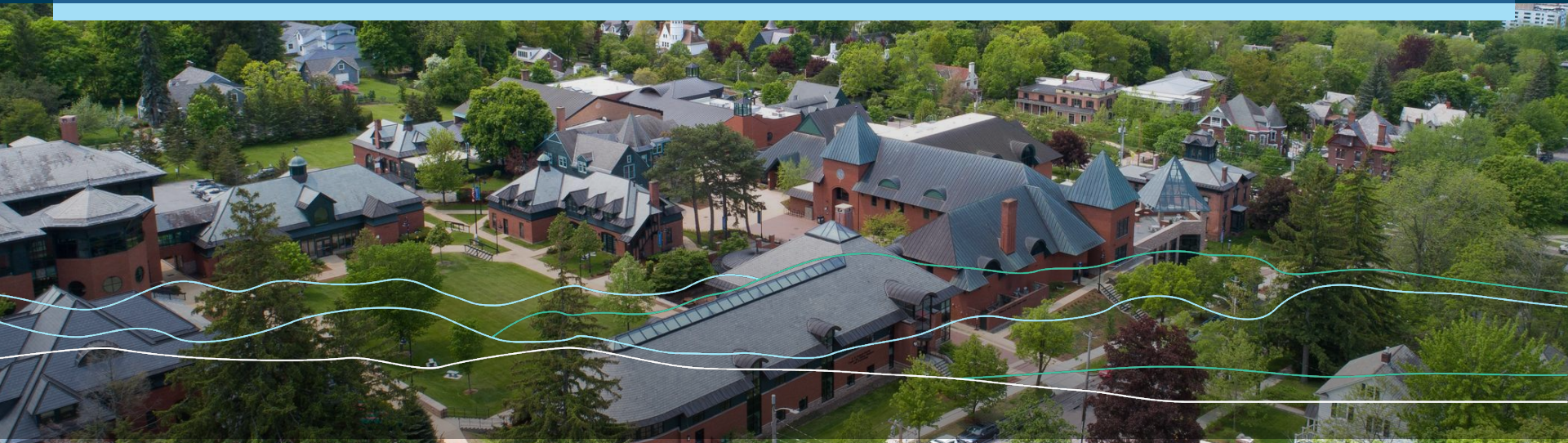
CHAMPLAIN COLLEGE

Introductions

SEC-110



Welcome to SEC-110: Cybersecurity Fundamentals

In this class we will explore different sides of cybersecurity and gain a better understanding of what cybersecurity is and why it's needed.

Class Time:
Wednesday from 12:00 PM to 1:15 PM **OR** 6:00 PM to 7:15 PM EST

Office Hours:
By Appointment using this booking link

Who is Your Professor

I am LaKysha Patnode (she/her), Assistant Professor at Champlain College.

I have worked as an Analyst at NuHarbor Security.

I am excited to be here to teach you about cybersecurity.

Fun Fact: I have three cats!

Who are Your Advisors

I am Angela Koukoulas (she/her), Project Manager & Advisor at Champlain College.

This is my 3rd time advising CyberStart students!

Fun Fact: I am trying to read 25 books in 2025!

Who are Your Advisors

I am Kerry Zuccareno (she/her), High School Pathways Program Manager.

I help students take advantage of all Champlain has to offer, while still in high school.

Fun Fact: I'm learning to speak Irish.

Who are your TA's

I'm Ben (He/Him), the supervisor of the CyberTech Awareness Program.

My team and I help create activities and teach your class!

Fun Fact: I've been in two musicals!

What is CyberTech?

(https://www.cybervt.com/)

- Non-profit Program
- Make cybersecurity accessible for high school students
- Raising awareness of cybersecurity issues
- Introducing safe computer practices
- Projects:
  - CyberStart class development and support
  - Creating educational resources
  - Cybersecurity research/blogposts

Who Are All of You?

Please share your:

- First Name
- Home School
- Cybersecurity Interests
- Fun Fact

Note Taking in College

Why is note-taking important?

- Organization and Time management
- Memory and Comprehension
- Continuous Improvement
- Not Just for Classwork!

When should notes be taken?

