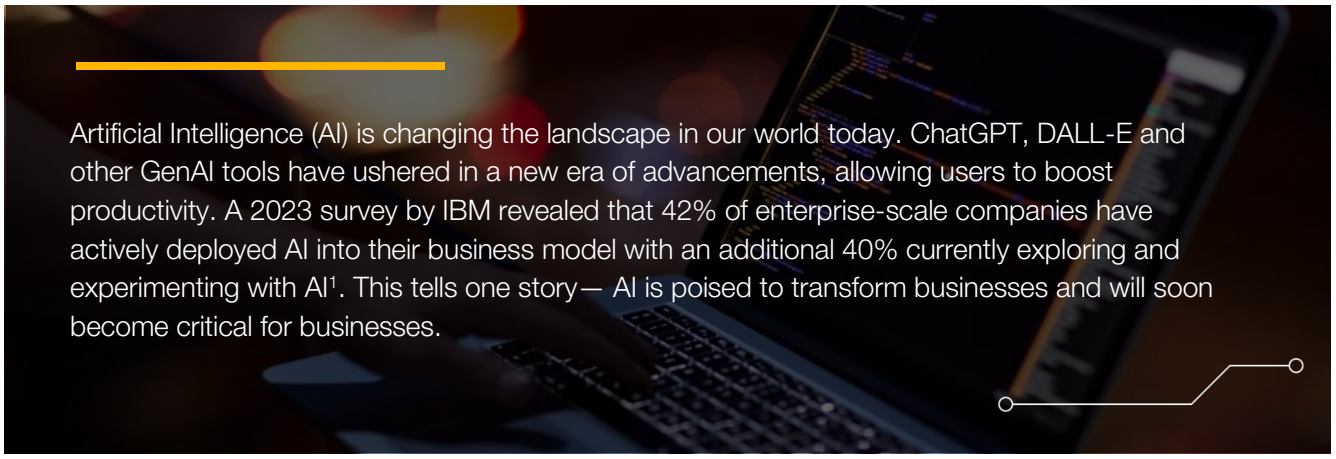
The emerging threat of AI-powered fraud

What companies can do to prepare

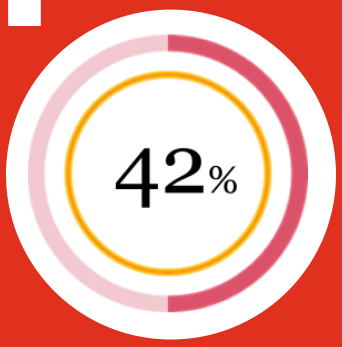
pwc

www.pwc.com/ng



Artificial Intelligence (AI) is changing the landscape in our world today. ChatGPT, DALL-E and other GenAI tools have ushered in a new era of advancements, allowing users to boost productivity. A 2023 survey by IBM revealed that 42% of enterprise-scale companies have actively deployed AI into their business model with an additional 40% currently exploring and experimenting with AI[1]. This tells one story— AI is poised to transform businesses and will soon become critical for businesses.

However, the widespread adoption of AI by businesses also means that the technology will attract malicious actors such as fraudsters and cybercriminals. As legitimate businesses seek to grow using this new technology, fraudsters are also exploring how to use AI to advance their "business". As a result, understanding the strategic opportunities and the inherent fraud risks that comes with AI is now of paramount importance for today's business leaders.



42% of enterprise-scale companies have actively deployed AI into their business model.

Source: IBM Global AI Adoption Index 2023

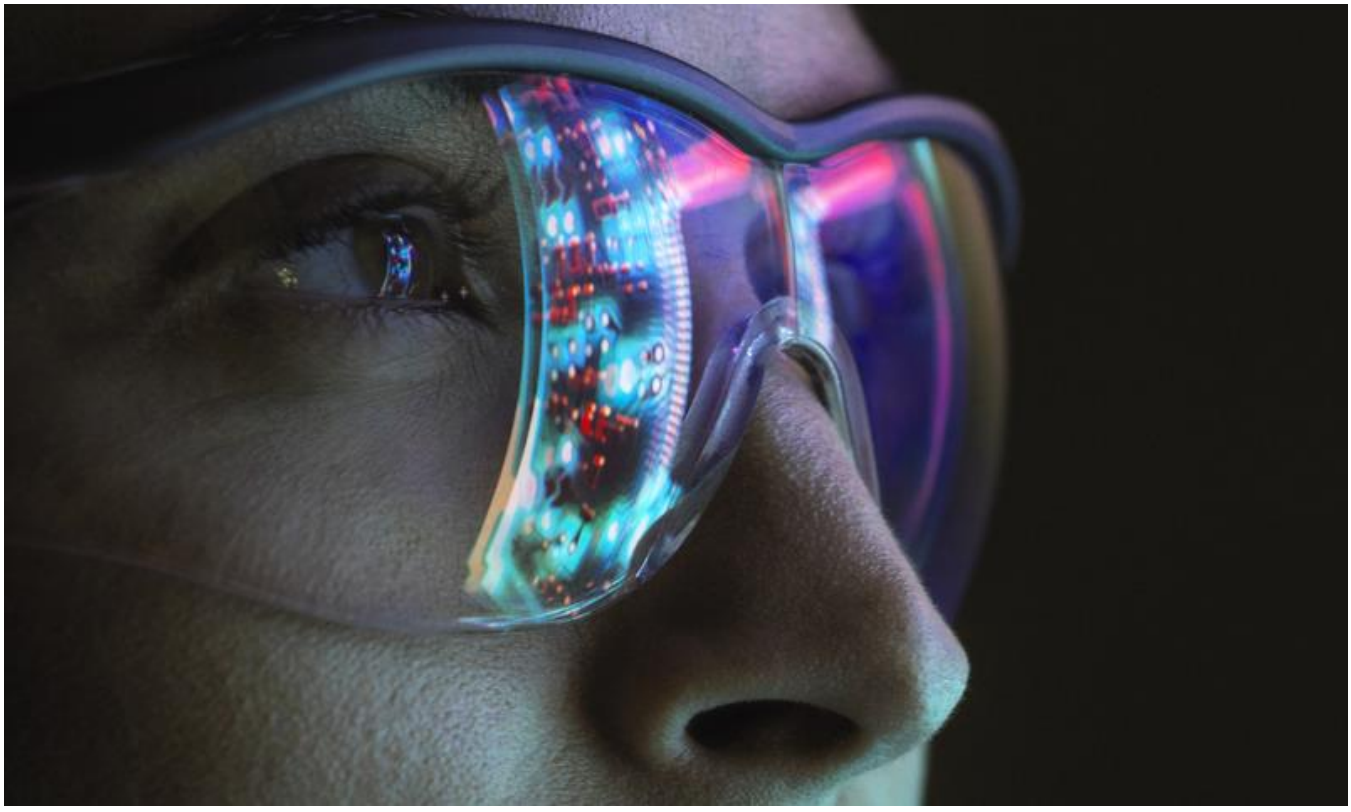
1. BM Newsroom. 2024. "Data Suggests Growth in Enterprise Adoption of AI is Due to Widespread Deployment by Early Adopters, But Barriers Keep 40% in the Exploration and Experimentation Phases." IBM Newsroom. https://newsroom.ibm.com/2024-01-10-Data-Suggests-Growth-in-Enterprise-Adoption-of-AI-is-Due-to-Widespread-Deployment-by-Early-Adopters.

History of fraud and technology

Historically, adoption of technology by individuals and businesses resulted in a corresponding adoption by fraudsters. Emails led to the rise of phishing emails and email scams, social media platforms led to the rise of fake profiles for scamming as well as outright theft of online identity, and e-commerce and digital payment platforms resulted in high rates of online payment fraud. A recent study estimates that global cumulative merchant losses to online payment fraud will exceed $343 billion between 2023 and 2027.[2]

USSD banking introduced in Nigeria also resulted in a surge in sim swap frauds enabling fraudsters to access funds, obtain loans and make other transactions on victims accounts. Gift cards and reward programmes have led to a wave of scams, forcing many establishments to either scrap them entirely or implement stricter regulations. In 2022, Bloomberg reported that PayPal shut down 4.5 million accounts linked to exploiting their incentive and rewards program.

These examples show that technological advancements have also led to new frauds and vulnerabilities to businesses and individuals. Consequently, the prevalent adoption of AI also means that AI-powered fraud is coming.



