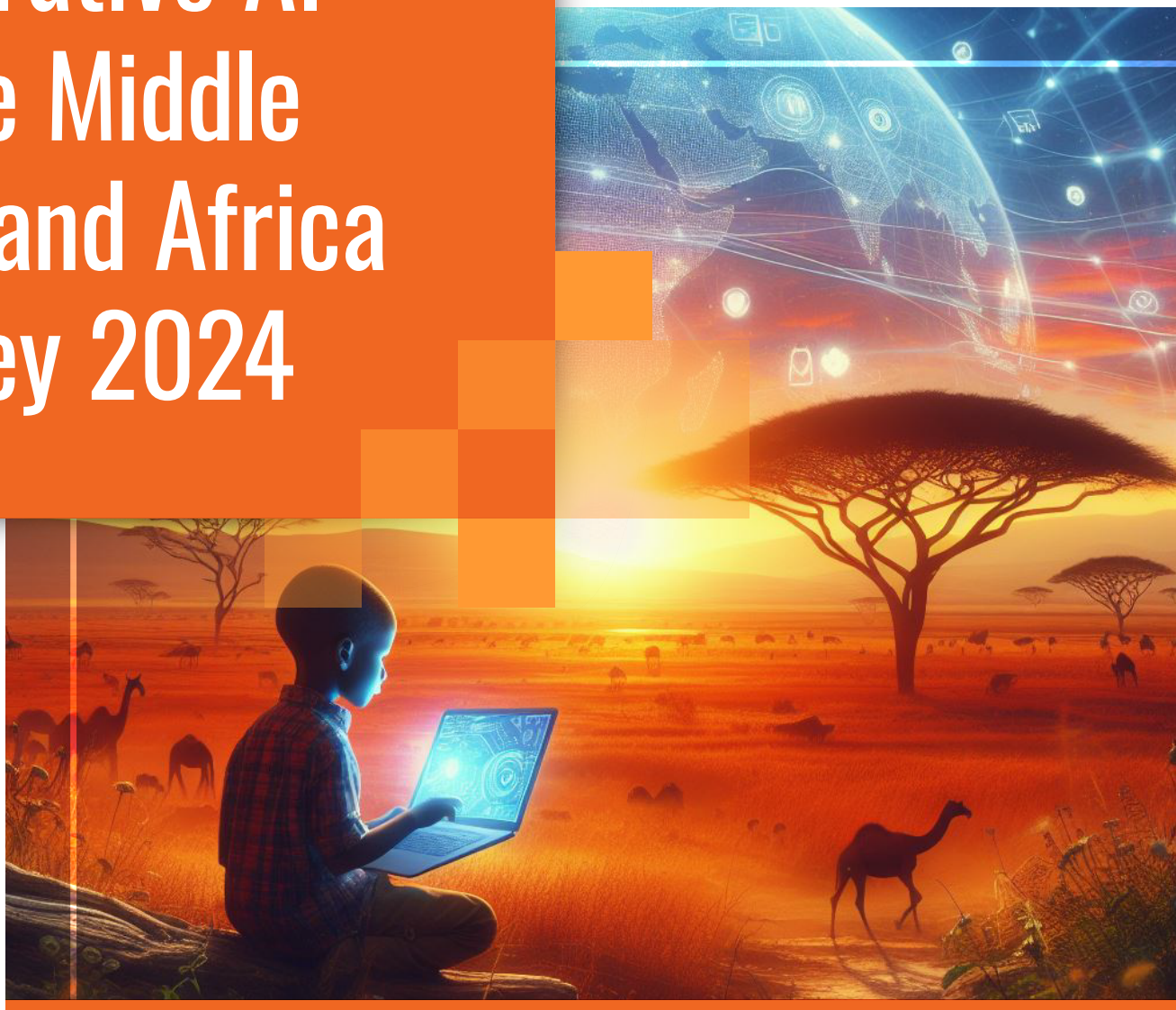
KnowBe4
Human error. Conquered.

Generative AI in the Middle East and Africa Survey 2024



by Anna Collard

SVP Content Strategy & Evangelist
KnowBe4 Africa

Generative AI in the Middle East and Africa Survey 2024

Table of Contents

Introduction: Generative AI Unleashed 2

Key Findings 3

Uses and Benefits of Generative AI 4

What do you use generative AI for? 4

What are the benefits of using generative AI? 5

A Threat to Job Security and Critical Thinking? 6

Security and Ethical Concerns 7

Looking Ahead: Embracing Generative AI Responsibly 8

References 9

INTRODUCTION: GENERATIVE AI UNLEASHED

2023 was the year of generative Artificial Intelligence (generative AI) with users all over the world delighted by the friendly generative AI chatbots, such as ChatGPT answering emails, drafting marketing content, program code and creative content such as audio, images and videos.

