Career Kickstart™
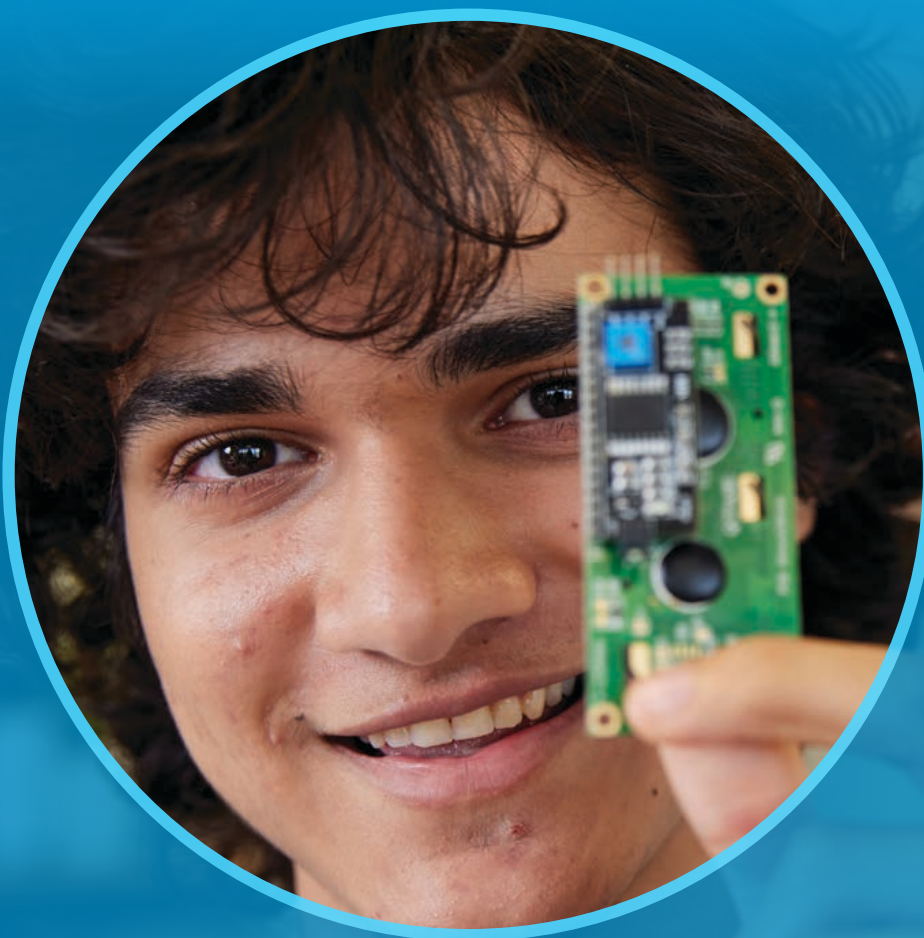
Powered by ◆AP®

Cybersecurity Pilot

INSTRUCTIONAL OVERVIEW

Clearing a path for all students to own their future through career preparation.

Contents

Career Kickstart Cybersecurity opens countless doors for CTE students by offering real-life experiences in the field of cybersecurity. It prepares students for the workforce and equips them for both two- and four-year colleges. This program is particularly beneficial for hands-on learners, providing inclusive opportunities for all students to engage with the subject.

— Beth Cerrone,
Cybersecurity K-12 Educator,
St. Vrain Valley Schools,
Career Kickstart Advisory Board Member

Career Kickstart Program

Career Kickstart™ is a new career-focused program that will lead to credentials and college credit for all students who want to prepare for a career, whether they are heading to two- or four-year colleges, technical schools, or the workforce. With a focus on high-demand fields like cybersecurity, Career Kickstart will bring the best of Advanced Placement to courses designed for career and technical education (CTE).

Career Kickstart courses are powered by the AP® features that educators value: robust teacher training, dedicated educator communities, free student resources, high-quality assessments, and the broadest national network of college credit policies.

Career Kickstart offers two-course pathways that equip students for in-demand careers. Both industry experts and college faculty participate in defining the scope and sequence of the courses. Courses emphasize hands-on experience, teach professional and technical skills, and align to career and technical education (CTE) standards and credentials valued by industry.

