



AI Enhance Cybercrime: How Generative AI is Changing Digital Attacks

Generative Ai is transforming many Sectors, but it is also giving cybercriminals new and powerful tools like deepfake scams to automated phishing emails. Ai is making cybercrimes and attacks faster smarter and more dangerous

By **Zahida Ahsraf** | Department of Computer Science | Published: October, 2026

✉ ashrafzahida20@gmail.com | Position: Software Engineer

Introduction

Artificial Intelligence is transforming the digital word, but it is also developing new problems and challenges for cybersecurity. Recently Criminals starts using generative AI tools to automate scams create realistic phishing emails and starts generate malicious software.

These technologies allow attackers to supervise cybercrimes on large-scale by making less efforts instead of writing scams messages, criminals now use Ai to produce thousands of convincing messages. For Pakistan's growing digital economy this is a serious risk. As more businesses adopt online services it's become a national priority to protect systems

" AI is making cybercrimes easier Even people who are not skilled can now use AI tools to launch Sophisticated Scams."

Technology Overview

Generative Ai models can produce text, images, audio and video that closely look like real human communication. Tools such as FraudGPT and WarmGpt are made specially for malicious purposes.

In Pakistan where digital Banking and Online services are Fastly growing, such Ai powered scams targeted business, freelancers and government institutions.

Key Findings & Impact

Recent cybersecurity reports show that Ai generated phishing emails are more effective and better than traditional scams. Some studies report 54% click rate for Ai generated phishing messages compared with only 12 % for human written phishing emails.

Cybercriminals are also using Ai for voice cloning and deepfake videos. In one well-known case in 2024 attackers used Ai to generate video and voice to pose a company employee and trick employees into transferring \$25 million.

For Pakistan's tech ecosystem especially startups Tech companies and digital service providers these developments highlight need for stronger cybersecurity strategies and improve awareness.



Discuss implications for Pakistan's tech industry — startups, enterprises, policy, or talent development. Give readers something to act on or think about.



Figure 1: AI-driven cybercrime is evolving rapidly, where generative AI tools enable phishing attacks, deepfake scams. Credit: Author / Source

What's Next?

The rise of AI driven cybercrime has created a new challenge for cyber security professionals. Organization must enhance and improve advance defenses such as multi-factor authentications , AI based threat detection systems and stronger employee training programs.

For Pakistan investing in cybersecurity education and research will be essential to protect businesses and users from emerging threats. The organization that adapt quickly will be better prepared for the future of digital security.

About the Author

Author Zahida Ashraf is a information Technology student with an interest in cybersecurity, artificial intelligence. Her research focuses on emerging cyber threats and their impact on modern digital ecosystems. She can be reached at ashrafzahida20@gmail.com.

Keywords: Artificial Intelligence; Cybersecurity; IoT; Software Engineering; Pakistan Tech

References

1. World Economic Forum (2026). *Global Cybersecurity Outlook 2026*. Geneva: World Economic Forum.
2. Soliman, R. (2026). *Generative AI Cyber Threats 2026: Deepfake Fraud Scams and Synthetic Identity Fraud Surge*. TechTimes.