In response to the wide adoption of this technology, KnowBe4 conducted a survey on the use of generative AI in Africa and the Middle East, focusing on how widespread it is, what it is being used for, and the threats and opportunities it creates for the continent.

The survey spanned 1,300 individuals across South Africa, Botswana, Nigeria, Ghana, Kenya, Egypt, Mauritius, Morocco, the United Arab Emirates and Saudi Arabia. It included a wide range of age groups, with most participants falling into the 25–34 age group (41%), followed closely by the 18–24 age group (28%) and the 35–44 age group (22%). The gender distribution was approximately 55% male and 45% female. *Note: the respondents used smartphones and 88% were employed during the time of the survey, making them a more privileged subset of the general African population.*

Generated by DALL-E 3

We identified several key themes, particularly the rapid adoption of the new technology and the respondents' lack of awareness regarding the risks associated with using generative AI.

Overall, sentiment towards the new technology is highly positive, with 42% rating the impact of generative AI tools on society as very positive and 41% as somewhat positive. Nevertheless, respondents pointed out several notable concerns about generative AI.

From a cybersecurity perspective, it is concerning that a significant percentage of users are comfortable sharing their personal information with generative AI. A large majority feel confident about the accuracy and reliability of generative AI. However, it is important to encourage critical thinking and address users' blind trust in this technology.

The findings of the report highlight the need for more user education regarding the potential dangers of AI tools, particularly the growing threat of deepfake technology. This report analyses the results to shed light on both the positive and negative implications of generative AI for users in Africa and the Middle East.

42% of respondents use generative AI **several times a week**

67% of respondents use generative AI for **doing research**

81% of respondents use generative AI to **save time**

95% of respondents are **concerned** about adversaries' use of generative AI

KEY FINDINGS

KnowBe4 polled 1,300 individuals across various African and Middle Eastern countries.

The survey particularly focused on understanding the adoption rate, applications, identified benefits and threats, and the potential impact on job security due to generative AI.

Here are the key findings about the use of generative AI:

Generated by DALL-E 3

- A significant number of people in Africa and the Middle East use generative AI regularly. Specifically, 26% of respondents use it daily, 42% use it several times a week, and 25% use it occasionally.
- The most common purposes for using generative AI in this region are research and information gathering, with 67% of users engaging in this activity. Other popular uses include writing emails (52%), generating creative content (47%), drafting documents and reports (45%), entertainment (46%), and writing code (24%).
- Additionally, some individuals utilise generative AI for learning a new language, writing promotional content for social media, photo editing, and even writing lyrics.
- Users of generative AI in Africa and the Middle East experience several benefits. The majority of respondents reported that it saves them time (80%) and provides assistance with complex tasks (70%). Moreover, it improves productivity (63%) and enhances creativity (59%).

These findings highlight the widespread adoption of generative AI in the region, its diverse applications, and the positive impact it has on users' efficiency and creativity. The level of comfort users have in sharing their sensitive data with ChatGPT and other, similar applications varies across countries.

- In South Africa, only 54% of users feel comfortable sharing their personal information with generative AI tools, compared to 67% in the UAE and 75% in Nigeria.
- Some findings were paradoxical. While 80% of respondents did not feel that generative AI posed a threat to their job security, 57% believed that it has the potential to replace human creativity.
- Additionally, a majority of respondents (67%) felt that artists should have stronger protection against copyright violations, considering that much of the machine learning used to generate AI images and text is trained on human input.
- Another paradoxical finding was the level of trust users placed in generative AI. Despite 83% of users expressing confidence in its accuracy and reliability, 80% also had ethical reservations about it.
- A significant majority (95%) of respondents expressed some level of concern about the use of generative AI by adversaries.

From a cybersecurity perspective, there is still a lot of work to be done at both a governmental and organisational level to protect users from social engineering threats, specifically the use of deepfake technology. For example, 90% of respondents believe AI tools should be regulated to ensure responsible use. Surprisingly, almost half (46%) of the respondents reported their workplace has no policy regarding the use of generative AI tools. This suggests that many organisations have been slow to regulate the use of this technology. 8% of users stated they are not allowed to use generative AI tools at work.