2. Maynard, Nick. 2022. "Online Payment Fraud Losses to Exceed $343 Billion Globally Over the Next 5 Years | Press." Juniper Research. https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/.

How businesses are using GenAI

Companies are integrating AI into their business strategies. PwC's 27th Annual Global CEO Survey West Africa report found that 51% of companies have adopted GenAI across their companies and 47% believe that GenAI will improve the quality of their company's products and services[3]. Businesses are using AI to automate customer service, screen candidates in the recruitment process, predict market trends, optimise energy distribution etc. In Nigeria, companies in the financial services industry have integrated GenAI in customer service with the introduction of chatbots.

When adopting new technology, businesses need to consider the risks adoption exposes them to. There have been instances where researchers manipulated AI and convinced chatbot users to visit a website containing malware or a phishing text in order to get credit card details[4]. Another paper on Large Language Models (LLM) found random words that when fed to chatbots, will cause them to ignore their boundaries, resulting in these chatbots providing instructions for building an explosive device and manipulating elections[5].

51% of companies have adopted GenAI across their companies.

Source: PwC's 27th Annual Global CEO Survey West Africa report

This leads to an important question - how are companies managing the fraud risks and other threats arising from this new technology? Business leaders should mandate their teams to conduct extensive risk assessment to ascertain how AI exposes their business to vulnerabilities or fraud. This is not only important for entities that are adopting or plan to adopt AI. It is equally important for those entities who are yet to embark on any AI journey. PwC's CEO Survey further highlights that business leaders are concerned GenAI adoption will expose their businesses to cybersecurity and misinformation risks.

3. PwC Nigeria. 2024. "PwC's 27th Annual Global CEO Survey - West Africa." PwC. https://www.pwc.com/ng/en/publications/pwc-ceo-survey.html.
4. Greshake, Kai, Sahar Abdelnabe, Shailesh Mishra, Christoph Endres, Thorsten Holz, and Mario Fritz. 2023. "Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection." AISec '23: Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security, (November), 79-90. https://doi.org/10.1145/3605764.3623985.
5. Zhou, Andy, Zifan Wang, Nicholas Carlini, Milad Nasr, J. Z. Kolter, and Matt Fredrikson. 2023. Universal and Transferable Adversarial Attacks on Aligned Language Models. https://doi.org/10.48550/arXiv.2307.15043.

How fraudsters are using GenAI

The developments in artificial intelligence have the potential to increase the volume and sophistication of fraud. Here are some possible exploitations of AI for fraud[6].

Generating text and image content.

GenAI can be used to create tailored emails, instant messages and image content as the bait to hook potential scam victims, for example, in phishing and smishing attempts, or through fraudulent adverts. GenAI can also make these scams harder to detect by eliminating the traditional 'tells' such as poor spelling and grammar. There have been instances where AI generated images (e.g. of damaged property) were used to support insurance claims.

AI-enabled chatbots.

Fraudsters are leveraging elements of AI in chatbots that converse with victims to manipulate them in a scam. Chatbots have the potential to amplify fraudsters' ability to reach victims, delivering volumes of scams that would previously have required a large team of individuals operating in a scam centre.

Sophisticated targeting of victims.

Other instances where AI tools may be of benefit to cybercriminals is in the review of large volumes of data to identify potential victims and tailor scam content to an individual's specific vulnerabilities. For example, using online content to identify an individual's employment details, family circumstances, where they have recently been on holiday etc. GenAI could make it easier for fraudsters to analyse large sets of data for their pig-butchering scams and perform them at scale.

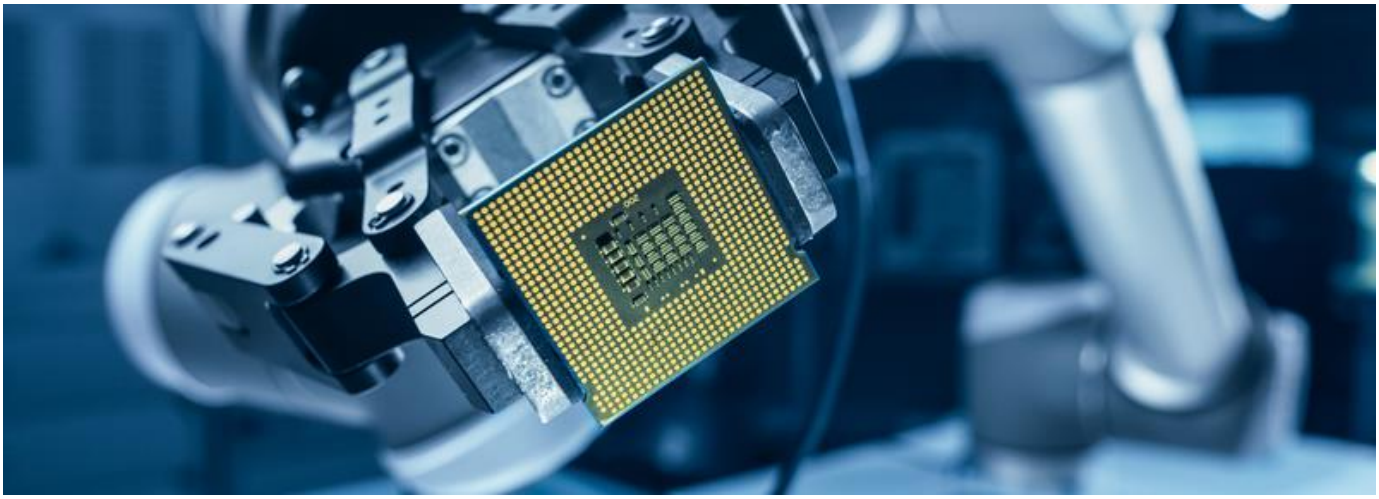
6. PwC UK. 2024. "Written evidence submitted by PwC." Committees. https://committees.parliament.uk/writtenevidence/125808/pdf/

Deep fake videos.

Deep fakes are now used as ‘click bait’ to direct users onto malicious websites (where their credit card information may then be harvested) or which use a trusted persona to encourage investment in a scam. In April 2024, a video posted on social media featured a Channels Television news anchor and Nigerian business mogul, Aliko Dangote. In the video, Dangote appears to be promoting a cryptocurrency investment scheme. Channels Television subsequently released a statement where it clarified that the video was doctored using existing footage and a generated voiceover.

Voice cloning.

Deep fake technology can copy voices to an increasingly high degree of accuracy. Currently, voice clones potentially require as much as an hour of training data to perfect, but that requirement is reducing all the time. Voice clones can then be used to trick individuals into making payments and can be used to break through systems where voice biometrics are used for ID verification. In the upcoming 2024 US election, there are growing concerns about the implications of deepfakes as AI-imitation of Joe Biden’s voice was used to discourage voters in New Hampshire[7].



