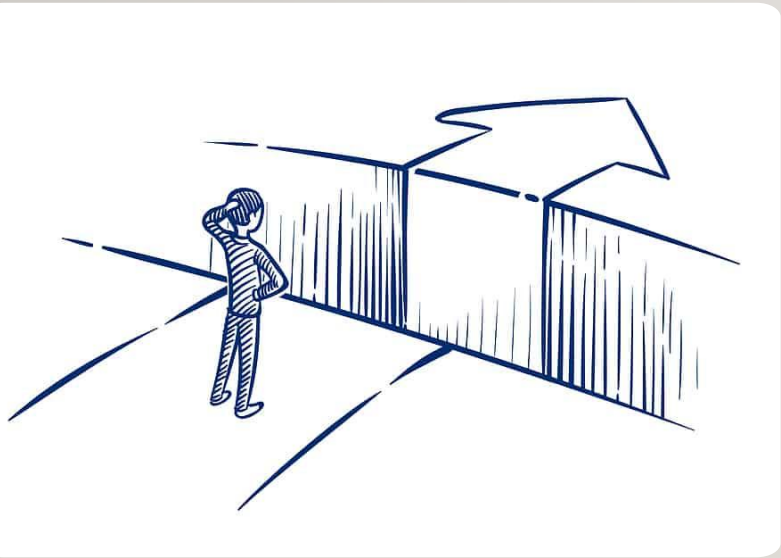
BUILDING A CYBERSECURITY AND AI INTEGRATED LEARNING PATHWAY FOR CRIMINAL JUSTICE PROFESSIONALS

DR. YAN BAI, DR. JUAN LI

CYBERSECURITY EDUCATION GAP FOR CJ PROFESSIONALS



Limited Cybersecurity Education:

- Few CJ programs in the U.S. offer cybersecurity courses or programs
- Traditional Lecture Format, lacking innovation and practical training.
- Historical Neglect: security was primarily considered a business concern.

Frontline Skills Gap:

- Lack necessary training
- Unclear roles

Interdisciplinary Demands:

- Criminal justice standards
- Cybersecurity technology

Shortage of qualified instructors

Continuous Evolution

Resource and Time Constraints:

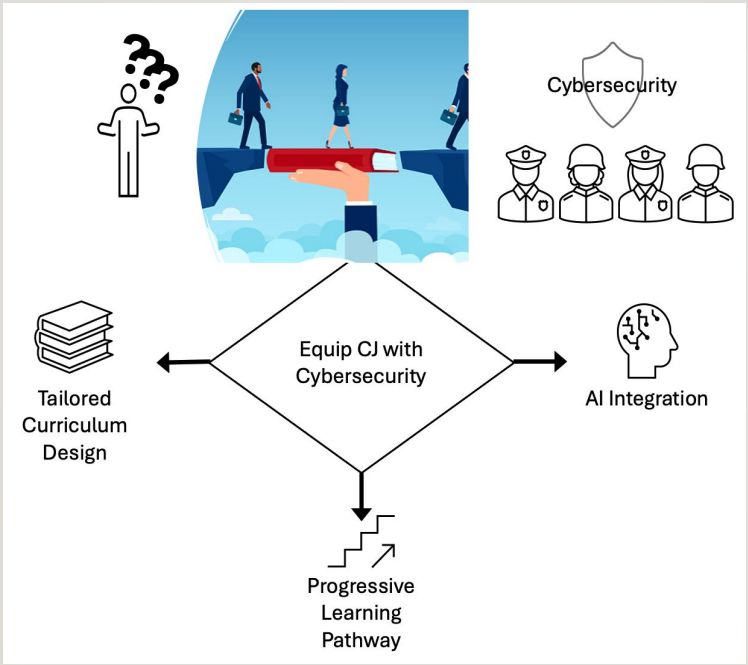
Redefining Cybersecurity Education for Criminal Justice Professionals: Bridging the Gap in National Cyber Capabilities

Objective & Challenge:

- **Bridging the Gap** of Cybersecurity Education for CJ Professionals

Approaches & Solution:

- Need-based Curriculum Design
- Progressive Learning Pathway tailored for CJ professionals
- Integrate AI into the curriculum to enhance CJ professionals' capabilities of defending cybercrime



Scientific Impact:

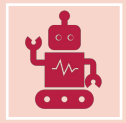
- Identify key areas of cybersecurity and privacy knowledge that are essential for CJ professionals
- Provide CJ professionals with necessary skills and knowledge to identify, investigate, and prosecute cybercriminals effectively

Broader Impact and Broader Participation:

- Build CJ workforce's cybersecurity and privacy knowledge
- Establish strategic partnerships between academia and CJ agencies, fostering collaboration and knowledge-sharing.
- Diversify the cybersecurity workforce by empowering underrepresented minority students.

