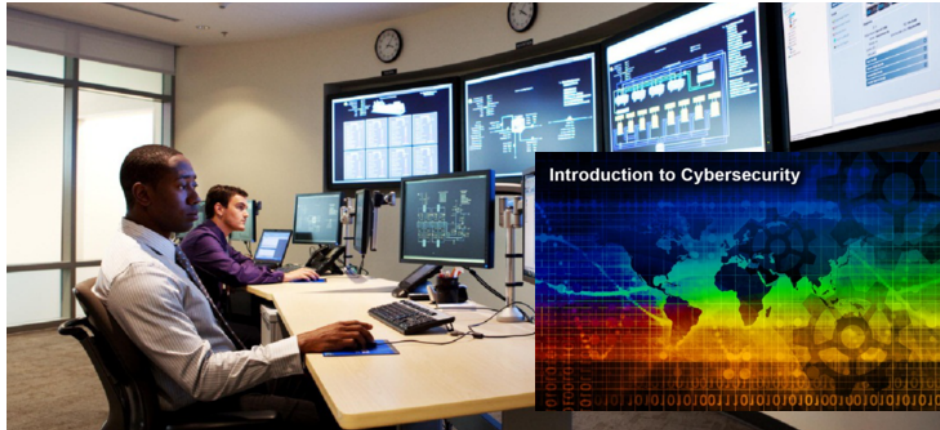


Introduction to Cybersecurity At-a-Glance



Digitization creates business value through digitized assets and expanded connectivity. But it is also increasing exposure to cyber attacks. The exponential growth of networked connections leaves data more vulnerable to attacks, creating a growing need for Cybersecurity skills and professionals.

Be Safe on Cyberspace

The Internet is a staple in many people's everyday lives. It is a great place filled with lots of information, but it is also full of dangers. Staying safe on Cyberspace is no longer an option as we have much to lose if we do not exercise caution. Introduction to Cybersecurity covers the importance of cybersecurity, awareness, data confidentiality and good practices when using the cyber space and social media. It walks students through every aspect of security in a broad, easy to understand way and explains the value of securing data, both personal and for businesses.

The course shows students the great demand for cybersecurity professionals and opportunities in pursuing a career in security.

The course modules define cybersecurity, explain why it's important, the impact of cyber attacks, and introduce the processes used to secure data.

The course offers the following:

- Interactive content
- Activities and lab exercises that reinforce learning
- Links to articles and websites to help you explore cybersecurity on your own
- Quizzes to check your understanding of the information presented

Cybersecurity Careers

Training a cybersecurity workforce is a national priority for many countries, and the demand for cybersecurity professionals is projected to rise to six millions job openings globally by 2019.

There are many opportunities for career growth in this field. As people become increasingly dependent on networks to store their personal, financial, and business data, there's greater incentive for cybercriminals to steal or manipulate that data. The world needs people who are trained to proactively mitigate and address these threats.

Introduction to Cybersecurity is delivered through the Cisco NetAcad.com learning environment. Students can self-enroll to take the course at your own pace. Instructors can enroll students and teach the course through the same process used for other NetAcad™ courses.

Module	Learning Objectives
The Need for Cybersecurity	<ul style="list-style-type: none"> • Explain the need and importance of cybersecurity. • Explain the characteristics and value of personal data, and data within an organization.
Attacks, Concepts and Techniques	<ul style="list-style-type: none"> • Recognize the characteristics and operation of a cyber attack. • Interpret the trends in the cyber threat landscape.
Protecting Your Data and Privacy	<ul style="list-style-type: none"> • Understand how to protect devices from threats. • Master how to safeguard your privacy.
Protecting the Organization	<ul style="list-style-type: none"> • Learn techniques to protect organizations from cyber attacks. • Recognize the behavior-based approach to cybersecurity. • Explain Cisco's approach to cybersecurity.
Will Your Future Be in Cybersecurity?	<ul style="list-style-type: none"> • Understand legal and ethical issues in cybersecurity. • Explain the opportunities for pursuing an education and a career in cybersecurity.