Cybersecurity is the first pathway Career Kickstart will launch. We are exploring additional pathways in other high-growth sectors like health sciences and business.

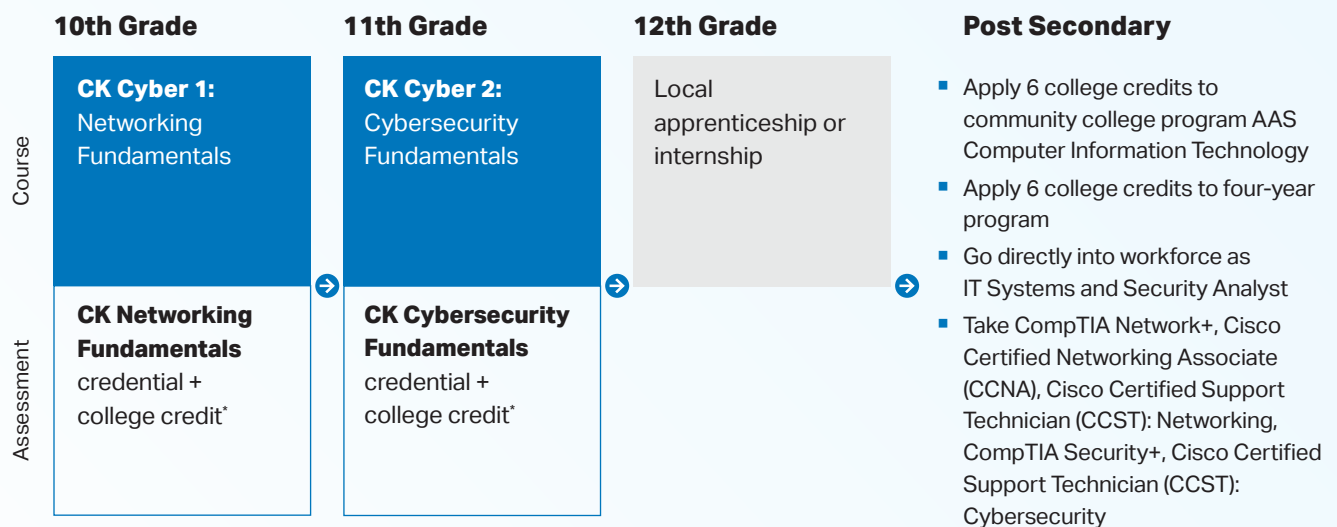# Why College Board Is Developing Career Kickstart

College Board reaches more than 7 million students a year, helping them navigate the path from high school to college and career. Our not-for-profit membership organization was founded more than 120 years ago. We pioneered programs like the SAT® and AP® to expand opportunities for students and help them develop the skills they need. Our BigFuture® program helps students plan for college, pay for college, and explore careers.

To continue these pioneering efforts, College Board is building Career Kickstart to strengthen and expand CTE education nationwide. Students want more career exploration in high school to help them turn a passion into a profession, but many lack access to quality career-focused programs that lead to in-demand jobs. College Board launched Career Kickstart to provide a pathway for these students.

With a proven record of designing high-quality educational opportunities at scale, College Board is building Career Kickstart in partnership with industry, higher education, and high school educators to assure national access to outstanding career education that today is only available in some communities.

College Board's aim is to clear a path for all students to own their future, saving students time and money on their educational journey. Career Kickstart is an important new program to meet that mission.

Career Kickstart Student Experience

	10th Grade	11th Grade	12th Grade	Post Secondary
Course	**CK Cyber 1:** Networking Fundamentals	**CK Cyber 2:** Cybersecurity Fundamentals	Local apprenticeship or internship	■ Apply 6 college credits to community college program AAS Computer Information Technology ■ Apply 6 college credits to four-year program ■ Go directly into workforce as IT Systems and Security Analyst ■ Take CompTIA Network+, Cisco Certified Networking Associate (CCNA), Cisco Certified Support Technician (CCST): Networking, CompTIA Security+, Cisco Certified Support Technician (CCST): Cybersecurity
Assessment	**CK Networking Fundamentals** credential + college credit*	**CK Cybersecurity Fundamentals** credential + college credit*		