A PROGRESSIVE LEARNING PATHWAY

Course 1: Introduction to Cybersecurity and Privacy



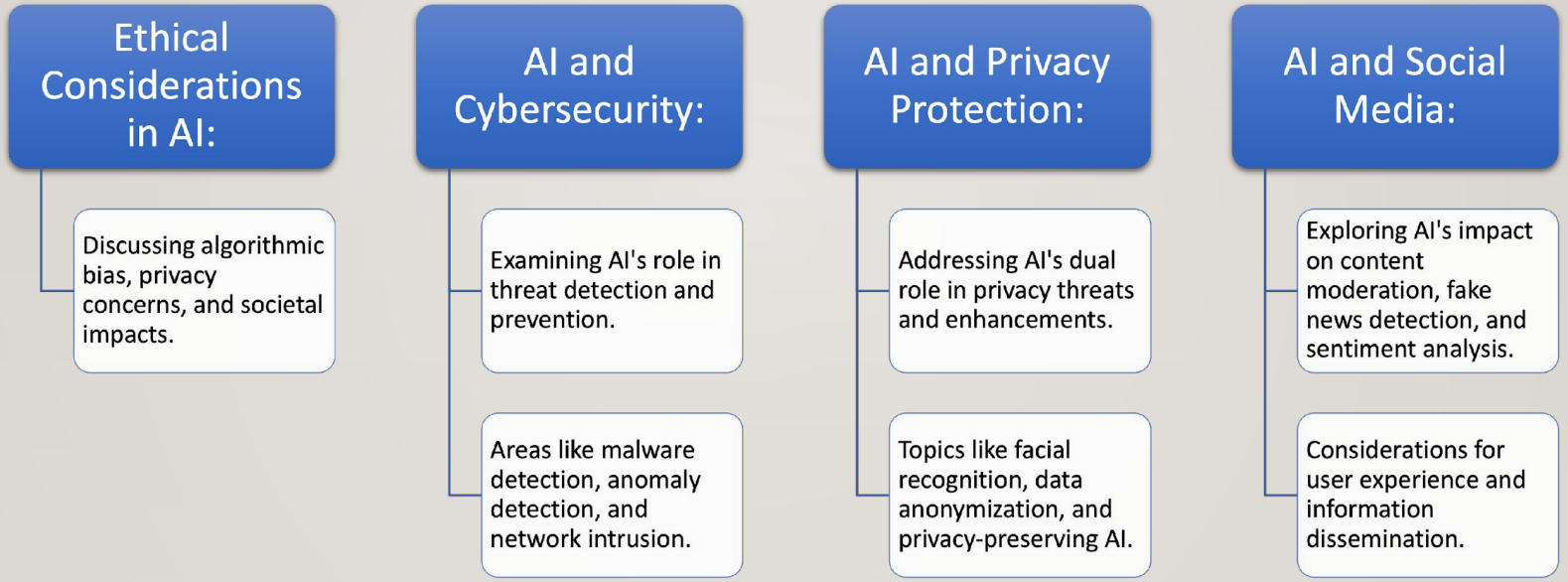
Course 2: Cyber Forensics and Cyber Intelligence

