

# THE TECH TALK

## Understanding Cybersecurity in Modern Era

Cybersecurity encompasses the practice of safeguarding digital systems, networks, and sensitive information from malicious intrusions and unauthorized access.

Its core objective is to preserve the confidentiality, integrity, and availability of data. In an era dominated by hyper-connectivity and digital transformation, robust cybersecurity measures have become indispensable for both enterprises and individuals.



## Evolving Cyber Threats

Cyberattacks have grown far beyond basic, detectable methods. Modern adversaries exploit AI and Generative AI to launch sophisticated, adaptive, and stealthy attacks—automating exploits, creating realistic fake content, and uncovering vulnerabilities at unprecedented speed and scale.

## Rising Sophistication of Cyber criminals : How Cybercrime is Evolving with AI

- **Phishing Attacks:** Cybercriminals disseminate deceptive emails that mimic legitimate communications with alarming precision. AI-driven personalization makes these messages highly convincing, luring victims into clicking malicious links or divulging confidential credentials.
- **Ransomware:** Among the most perilous threats, ransomware encrypts critical files and demands payment for restoration. AI accelerates this menace by enabling attackers to pinpoint high-value targets and propagate infections rapidly across networks.
- **Data Breaches:** Exploiting systemic weaknesses, hackers infiltrate systems to exfiltrate sensitive information such as passwords, financial records, and customer data. AI-powered reconnaissance tools streamline the identification of exploitable gaps, amplifying the risk.
- **Deepfakes:** AI-generated synthetic media—videos, audio, and images—are weaponized to impersonate individuals or disseminate disinformation. Such fabrications can deceive stakeholders and precipitate costly organizational missteps.

### Why Immediate Action Is Critical?

AI-driven attacks are growing smarter and more frequent, bypassing traditional defenses. Organizations and individuals must adopt layered security strategies, including AI-powered tools, strong authentication, and continuous awareness training, to stay protected.

## The Dual Nature of AI : Power & Peril

Artificial Intelligence (AI) and Generative AI have revolutionized the cybersecurity landscape. While these technologies empower security teams to predict and prevent attacks, they also arm cybercriminals with advanced tools to execute highly sophisticated threats. Here's how attackers leverage AI:

- **Automated Attacks:** Hackers now deploy AI-powered bots that can scan thousands of systems in seconds, looking for weak points. This automation means attacks happen faster and on a much larger scale than ever before.
- **Deepfake Technology:** Fraudsters use AI to create hyper-realistic videos, voices, and images. These deepfakes impersonate executives, spread misinformation, and trick employees into transferring funds or disclosing sensitive data.
- **AI-Driven Malware:** Unlike traditional malware, AI-driven variants learn and adapt, bypassing firewalls and antivirus tools with ease. Their evolving nature makes detection and containment extremely challenging.
- **Synthetic Phishing:** Generative AI crafts phishing emails that mimic authentic communication styles. These personalized messages are nearly indistinguishable from legitimate correspondence, increasing the likelihood of successful attacks.

**Call for Action:** AI-powered attacks are no longer a future concern—they're happening today. Organizations must implement advanced defenses, including AI-based threat detection, multi-layered security frameworks, and continuous employee awareness programs to stay ahead.

## Native Cybercrime vs AI & Generative AI Cybercrime

AI and Generative AI have transformed cybercrime into a fast-moving, adaptive, and highly targeted threat. Traditional defenses are no longer sufficient—organizations must embrace AI-driven security, zero-trust architectures, and continuous monitoring to stay ahead.

**Native vs. AI-Powered Cybercrime: Key Differences :**

| ASPECT                     | NATIVE CYBERCRIME                                  | AI & GENERATIVE AI CYBERCRIME                                      |
|----------------------------|----------------------------------------------------|--------------------------------------------------------------------|
| Speed and Scale            | Manual, slower execution                           | Automated, scans thousands of systems                              |
| Personalization            | Generic phishing emails and scams                  | Highly personalized phishing using                                 |
| Automation of Exploits     | Static malware easy to detect                      | AI-driven malware learns and evolves                               |
| Evolving Threats           | Static impersonation techniques                    | Deepfakes and synthetic voices for realistic identity              |
| Psychological Manipulation | Easier to identify with traditional security tools | Extremely hard to detect with AI tools and less human intervention |
| Resource Requirement       | Requires skilled hackers and manual effort         | Requires AI tools, but less human intervention                     |

**"Cybersecurity is not just defense—it's the foundation of trust in a connected world"**

## Our Vision:

"Act as a catalyst to make housing affordable in India by enabling risk optimization through data technology leverage"

## Our Mission:

- Partner with the housing finance industry to drive financial inclusion goals and promote responsible lending
- Maximise shareholder value while maintaining prudent risk discipline



**PROVIDED GUARANTEES IN OVER 700 LOCATIONS**  
to customers across India



**HELPED OVER 1,50,000 FAMILIES**  
realise their dream of owning a home



For more information scan the QR  
or visit us at: [www.imgc.com](http://www.imgc.com)

Connect with us:  
Send "MG" at +91-73033 88455  
on  WhatsApp