



TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Why ChatGPT is the Big Problem for Cyber Ethics

ChatGPT is changing the way we think about cyber threats and security systems.

By **Dipak Chaudhary** | Department of Computer Science, University of Agriculture Faisalabad | Published: 11 April 2026

✉ dipakborat123@email.com | Position: Computer Science Student

Introduction

Artificial Intelligence is changing a lot of things. It is even changing cybersecurity. ChatGPT is a part of this change. It can write like a human and help with coding. It is also very good at automating communication. This makes it very useful for professionals and organizations.. It also raises some big cybersecurity issues. The more Artificial Intelligence is used in systems the more cyber threats there are. ChatGPT is a part of this problem. It can be used by people to do bad things.

"The big problem for cyber ethics in 2026 is that Artificial Intelligence has made it easy for people to deceive others. This makes it hard to trust anything online."

Technology Overview

Artificial Intelligence is a part of new technology. It is used in healthcare, education, finance and cybersecurity. ChatGPT is one of the advanced Artificial Intelligence tools. It can. Write human language very well. It was made using language models. It can help people write, code solve problems and communicate.

Chatgpt is also a big problem for cybersecurity. It is easy to use bad people can use it to do bad things.

Cybersecurity is about protecting systems, networks and data from attacks. New Artificial Intelligence is making these attacks worse. This research is about how ChatGPT's making faces a new dimension Cybersecurity risks worse and what we can do about it.

Key Findings & Impact

- **Facilitation of Cybercrime**

One of the risks of ChatGPT is that it makes it easy for people to commit cybercrime. In the past you needed to be a computer expert to launch cyberattacks.. ChatGPT makes it easy for anyone to do it. It can generate phishing emails and scam messages. It can even give people step-by-step instructions on how to commit cybercrime.



- **Phishing and Social Engineering Attacks**

Phishing attacks are about deceiving people. ChatGPT makes these attacks worse by generating realistic emails and messages. These messages look legitimate and trustworthy. This makes it more likely that people will fall for them.

This idea significantly increases the success rate of attacks. **Social engineering** attacks are also amplified, as attackers can simulate realistic conversations and manipulate victims more effectively.

- **Automation of Cyber Attacks**

ChatGPT can automate cyberattacks. It can generate a lot of phishing emails and automate responses to scam operations. This makes cyberattacks more efficient and harder to stop.

- **Misinformation and Fake Content Generation**

ChatGPT can also generate news and articles. It can create reports and fabricated stories. This can be used to manipulate opinion or damage reputations. In cybersecurity misinformation can be used to trick people into doing something

What's Next?

So Now What?

So what do we do now? We cannot just ignore this problem. Governments and organizations need to make rules to control Artificial Intelligence tools like ChatGPT. Cybersecurity systems need to be improved to spot and respond to threats. People need to understand the risks of phishing and how to protect themselves online. Businesses need to secure their data and use encryption.

ChatGPT is not going to stop evolving. It will keep getting better. Cyber threats will get worse. We need to make sure we use these tools responsibly and do not let them fall into the wrong hands.

About the Author

Dipak Chaudhary is the student of BS(Computer Science) in the department of Computer Science in University of Agriculture of Faisalabad. Current Semester is 6th and Digital Marketing and Business Development experts with solid experience in Meta platforms and online brand-buildings. My email is dipakborat123@gmail.com.

Keywords: intelligence; Cybersecurity; ChatGPT; Phishing attacks; data privacy; digital security

References

1. IEEE, "Generative AI and Cybersecurity Risks" Document ID: 10443401.
2. A. Author, "ChatGPT for Cybersecurity: Applications and Challenges" Journal of Cyber Studies 2023.
3. B. Author, "AI and Phishing Attacks" IEEE Security & Privacy 2023.
4. C. Author, "Risks of Large Language Models, in Security" Information Journal, 2023.