



Cybersecurity Basics: Protecting Your Data in the Digital Age

Veronica Semenova, Ph.D. - Webinar Speaker

Romana Riyaz, Ph.D. - Webinar Speaker

Summary of Key Concepts Covered in the Webinar

➔ *Why Cybersecurity Matters*

Cybersecurity is essential in today's digital world due to increased reliance on:

- Online learning platforms
- Cloud storage services
- Mobile devices
- Remote work and collaboration tools

Cyber threats can compromise personal privacy, academic records, financial security, and professional reputation.

➔ *The CIA Triad: Foundations of Cybersecurity*

The CIA Triad represents the three core principles that guide all cybersecurity practices:

- Confidentiality
Ensures that information is accessible only to authorized users.
- Integrity
Protects data from unauthorized modification or destruction, maintaining accuracy and trustworthiness.
- Availability
Ensures that systems and data are accessible when needed by legitimate users.

Together, these principles form the backbone of effective cybersecurity strategies.

➔ *Common Cybersecurity Threats*

Participants were introduced to common digital threats, including:

- Phishing attacks designed to steal sensitive information
- Malware and ransomware that damage or lock data
- Weak or reused passwords that allow unauthorized access
- Insecure networks, especially public Wi-Fi



→ *Tools and Resources for Data Protection*

The essential tools used to safeguard data:

- Antivirus and anti-malware software
- Password managers for secure credential storage
- Firewalls to control network traffic
- Two-Factor Authentication (2FA) for added account security

→ *Cyber Hygiene and Best Practices*

Strong cybersecurity depends on daily habits such as:

- Using strong, unique passwords
- Keeping systems and software updated
- Backing up data regularly
- Recognizing and avoiding suspicious emails or links

Links to Relevant Articles, Tools, and Frameworks

→ *Foundational Cybersecurity Concepts*

- **NIST Cybersecurity Framework (CSF)**
<https://www.nist.gov/cyberframework>
Widely used framework for managing and reducing cybersecurity risk.
- **CISA – Cybersecurity Basics**
<https://www.cisa.gov/cybersecurity>
Trusted U.S. government resource explaining threats, protections, and best practices.
- **IBM – What Is Cybersecurity?**
<https://www.ibm.com/topics/cybersecurity>
Clear overview of cybersecurity concepts, threats, and solutions.

→ *Understanding Common Threats (Phishing, Malware, Ransomware)*

- **FTC – How to Recognize and Avoid Phishing Scams**
<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>



- **Google – Phishing Quiz**
<https://phishingquiz.withgoogle.com>
Interactive quiz to practice identifying phishing emails.
- **CISA – Ransomware Guidance**
<https://www.cisa.gov/ransomware>

➔ Practical Tools for Data Protection

- **Password Managers**
 - Bitwarden (Free & Open Source): <https://bitwarden.com>
 - LastPass: <https://www.lastpass.com>
- **Two-Factor Authentication (2FA)**
 - Google Authenticator: <https://support.google.com/accounts/answer/1066447>
 - Microsoft Authenticator: <https://www.microsoft.com/security/mobile-authenticator-app>
- **Antivirus / Anti-Malware**
 - Microsoft Defender: <https://www.microsoft.com/windows/comprehensive-security>
 - Avast Free Antivirus: <https://www.avast.com/free-antivirus-download>

➔ Learning & Skill-Building Resources

- **Cybrary (Free Courses)**
<https://www.cybrary.it>
- **Coursera – Cybersecurity for Beginners**
<https://www.coursera.org/browse/information-technology/security>
- **OpenLearn – Introduction to Cyber Security (The Open University)**
<https://www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0>

Practical Cybersecurity Tips & Best Practices

➔ Password & Account Security

- Use **long, unique passwords** for every account (12–16 characters minimum)
- Avoid reusing passwords across personal, academic, and work accounts
- Use a **password manager** to generate and store passwords securely
- Enable **Two-Factor Authentication (2FA)** wherever possible



➔ Email & Phishing Awareness

- Do not click links or download attachments from unknown senders
- Check the sender's email address carefully (look for misspellings)
- Be cautious of messages that create **urgency** or request personal information
- When unsure, **verify through another channel** before responding

➔ Device & Software Protection

- Keep operating systems, apps, and browsers **up to date**
- Enable **automatic updates** for security patches
- Use reputable **antivirus / anti-malware software**
- Lock your device with a **PIN, password, or biometric authentication**

➔ Data Protection & Backups

- Back up important files regularly using **cloud storage + external drives**
- Encrypt sensitive files when possible
- Log out of accounts on **shared or public computers**
- Avoid using public Wi-Fi for sensitive tasks (banking, academic portals)
-

➔ Everyday Cyber Hygiene Habits

- Review privacy and security settings on apps and platforms
- Remove unused apps and browser extensions
- Separate **personal and academic/professional accounts**