- Classes (Lectures)
- At home
- During Projects and Assignments

Notes for this class:

- Create a Tech Journal!

Note-taking and time management guide

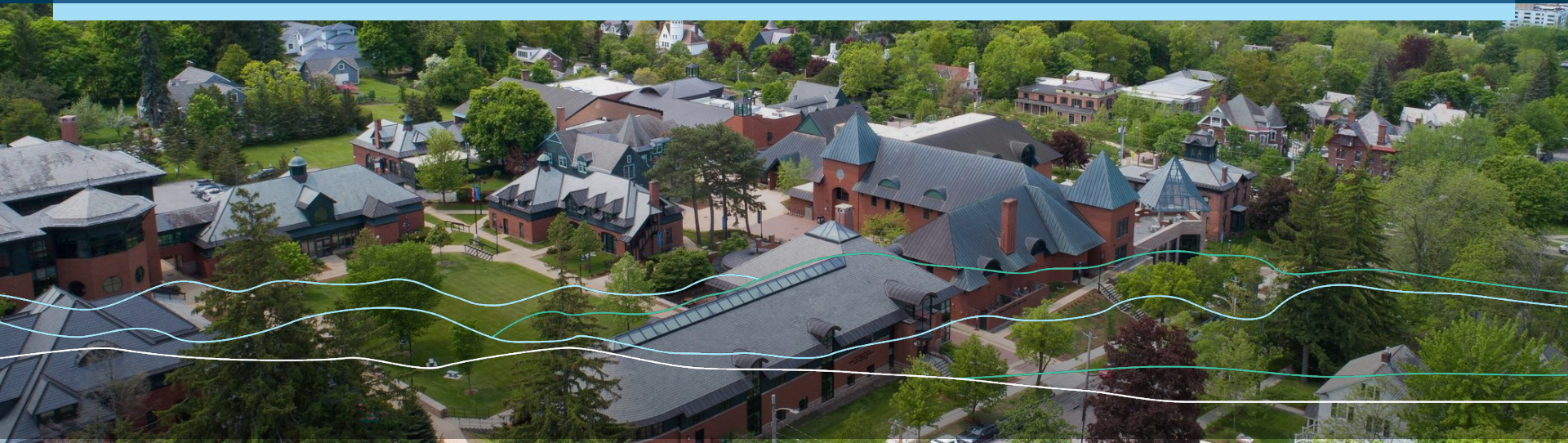
SEC-110 Note taking template

Example SEC-110 Note taking

CHAMPLAIN COLLEGE

Mod 1 – What is Cybersecurity?

SEC-110



How Do You Secure Your House?

How Do You Secure Your Phone?

What is Cybersecurity?

Definition:

The method of defending computer systems, networks, and data from illegal access, harm, or utilization.

- Methods
- Processes
- Tools
- Behaviors
- Policies

Why Cybersecurity Matters

The world is becoming increasingly digital.

- Critical infrastructure has digital components
- Data is a valuable asset, so it needs to be protected
- Your personal information may be vulnerable
- Cyberattacks can cost companies millions
- Necessity to comply with regulations like GDPR, GIPAA, and PCI-DSS

History of Cybersecurity

1834 - French Telegraph System

- Two criminals gained unauthorized access to the telegraph to take financial market information.

1950s - Phone Phreaking

- Phone phreaking was the first demonstration of hacking, by hijacking telephone protocols to make cheaper or no-cost calls.

1970s - Origins of the Internet

- The first operational packet-switched network through advanced research projects agency network (ARPANET), it served as the internet's fundamental framework.

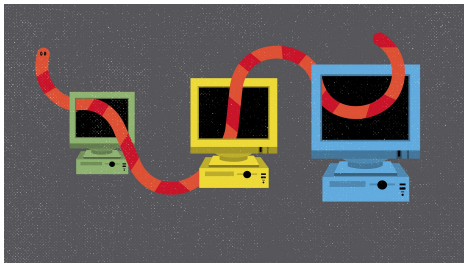
History of Cybersecurity

1979 - The Ark

- At 16 years old, Kevin Mitnick was dared to hack a computer system, The Ark which was used by Digital Equipment Corporation.

