Navigating the digital landscape in the agri-food sector

Chances & Strategies to Grow & Expand your Business Using Modern Technology

PRESENTED BY:
Ines & Eric Batterton of

My NORDIC Garden
Natural & Sustainable Kitchen Gardens

Réseau Agroalimentaire de l'Est ontarien
Eastern Ontario Agri-Food Network

MODULES

1. INTRODUCTION TO DIGITAL TRANSFORMATION IN AGRI-FOOD
2. BUILDING A DIGITAL PRESENCE
3. E-COMMERCE & ONLINE SALES
4. DIGITAL MARKETING STRATEGIES
5. DATA ANALYTICS & INSIGHTS
6. MOBILE TECHNOLOGY & APPS
7. INTERNET OF THINGS (IOT) IN AGRICULTURE
8. ONLINE NETWORKING & COLLABORATION
9. CYBERSECURITY & DATA PRIVACY
10. FUTURE TRENDS & ADAPTATION STRATEGIES

Cybersecurity & Data Privacy

- Understand key concepts of cybersecurity & data privacy
- Identify common threats & vulnerabilities in the agri-food sector
- Implement best practices for protecting data & systems
- Recognize the importance of compliance

1) Introduction to Cybersecurity

Definition

Cybersecurity is the practice of **protecting computer systems, networks** and **data** from **digital attacks** and **unauthorized access**. It involves implementing technologies and policies to safeguard sensitive information against threats like malware and phishing.

Relevance to Agriculture

Cybersecurity is increasingly relevant to the agri-food sector due to the **growing reliance on technology** in farming, food processing and supply chain management. As agricultural operations adopt **smart technologies, IoT devices** and **data analytics** they become more vulnerable to cyber threats that could **disrupt operations, compromise data** or lead to **food safety issues**.

2) Common cyber threats & vulnerabilities

Cyber Threats

Malware

Is short for **malicious software**.
Refers to any software designed to **harm, exploit or otherwise compromise a computer system, network or device**.

- viruses
- worms
- trojan horses
- ransom ware
- spyware

This software can steal data, disrupt operations or gain unauthorized access to systems.

2) Common cyber threats & vulnerabilities

Cyber Threats

Phishing

Is a cyber attack technique that involves tricking individuals in providing sensitive information such as passwords and credit card numbers.
This often occurs through deceptive emails, messages or websites that appear legitimate.

- **Email Phishing**: attacker sends email that appears to be from a legitimate source (bank, popular service), prompting the recipient to click a link & enter personal information on a fake website
- **Spear Phishing**: targeted attack where the scammer customizes the message for a specific individual or organization often using professional information to make it more convincing

2) Common cyber threats & vulnerabilities

Cyber Threats

Phishing

- **Smishing**: conducted via SMS where the sender tricks the recipient into clicking a link or providing personal information often claiming to be from a trusted source
- **Voice Phishing (Vishing):** phone call from someone pretending to be from an organization urging the recipient to provide sensitive information or make an urgent payment to resolve an issue
- **Clone Phishing**: a scam where a legitimate email that the victim has previously received is replicated with malicious links or attachments added and sent from a spoofed address
- **Social Media Phishing**: fraudulent messages or posts on social media platforms that encourage users to click on links or provide personal information often disguised as contests or urgent allerts

2) Common cyber threats & vulnerabilities

Cyber Threats

Ransomware

A type of malicious software that **encrypts a victims files** or **locks them out of their system, demanding a ransom payment to restore access**. It often spreads through phishing, emails or malicious downloads and can lead to significant data loss and financial damage.

Identification

- suspicious behavior, files suddenly become inaccessible
- ransom notes
- look for unexpected pop-up messages demanding payment
- system slowdown

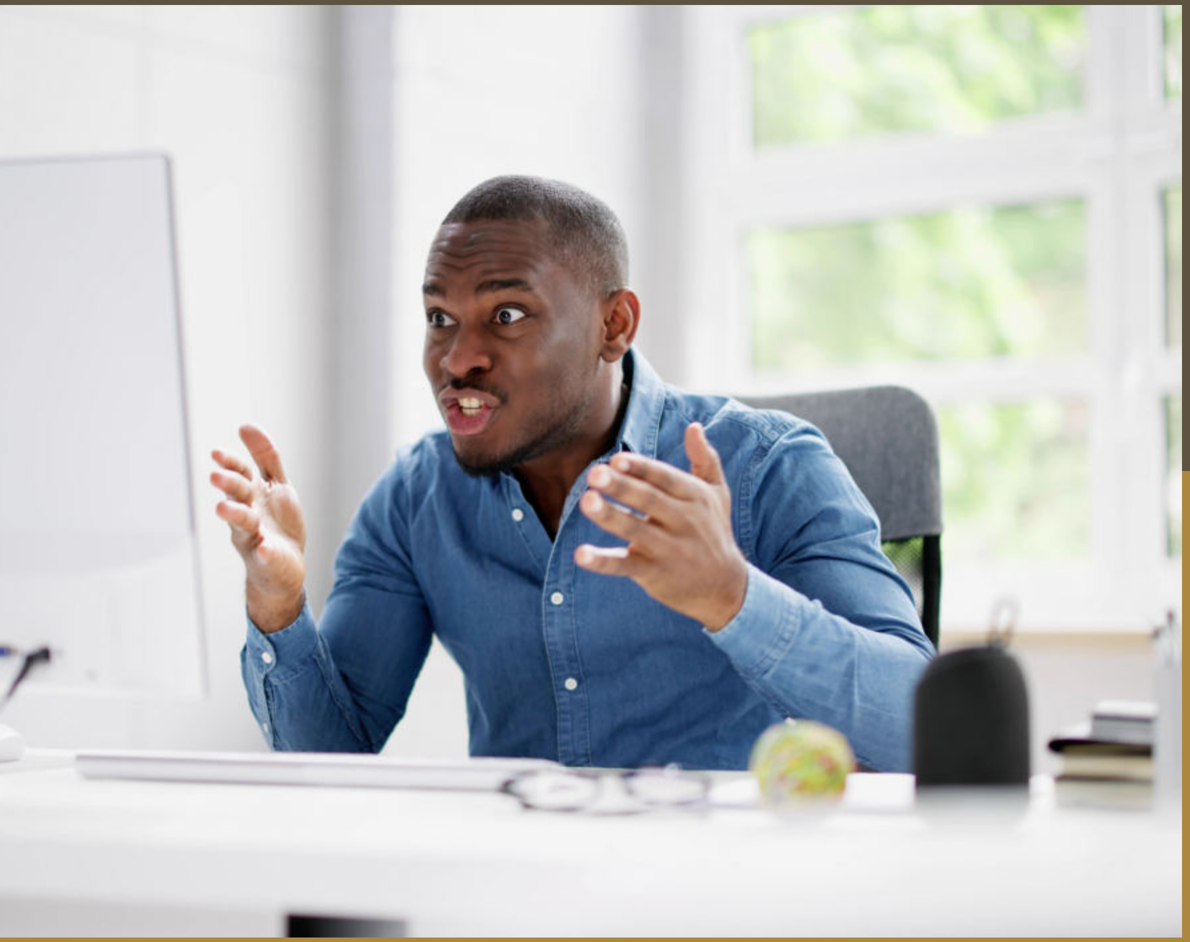
Avoidance

- regular backups
- email vigilance
- security software
- system updates
- user training
- network segmentation

2) Common cyber threats & vulnerabilities

Cyber Threats

Insider Threats



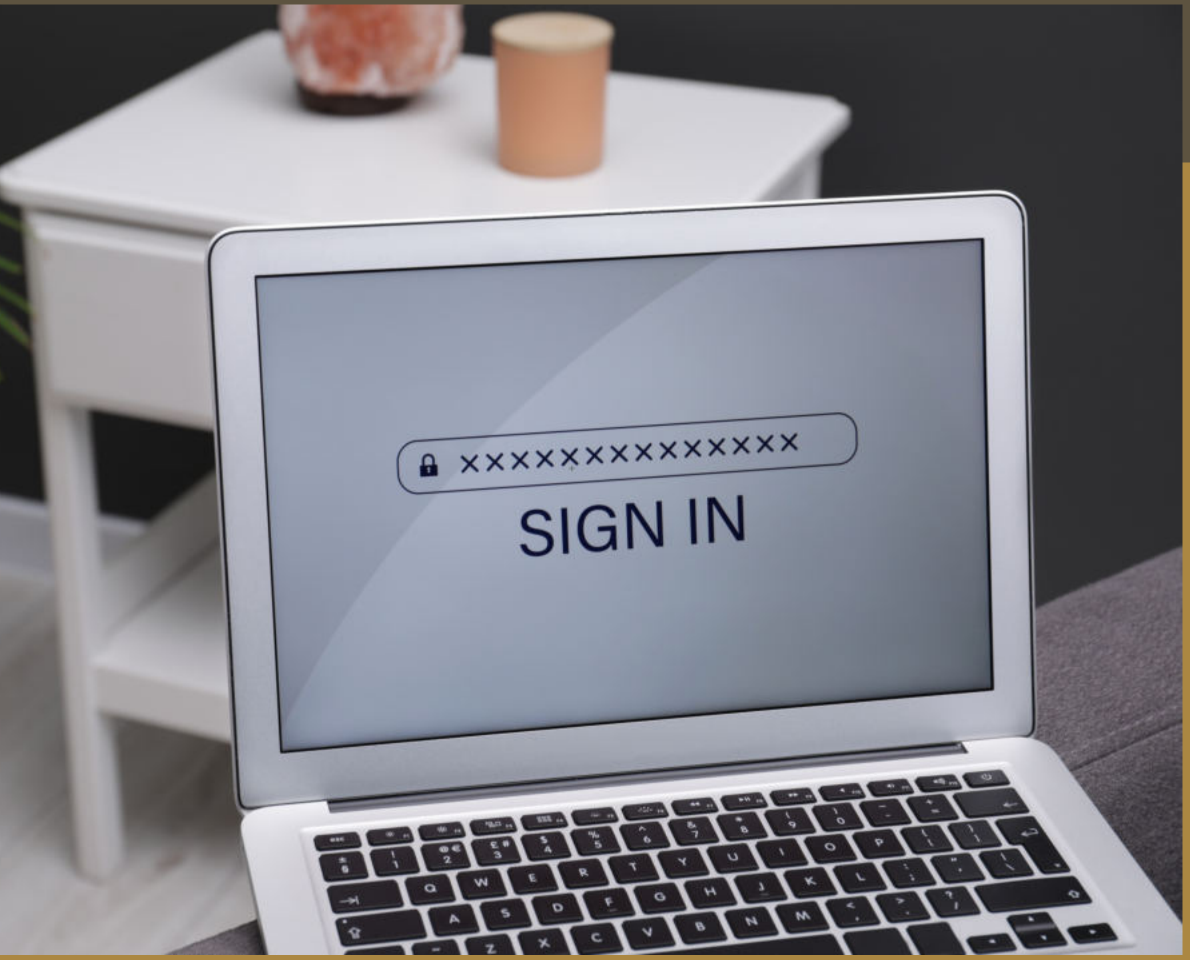
Refers to security risks posed by **individuals within an organization** such as employees, contractors or business partners who have authorized access to systems and data. These individuals may cause intentional or unintentional sabotage to operations.

❗ Insider Threats can be particularly challenging to detect and prevent due to the trusted status of the individuals involved

2) Common cyber threats & vulnerabilities

Vulnerabilities

Weak Points



Identifying vulnerabilities in cybersecurity and implementing **prevention strategies** is a crucial part of maintaining a secure environment.

Identification

- conduct regular security audits
- utilize vulnerability scanners
- penetration testing
- review configuration settings
- monitor logs and alerts
- stay informed

Steps for Prevention

- regular patch management
- implement strong access controls, firewalls & IDS (intrusion detection systems)
- strong passwords
- encrypt data
- backup data
- incident response plan
- limit external connections
- review & update security policies

3) Best practices for data protection

Strong Passwords

- complex & unique passwords

Regular Software Updates

- ensure all systems & applications are up to date

Data Encryption

- protecting sensitive data through encryption methods

Employee Training

- educating staff on recognizing threats & safe online practices

3) Best practices for data protection

Anti-Virus & Anti-Malware

Norton Antivirus, Bitdefender, Kaspersky

Vulnerability Scanning

Nessus, OpenVAS, Qualys

Penetration Testing

Metasploit, Burp Suite, Kali Linux

Security Information & Event

Splunk, IBM QRadar, LogRhythm

3) Best practices for data protection

Firewall & Network Security

Palo Alto Networks, Cisco ASA, Fortinet FortiGate

Data Loss Prevention (DLP)

Symantec DLP, Forcepoint DLP, Digital Guardian

Identity & Access Management (IAM)

Okta, Microsoft Azure Active Directory, Ping Identity

Threat Intelligence

Recorded Future, ThreatConnect, Anomali

Compliance & Risk Management

RSA Archer, ServiceNow GRC, LogicManager

4) Data Privacy Regulations

PIPEDA (Personal Information Protection and Electronic Documents Act)

- enacted in 2000, applies to private-sector organizations across Canada
- governs how organizations collect, use & disclose personal information in the course of commercial activities

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

5) Building a cybersecurity culture

Promoting Awareness

- encouraging a culture of security within the organization

Incident Response Plans

- developing & communicating a plan for responding to cyber incidence

Continuous Improvement

- regularly reviewing and updating cybersecurity measures

6) In Conclusion

Cybersecurity and data privacy are vital in safeguarding the integrity and confidentiality of information in the agri-food sector.
By understanding threats, implementing best practices and ensuring compliance agri-food producers can better protect their organizations and enhance trust with their stakeholders.

7) Active Engagement Exercises

Researching

Find a case study of a cybersecurity incident in the agri-food sector and review it.
Example:
https://agriculture.canada.ca/sites/default/files/documents/2024-09/cyber-security-infographic-en.pdf

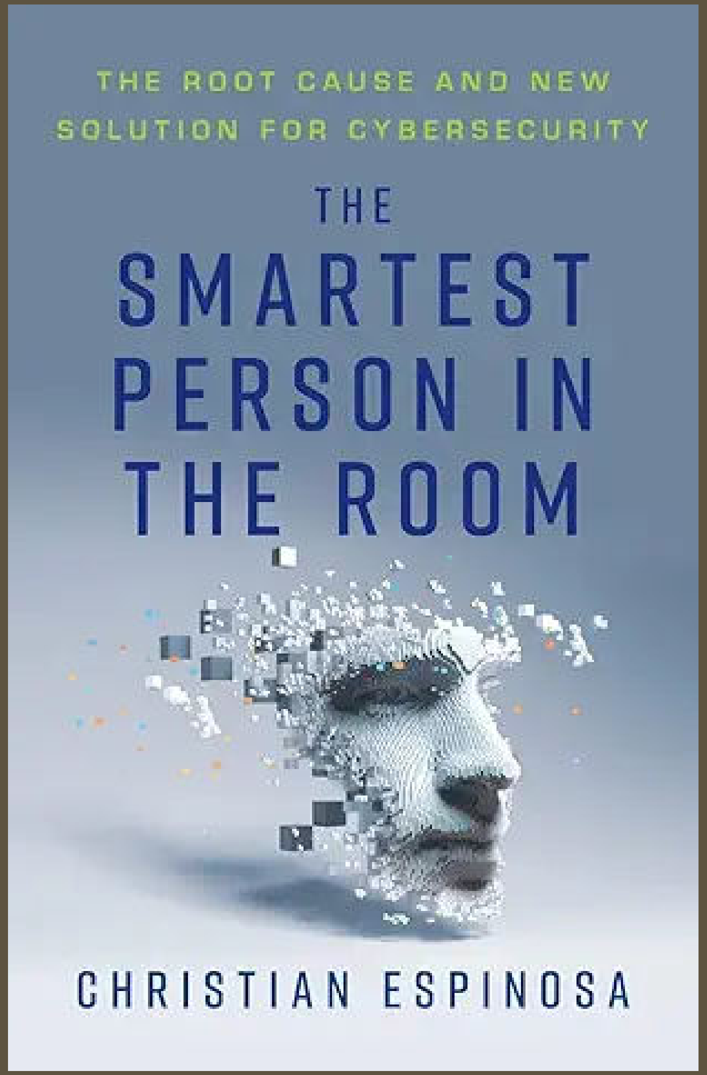
Threat Identification Exercise

Identify potential cybersecurity threats relevant to your (agri-food) operation

Reviewing

Policy Review: Review the policies on your website and analyze their compliancy with official regulations.

