GreenariA
Go Green, Learn Green
An Agricultural Monthly e-Magazine
Volume 03, Issue 11, 2025
ISSN: 2584-153X
Article ID: G-25-1106

CYBERSECURITY: SAFEGUARDING DIGITAL AGRICULTURE IN A CONNECTED WORLD

Kamali S P[1*], Ponsneka I[2], Punitham M[2], Jayashree V[1] and Dhivya C[1]

[1]Research Scholar (Agricultural Extension Education), Department of Agricultural Extension and Rural Sociology, Tamil Nadu Agricultural University, Coimbatore

[2]PG Scholar (Agricultural Extension Education), Department of Agricultural Extension and Rural Sociology, Tamil Nadu Agricultural University, Coimbatore

**Corresponding Author Mail ID: kamaliselvaraj28@gmail.com*

Introduction

The agricultural sector is undergoing a paradigm shift through the rapid integration of digital technologies. From precision farming and data-driven decision-making to automation and cloud-based advisory systems, digital transformation is redefining how farming systems operate globally. This digital transformation also exposes agriculture to emerging cyber risks. As agriculture becomes increasingly reliant on digital infrastructures ranging from Internet of Things (IoT) devices and satellite data to mobile-based platforms. It becomes more vulnerable to data breaches, hacking, misinformation and system disruptions. The potential consequences of such cyber incidents are not limited to individual farmers but can extend to national food security and supply chain stability. Thus, cybersecurity has become an integral component of digital agricultural resilience. Safeguarding data, ensuring system integrity and building farmers digital literacy are essential to realizing the full potential of digital agriculture in a safe and sustainable manner.

Digital Agriculture

Digitalization has transformed traditional farming into a knowledge-intensive, technology-driven enterprise. The adoption of smart farming technologies such as remote sensing, drones, precision irrigation and artificial intelligence (AI)-based analytics has enabled farmers to make informed decisions regarding crop management, resource allocation and risk mitigation. IoT-enabled devices continuously collect data on soil health, temperature and moisture, helping optimize inputs and reduce environmental footprints. These innovations contribute to the broader objectives of climate-smart agriculture, productivity enhancement, and sustainability. Furthermore, the emergence of mobile-based agricultural advisory platforms has enhanced information accessibility among smallholder farmers, bridging gaps in extension service delivery. However, increased connectivity also means increased vulnerability. Each connected device or digital platform can become a potential entry point for cyberattacks if not adequately secured. Consequently, the pursuit of agricultural modernization must be accompanied by robust cybersecurity mechanisms that protect digital assets, maintain data confidentiality and ensure operational continuity.

Cyber Threats in Agriculture

The integration of technology into agricultural systems has introduced new and complex forms of risk. While farmers are familiar with climatic, biological, or market-related risks, cyber threats represent an unfamiliar yet potentially devastating dimension. Cyber risks in agriculture may manifest in several forms:

- **Ransomware attacks**, where hackers encrypt farm management data and demand payment for its release.
- **Phishing and social engineering**, in which fraudulent messages deceive farmers or agribusinesses into revealing sensitive information.
- **Data manipulation or theft**, where unauthorized access alters or steals vital information related to weather, markets, or production.
- **IoT device hacking**, which could compromise precision equipment such as automated irrigation systems or drones.
- **Misinformation campaigns**, which spread false advisories or market updates to manipulate decisions or cause panic.

Such attacks can disrupt production cycles, distort market signals, and lead to significant economic losses. More importantly, they can erode trust in digital platforms, discouraging farmers from engaging with beneficial technologies. Hence, identifying, assessing, and mitigating cyber risks are crucial to ensuring the sustainable adoption of digital agriculture.

Simple Ways to Stay Cyber Safe

Cyber resilience begins with awareness and proactive behaviour. While institutional frameworks and advanced technologies play a role in cybersecurity, individual digital practices are equally significant. Farmers and agricultural stakeholders can adopt several measures to enhance their online safety:

- Use strong and unique passwords for digital platforms and IoT devices, and update them periodically.
- Avoid sharing sensitive information, such as OTPs or bank details, through calls or unsolicited messages.
- Regularly update software and mobile applications, as updates often fix security vulnerabilities.
- Backup critical data in secure offline or cloud-based storage systems.
- Install legitimate antivirus and security software to detect and block potential threats.
- Verify information sources before acting on digital advisories or online messages.
- Participate in digital literacy and cybersecurity training programs, often organized by agricultural universities, government agencies, and extension departments.

Conclusion

As Agriculture becomes more dependent on digital tools and data networks, protecting these systems from cyber risks is vital for long-term growth and farmer confidence. Cybersecurity plays a crucial role in keeping agricultural data safe, maintaining trust in digital platforms, and ensuring that technology continues to serve farmers effectively. By improving awareness, encouraging safe online behaviour, and developing strong security systems, the agricultural sector can build a secure and dependable digital environment that supports both productivity and sustainability in the modern connected era.