BIZCOMMUNITY

ChatGPT and cybersecurity: what AI means for digital security

Issued by ESET

13 Mar 2023

As AI technology like ChatGPT evolves, so do the strategies and tactics used by cybercriminals. Steve Flynn, sales and marketing director at ESET Southern Africa, says ongoing awareness is crucial in understanding how to manage potential cybersecurity challenges posed by these developing tools.

As artificial intelligence (AI) technology becomes a new reality for individuals and businesses, its potential impact on cybersecurity cannot be ignored. OpenAI and its language model, ChatGPT, are no exception and while these tools offer significant benefits to almost every industry, they also present new challenges for digital security.

> *ChatGPT raises concerns due to its natural language processing capabilities, which could be used to create highly personalised and sophisticated cyberattacks.*

The impact of AI on cybersecurity

1. The potential for more sophisticated cyberattacks: AI and ChatGPT can be used to develop highly sophisticated cyberattacks, which can be challenging to detect and prevent as natural language processing capabilities may bypass traditional security measures.

2. Automated spear phishing: With the ability to generate highly personalised messages, AI can be used to send convincing targeted messages to trick users into revealing sensitive information.

3. More convincing social engineering attacks: AI and ChatGPT can also be used to create fake social media profiles or chatbots, which can be used to engage in social engineering attacks. These attacks can be difficult to detect, as the chatbots can mimic human behaviour.

4. Malware development: AI can be used to develop and enhance malware, making it more difficult to detect and clean out.

5. Fake news and propaganda: ChatGPT can be used to generate fake news and propaganda, which can manipulate public opinion and create panic and confusion.

Weapon or tool: it's in the user's hands

However, as with any other tool, the use (or misuse) depends on the hand that wields it. Organisations like OpenAI are visibly committed to ensuring their technology is used ethically and responsibly and have implemented safeguards to prevent misuse. Businesses can do the same.

> *"To protect their digital assets and people from harm, it is essential to implement strong cybersecurity measures, and to develop ethical frameworks and regulations to ensure that AI is used for positive purposes and not for malicious activities."*

Steps organisations can take to enhance safety

1. The implementation of Multi-Factor Authentication (MFA): MFA adds an extra layer of security, requiring users to provide multiple forms of identification to access their accounts. This can help prevent unauthorised access, even where a hacker has compromised a user's password.

2. Educating users about security dos and don'ts: Continuous awareness training about cybersecurity best practices, such as avoiding suspicious links, updating software regularly, and being wary of unsolicited emails or messages, can help prevent people from falling victim to cyberattacks.

3. Leveraging advanced machine learning algorithms: Advanced machine learning algorithms can be used to detect and prevent attacks that leverage OpenAI and ChatGPT. These algorithms can identify patterns and anomalies that traditional security measures might miss.

4. Implementing network segmentation: Network segmentation involves dividing a network into smaller, isolated segments, which can help isolate the spread of an attack if one segment is compromised.

5. Developing ethical frameworks for the use of AI: Developing ethical frameworks and regulations can help ensure that ChatGPT is used for positive purposes and not for malicious activities.

6. Increasing monitoring and analysis of data: Regular monitoring and analysis of data can help identify potential cybersecurity threats early and prevent attacks from unfolding.

7. Establishing automated response systems: Detect and respond to attacks quickly, minimising damage.

8. Updating security software regularly: Ensuring that security software is up to date can help protect against the latest cybersecurity threats.

Safeguard against misuse

By leveraging the power of AI technology, businesses and individuals can drive innovation, improve productivity and business outcomes with powerful new solutions. However, it is important to balance the potential benefits of AI technology with the potential risks and ensure that AI is used ethically and responsibly. By taking a proactive approach to AI governance, we can help minimise the potential risks associated with AI technology and maximise the benefits for business and humanity.

As AI technology evolves, so too must our cybersecurity strategies.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don’t gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed