



RCCS

**ROCHESTON CERTIFIED
CYBERSECURITY
SPECIALIST**

ROCHESTON[®] CERTIFIED
CYBERSECURITY SPECIALIST

ROCHESTON CERTIFIED CYBERSECURITY SPECIALIST CERTIFICATION

The Rochester Certified Cybersecurity Specialist (RCCS) certification program is designed to provide individuals with the knowledge and skills necessary to protect their organizations from cyber threats. The program consists of a series of online courses and practical exercises designed to help participants understand the fundamentals of cybersecurity and how to identify, prevent, and respond to cyber threats.

The RCCS program begins with an introduction to the fundamentals of cybersecurity. Participants learn about the different types of cyber threats, the basics of network security, and the importance of strong passwords. The course also covers basic techniques for protecting sensitive data, the different types of malware, and the basics of data encryption.

Participants then go on to develop a deeper understanding of cyber threats, learning about the different types of attack vectors, the latest tools and techniques used by cyber attackers, and the different methods used to detect and respond to cyber attacks. The course also covers the fundamentals of incident response, including how to identify and contain a breach, and how to establish a response plan.

The program also includes a comprehensive cyber security awareness training course. This course covers topics such as identifying phishing emails, avoiding social engineering attacks, understanding the implications of using public WiFi, and other security-related topics.

At the end of the program, participants complete a series of practical exercises designed to test their ability to identify and respond to cyber threats. Participants who successfully complete the program become Rocheston Certified Cybersecurity Specialists, earning a certification that is recognized by employers across the globe.

Overall, the Rocheston Certified Cybersecurity Specialist program is an excellent way to gain the skills and knowledge needed to effectively protect organizations from cyber threats. The comprehensive training provided by the program is invaluable for individuals looking to build a career in the field of cybersecurity.



WHY CYBERSECURITY IS A CHALLENGE FOR COMPANIES?

Cybersecurity is one of the greatest challenges that office users face today. With the increased use of technology in the workplace, businesses are being targeted more and more by cyber criminals. This can be particularly damaging to businesses as cyberattacks can cost them a great deal of money, cause major disruption to their operations, and potentially harm their reputation.

The threat of cybercrime is increasing all the time. Hackers are constantly developing new methods to gain access to companies' networks and data. Businesses need to be aware of the potential risks and take steps to protect their systems.

One of the main challenges that office users face is the lack of awareness about the risks of cybercrime. Employees may not be aware of the potential threats or how to protect themselves from them. Even if they are aware, they may not understand the importance of taking precautions. Without adequate security measures, companies are vulnerable to attack.

Another challenge is the sheer number of devices used in the workplace. With the rise of mobile devices, laptops, tablets and other connected devices, companies need to ensure that

their networks and data are protected from unauthorized access. It is essential to have the right security measures in place to protect all devices connected to the network.

One of the key challenges that office users face is the need to constantly update their security measures. Cybercriminals are constantly finding new ways to gain access to systems, so businesses need to make sure that they are regularly updating their security measures to ensure they remain protected.

WHY CYBERSECURITY TRAINING IS ESSENTIAL FOR EVERYONE?

Cybersecurity training is essential for all users of computers, from regular officers and employees to everyday people who use their computers for everyday activities. The internet and the use of computers and other digital systems have become integral components of our lives, so it is important that we all understand the basics of cyber security and how to protect ourselves from potential cyber attacks.

Cybersecurity training helps to ensure that users are aware of the risks associated with using computers, as well as how to properly use them and access secure networks. It also teaches users how to spot potential threats, such as malware, phishing emails and other malicious software, and what steps to take if they suspect that their systems have been compromised. Furthermore, it provides users with the skills to ensure their data and information is properly protected, and to prevent unauthorized access of their systems and data.

The importance of cyber security training cannot be overstated. Cyberattacks can cause serious damage to businesses, organizations, and individuals. By teaching users how to stay secure online, they can help protect their systems, networks, and data from potential intrusions and breaches. Cybersecurity training also helps users recognize the signs of a potential attack, and gives them the tools and resources needed to respond quickly and effectively.



WHAT WILL YOU LEARN IN RCCS TRAINING PROGRAM?

The Rochester Certified Cybersecurity Specialist (RCCS) training program is designed to provide a comprehensive overview of the fundamentals of cybersecurity. It is designed to teach participants the basic knowledge and skills necessary to protect their personal data and corporate networks from malicious cyberattacks. This training program combines lectures, hands-on exercises, and multimedia resources to provide a comprehensive education on cybersecurity best practices.

In the RCCS training program, you will learn about best practices for protecting your online accounts and data. You will learn how to recognize phishing emails, malicious websites, and other cybersecurity threats. You will also learn about how to create strong passwords, how to use two-factor authentication, and how to use encryption to protect your data.

The program is aimed at both novice and experienced users of computers, and is suitable for everyone from individuals to large corporations. It is also suitable for anyone who wants to develop their skills and knowledge in the field of cybersecurity.

The program also covers the fundamentals of cybersecurity, such as how to identify and respond to security incidents, how to create and maintain an incident response plan, and

how to use security tools to protect your data. You will also learn about the latest trends and developments in the cybersecurity industry.

At the end of the program, you will be required to take a comprehensive exam to demonstrate your understanding of the material. Upon successful completion of the exam, you will be awarded the Rocheston Certified Cybersecurity Specialist (RCCS) certification. This certification is a great addition to your resume and can help you stand out in the job market.