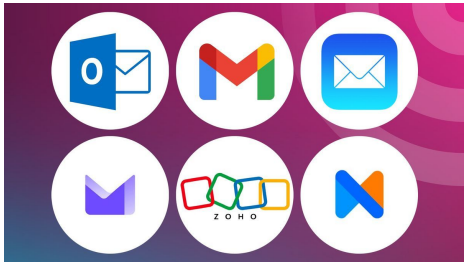
1988 - Morris Worm

- Created to spread quickly throughout the internet, leading to huge disruptions and raising awareness about malicious software.



1999 - Melissa Virus

- An email-borne virus that created universal damage, underlining the weaknesses in email systems, and that malicious content can spread quickly.



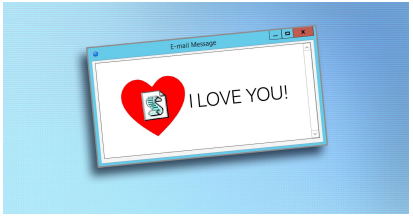
History of Cybersecurity

1999- NASA Cyber Attack

- A hacker utilized a vulnerability to gain unauthorized access to NASA's computer systems. Which led to a 21-day shutdown.

2000 - ILOVEYOU Worm

- A worm that spread worldwide through email attachments, led to billions of dollars in damages and stimulated security practices.

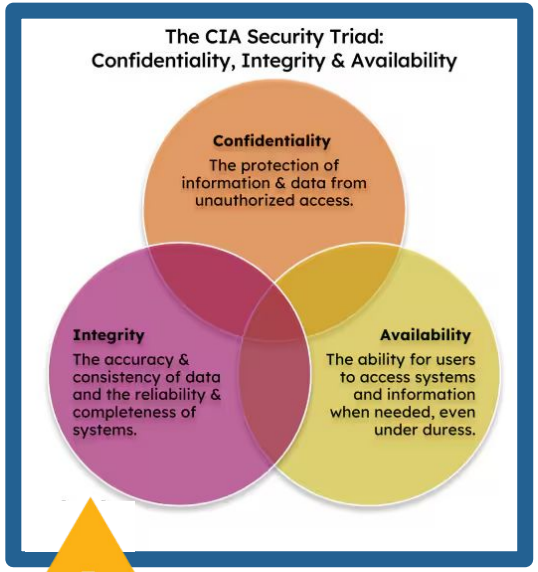


2000 - Anna Kournikova Worm

- A worm that used vulnerabilities in Microsoft Outlook and depended on user's curiosity to spread by promising photos of a famous tennis player, Anna Kournikova.

CIA Triad

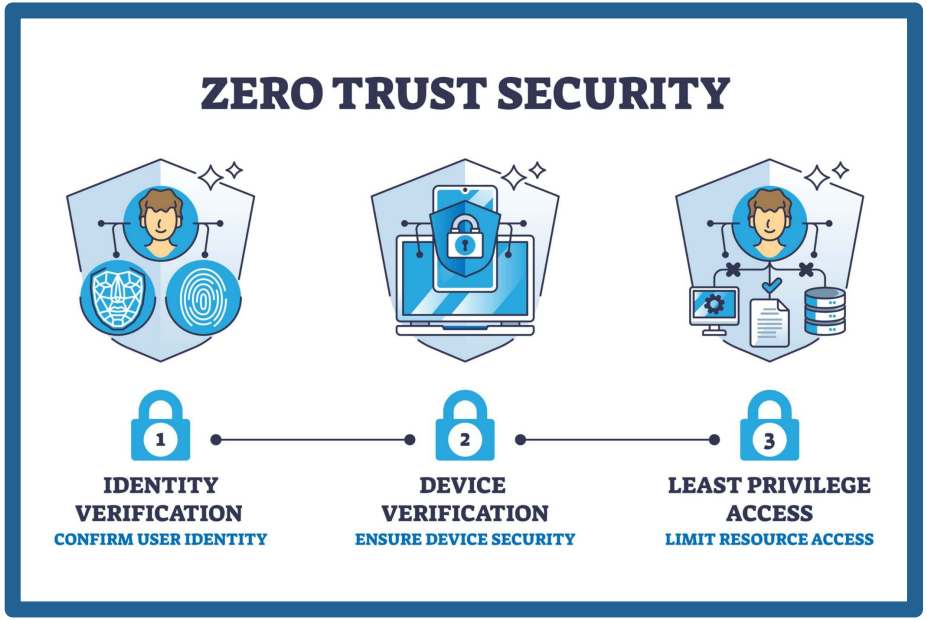
- **Confidentiality:** protecting personal information from unauthorized access, securing only authorized persons can access sensitive data.
- **Integrity:** securing information is correct, complete, and hasn't be changed without authorization.
- **Availability:** securing that authorized individuals can access data and resources when needed.



