina, Toronto and Montreal. The opinions, estimates and projections contained herein are those of the author as of the date hereof and are subject to change without notice and may not reflect those of Research Capital Corporation ("RCC"). The information and opinions contained herein have been compiled and derived from sources believed to be reliable, but no representation or warranty, expressed or implied, is made as to their accuracy or completeness. Neither the author nor RCC accepts liability whatsoever for any loss arising from any use of this report or its contents. Information may be available to RCC which is not reflected herein. This report is not to be construed as an offer to sell or a solicitation for an offer to buy any securities. This newsletter is intended for distribution only in those jurisdictions where both the author and RCC are registered to do business in securities. Any distribution or dissemination of this newsletter in any other jurisdiction is strictly prohibited. RCC and its officers, directors, employees and their families may from time to time invest in the securities discussed in this newsletter.*

© 2025 Research Capital Corporation. Member-Canadian Investor Protection Fund / member-fonds canadien de protection des épargnants

*Research Capital Corporation (RCC) makes no representations whatsoever about any other website which you may access through this one. When you access a non-RCC website please understand that it is independent*

*from RCC and that RCC has no control over the content on that website. The content, accuracy, opinions expressed, and other links provided by these resources are not investigated, verified, monitored, or endorsed by RCC.*