

How to Study for Cyber Security Courses

Cyber security is an exciting and lucrative field for professionals, and job openings are growing fast.<https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1> As a cyber security specialist,...

Method 1 of 5:

Earning an MTA Security Fundamentals Certificate

- 1. Register for Microsoft Exam 98-367.** The Microsoft Technology Associate Security Fundamentals Certificate is a basic, introductory certification to enter cyber security. It measures basic knowledge of the field. Passing the exam is rarely enough to get a job on its own, but it helps increase your credentials and overall knowledge.^[2]
 1. There are no prerequisites for this exam and it's popular with high school seniors and early college students who are interested in cyber security. Mid-career professionals can also take it if they want to make a career change.
 2. The exam currently costs \$127. It's given online.
- 2. Get hands-on experience using the Windows operating system.** The MTA test runs on the latest version of Windows. The best way to prepare for this is use Windows in your everyday life. Learn the main features of the operating system. Pay particular attention to its security features, like the firewall and antivirus settings.^[3]
 1. The test currently runs on Windows 10. When Microsoft releases a new version, the test will probably update to reflect that, so stay on top of new developments.
 2. If you use an Apple product, you can download a Windows for Mac package and run it to practice.
- 3. Learn the physical security measures that computers use.** Physical security measures are the most basic types of protection for computers. They include desktop passwords, removable discs, and on-site sign-in procedures. These are generally more secure than wireless measures because they're less likely to get hacked.^[4]
 1. Also understand the advantages and disadvantages of physical security. For example, removable discs are more secure than cloud storage, but they could be lost or damaged.
 2. Physical security measures make up 25-30% of the MTA exam.
- 4. Study basic wireless and web security measures.** Wireless and web security measures protect a computer when it's connected to a network. They try to prevent outside hacking and viruses from entering the system. Security specialists usually become experts in wireless security, so pay attention to these different systems.^[5]
 1. Typical wireless security measures are firewalls, encrypted web browsers, secure websites, and site monitoring.
 2. You don't need to understand how to build or maintain these systems at this point. Just understand how they work and prevent unauthorized access to networks.
- 5. Understand the pros and cons of physical and wireless security.** Most networks use a combination of physical and wireless security measures. Study the basic differences between the two types, and what the

advantages and disadvantages of each one are. [6]

1. Also understand the purpose of using each security type. Each serves a specific function, and you'll be well-prepared for the test if you
 2. Remember that in most cases, neither security type is superior. It takes a combination to prevent hacks and unauthorized access.
6. **Study typical types of malware and what they do.** Malware is an umbrella term for viruses and other malicious programs that could enter networks without permission. Identifying different types of malware makes up a portion of the MTA exam, so review them and understand how they affect networks. Also get a basic understanding of how to counter these threats, although countermeasures only make up a small part of this exam.[7]
1. Common malware types are viruses, spyware, ransomware, and trojans. There are others as well, but there are the basic types that you'll probably encounter on this exam.
 2. Preventing malware from entering a network is one of the main functions of security specialists. Start early and learn as much as you can about these programs and their countermeasures to prepare yourself for a security career.

Method 2 of 5:

Gaining Skills for Intermediate Certifications

1. **Look for certificate programs from CISCO or CompTIA.** Both companies offer a range of certifications from beginner to advanced, and employers recognize their credentials. Find tests that measure beginner or intermediate skills to bolster your resume and earn more experience.[8]
 1. For beginner or intermediate certifications, look for CompTIA's Network+ or Security+ exam, or CISCO's CCNA exam. These are all inexpensive and give you solid qualifications for cyber security jobs.