Course 3: Cyber Challenges in Criminal Justice

COURSE I OVERVIEW

Computer Security	Internet Security	Privacy
		

COURSE II OVERVIEW



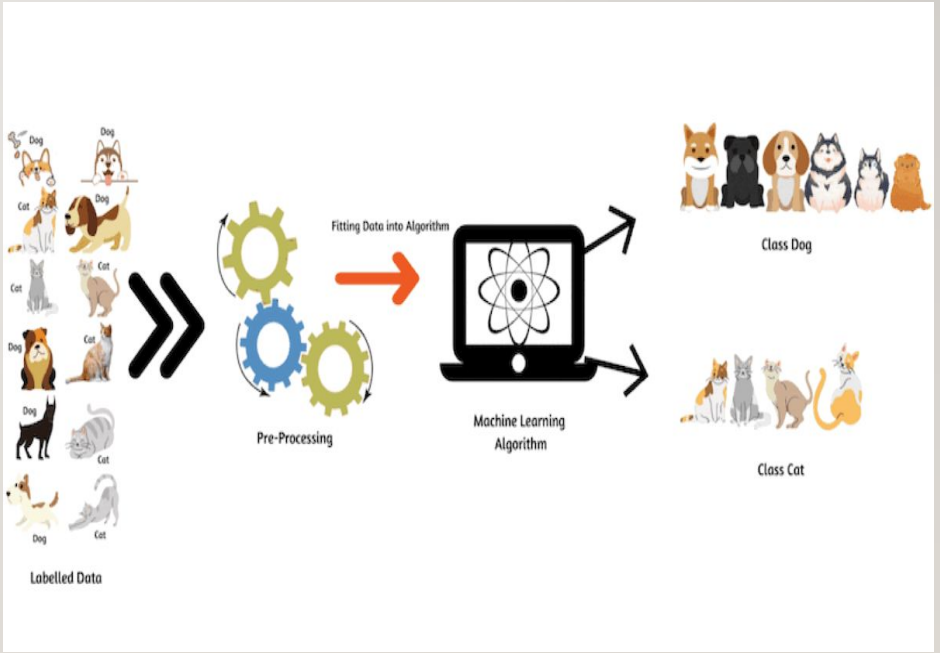
COURSE III OVERVIEW

- Scenario 1: Data Loss and Misuse
- Scenario 2: Segregation of Duties
- Scenario 3: Fraud Detection

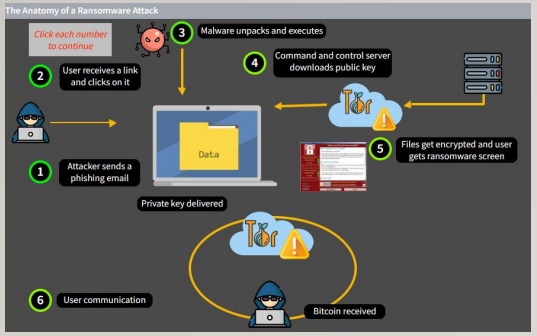
COURSE DESIGN AND ACTIVITIES

INTERACTIVE SIMULATIONS FOR CONCEPTS EXPLAINED

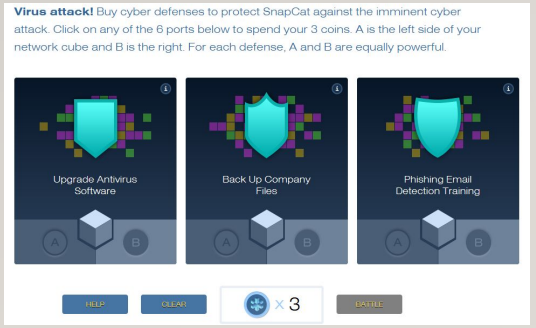
Supervising learning is when a computer learns by practicing with examples that are already marked with the right answers. It's like a practice test where every question comes with the correct answer, so the computer can learn the pattern. After practicing, the computer is given a real test with questions it hasn't seen before. The answers are there but hidden from the computer, to check if it has learned well enough to figure out the answers on its own. This real test helps to see if the computer can now make good guesses without being told the answers.



WEB-BASED LABS (1)

