Cybercriminals are using AI to target your finances

Cybercrime has become more advanced over the years, but the level of sophistication could take a quantum leap forward with the explosive growth of generative artificial intelligence (AI). The threat is keeping security professionals up at night.

AI is making it easy to mimic a real person's voice or create a scam website that looks exactly like a real one, making it far more difficult for the average person to know whether a call, email or link is real. According to one 2023 survey [1], 75% of security professionals reported an uptick in attacks over the past year, most attributing the increase to generative AI.

Larry Zelvin, Executive Vice President and Head of the Financial Crimes Unit at BMO Financial Group, is one of the foremost authorities on cyber risk. He sat down for a wide-ranging conversation about the many online issues ultra-high-net-worth families face and how to defend against them.

When it comes to cybersecurity, what are some of the growing risks people need to be aware of?

The threat landscape continues to evolve and I advise our clients to be mindful of deepfake videos that leverage AI, increasingly sophisticated phishing scams (that may also now be generated by AI), and fraudulent ads or social engineering attempts you may encounter online—on social networking platforms or when making online purchases.

How is AI changing the game?

It only takes somebody a couple of hours and a minimal fee to create a very credible deepfake video, which is a fake video that appears to be real. These videos can be developed using AI tools and a two- to three-second voice recording gathered online. What we're concerned about is that criminals are using the voice recording to develop a fake message about a potential family emergency. What the recipient sees or hears is their loved one in trouble, expressing an urgent need for money or information. In this sense, the "phishing" experience is becoming much more complex.

Criminals are also using AI to improve the tailoring of their phishing attacks through enhanced social media and other publicly available information searches, making it more complicated to detect and validate the legitimacy of an email. We used to watch for red flags like misspellings or poor grammar, but with AI, messages are much more sophisticated. We've even seen examples where clients have received detailed, professional-looking financial brochures, but it's all fraud.

Are criminals using AI to impersonate executives?

When a CEO is talking to their direct reports, these individuals have a sense of what the CEO typically asks and how he or she speaks. The concern is less at the executive level and more with employees a few levels down within the organization who don't always have direct interaction with the CEO or organization leaders. An employee may receive a message along the lines of: 'Hey, I'm coming to you because I've got a matter of urgency, and I can't reach the Chief Financial Officer or deputy and need you to send this wire.' The message seems legitimate; it may have the general tone of the executive and come from their email address. In an effort to help their leader, the employee sends the wire.

Larger organizations have an advantage over small- and medium-sized businesses because they have established processes, procedures and employee training to watch for this type of fraud. When you don't have that security infrastructure and awareness programming in place, the organization is at a greater risk.

Continued

Larry Zelvin is the Head of the Financial Crimes Unit at BMO Financial Group where he is responsible globally for cyber security, fraud, physical security and crisis management. Prior to BMO, Larry was a Managing Director and the Global Head of Cyber Security at Citigroup. Larry has also held several roles in the U.S. Government that include Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security; Senior Director for Response, National Security Council, The White House; and, Director, Homeland Defense Integration, Office of the Secretary of Defense, The Pentagon. He served as a U.S. Naval Officer and Aviator for 26 years and retired as a Captain. Larry has a Bachelor of Arts from Boston University, a Master of Arts from the U.S. Naval War College and a Master of Science from the U.S. Defense Intelligence College.

Criminals are also targeting high-net-worth clients. What can these families do to protect themselves?

Whether you're a high-net-worth client or a family office business, there is a risk that needs to be monitored and closely managed. The good news is many of these individuals have access to experts who can offer advanced security controls and programming.

We know criminals are actively looking for situations to exploit, could that pose a risk to some families? Should families introduce their kids to their financial advisor?

First, if you receive a cold call from a financial advisor, always be sure to verify their credentials through multiple sources. For example, if they claim to be from a bank, call the bank to verify using information from the organization's legitimate website.

When it comes to family members having access to funds, identify who may put you at risk. If you have somebody that actually has the ability to move funds, that's a risk. If you have somebody that is of a legal age where they could potentially take out loans or create other indebtedness, that's a risk.

Once you have identified those who have the power to make significant business decisions, bring them in by educating them on security best practices, the latest scams and introduce them to your wealth professional or team.

What should you do if you suspect that you are interacting with a fraudster?

I recommend that you investigate. Look up the contact on LinkedIn® or Google—and contact the company they work for to validate they are who they say they are. When calling the organization, always make sure you're using phone numbers you've used in the past or have been taken from their website.

If you have reason to believe it is a fraud, we recommend reporting it immediately and have resources to help you on our BMO Security site.

How is BMO keeping ahead of cybersecurity risks?

Founded in 2019, our Financial Crimes Unit combines expertise from our cyber security, fraud, physical security, and crisis management teams to detect, prevent, respond to, and recover from security threats. In addition to using leading-edge security technology, data and analytics tools, we operate on a global scale to help ensure our clients' safety in different time zones.

When it comes to addressing AI, we have technology in our call centers that uses AI to match people's voices. We also work with a company that has a database of people who have committed fraud; this team has captured their voiceprint and will notify our agents in real-time that they may be talking to a fraudster. We continuously educate our employees on deepfakes—what they look like, red flags to watch for, and where to report them.

What are your thoughts about the evolving nature of cyber risk?

I recently wrote an op-ed in the *Chicago Tribune*[2] about how fraudsters are leveraging AI to make fraud attacks more sophisticated. AI is an area of risk that we see, not only for the bank, but more importantly, for our customers. We are a resource, and we're happy to talk to folks about this topic and keep them informed. Our clients can also visit our website[3] for the latest trends to help them stay protected.

BMO | Wealth Management

[1] Gallagher (2023), "AI: Keeping Pace With the Cybercriminals," https://www.ajg.com/news-and-insights/features/ai-keeping-pace-with-the-cybercriminals/

[2] Zelvin, Lawrence K. "Fraudsters have artificial intelligence too." *Chicago Tribune*. Updated March 28, 2024. https://www.chicagotribune.com/2024/03/28/opinion-ai-bank-financial-fraud-security/

[3] https://www.bmo.com/en-us/main/personal/security-center/

CAS00038471 (1/25)