Identify all the potential threats a network might face. As a cyber security specialist, you'll be expected to understand and counter threats to a network. Most tests and certifications will probably include a few questions on specific threats, so review any of these programs you've covered in the unit. Make sure you can differentiate between different threats and can define each one.[9]

1. Understand the differences between spyware, malware, ransomware, worms, Trojan horses, phishing, and other data attacked. Each has a specific meaning and countermeasure.
2. Also memorize the countermeasures for each threat. Even if this isn't on the exam, knowing this information will help you on the job.
3. **Learn the differences between typical operating systems.** Security specialists need to understand the different operating systems a computer might use to protect them. Certification tests will probably ask you the differences between these systems. Different operating systems use different interfaces, firewalls, antivirus applications, and other security measures. Learn the security measures that the common operating systems use so you can maintain different computers.^[10]
 1. Basic pre-loaded operating systems are Windows, macOS, and Linux.
 2. Mobile devices use different operating systems as well. If you think that you may have to work with these devices at some point in your career, learn about these operating systems as well.
 3. If you want to get a good grasp of how operating system work, you can download them onto your computer and use them regularly. This may cost some money, but you'll get very good at understanding the distinctions between operating systems.
4. **Practice installing different types of security software.** Network administrator exams usually require you to know which software to install for ideal security and how to install it. For example, tests may give you a particular situation and ask which antivirus software would be best. Learn the different features of antivirus and other security software to respond effectively on the exams and on the job.^[11]
 1. Also understand which software works best with different operating systems. Malwarebytes is a good choice for Windows, but doesn't as well work with Linux, for example.
5. **Study how to set up secure user accounts.** Granting secure user access is a major part of the cyber security field. This involves setting up passwords, giving usernames, setting permissions and restrictions, and designing networks to work with different devices. More advanced certifications will you're your knowledge of account setup, so begin reviewing these concepts as soon as possible for an advantage.^[12]
 1. Using two-factor authentication is a newer security measure that's making systems much harder to hack. Learn how to set this up and administer the network.
 2. Remember to set secure password guidelines. You can set up a system to reject easy or obvious passwords for more security. You can also require users to change their passwords after a set amount of time to keep hackers guessing.

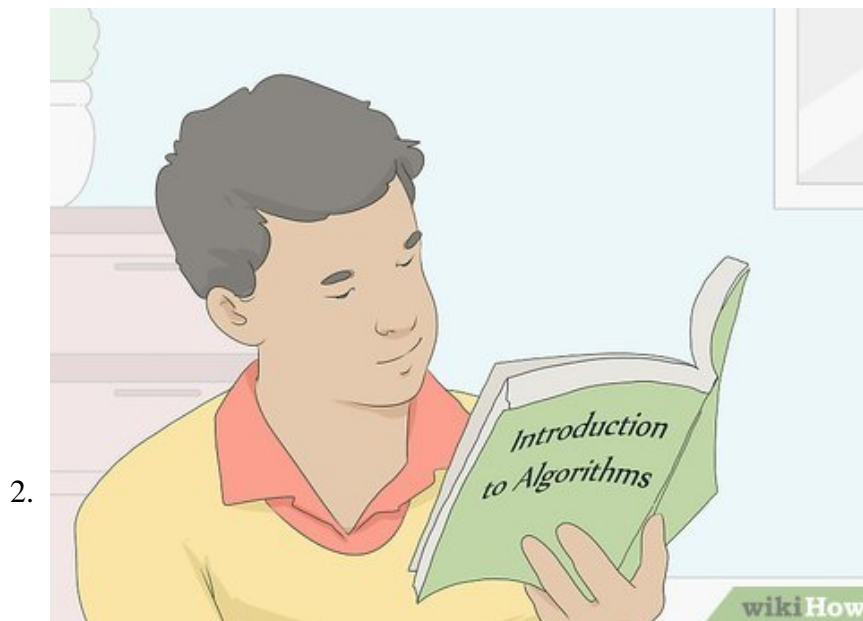
Method 3 of 5:

Identifying Key Concepts to Study



Memorize the key vocabulary so you don't get confused. There are many terms in computer science and security that you'll need to know for almost any test. Usually, your textbook introduces these keywords at the start of the book or chapter beginnings. Review and memorize these terms so you can effectively understand what test questions are asking you.^[13]

1. The specific words will depend on the class and topic you're studying, but some important terms are malware, spyware, network map, firewall, breach, worm, Trojan horse, and phishing.
2. If you're rusty on vocabulary, try checking the first few chapters of your textbook and seeing the terms that were introduced early on. These are probably important for the rest of the semester.
3. Flashcards are very helpful for working on vocabulary. Write the words on the front and definitions on the back, then quiz yourself whenever you have free time.