Cybersecurity Essentials At-A-Glance



Cybersecurity risks and threats are ever-present. The Internet and network infrastructures are increasingly vulnerable to a wide variety of physical and cyber attacks. Sophisticated cyber criminals and nations exploit these vulnerabilities stealing information, money, and more. These threats and vulnerabilities are fueling the growing need for skilled cybersecurity professionals.

Learn Cybersecurity Essentials Knowledge and Skills

Cybersecurity leads media headline news – “New malware steals \$4 million at U.S., Canada Banks”, “Hackers broke into hospitals despite software flaw warnings”, “Newer type of ransomware is harbinger of danger” (Source: Cisco 2016 Annual Security Report). Today, cybersecurity concerns everyone, from individuals to private business to country governments. Evolve your online safety knowledge; learn cybersecurity skills and choose a career in cybersecurity.

The Cybersecurity Essentials course covers foundational knowledge in all aspects of security in the cyber world, including information security, systems security, network security, mobile security, physical security, ethics and laws. It builds students' skills in

related technologies, procedures, defense and mitigation techniques used in protecting businesses.

The 30 hour course offers the following:

- Interactive, multimedia content
- Activities, lab exercises, Cisco Packet Tracer activities that reinforce learning
- Links to articles and websites for enhanced learning on specific topics
- Quizzes and exams to check students' understanding of the information covered

Cybersecurity Careers

Training a cybersecurity workforce is a national priority for most countries, with a demand for cybersecurity professionals projected to rise to six millions job openings globally by 2019.

There are many opportunities for career growth in this field. As people become increasingly dependent on networks to store their personal, financial, and business data, there's greater incentive for cyber criminals to steal, manipulate, and monetize that data. The world needs specialists to proactively defend and address these threats.

Cybersecurity Essentials is delivered through the Cisco NetAcad.com learning environment. Students can enroll into the self-paced course to take at their own pace or find an academy where instructors enroll students into the course and teach the through the same process used for other Cisco Networking Academy™ courses.

Module	Learning Objectives
Cybersecurity – A World of Wizards, Heros and Criminals	<ul style="list-style-type: none"> • Describe the cybersecurity world, criminals, and professionals . • Compare how cybersecurity threats affect individuals, business and countries. • Explain the structure and efforts committed to expanding the security workforce.
The Cybersecurity Sorcery Cube	<ul style="list-style-type: none"> • Explain the three dimensions of the McCumber Cube. • Detail the ISO cybersecurity model. • Explain the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
Cybersecurity Threats,	<ul style="list-style-type: none"> • Describe tactics, techniques and procedures used by

Module	Learning Objectives
Vulnerabilities, and Attacks	<ul style="list-style-type: none"> cyber criminals. Explain the types of malware, malicious code and social engineering.
The Art of Protecting Secrets	<ul style="list-style-type: none"> Outline technologies, products and procedures used to protect confidentiality. Explain encryption techniques and access control techniques. Present concepts of obscuring data.
The Art of Ensuring Integrity	<ul style="list-style-type: none"> Explain technologies, products and procedures used to ensure integrity. Detail the purpose of digital signatures and certificates. Explain the need for database integrity enforcement.
The Realm of Five Nines	<ul style="list-style-type: none"> Explain the concepts of five nines. Name the technologies, products, and procedures used to provide high availability. Represent how incident response plan and disaster recovery planning improves high availability and business continuity.
Fortifying the Kingdom	<ul style="list-style-type: none"> Describe system, servers and data protection Explain network infrastructure and end device protection Detail physical security measures used to protect network equipment
Joining the Order of Cybersecurity Specialists	<ul style="list-style-type: none"> Discuss cybersecurity domains and controls Explain ethics and cybersecurity laws. Name the cybersecurity tools. Explain how to become a cybersecurity professional.