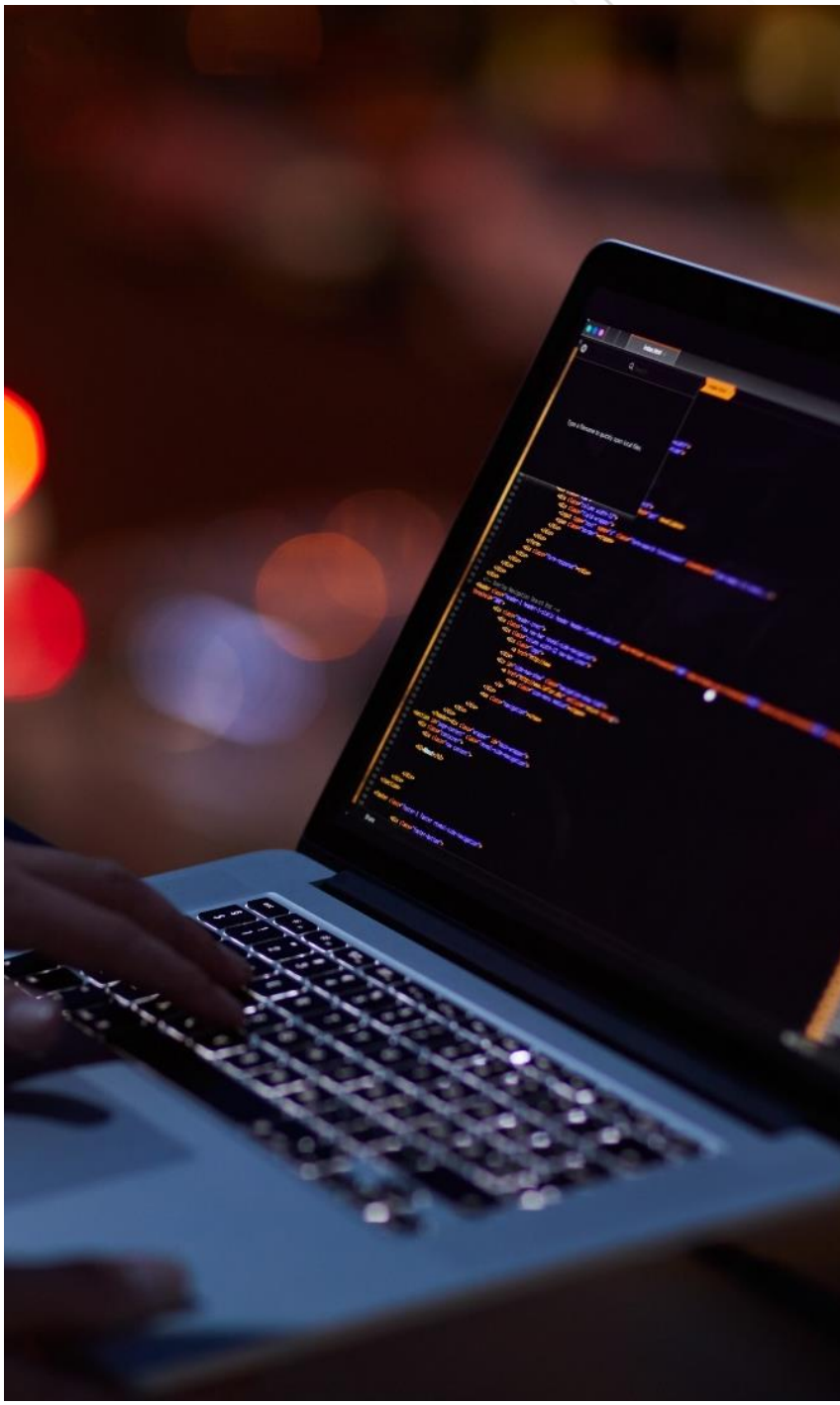
7. SWENSON, ALI, and WILL WEISSERT. 2024. “Fake Biden robocall being investigated in New Hampshire.” AP News. https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5.

The key impact of AI will be to enable fraudsters to create content at greater speed and in greater volume, and to make scams more believable. For example, a fraudster who has stolen the sim or WhatsApp profile of a business leader could clone the owner's voice and use it to authorise payments or use AI to generate content and use it to defraud the business leader's networks etc.

In February 2024, a finance officer in Hong Kong had a video conference call with his Chief Financial Officer and other team members. On the call, he was directed to pay out $25 million. The Hong Kong police reported that after checking with the head office, the employee discovered that everyone on the multi-person conference call was (deep) fake[8]. In May 2024, Financial Times identified the company as UK-based engineering group, Arup[9].

In May 2024, the CEO of WPP was the target of a deepfake scam. Fraudsters created a fake WhatsApp account using his image and set up a Microsoft Teams meeting with an agency leader, impersonating the CEO and another senior executive. They used AI voice cloning and YouTube footage to make the scam more convincing. The scammers attempted to trick the agency leader into setting up a new business and revealing sensitive information[10]. WPP noted that the scam attempt was unsuccessful.

These reports show that businesses are vulnerable to AI fraud.



8. Chen, Heather, and Kathleen Magramo. 2024. "Finance worker pays out $25 million after video call with deepfake 'chief financial officer.'" CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.
9. Financial Times. 2024. "Arup lost $25mn in Hong Kong deepfake video conference scam." Financial Times. https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea.
10. Robins, Niick. 2024. "CEO of world's biggest ad firm targeted by deepfake scam." The Guardian. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam.

How businesses can prepare for AI fraud

Perform proactive fraud risk assessment.

Businesses should conduct periodic and proactive fraud risk assessments to protect their organisation from AI-powered fraud. Such risk assessments should start from reviewing existing processes and identifying how malicious actors can leverage GenAI to exploit the processes. This would entail the business staying updated on AI developments.