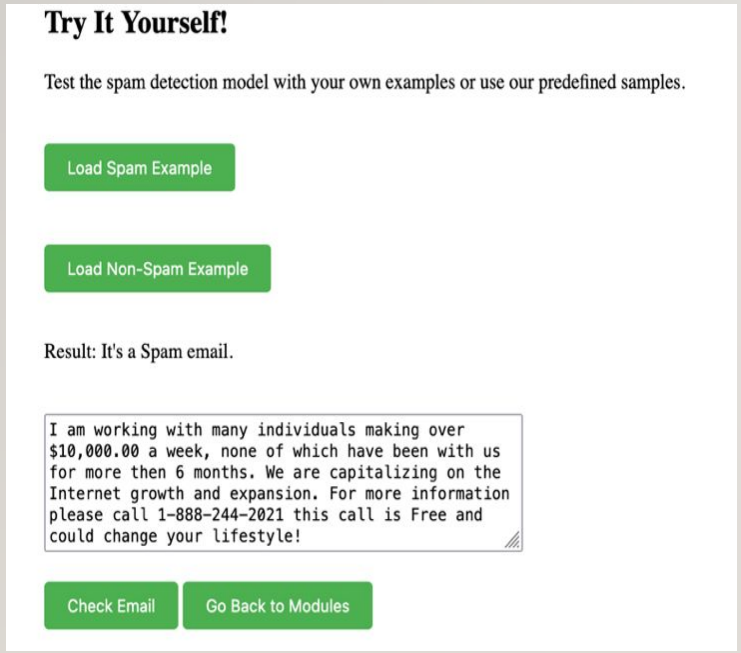


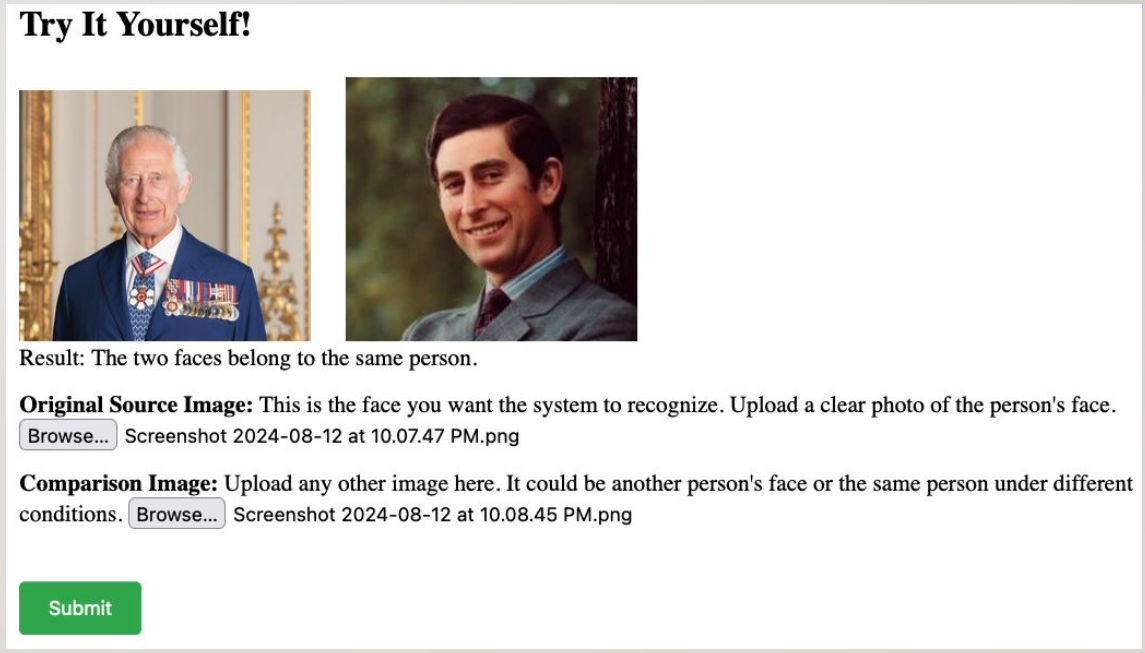
- The Anatomy of a Ransomware Attack
  - https://www.myemates.com/ransomware/RansomwareAttack.html



- PBS Nova Labs – Cybersecurity Lab
  - https://www.pbs.org/wgbh/nova/labs/lab/cyber/

WEB-BASED LABS (2)





CASE STUDY:

A CONSTRUCTION COMPANY GETS HAMMERED BY A KEYLOGGER

- **Scenario:**
  A small family-owned construction company, relying heavily on online banking and ACH transfers, suffered a major cyberattack. An employee unknowingly opened a malware-infected email, allowing cyber criminals to install a keylogger and capture banking credentials.
- **Attack:**
  The keylogger enabled unauthorized access, leading to six fraudulent transfers totaling $550,000.
- **Response:**
  The bank recovered $200,000, but $350,000 remained missing. The company, lacking a cybersecurity plan, faced delays in responding. They hired a cybersecurity firm for a system review and security upgrades.
- **Impact:**
  The company eventually recovered the full $550,000 but incurred significant losses in time and legal fees.

Lessons Learned

1. Get notified - set up transaction alerts on all credit, debit cards and bank accounts.
2. …

CASE STUDY:

A CONSTRUCTION COMPANY GETS HAMMERED BY A KEYLOGGER

- **Scenario:**
  A small family-owned construction company, relying heavily on online banking and ACH transfers, suffered a major cyberattack. An employee unknowingly opened a malware-infected email, allowing cyber criminals to install a keylogger and capture banking credentials.
- **Attack:**
  The keylogger enabled unauthorized access, leading to six fraudulent transfers totaling $550,000.
- **Response:**
  The bank recovered $200,000, but $350,000 remained missing. The company, lacking a cybersecurity plan, faced delays in responding. They hired a cybersecurity firm for a system review and security upgrades.
- **Impact:**
  The company eventually recovered the full $550,000 but incurred significant losses in time and legal fees.

Discussion:

- **Knowing how the firm responded, what would you have done differently?**
- **What are some steps you think the firm could have taken to prevent this incident?**
- **Is your business susceptible? How are you going to reduce your risk?**

ACKNOWLEDGEMENT