AI IN CYBERSECURITY

Gabriela Palau Mas de Xaxars - *Frederic Mistral Tecnic Eulalia*

Imagine getting a call from someone you care about, only to discover that the voices on the other end were not theirs but an artificial imitation. Many people worldwide are dupped every year. According to several studies, these days the number of scammers could have gone up because of the improvements in artificial intelligence technologies. Seen as among the most harmful types of cybercrime where unauthorized use of personal data is used to access systems, carry out frauds, and even impersonate individuals. Artificial intelligence has turned into a powerful tool for cybercriminals thanks to steady technological advances. By allowing them to operate faster, they manage to create highly convincing and targeted attacks. Scammers do this by implementing different techniques such as impersonation or voice cloning. From cloning voices to faking images, AI is capable of creating believable fabrications that can deceive even the most vigilant individuals, making identity theft a silent and deceptive method of committing cybercrimes. At the same time, as technology evolves, artificial intelligence is also being used to prevent and detect attacks, offering tools to make the internet a safer place. This presents us with a clear dilemma: is AI inherently dangerous, or is the way people choose to use it?

As mentioned earlier, AI has become a transcendental tool for scammers. The combination of phishing techniques with social engineering, and the power of AI, facilitates the execution of identity theft attacks with a level of precision that would have been previously unimaginable. Real-world studies reveal that just over half of businesses in the U.S. and U.K. have been targets of financial scams involving “deepfake” technology. One notable case involved an engineering firm that unknowingly transferred over $25 million to fraudulent accounts after following a series of video conferences that appeared to be generated using artificial intelligence. These sophisticated scams not only use realistic face videos and voices but often incorporate AI-powered chatbots to simulate real-time interactions. This combination of techniques allow attackers to gain their target’s trust and exploit them with greater accuracy.

While cybercriminals manipulate this advanced technology to carry out sophisticated attacks, cybersecurity professionals are turning to the same technology to stay ahead, harnessing artificial intelligence as a valuable asset against identity theft. When using AI-driven strategies to fight identity theft, it must be taken into consideration that cybercrime tactics evolve over time. To ensure they’re ready to detect new threats and adapt to emerging fraud methods, they need to be updated frequently. Moreover, as AI systems get more into cybersecurity defenses, organizations must also prioritize data privacy and confidentiality, ensuring that sensitive customer information is adequately protected while their tools operate effectively. These systems are especially important for organizations that handle critical data, such as banks. A notable example is PayPal, which employs AI to detect unusual patterns in user behavior, such as transaction volume, locations, and times that may indicate fraudulent activity.

As AI becomes more integral to cybersecurity, it simultaneously introduces new vulnerabilities that cybercriminals are eager to exploit, highlighting the constant struggle between its protective and exploitative roles. It is no surprise that systems designed to detect and prevent fraud are increasingly susceptible to manipulation, as cybercriminals are keen to circumvent new security techniques. Clear examples are facial recognition systems that can be fooled through subtle alterations, and voice recognition systems that can be tricked by AI-generated voice clones. AI’s efficiency in security can be compromised by the simple ability of cybercriminals to circumvent security procedures and unauthorized access. This is why cybersecurity professionals work to create more advanced and strong models to prevent such events, such as using multi-layered security measures to reduce the possibility of manipulation.

AI’s rising impact in cybersecurity emphasizes its dual capability to protect and interrupt, drawing attention to the need for careful application and strategic planning. Artificial intelligence, as shown before, has become a vital part of fighting cyber crimes since it provides refined technology to track anomalies and identify assaults. Nevertheless, artificial intelligence is a double-edged sword, given its great potential and cyber criminals also using its capabilities for nefarious purposes. Looking ahead, the future of cybersecurity will rely on both technological advancements and responsible AI usage. Navigating this complex landscape will require continuous innovation, as well as collective efforts and ethical AI deployment. Equally important, developers must prioritize ethics in AI development, ensuring it remains a protective tool rather than a weapon in the hands of cybercriminals. Furthermore, both security professionals and the public must stay aware of AI's potential risks and benefits fostering greater awareness and preparedness.

Ultimately, the true impact of AI on cybersecurity lies in the hands of the users, making it a subjective decision whether it becomes a powerful tool or a weapon for exploitation. And of course, the role of regulators is crucial in defining the regulatory framework for the use of technology and ensuring that AI adheres to ethical guidelines, so it becomes a tool for assistance rather than a threat.