About the Cybersecurity Pathway

Cybersecurity is a high-growth field with entry-level jobs that pay well and don't require a four-year degree. There are currently more than 500,000 open cybersecurity jobs across the country, but less than 2% of high school students have access to cybersecurity pathways.[1]

The two yearlong courses in the Career Kickstart Cybersecurity Pathway—first **Cybersecurity 1: Networking Fundamentals** and then the **Cybersecurity 2: Cybersecurity Fundamentals** course—are designed to provide students with stackable credentials that they can apply to entry-level jobs and to college, and to help connect them to jobs that provide good salaries in this in-demand, high-growth industry.

After demonstrating competency through Career Kickstart cybersecurity coursework, students have multiple options to continue their career development:

- Go directly into the workforce or secure an apprenticeship.
- Continue progress toward taking common industry certifications including CompTIA Network+, Cisco Certified Networking Associate (CCNA), Cisco Certified Support Technician (CCST): Networking, CompTIA Security+, and Cisco Certified Support Technician (CCST): Cybersecurity.
- Apply college credits to a relevant community college degree or certificate program.
- Apply college credits to a relevant four-year degree.

Several early-career jobs associated with the cybersecurity pathway do not require a college degree and pay median salaries in the range of $62,000 to $137,000, including:[2]

- Cloud Architect
- Cyber Crime Investigator
- Cyber Defense Incident Responder
- Cyber Ops Planner
- System Testing and Evaluation Specialist
- Systems Administrator
- Vulnerability Assessment Analyst

SOURCES

1 **Cyberseek.org**, "Cybersecurity Supply/Demand Heatmap," accessed May 27, 2024, **https://www.cyberseek.org/heatmap.html**
2 **Cyber.org**, "Cyber Career Profiles," accessed May 27, 2024, **https://cyber.org/career-exploration/cyber-career-profiles**.

Cybersecurity is essential as it touches every aspect of our digital, societal, economic, political, and physical lives. It protects systems, networks, and data ensuring confidentiality, integrity, and availability of information. By securing these areas, we maintain the safety, trust, and integrity of our interconnected world.

Career Kickstart Cybersecurity offers students the foundational knowledge and a head start for a wide range of in-demand career opportunities in the cybersecurity field, a competitive edge through industry-recognized credentials, and college credit opportunities.

— Carol Kim,
Executive Director, IBM
Career Kickstart Advisory Board Member

About the Networking Fundamentals Course

Description

This is a full-year high school course that covers the fundamentals of networking. It is equivalent to a college-level Introduction to Networking course. The course interweaves essential networking concepts with relevant, hands-on problem-solving activities to maximize students' understanding of network hardware and configuration, the use of protocols to enable reliable and accurate transmission of data between different hosts around the world, and relevant security practices that secure the transmission of data both within and between computer networks.

College Course Equivalent

Career Kickstart Networking Fundamentals is designed to be the equivalent of a 3-credit course taken in the first or second year of a college cybersecurity degree or certificate program. Developed in partnership with higher education faculty, this course meets all of the requirements necessary to earn college credit.

Certification

Career Kickstart Networking Fundamentals is designed to help students develop understanding and skills that will contribute to their ability to pass widely recognized professional cybersecurity certifications such as CompTIA Network+, Cisco Certified Networking Associate (CCNA), and Cisco Certified Support Technician (CCST): Networking.

As we attempt to better the lives of our students, Cybersecurity is a field that is here to stay and will help provide our students with upward mobility opportunities, create new opportunities for generational wealth, change their families' lives, and help improve their communities.