Review basic algorithms and how to use them. No matter what the topic, algorithms are almost always part of computer science tests. Usually, different topics have a few baseline formulas that you'll use

repeatedly throughout the course. Make note of these a review them so you know how to properly apply them during your exam.^[14]

1. The particular algorithms depend on what course this is. A basic security class might have a few encryption algorithms, while a more advanced class might have data breach algorithms. Keep up with all your work to know which formulas you need.



Practice encryption methods and codes. If you're a more advanced student, you may be taking classes on encrypting networks. This means embedding a code that potential hackers can't get around. If you've reached this point, review encryption concepts from your classwork and practice building encryption codes.^[15]

1. Encryption is an active process, so the exam may be on a computer or module rather than a written test. The grade will measure how secure your code is.
2. Building an encryption usually requires a knowledge of algorithms, so review these concepts if you're having trouble.

4.



Do practice problems from your class and homework. The best preparation for cyber security exams is practice with applying key concepts. Find blank problems in your textbook or worksheets and make a list. Solve them using the concepts you've learned in class. Then, review all the problems and correct any that you got wrong.^[16]

1. If you get any problems wrong, make sure to speak with your teacher about finding the right answer.
2. Ask your teacher for practice problems if you've run out or don't have any.
3. There are also practice problem sets for different topics online, but make sure these problems are consistent with what you've learned in class. If you do problems that are different from your class material, you risk teaching yourself the wrong material.

Method 4 of 5:

Building Additional Skills

1.



Study basic coding to design security programs. Cyber security specialists aren't programmers, so you don't have to know how to build complex programs. However, basic coding knowledge will help you on exams and on the job. Review the coding work you did in earlier classes, or do some online programs to bring yourself up to speed.^[17]

1. If you're studying cyber security in college, then you'll probably have to take some intro computer science classes that teach coding. Use this material to help on your exams.
2. If you didn't learn coding in college, there are many books, programs, and videos online that can help you. Try checking out some of the programs that coding classes use and read them on your own.

2.



Practice applying math concepts to computer science. Math and computer science go together. Programmers and engineers use math all the time to test their programs for accuracy. Computer science majors take several foundational math courses to build a base of knowledge. Pay attention in these

courses, and review them periodically so you don't forget the key math concepts you need to succeed.^[18]

1. Math subjects most important to cyber security are graphing, probability, and rational algebra. Review these topics if you don't have a good grasp of them.
2. Save the notebooks you used in your math courses, or scan them in and make a digital database. This way, you can look up old concepts if you forget them.



Improve your data analysis skills. Cyber security specialists have to look at a large amount of data to spot potential security breaches. Get used to observing and tracking large amounts of data closely to spot potential problems. This skill will help you with your courses and in your job.^[19]

1. At a basic level, get competent with a spreadsheet program like MS Excel to work on your data collecting and analysis skills. Professionals also use more precise tools to track information.
2. Learning what normal code should look like is a good way to spot breaches and anomalies.



Be enthusiastic when you work with team members. Cyber security courses are often collaborative and have a few group assignments. Get comfortable working with people, sharing ideas, and delegating duties to multiple team members. This will make group assignments much easier and more successful.^[20]

1. Remember that group assignments help you prepare for your career. In most workplaces, you'll work with a team, so get used to working with other early on.
2. Working with a group can also make studying go easier. With a study group, you can check each other's codes and solutions and cover more material than you would alone.



Do additional studying on your own time to build your expertise. Cyber security is a dynamic field, and the classroom won't teach you everything you need to know. You can significantly increase your chances of passing exams if you build outside knowledge. Make cyber security a part of your life outside school to experience greater success.^[21]

1. Stay up-to-date on the latest software and methods available. There are many magazines or newsletters you could subscribe to that will give you updates on new developments in the field. Popular choices are Cybercrime Magazine, Cyber Defense Magazine, or CISO Mag.
2. Join groups, clubs, or online forums to become part of the security community. These groups can share information and techniques that could help you in your courses.
3. Having a high-quality computer setup at home is a big help for practicing on your own time. Malware and viruses are always updating, so a new computer and software lets you stay current on the newest developments.

Method 5 of 5:

Using Good Study Habits

1.



