# Module 2

This Module will help you understand **ethics in the digital world** and **societal issues related to computing**. You will learn about **the impact of computers on society and the various computer careers available** in the here and now. You will also explore the need and the implementation of **information security**, and much more.

**Module Sections**

* 1. Computer Ethics
	2. Computers in Society
	3. Computer Security

# 2.1 Computer Ethics

According to Dictionary.com, ethics is “a system of moral principles” which leads us to the understanding that computer ethics would be the system of moral principles regarding all aspects of computing.

The Ten Commandments of Computer Ethics

by the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

There really is no universal standard set by one entity regarding computer ethics. There are several professional societies that have created some basic computer ethics guidelines. **Research and review the following entities and their specific computer ethics guidelines. Pay special attention to any similarities and/or differences between them.**

**Association for Computing Machinery (ACM)**

 ACM Code of Ethics and Professional Conduct

**Australian Computer Society (ACS)**

 ACS Code of Ethics

 ACS Code of Professional Conduct

**British Computer Society (BCS)**

 BCS Code of Conduct

 Code of Good Practice

**Institute of Electrical and Electronics Engineers (IEEE)**

 IEEE Code of Ethics

 IEEE Code of Conduct

**Information Technology Alliance (ITA)**

Code of Professional Conduct

**League of Professional System Administrators (LOPSA)**

 The System Administrators' Code of Ethics

Under the umbrella of computer ethics, a person could easily parse out subcategories such as Internet Ethics, Cyber Ethics, E-Commerce Ethics, Web Ethics, Business Computer Ethics, and Consumer Computer Ethics. **Consider each subcategory and devise an ethical scenario that fits each one of the categories. Write these down! You will need them later!**

Watch the video to view more. Think about this question: Can a computer be ethical or is only the end-user responsible for the practice of ethics?

Digital ethics and the future of humans in a connected world



Direct video URL: <https://youtu.be/bZn0IfOb61U>

Video length: 19:52

# 2.2 Computers in Society

Computers have inarguably made our lives easier yet there have been a few drawbacks as well. Think about things like privacy, communication, fraud, bullying, addiction, health, and employment opportunities before and after computers. How has the mass implementation of technology affected these topics? Are there solutions to these issues?

Review the videos and article links below while considering these questions.



Direct video URL: <https://youtu.be/tvbU00dpnlg>

Video length: 14:58

**What Are the Benefits of Computers in Society?**

<https://tinyurl.com/yy4fvzby>

**Disadvantages of Computers in Society**

<https://tinyurl.com/y3z8tmzf>

**The Impact of Computers on Employment**

<https://tinyurl.com/y5j989n8>

**15 of the most promising jobs in the US in 2019, according to LinkedIn**

<https://tinyurl.com/yadkdrht>

**The 25 most in-demand technical skills of 2019, according to LinkedIn**

<https://tinyurl.com/yypx2zle>

# 2.3 Computer Security

According to Dictionary.com, security is defined as the precautions taken to guard against crime, attack, sabotage, espionage, etc. Therefore, computer security would be the precautions taken to guard computers and our digital environments. The current buzzword for computer security is cybersecurity and before that it was information security, but sometimes terms are not appropriately interchangeable.

Let’s begin with information security. According to the SANS institute (SysAdmin, Audit, Network and Security), information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. In the simplest terms, this means that a locked door to a file room with both paper and electronic files is considered information security.

Cybersecurity is a more defined subset of information security. According to National Institute of Standards and Technology (NIST), a unit of the U.S. Commerce Department, cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (the assurance that a sender cannot deny authenticity). Nowadays we have separate focus on different types of information and a much stronger focus on electronic information.

Check out this article for a more in-depth explanation the watch the videos below for a better understanding of these concepts:

**Cybersecurity vs. Network Security vs. Information Security**

<https://tinyurl.com/ya4n3atg>



Direct video URL: <https://www.youtube.com/watch?v=d30n-YxOHo4>

Video length: 22:17



Direct video URL: <https://www.youtube.com/watch?v=ooJSgsB5fIE>

Video length: 19:08

For in-depth coverage of Cybersecurity, complete the tutorial below.

<https://www.javatpoint.com/cyber-security-tutorial>

These tutorials are provided by [JavaTpoint](https://www.javatpoint.com/) and cover the following topics.

1. What is Cyber Security
2. Cyber Security History
3. Cyber Security Goals
4. Types of Cyber Attacks
5. Types of Cyber Attackers
6. Cyber Security Principles
7. Data Security Considerations
8. Cyber Security Technology
9. Threats to E-Commerce
10. Cyber Security Policies
11. Cyber Security Standards
12. Digital Signature
13. Cyber Security Tools
14. Cyber Security Challenges
15. Security Risk Analysis

To navigate through the tutorial, click the green “next” button located both at the top and at the bottom of each page.

# Module 2 Project

The goal of this project is to improve on your IoT concept using your new knowledge. Reflect on your Module 1 Project. Now that you have a frame of reference for the concepts of computers in society, computer ethics, and computer security, you will need to apply that frame to your Module 1 Project.

1. Consider your IoT concept and devices and run every aspect of it through each of the ten commandments of computer ethics. Are there violations? How can you fix the violations? Write your findings out in well-formed paragraphs.
2. Use the scenarios you devised in section 2.1 and apply those to your IoT concept. Scope each scenario to fit your IoT concept and devices if possible. Are there potential ethical conflicts in each scenario? What are they and how can they be circumvented? Write your findings out in well-formed paragraphs.
3. Now apply what you have learned regarding computer security to your IoT concept and devices. What are the potential risks? How can they be mitigated or avoided altogether? Write your findings out in well-formed paragraphs.
4. Post your responses to items one through three in well-formed sentences and paragraphs in the appropriate discussion forum.
5. **You must also provide respectful feedback to at least two (2) other students’ posts. This includes identifying what you may see as errors or maybe other conflicts or risks that you see. Compliments are also always welcome however; all comments are to be at least two complete sentences and contain more than phrases such as “I agree.”**