— **Dr. Diego Tibaquirá,**
Professor at Miami Dade College
Career Kickstart Advisory Board Member

Course at a Glance—
Networking Fundamentals

	Unit	Topics
UNIT 1	**Introduction to Cybersecurity and Networking**	■ Introduction to Cybersecurity ■ Personal Digital Security ■ Enterprise Security ■ Introduction to Computer Systems ■ Introduction to Command Line ■ Introduction to Networks ■ SOHO vs. Enterprise Networks
UNIT 2	**Layers, Protocols, and Addressing**	■ OSI and TCP/IP Models ■ Introduction to Protocols and Servers ■ Cabling ■ Network Topologies ■ Physical Addressing ■ Logical Addressing ■ IP Configuration
UNIT 3	**Configuring a LAN**	■ Switching ■ Switch Security ■ More on Protocols ■ LAN Configuration and Troubleshooting
UNIT 4	**Advanced LAN Topics**	■ IPv4 Addressing ■ Routing ■ Subnetting ■ Wireless Networks ■ Network Troubleshooting
UNIT 5	**Network Security**	■ Introduction to Security Controls ■ Physical and Administrative Controls ■ Technical Controls: Firewalls ■ Technical Controls: Network Segmentation ■ Technical Controls: Network Monitoring ■ Defense in Depth

CYBERSECURITY 1
Technical Skills

EXPLAIN NETWORKING AND CYBERSECURITY CONCEPTS

1. Describe and explain concepts and processes related to data, computer networking, and cybersecurity.
2. Explain relationships among data, computer networking, and cybersecurity.

DESIGN A SECURE NETWORK

1. Determine appropriate endpoints, network appliances, transmission media and communication protocols to meet network requirements.
2. Determine security controls that address potential vulnerabilities.

CONFIGURE A SECURE NETWORK

1. Connect and configure network components using appropriate media, communication protocols, and commands.
2. est network connectivity, verify network requirements, and troubleshoot network issues.
3. Create technical documentation of network layouts, settings, and configurations.

CYBERSECURITY 1
Professional Skills

COMMUNICATION

Communicate technical information to both technical and nontechnical audiences.

1. Identify the purpose of communication.
2. Synthesize relevant information from multiple sources.
3. Distill, tailor, and contextualize content for a specific audience or setting (e.g., verbal, written, or presentation form).

PROBLEM SOLVING

Use methodology to solve complex problems.

1. Identify/define the problem.
2. Identify and evaluate potential root cause(s).
3. Identify and evaluate potential solutions.
4. Implement and justify a best solution.
5. Evaluate the outcome of the solution and iterate, if necessary.
6. Document and reflect upon the process and outcome.

COLLABORATION

Effectively collaborate with a team to meet a shared goal.

1. Use strategies to build trust and rapport with members of the team.
2. Develop clear, shared team objectives.
3. Define clear roles and responsibilities for members of the team.
4. Use strategies to resolve conflicts and differences of opinions among team members.
5. Follow through on agreed upon deliverables.

CYBERSECURITY 1
Course Pacing Summary by Unit

UNIT	UNIT NAME	MIN TOTAL	MAX TOTAL
1	Introduction to Cybersecurity and Networking	22	30
2	Layers, Protocols, and Addressing	18	31
3	Configuring a LAN	14	21
4	Advanced LAN Topics	21	28
5	Network Security	17	30
	TOTAL	**92**	**140**

Networking Fundamentals Materials List

Required

Computers with internet access and an installed network simulator like Cisco Packet Tracer.

Suggested

- Computer hardware exploration (Topic 1.4)
- Basic desktop PCs (for assembly/disassembly)
- Basic PC toolkit (screwdrivers, etc.)
- Desktops with the ability to run virtual machines (e.g., with Virtual Box; could also be done using a cyber range like the range provided by **Cyber.org**)
- SOHO network setup (Topic 1.6)
- SOHO router
- Ethernet cables
- Computer capable of providing basic network services (e.g., FTP, DHCP, HTTP/HTTPS and website hosting, etc.)
- Hardware examples: Raspberry Pis, decommissioned district IT hardware, desktop PCs, etc.
- Computers that can run packet sniffing software (e.g., Wireshark)
- Cable construction tools (Topic 2.3):
  - Box of 5e and/or 6a bulk cable
  - Cable crimpers
  - RJ-45 connectors
  - Cable connectivity testers
- Basic LAN configuration and troubleshooting materials
- Small business switches (managed)
- Business routers and firewalls
- Wireless access points
- Access to a cyber range or sandbox (e.g., **Cyber.org**'s cyber range)

About the Cybersecurity Fundamentals Course

Description

Career Kickstart Cybersecurity 2: Cybersecurity Fundamentals is a full-year course covering foundational cybersecurity concepts and skills and is equivalent to a college-level Introduction to Cybersecurity course. Students will explore the current cyber threat landscape to understand the types of adversaries organizations face and the techniques adversaries use to compromise systems and data. Students will learn how vulnerabilities create risk and how organizations implement security controls to manage that risk. Topics in the course include physical, operational, application, and network security; security controls; cryptography; access control; attacks and detection; and response and recovery. Students will research emerging trends in cybersecurity and gain hands-on experience implementing security protocols.