Zero Trust

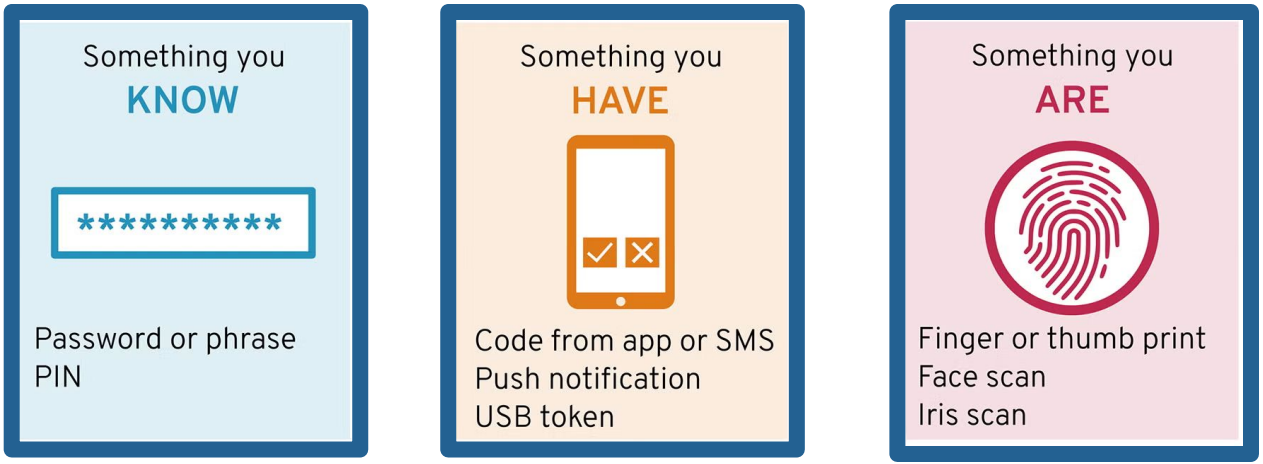
Zero Trust is a cyber approach assuming no user or device should be trusted by default.

- Users only receive access to what they need
- Authenticate and authorize every time
- Designs systems assuming attackers are already inside



Authentication

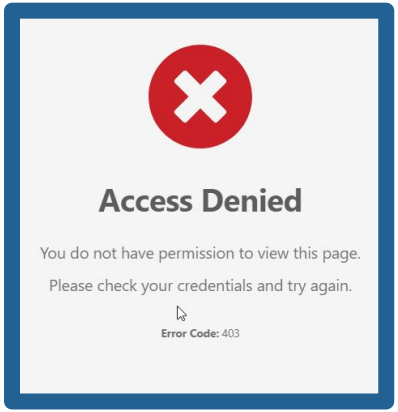
- **Authentication:** *Who are you?*
    - Authentication is the process of verifying a person's identity.
    - **Methods:**

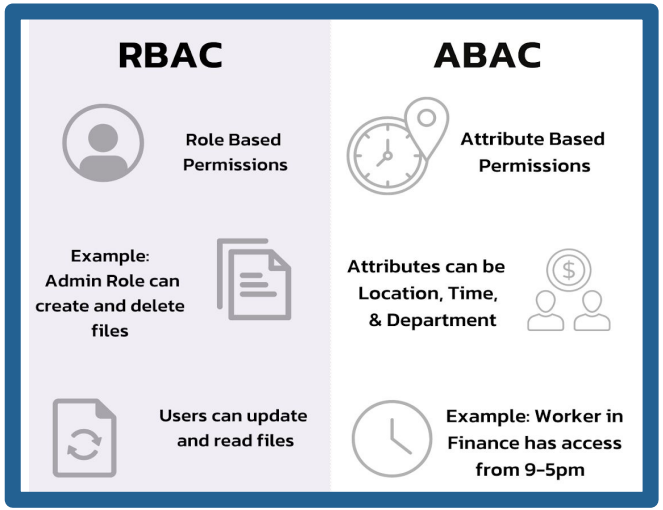


* Multi-factor authentication uses 2 or more of the above categories to authenticate securely