These statistics emphasise the need for greater awareness of the inherent threats associated with generative AI. It also highlights the importance of mindfulness and training to better equip employees to deal with these risks. Similar to most respondents (83%), KnowBe4 acknowledges the positive implications of generative AI, but we are also cautious about the potential risks involved.

USES AND BENEFITS OF GENERATIVE AI

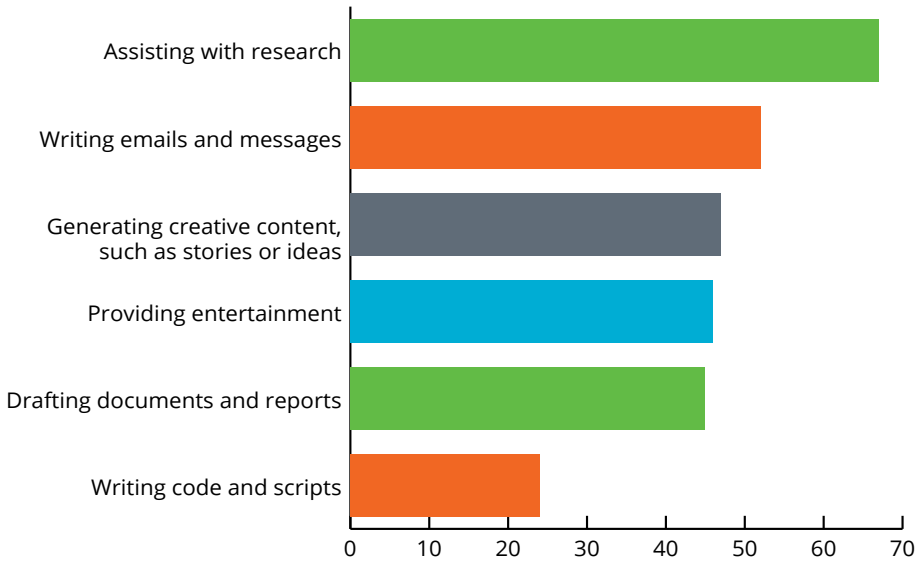
The survey aimed to discover how respondents in Africa and the Middle East are using generative AI and the advantages they gain from it. Remarkably, 100% of the participants stated that they have used a tool like ChatGPT, and 68% mentioned that they incorporate these tools into their daily and weekly work routines. Delving into the specific applications of generative AI in the next section, we can explore its professional, academic, and personal uses.

What do you use generative AI for?

People primarily use generative AI tools, like ChatGPT, for the following purposes:

- Assisting with research (67% of respondents);
- Writing emails and messages (52% of respondents);
- Generating creative content, such as stories or ideas (47% of respondents);
- Providing entertainment (46% of respondents);
- Drafting documents and reports (45% of respondents); and
- Writing code and scripts (24% of respondents).

Additionally, some respondents reported using generative AI apps to write essays and lyrics, as well as generate images and edit photos.

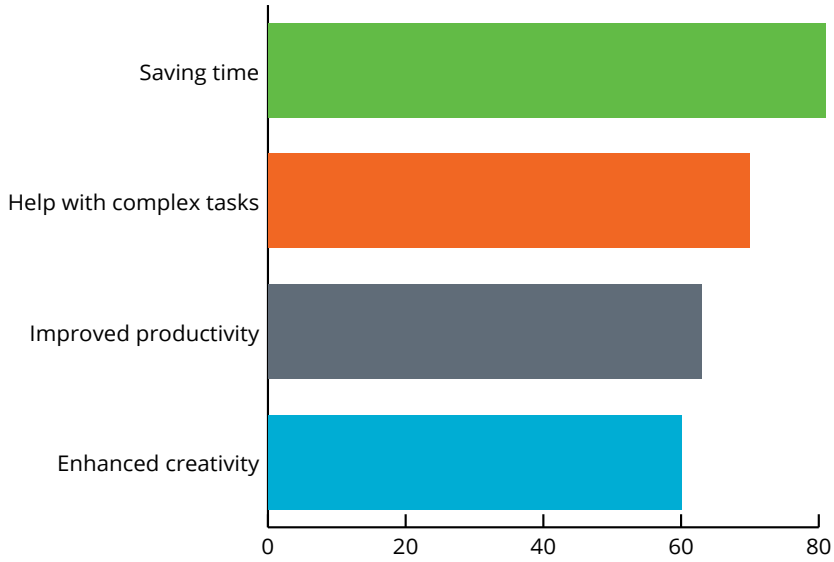


What are the benefits of using generative AI?