College Course Equivalent

Career Kickstart Cybersecurity Fundamentals is designed to be the equivalent of a 3-credit course taken in the first or second year of a college cybersecurity degree or certificate program. Developed in partnership with higher education faculty, this course meets all of the requirements necessary to earn college credit.

Certification

Career Kickstart Cybersecurity Fundamentals is designed to help students develop understanding and skills that will contribute to their ability to pass widely recognized professional cybersecurity certifications such as CompTIA Security+ and Cisco Certified Support Technician (CCST): Cybersecurity.

Course at a Glance—
Cybersecurity Fundamentals

UNIT 1

Assessing Risk

- Cybersecurity Fundamentals
- Develop a Threat Model
- Conduct a Risk Assessment

UNIT 2

Configuring Security Controls

- Defense in Depth
- Physical, Administrative, and Operational Controls
- Technical Controls: Network Security
- Technical Controls: Computer Security
- Technical Controls: Access Control

UNIT 3

Encrypting Data

- Technical Controls: File Security
- Symmetric Cryptography
- Asymmetric Cryptography
- Digital Signatures and Public Key Infrastructure (PKI)

UNIT 4

Detecting Cyberattacks

- Attack Detection
- Attack Methodology
- Password Attacks
- Application Attacks
- Network Attacks

UNIT 5

Responding to Cyberattacks

- Investigation and Analysis
- Containment and Eradication
- Recovery

Technical Skills

EXPLAIN CYBERSECURITY CONCEPTS AND PROCESSES

1. Describe concepts and processes related to cybersecurity.
2. Explain concepts and processes related to cybersecurity.

HARDEN A NETWORK

1. Evaluate mitigation strategies to detect and address vulnerabilities.
2. mplement controls to strengthen the security of a computer.

INVESTIGATE A CYBERATTACK

1. Examine evidence related to a cyberattack.

Professional Skills

COMMUNICATION

Communicate technical information to both technical and nontechnical audiences.

1. Identify the purpose of communication.
2. Synthesize relevant information from multiple sources.
3. Distill, tailor, and contextualize content for a specific audience or setting (e.g., verbal, written, or presentation form).

PROBLEM SOLVING

Use methodology to solve complex problems.
Identify/define the problem.

1. Identify and evaluate potential root cause(s).
2. Identify and evaluate potential solutions.
3. Implement and justify a best solution.
4. Evaluate the outcome of the solution and iterate, if necessary.
5. Document and reflect upon the process and outcome.

COLLABORATION

Effectively collaborate with a team to meet a shared goal.

1. Use strategies to build trust and rapport with members of the team.
2. Develop clear, shared team objectives.
3. Define clear roles and responsibilities for members of the team.
4. Use strategies to resolve conflicts and differences of opinions among team members.
5. Follow through on agreed upon deliverables.

Course Pacing Summary by Unit

UNIT	UNIT NAME	MIN TOTAL	MAX TOTAL
1	Assessing Risk	21	23
2	Configuring Security Controls	34	36
3	Encrypting Data	34	36
4	Detecting Cyberattacks	13	15
5	Responding to Cyberattacks	13	15
	TOTAL	115	125

Materials

Cybersecurity 2 students just need computers with access to the internet.

Teacher Resources

Lesson Plans

In addition to the course framework, sequencing, and pacing, pilot teachers will have access to approximately two Career Kickstart–provided lesson plans per unit, including any digital resources associated with each plan (e.g., presentation slides, teacher notes, student handouts, etc.).