Review the material you learned after every class period. Computer science is a cumulative field. Everything you learn builds on something that came before it. Improve your chances of success by reviewing everything you do in class after it concludes. Reread your notes, check your homework, skim the assigned reading again, and double check everything you did so you're always prepared for an exam. [22]

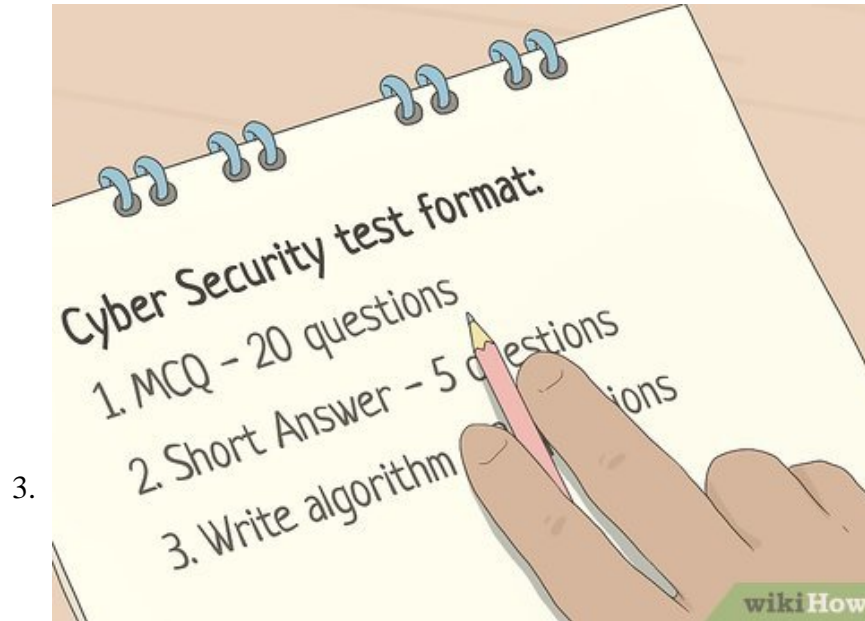
1. For cyber security courses, topics you might review are systems administration, malware, risk assessment, or data breaches.
2. This practice sets you up for success later in your career. If you just study to pass tests without learning any material, you won't be able to perform as well on the job.

2.



Complete all of your assignments to learn the material. Keeping up with your class assignments helps you learn the material more effectively. It also lets you avoid cramming for tests later on. Follow your syllabus and finish each assignment in by its due date to keep your grades up. [23]

1. If you have trouble with your assignments or get any questions wrong, make sure you speak with your teacher for clarification. That way, you'll know the material in time for the test.



Understand the material and format of the test. Before you even start studying, make sure you understand exactly what's on the test. Review any material the teacher gave you to find the important information. Make a list of the main concepts, formulas, and algorithms that you'll need to study for the exam.^[24]

1. Re-check your notes to see where you underlined or highlighted anything. This indicates it's important and will probably be on the test.
2. If you have any questions about what's on the exam, ask your teacher to explain.



Make a study schedule to avoid cramming before the test. Studying at the last minute doesn't work, especially for a field like computer security. You'll have to build a knowledge base and know how to apply it in different situations. Start studying as soon as a test is scheduled so you don't have to cram the night

before. Your grades will benefit from getting a head start.^[25]

1. The amount of time you'll need to study depends. In general, spend 5-7 days before the test studying a little every night. This spreads the work out so you won't get overwhelmed.
2. If you've kept up with your class and homework, then you've done a lot of the work already. The knowledge base you've already built will help you avoid cramming.
3. Some teachers announce all the tests at the start of the semester. In this case, you should definitely draw up a schedule to prepare for all of them ahead of time.



Make sure there is computer space available if you need the lab to study. For cyber security and computer science tests, you sometimes need the computer lab to study. This is another reason to plan ahead and start prepping early. If possible, book time in the lab so you have a spot when you need to study. Otherwise, get to the lab early or on off-hours to make sure you get a computer.^[26]

1. This isn't always applicable, and some work can be done on your own computer.

You finished reading the article "**How to Study for Cyber Security Courses**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.