Authorization

- **Authorization:** *What can you do?*
  - Authorization determines what resources or actions a person is allowed to access.



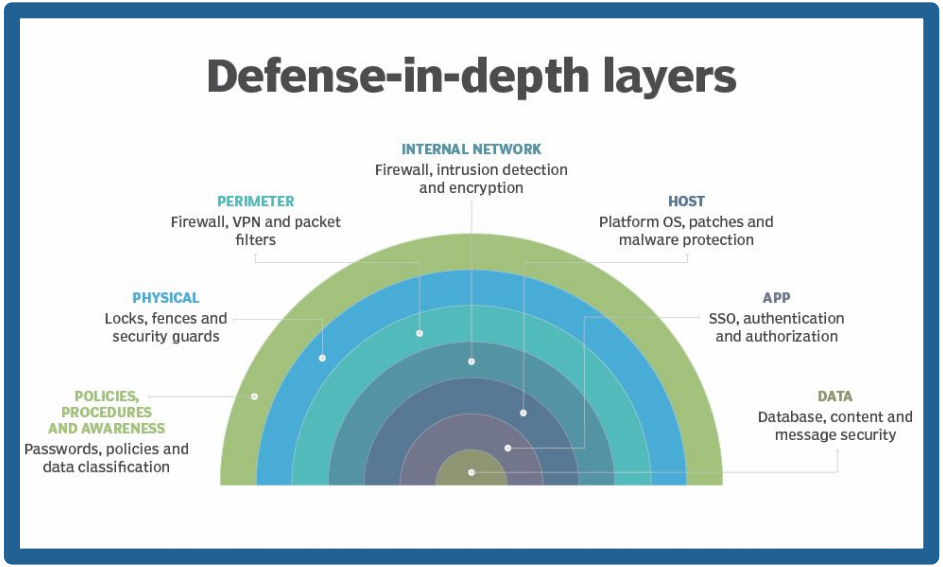


- **Types:**
  - ➢ Role-based Access Control (RBAC): Access based on job role
  - ➢ Attribute-based Access Control (ABAC): Access based on the person's attributes and conditions

Defense In Depth

Defense in Depth describes a multi-layered approach to security controls.

- Ensures that if one security measure fails, there are others in place
- Minimizes likelihood of breach
- Gives time for an organization to launch countermeasures against an attack



Human Factors

Humans are the weakest link in cybersecurity

- Somewhere between 68%-95% of cyber incidents can be attributed to human error. This can include:
  - Social engineering attacks
  - Lack of security awareness and training
  - Poor password hygiene or authentication
  - Poor communication

Ethics in Cybersecurity

- **User Privacy:** clear boundaries when monitoring
- **Transparency:** Users should be informed about breaches and what data was exposed
- **Resource Allocation:** Balance security needs with business priorities when there are limited resources
- **Auditing:** Regularly review policies to ensure compliance

The Cybersecurity Mindset

Having a cybersecurity mindset is about more than just stopping hackers.

- **Cybersecurity professionals are:**
  - Prepared, alert, and ethical in their approach
  - Aware of their online presence and digital footprint
  - Part of a cyber-aware society and willing to teach others how to be safe
  - Always learning new technologies, tools, or exploits

Domains of Cybersecurity

- Ethical Hacking
- Governance
- Project Management
- Network and System Security
- Threat Intelligence
- Cryptography
- Security Operations
- Client Success
- Incident Response
- Software Security
- Legal and Regulations
- Security Awareness
- Physical Security
- Security Architecture
- Frameworks and Standards

Cybersecurity is for EVERYONE!