CYBERSECURITY 1
Sample Lessons

UNIT 1	**Paper Messages**	Use double-sided origami paper as a physical representation of the on/off states of bits to prompt students to demonstrate how information is transmitted digitally. Use the strengths and limitations of this representation to motivate the need for protocols and multiple bits in a row to represent and transmit data.
UNIT 1	**Binary Number Cards**	Students use printable base-10 (decimal) and base-2 (binary) cards to physically model a number's place value. This activity develops students' conceptual understanding of number systems and provides the basis for teaching base-16 (hexadecimal) in the next unit.
UNIT 2	**Cable Construction**	Students build their own ethernet cables to deepen their understanding that all data sent in a network eventually run through a physical cable. Students learn that the strengths and drawbacks of cables are related to the physical properties of the transmission medium.
UNIT 3	**CS Disconnected**	There's trouble in the computer lab! Using Cisco Packet Tracer, students must exercise their troubleshooting skills to identify and fix multiple connectivity issues in the lab.

For SY2025-26, Career Kickstart looks to partner with curriculum providers to build out even more high-quality instructional resources for teachers to use in the classroom..

CYBERSECURITY 2
Sample Lessons

UNIT 1

Vulnerability Testing

In a safe virtualized environment, students probe a file server for vulnerabilities using automated tools, document their findings, and present a vulnerability report suggesting mitigations for the vulnerabilities they've detected.

UNIT 3

Secure Communication

Using open-source tools, students generate asymmetric key pairs and practice using encryption and digital signature protocols to securely communicate with a classmate. Through sending and receiving messages, students gain an understanding of how encryption works to protect the contents of a message, verify the integrity of a message, and verify the source of a message.

UNIT 5

Cyber Incident Analysis

In this lesson, students role-play as cyber incident responders investigating a cybersecurity incident. Students work in teams to analyze evidence from a cybersecurity incident and determine who was responsible, how they carried out the cyberattack, and what their motivations were. Student teams practice communication by presenting their analyses to the class.

Summer Training and Professional Learning

Pilot teachers will engage in a required weeklong Summer Institute. There will be multiple dates and locations to ensure everyone can attend. This institute will prepare teachers for Day 1 of their Career Kickstart program, so they'll feel confident delivering Career Kickstart in a way that emphasizes real-world, job-related applications; problem-solving; and the development of students' technical and professional skills. Teachers will also leave the institute as part of a larger community of Career Kickstart cybersecurity educators, able to collaborate with one another throughout the year.

A high-level overview of a teacher's journey through the Summer Institute:

DAY 1 **Grounding Our Work**	**Develop** your understanding of the Career Kickstart program and your role as a pilot teacher.
DAY 2 **Building Foundations**	**Deep dive** into the course guide, sample lesson plans, and Career Kickstart pilot assessment. **Develop** skills for coaching students' professional skills.
DAY 3–4 **Building Engaging Lessons**	**Build** our engaging instructional practice: lesson planning, scaffolding strategies, and lesson delivery. **Incorporate** professional skills and career-oriented learning opportunities.
DAY 5 **Putting Theory into Practice**	**Create and share** new lesson plans to bring the course to life. **Collaborate** with others and begin planning your year.

In addition to summer training, there will be online professional learning opportunities throughout the year.

Online Teacher Community

During Career Kickstart Summer Institute, teachers will leave with at least one lesson per topic authored by the Career Kickstart pilot teacher community in the online teacher community (OTC). The OTC is a place for teachers to engage in discussions and share resources with the wider pilot teacher community.

In the future, Career Kickstart aims to develop something similar to AP Classroom, which will house additional student and teacher resources for Career Kickstart courses.

Assessment Overview

Cybersecurity 1: Networking Fundamentals and Cybersecurity 2: Cybersecurity Fundamentals will each include an exam that measures the learning objectives and skills outlined in the course frameworks. Students will receive a score for their performance on the Career Kickstart Cybersecurity Pathway exams. Just like AP, that score will range from 1–5. College Board is actively working with community colleges, four-year institutions, and technical schools to expand credit policies and ensure that Career Kickstart Cybersecurity Pathway courses set a strong foundation for student success.

More information about exam design and administration will be available by early 2025.