Virginia Cooperative Extension
Virginia Tech • Virginia State University
www.ext.vt.edu

# Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity

*Authored by Renata Carneiro, Postdoctoral Researcher, Department of Food Science and Technology, Virginia Tech; Susan Duncan, Professor, Department of Food Science and Technology, Virginia Tech; Ford Ramsey, Assistant Professor, Department of Agricultural and Applied Economics, Virginia Tech; Hasan Seyyedhasani, Assistant Professor, School of Plant and Environmental Science, Virginia Tech; and Randall Murch, Affiliate Faculty, Center for Advanced Innovation in Agriculture, Virginia Tech.*

## Are you susceptible to cyber attacks?

In the last decades, computers, laptops, smartphones, tablets, as well as other technological devices and the internet, became of great importance in our modern lives and have been supporting the development of diverse agribusinesses worldwide. The use of computer-controlled machines, autonomous vehicles, robots, drones, cameras, sensors, wireless networks, and smart technology, for example, has led to major changes in how food is produced in the United States. Overall, the use of internet connected devices (internet of things or IoT) and artificial intelligence in precision agriculture or smart farming has helped to reduce costs, as well as increase yield and profitability.

Nevertheless, the wide use of technology in agriculture has brought a new threat to crop and livestock farming in the country: "cyber attacks". The prefix "cyber" is associated with computers and over the last decades it has enriched our vocabulary to describe the growing and important virtual world. Examples of possible cyber attacks include: phishing attempts (e.g., malicious emails), malware or malicious software (e.g., virus, spyware, ransomware), denial of service attacks, etc. If you use IoT devices and/or smart technology in your farm and small business, it is susceptible to cyber attacks.

## What is cyberbiosecurity?

The concept of "cybersecurity" emerged from the need to keep technology-based systems, software, programs, and sensitive information shared and/or stored in the virtual space safe from malicious attacks and sabotage. More recently, "cybersecurity" has been integrated with the concept of "biosecurity", which includes the need to protect humans, animals, and plants from biological harms, such as bioterrorism, diseases, outbreaks, and pandemics. The interface of cybersecurity, cyber-physical security, and biosecurity, has been called "cyberbiosecurity" (Duncan et al., 2019; Murch et al., 2018).

## Importance of cyberbiosecurity

- There are several reasons to care about cyberbiosecurity:
- Business and brand protection; avoid reputational and financial losses.
- Protect intellectual property, as well as confidential and critical information (data privacy).
- Ensure data integrity.
- Restrict access to important physical spaces, raw materials, supplies, data, and documents.
- Ensure availability and proper operation of critical systems, automated equipment, and machinery.

- Ensure quality and safety of the farm's end product and its traceability.
- Compliance with standards, certifications, contracts, and regulations.

# Protect your farm and small business from cyber attacks

The first step to protect your farm and small business from a cyber attack is to acknowledge the existence of this potential risk and raise awareness among personnel. Then, it is important to evaluate all the farm's systems and try to identify points of vulnerability (Peccoud et al., 2018). For instance, consider whether there is any critical point that is controlled automatically by an internet-connected system. How and how often do you verify this automatic system is working fine? Now, consider all the confidential and critical information the farm has collected over the years. Where is it stored and who has access to this data? How easy or difficult is it for external people to have access to this information and perhaps steal it, destroy it, use it, or share it without your permission? Would it be possible to recover this data? What would be the impact of losing this information? Although all risks cannot be completely eliminated, several of them can be significantly reduced and their effects can be mitigated.

Depending on how the questions above were answered, it might be important that your farm review or implement standard procedures to prevent, detect, and/or mitigate attacks that can compromise the quality and safety of the farm's end product, as well as the sustainability of your business. Other suggestions that can help protect your farm are:

- Provide training for employees; it can significantly reduce human errors.
- Separate personal, operational, and business devices when possible.
- Keep important devices (e.g., laptops, smartphones, tablets) safe and do not leave them unlocked.
- Use strong passwords, change them periodically, and do not share them with others.
- Use multi-factor authentication when possible.
- Control access to important areas and do not leave visitors or third-party service providers alone on them.
- Prefer using paid email services than free ones.
- Update software and apps regularly.
- Avoid the use of outdated operating systems, such as Windows 98 and early Linux.
- Backup critical data regularly, so it can be recovered if needed.

# References


Duncan, S. E., R. Reinhard, R. C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert, and R. Murch. 2019. "Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system". *Frontiers in Bioengineering and Biotechnology* 7(63): 1–7. https://doi.org/10.3389/fbioe.2019.00063

Murch, R. S., W. K. So, W. G. Buchholz, S. Raman, and J. Peccoud. 2018. "Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy". *Frontiers in Bioengineering and Biotechnology* 6(39): 1–6. https://doi.org/10.3389/fbioe.2018.00039

Peccoud, J., J. E. Gallegos, R. Murch, W. G. Buchholz, and S. Raman. 2018. "Cyberbiosecurity: From Naive Trust to Risk Awareness". *Trends in Biotechnology* 36(1): 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012


Visit Virginia Cooperative Extension: ext.vt.edu




2021 FST-387NP