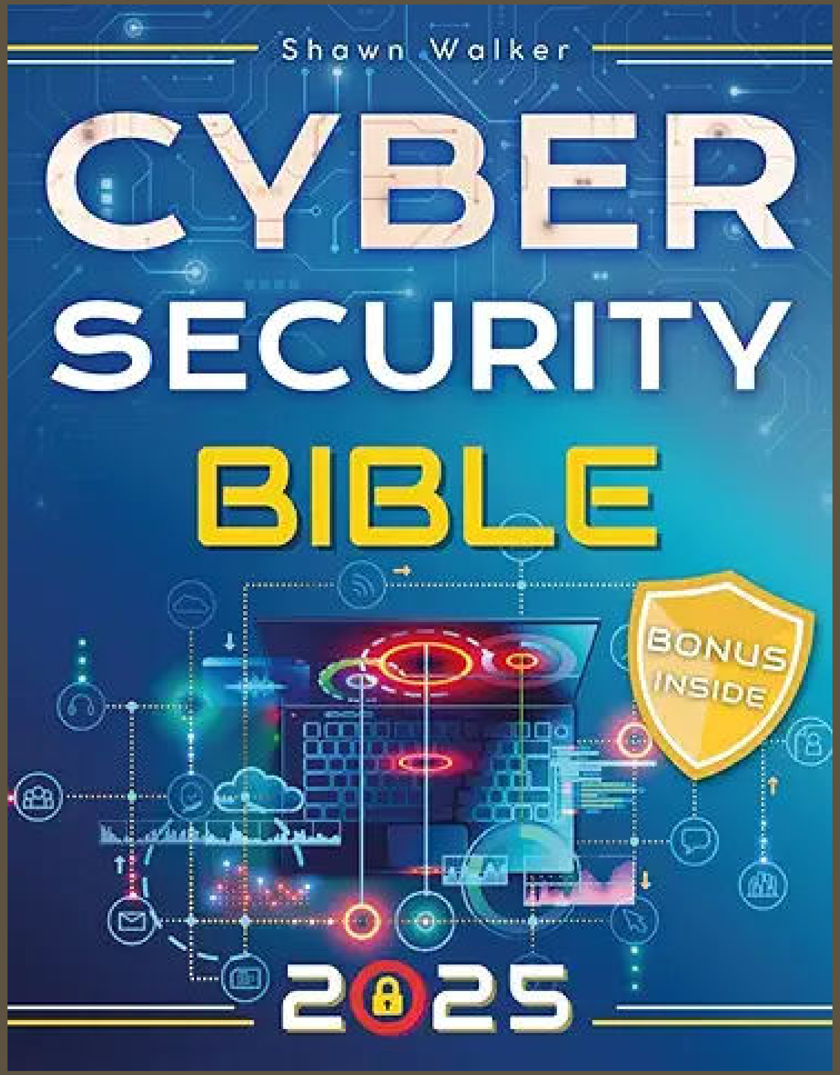
RESOURCES



THE ROOT CAUSE AND NEW SOLUTION FOR CYBERSECURITY

THE SMARTEST PERSON IN THE ROOM

CHRISTIAN ESPINOSA

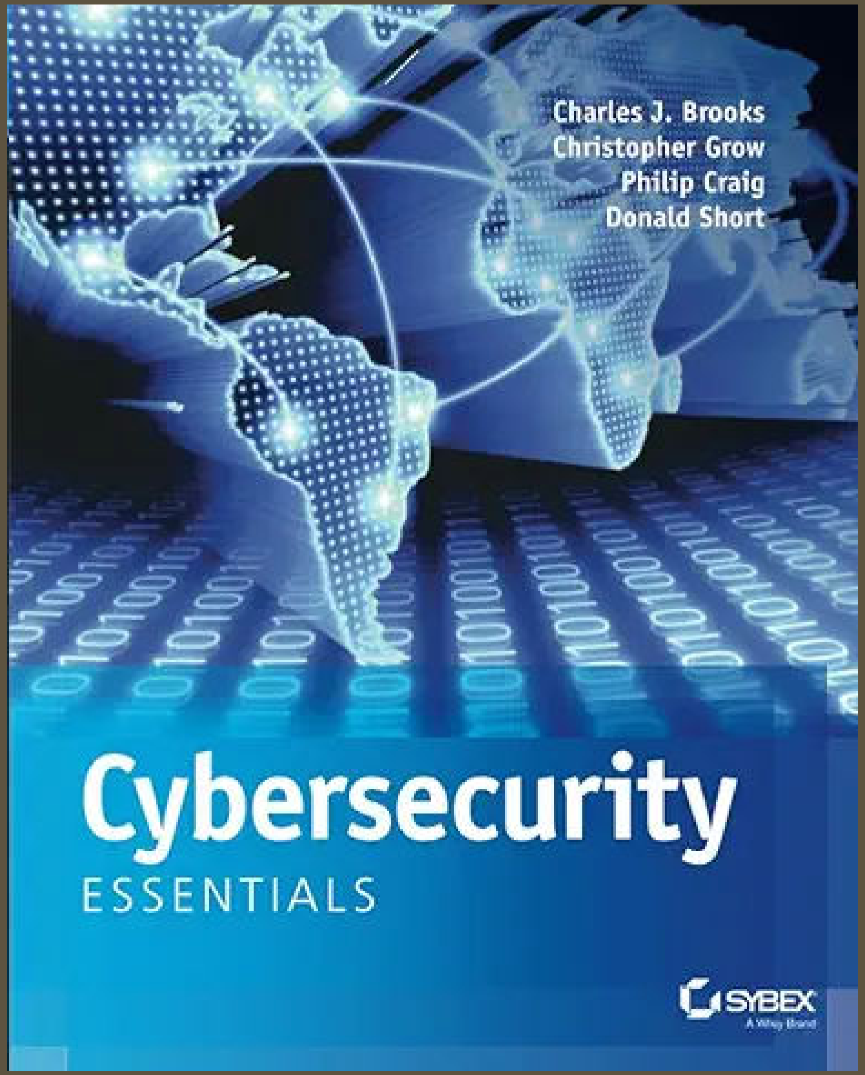


Shawn Walker

CYBER SECURITY BIBLE

BONUS INSIDE

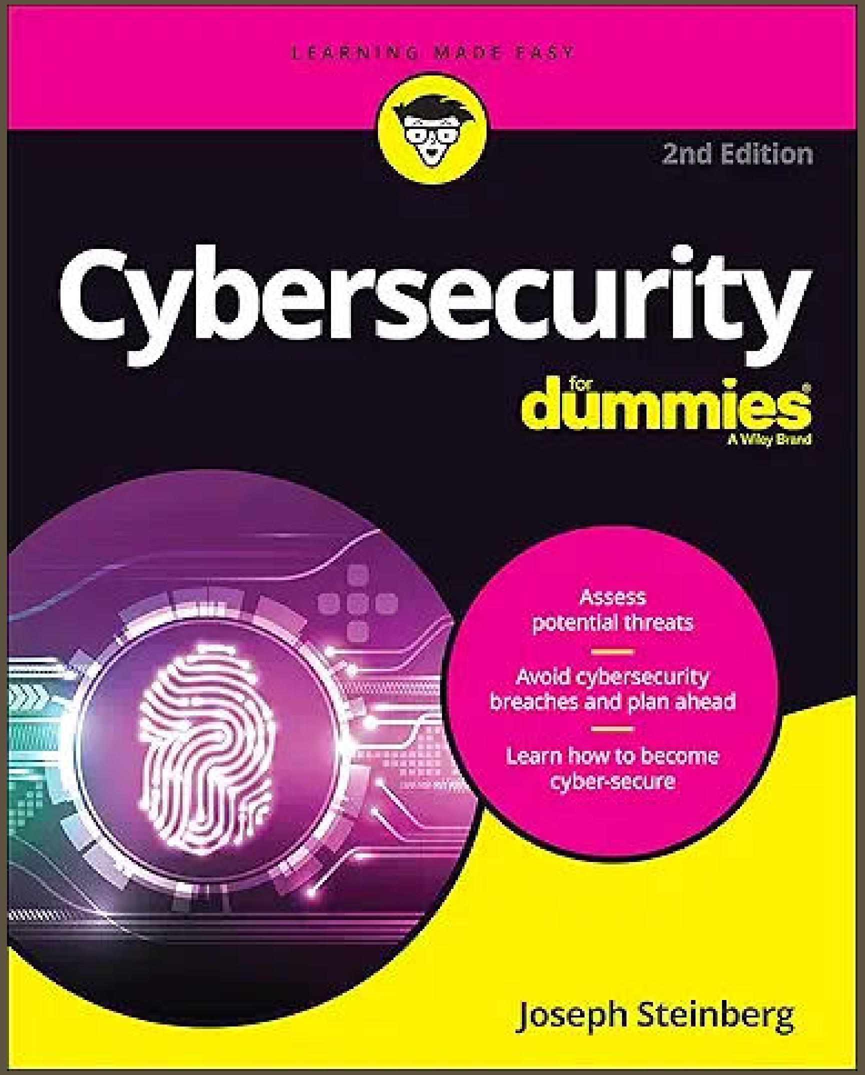
2025



Charles J. Brooks
Christopher Grow
Philip Craig
Donald Short

Cybersecurity ESSENTIALS

SYBEX A Wiley Brand



LEARNING MADE EASY

2nd Edition

Cybersecurity for dummies A Wiley Brand

Assess potential threats

Avoid cybersecurity breaches and plan ahead

Learn how to become cyber-secure

Joseph Steinberg

THANK YOU

COURSE CREATORS:
Ines & Eric Batterton of

My NORDIC Garden
Natural & Sustainable Kitchen Gardens

MADE POSSIBLE BY:
Eastern Ontario Agri-Food Network

Réseau Agroalimentaire de l'Est ontarien
Eastern Ontario Agri-Food Network