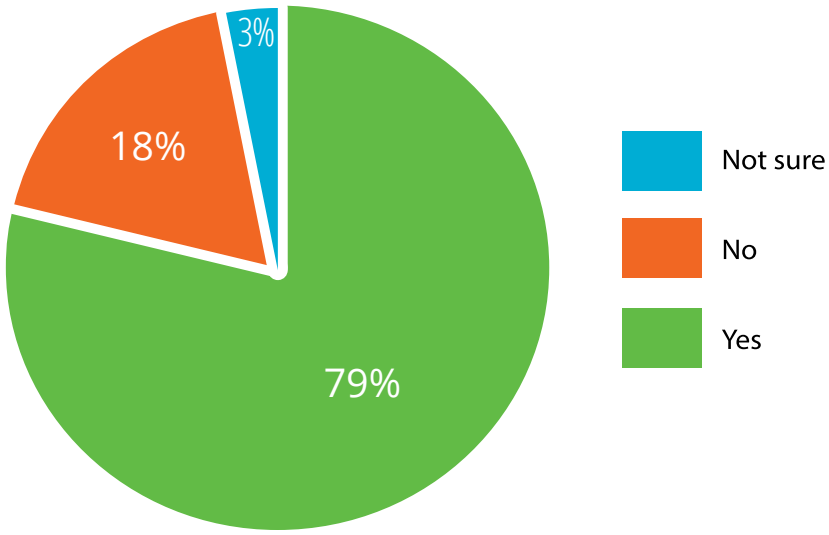
According to the survey, the major benefits reported by respondents were:

- 81% of respondents noted saving time as the main benefit;
- 70% mentioned that generative AI provided help with complex tasks;
- 63% believed that it improved productivity; and
- 60% stated that it enhanced creativity.

However, the results of the next question, which asked whether generative AI had the potential to replace human creativity, seemed to contradict the notion of AI boosting creativity. Most respondents (79%) answered yes, indicating that they believed AI could replace human creativity. On the other hand, 18% disagreed, while 3% were unsure. These findings underscore the hesitation many feel towards generative AI and whether it helps or hinders human creativity.



Does generative AI have the potential to replace human creativity?



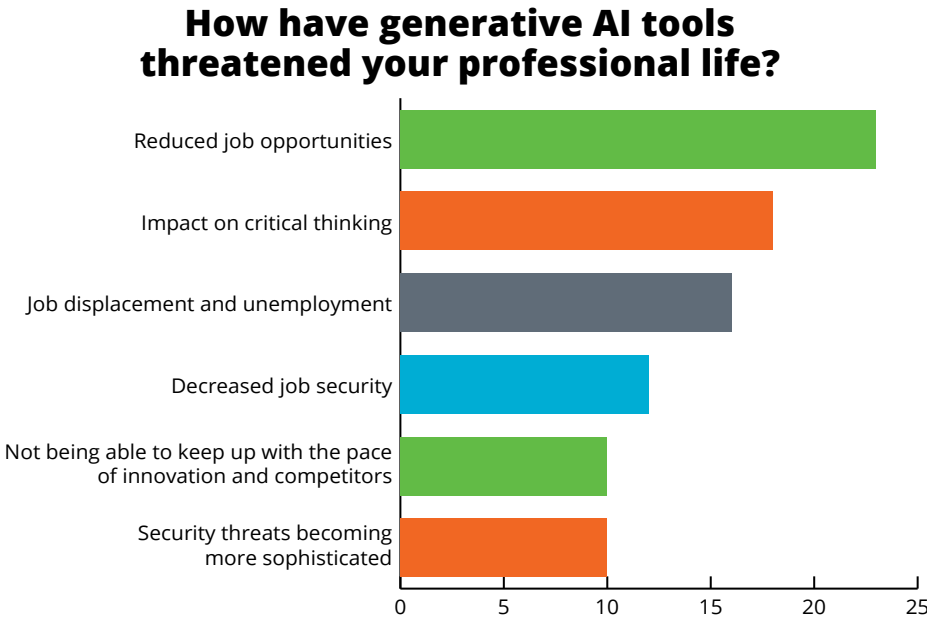
A THREAT TO JOB SECURITY AND CRITICAL THINKING?