In addition to this, businesses should incorporate fraud risk assessment into their internal frameworks and mechanisms for launching new products or adopting a new technology. This will help them identify how the new technology and product could create new risks or exacerbate existing ones, giving the advancement in AI at the time of launch.

Businesses will become aware of fraud risks they face in the light of changes in AI and should be able to take proactive measures to mitigate such risks.

Review and update the anti-fraud strategy and framework.

Most businesses have not updated their anti-fraud policies, despite the rapidly changing business environment powered by an equally rapid advancement in technology. Businesses should update their anti-fraud policies to reflect current state realities and incorporate how the organisation intends to deal with emerging fraud risks. In defining what constitutes fraud and misconduct, each organisation's anti-fraud policy should detail examples of use cases of AI and GenAI that would constitute fraud by employees, vendors and other stakeholders.

ACFE's 2024 Anti-fraud Technology Report highlighted that 83% of organisations plan to adopt GenAI in their anti-fraud strategy[11]. Similarly, 69% of respondents to PwC's 2024 Digital Trust Insight survey noted that they plan to use generative AI for cyber defence in 2024, and nearly half (47%) are already using it for cyber-risk detection and mitigation[12].

11. Association of Certified Fraud Examiners and SAS. 2024. "2024 Anti-Fraud Technology Benchmarking Report." ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/sas_benchmarkingreport_2024.pdf.
12. PwC. 2023. "2024 Global Digital Trust Insights Survey." PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html.

Businesses should adopt the use of GenAI in their fraud prevention and detection efforts. This would involve in-depth reviews of business needs and requirements before identifying the technology/system to adopt or deploy. This should include outlining the roles and responsibilities of AI systems and human analysts, establishing clear protocols for handling AI-generated alerts and insights, and ensuring compliance with relevant regulatory requirements.

The fraud awareness and training programme should be updated to include modules that educate employees on AI-enabled fraud and the potential impact to them and the organisation as a whole. Such sessions should provide employees with clear steps and procedures to take when they suspect or become aware of such fraud.

Empower anti-fraud teams with the right skillset and tools.

Businesses should invest in building the capacity of their anti-fraud teams to deal with and respond to Ai-enabled fraud. This includes providing them with access to AI training as well as investing in the right tools for investigating AI-powered fraud.

In the light of the advances in AI, every organisation's anti-fraud team must have digital forensics capabilities (i.e. training and tools) which will serve as a foundation for investigating and gathering evidence related to AI-enabled fraud. Earlier this year, ACFE's Anti-fraud Technology Report indicated that only 29% of organisations have an anti-fraud program that involves digital forensics or e-discovery software. This number would be significantly lower in Nigeria and other countries in Sub-Saharan Africa.

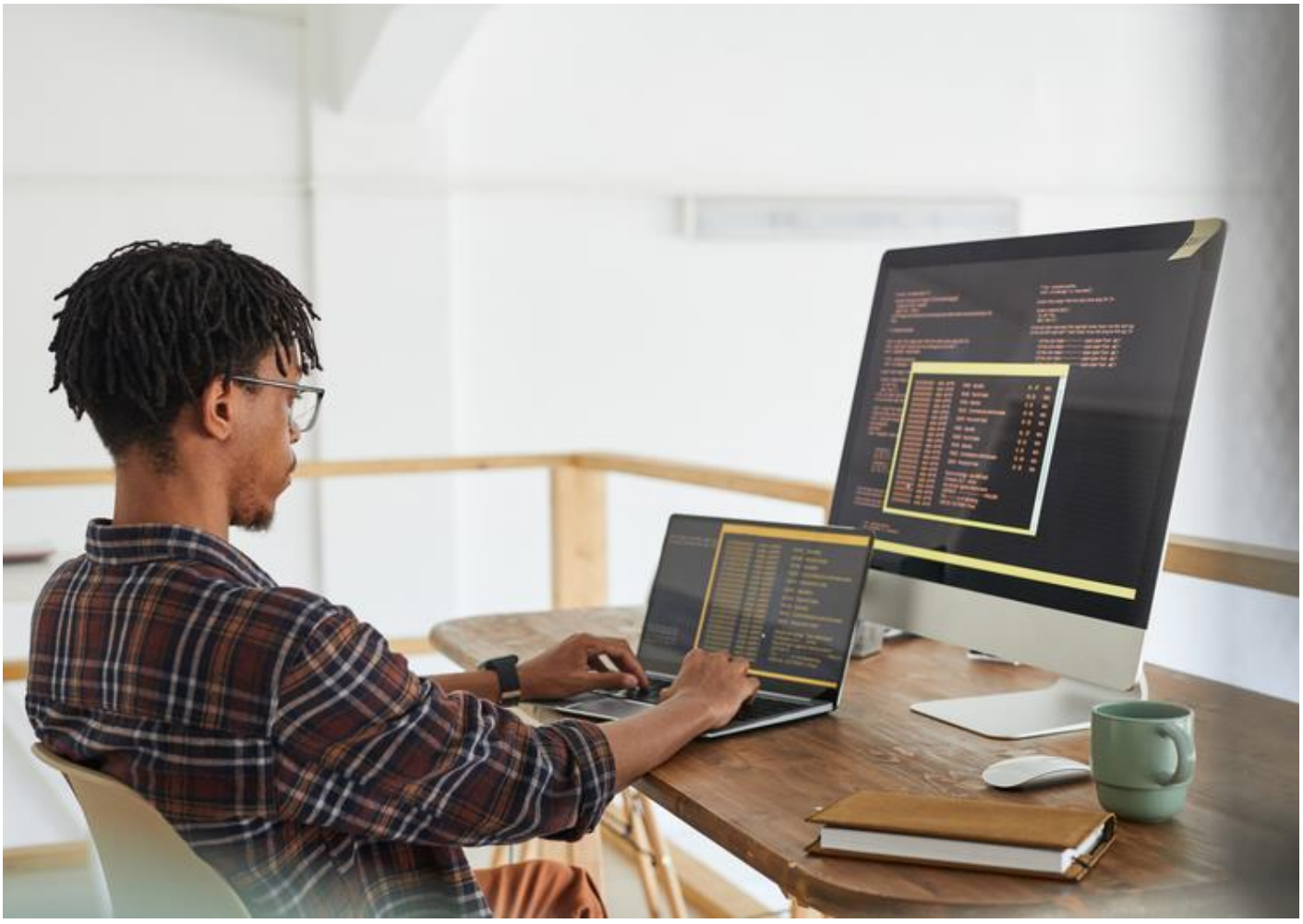
Business leaders should balance their enthusiasm for GenAI with a clear understanding of fraud and other risks that would be involved with its use. They should think through the controls they can implement to mitigate those unique risks. They can consider developing comprehensive training programs and guidelines to ensure the ethical and responsible utilisation of generative AI, and creating a controlled sandbox environment where employees can freely experiment and test innovative ideas without risk. Government can support businesses by raising awareness among individuals and law enforcement agencies. This is essential to combat GenAI-powered fraud effectively. The government can initiate online campaigns to inform the public about AI-driven fraud.

In addition, the government should promote collaboration between the players in public and private sectors to address the emerging threat of AI-powered fraud. By working together, these institutions can pool resources, share insights, and develop coordinated strategies to effectively fight fraud. Governments can encourage this collaboration by:

- Providing incentives for industry-led initiatives aimed at strengthening and enhancing fraud detection capabilities; and,
- Creating regulatory frameworks to enable information-sharing and cooperation, ultimately creating a more fraud-resilient ecosystem.

Conclusion

The increased reports of deepfake scams and attempted fraud schemes send a clear message and warning: AI-powered fraud is here. Business executives must update their fraud framework, perform risk assessment on areas of their businesses that are vulnerable to GenAI-enabled scams and ensure their anti-fraud team have the right skills and tools to detect and respond to threats from AI. Additionally, governments, industries and law enforcement should collaborate to develop a framework for preventing and responding to AI-enabled fraud.



Contact us

Habeeb Jaiyeola

Partner and Forensics Services Leader,
PwC Nigeria

habeeb.jaiyeola@pwc.com
+234(0)803-394-5167

Adeola Adekunle

Associate Director, Forensics Services,
PwC Nigeria

adeola.adekunle@pwc.com
+234(0)806-486-3890

pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with more than 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.