Despite the widespread anxiety that accompanied the launch of ChatGPT, DALL-E 3 image creator and other generative AI technology, the overwhelming majority of respondents (80%) said they did not feel threatened by it in their professional lives. This sentiment could be attributed to the fact that most respondents are employed (46%), while only 22% are self-employed and 12% are students.

Generated by DALL-E 3

Among those who felt threatened by generative AI, 23% believed it could lead to reduced job opportunities, 16% thought it might displace jobs and contribute to unemployment, 12% felt it decreased job security, and 10% were concerned about not being able to keep up with the pace of innovation and competitors. An additional 10% expressed worries about security threats becoming more sophisticated.

Roughly 18% of respondents who felt threatened by generative AI also voiced worries about its effect on critical thinking. This is an important consideration, as many experts argue that generative AI's remarkable command of language, which appears both familiar and objective, has the potential to make users more susceptible to cognitive biases.



The Overtrust Effect, a psychological aspect that is closely linked to automation bias, where individuals tend to overestimate a system's capability and place too much trust in it (Aroyo et al., 2021), is clear in the survey responses. Out of the respondents, about 82% expressed confidence, either somewhat or very confident, in the accuracy and reliability of generative AI. Only a small percentage, around 3%, were uncertain or very uncertain, while 15% remained neutral. These statistics highlight the rapid and unquestioned integration of generative AI tools into our daily personal and professional lives. However, it is crucial to raise awareness about the potential for biases to infiltrate the data obtained from large-language models like ChatGPT.

Another risk linked to the overtrust effect, is that research shows that people overestimate their abilities to detect deepfakes (Köbis et al., 2021) and in fact perceive AI-synthesized images as more trustworthy than real faces (Nightingale and Farid, 2022).

SECURITY AND ETHICAL CONCERNS

Overall, most respondents are concerned about the security and ethical implications of generative AI. This is reasonable, given that 13% of respondents work in the education sector, which has been significantly impacted by the threat of plagiarism presented by generative AI. Even though only 4% of respondents work in the arts, entertainment, or recreation industries, all those surveyed express a high level of concern about copyright violation.

An overwhelming 80% of respondents expressed concerns about the ethical implications of generative AI, while only 20% indicated they were not concerned or unsure. The concerns span issues such as transparency, privacy, misinformation and biased outputs. It appears that despite the prevalent ethical reservations, the organisations these respondents are affiliated with have inadequate policies in place to manage the integration of generative AI. This is evidenced by the fact that 46% of respondents reported the absence of a policy regarding the use of generative AI tools at their workplaces. An equal percentage (46%) stated they could use these tools in a controlled or limited capacity, with 8% being forbidden from using any generative AI tools.

In line with these strong views about ethical concerns, most respondents (90%) believed that there should be more regulation on generative AI to ensure responsible use, while the remaining 10% either disagreed or were not sure. Specifically, artists expressed notable concern, with 81% of respondents indicating varying degrees of worry about their art being replicated in some manner by generative AI.

Generated by DALL-E 3

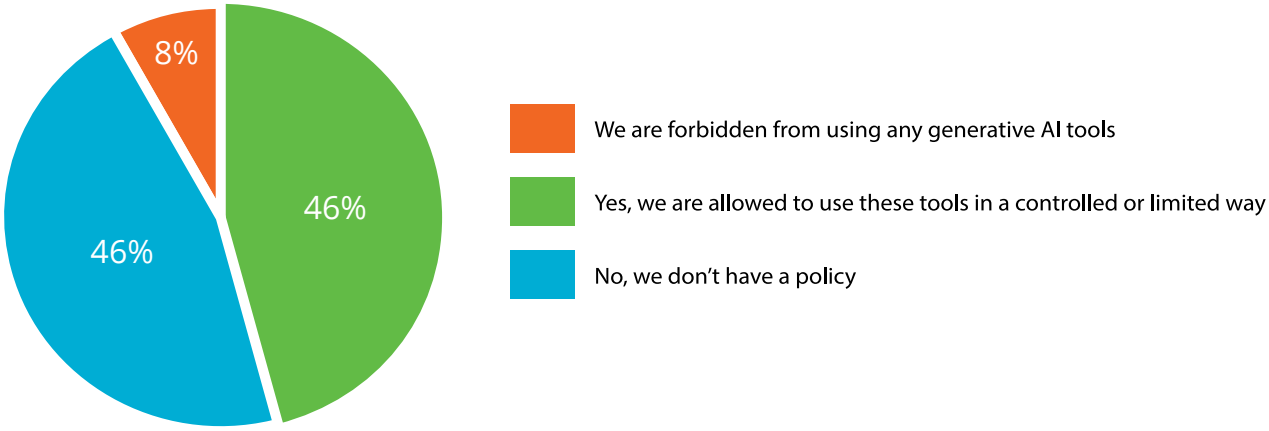
Likewise, the overwhelming majority of respondents believed that artists' copyrights should be better safeguarded, as 90% favoured moderate, strong, or stringent protection measures. Only 10% expressed that there was little to no need for artists' copyright protection.

In terms of cybersecurity, the majority of respondents expressed concern about the security threats associated with generative AI. Specifically, when asked about their level of concern regarding adversaries utilising generative AI tools like ChatGPT, or uncontrolled versions of it for attacks involving improved social engineering and deepfake technology, the overwhelming response was: 36% were concerned, 21% were somewhat concerned, and 39% were very concerned. This indicates that most respondents are aware of the cybersecurity risks posed by generative AI, but it is unclear whether they are adequately prepared to counter these attacks.

The vulnerability to attack is highlighted by the respondents' willingness to share their personal data with ChatGPT and similar tools. Out of those surveyed, only 10% expressed discomfort in sharing their personal information with generative AI. On the other hand, 62% stated that they were somewhat or very comfortable, while 27% remained neutral.

Some countries appear more relaxed about sharing their personal information with generative AI tools than others. For instance, South African users are more cautious, with just over half feeling comfortable sharing their personal information. In comparison, 67% of users in the UAE and 75% in Nigeria expressed comfort in sharing their personal information with generative AI tools.

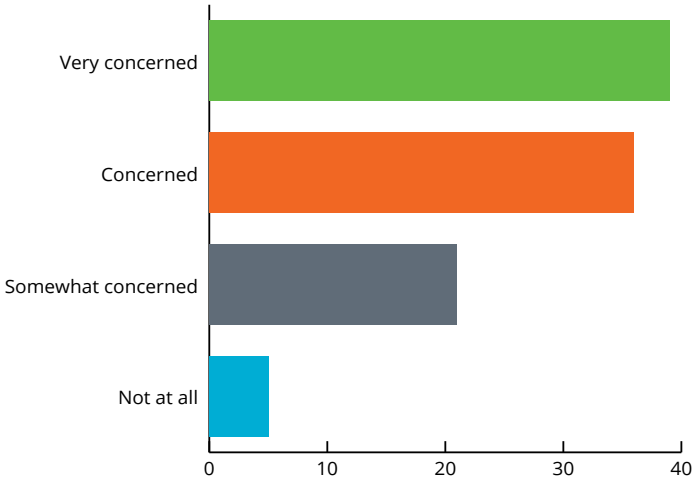
Does your place of work have a policy in place regarding the use of generative AI tools in performing your duties?

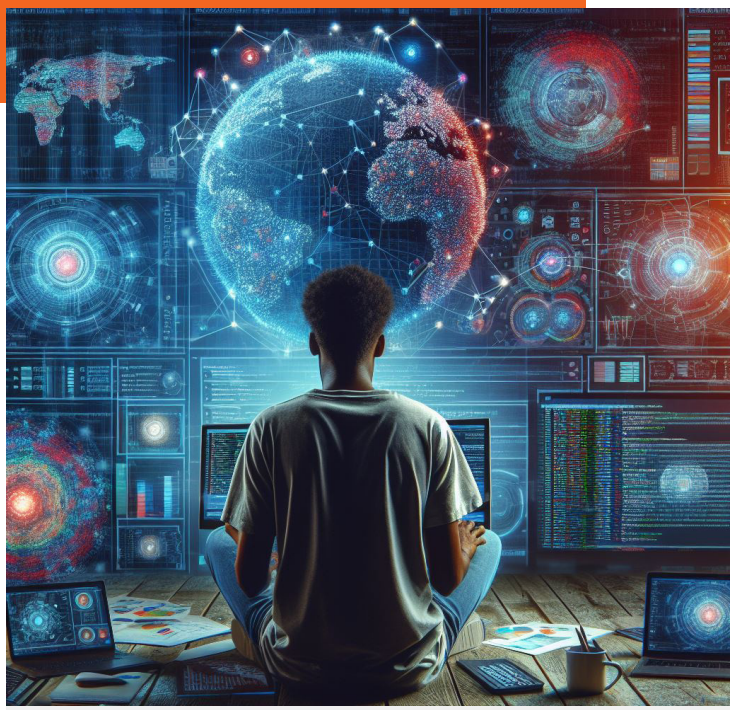


LOOKING AHEAD: EMBRACING GENERATIVE AI RESPONSIBLY

Based on the survey results, it is clear that generative AI offers unique opportunities for easily generating new content and ideas. However, it also poses threats to copyright infringement and cybersecurity. Using tools like ChatGPT was widespread among respondents, who recognised several benefits of incorporating generative AI into their workflow. These benefits include saving time (81%), helping with complex tasks (70%), and increasing productivity (63%).

How concerned are you about adversaries using generative AI tools in their attacks?





Generated by DALL-E 3

Interestingly, the survey findings reveal a paradox in how easily people trust generative AI despite being aware of its dangers. Roughly 82% of respondents expressed confidence in the accuracy and reliability of generative AI. However, a combined 95% of respondents expressed concerns about its potential use in social engineering and deepfake scams.

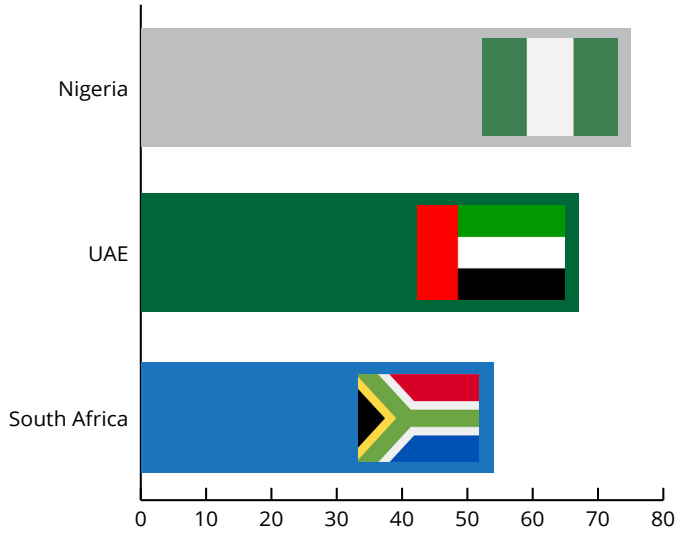
It is concerning that very few organisations have comprehensive policies to address the challenges associated with this new technology. According to the survey, 46% of respondents reported their workplace had no generative AI policy, and 8% said they were banned from using it. This policy vacuum drives employees to use generative AI in secret, which increases security risks and reduces its visibility within organisations.

To mitigate these risks, organisations should update their IT security systems and work policies to incorporate the use of generative AI. Additionally, employees should receive training on developing a zero-trust mindset to avoid falling victim to scams that could compromise their organisation's financial and data security.

With elections coming up in multiple countries, disinformation has been ranked as one of the top risks for this year by the World Economic Forum and deepfakes as one of the most worrying uses of AI, particularly when used for political manipulation (Caldwell, 2020).

It is crucial to empower users to defend themselves against the dangers associated with malicious use of generative AI in order for it to have a positive impact on society, as supported by 82% of the survey respondents.

How comfortable are you sharing your personal information on generative AI tools?



REFERENCES

Aroyo, A., de Bruyne, J., Dheu, O., Fosch-Villaronga, E., Gudkov, A., Hoch, H., Jones, S., Lutz, C., Sætra, H., Solberg, M. & Tamò-Larrieux, A. (2021). Overtrusting robots: Setting a research agenda to mitigate overtrust in automation. Paladyn, Journal of Behavioral Robotics, 12(1), 423-436.

Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. Crime Sci 9, 14 (2020).

Köbis,N., Doležalová,B., Soraperra,I., (2021). Fooled twice: People cannot detect deepfakes but think they can. iScience 24 (11)

Nightingale, S. J., & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proceedings of the National Academy of Sciences of the United States of America, 119(8).

World Economic Forum (2024). Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify.
https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4 Africa | The Planet Art, 32 Jamieson St, Cape Town, 8001, South Africa
Tel: +27.21.813.9264 | Email: Popcorn@KnowBe4.com

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E01K01