RCCS PROGRAM DURATION

The program is conducted over a two-day period, with the first day devoted to providing an overview of the various aspects of cybersecurity. This includes lectures on the fundamentals of network security, including an introduction to firewalls, malware, and other security threats. During this session, participants will also learn about common security practices, such as password management, backups, and data encryption.

The second day of the program focuses on the application of these concepts in a practical setting. During this session, users will develop their skills in identifying and responding to malicious activities, as well as in developing and implementing security policies. They will also gain an understanding of the various tools and technologies used to protect networks and systems, such as firewalls, intrusion detection systems, and antivirus software.

At the end of the program, participants will be given a final assessment to test their knowledge of the topics covered. Once successful, they will receive a certificate of completion that will attest to their knowledge and expertise in cybersecurity. The program is also ideal for those who wish to pursue a career in the field, as it is an excellent foundation for further education in the area.

WHO SHOULD ATTEND THE TRAINING?

The Rochester Certified Cybersecurity Specialist (RCCS) training program is essential for all users, regardless of their level of technical knowledge. By attending the program, users will gain an understanding of the risks involved with using the internet, as well as the steps they can take to protect themselves and their data. This program is also beneficial for companies that wish to improve their security posture, as it provides employees with the skills and knowledge necessary to protect their networks and systems.

At the end of the program, participants will be able to demonstrate an understanding of the latest cybersecurity practices, including how to protect user data, recognize and respond to threats, and understand the fundamentals of cyber-attack prevention and response.

YOU CAN CUSTOMIZE THE RCCS TRAINING FOR YOUR ORGANIZATION

The RCCS program is designed for both individuals and organizations, and can be tailored to meet the needs of a specific organization or user. It includes a comprehensive assessment to

evaluate the level of understanding and knowledge of each participant, as well as feedback and guidance from a professional cybersecurity trainer.

This program is ideal for those looking to stay up-to-date on the latest cyber trends and developments, as well as those who need to understand the basics of cybersecurity. It is also an excellent way to increase the knowledge and understanding of any organization's cybersecurity program.





RCCS COURSE OUTLINE

1. Module: Cyberthreats
2. Module: Cybersecurity Terminology
3. Module: Scams and Fraud
4. Module: Phishing Attacks
5. Module: Social Engineering
6. Module: Instant Messaging
7. Module: Smishing and Vishing
8. Module: Ransomware
9. Module: Search Engines
10. Module: Antivirus
11. Module: Password Managers
12. Module: 2-factor Authentication
13. Module: Web Browser Security
14. Module: Data Privacy
15. Module: Social Media Security
16. Module: Fake News
17. Module: Identity Theft
18. Module: Cyberbullying
19. Module: Encryption

- 20. Module: Windows Security
- 21. Module: macOS Security
- 22. Module: Mobile Device Security
- 23. Module: iOS Security
- 24. Module: Android Security
- 25. Module: Cloud Security
- 26. Module: GDPR
- 27. Module: VPN

RCCS EXAM INFORMATION

1. **Exam Title:** Rochester Certified Cybersecurity Specialist
2. **Exam Code:** RCT-99
3. **No. of Questions:** 50
4. **Exam Format:** Scenario Based MCQ
5. **Passing Score:** 70%
6. **Duration:** 2 hours
7. **Exam mode:** Online using Rochester Ramsys Exam Proctoring System
8. **How to register for the exam?**
Please register at <https://cert.rocheston.com>

RCCS COURSE OBJECTIVES

- Understand the different types of cyber threats that exist today, including malware, phishing, ransomware, spyware, and other malicious software.
- Identify the methods that attackers use to exploit security vulnerabilities and gain access to system resources.
- Learn how to recognize the signs of a cyber attack, including unusual traffic, slow system performance, and pop-up windows.
- Understand the importance of patch management and regular system updates to reduce the risk of cyber threats.
- Learn how to respond to a security breach and restore system integrity.
- Develop a comprehensive cybersecurity awareness training plan for an organization.
- Understand the importance of data privacy and the legal implications of a security breach.
- Appreciate the implications of cyber threats on a global scale and how they can be mitigated.
- Gain an understanding of the ethical considerations of cybersecurity and the role of the security professional.

- Understand the fundamental concepts of cybersecurity and the implications of a breach.
- Identify common cybersecurity threats and vulnerabilities.
- Understand the role of technology and security controls in preventing and mitigating cyber threats.
- Develop a strong understanding of the terminology used in the field of cybersecurity.
- Explain the importance of implementing effective security policies and practices.
- Understand the different cybersecurity roles and responsibilities.
- Recognize the importance of secure coding practices.
- Identify the different types of malware and how to protect against them.
- Implement best practices for creating and managing strong passwords.
- Recognize the role of cryptography in protecting data.
- Describe the fundamentals of network security and how to secure a network.
- Understand the legal and ethical implications of cybersecurity.
- Understand the role of IT auditing in a cybersecurity program.
- Explain the importance of developing a business continuity plan.

- Develop an understanding of the cybersecurity landscape and the tools available to security professionals.
- Understand the importance of cybersecurity awareness training and how to create an effective program.
- Learn the techniques used by cyber criminals to attract victims, including phishing and social engineering.
- Understand the different types of cyber scams and fraud, including identity theft, ransomware, and data breaches.
- Gain an understanding of the legal and ethical implications of cyber scams and fraud.
- Develop the skills necessary to recognize and respond to potential cyber scams and fraud.
- Develop an awareness of the steps necessary to protect oneself and their organizations from cyber scams and fraud.
- Learn how to respond if they or their organization become victims of cyber scams and fraud.
- Develop the skills necessary to protect their online identities and accounts.
- Understand the importance of reporting cyber scams and fraud to law enforcement and other relevant authorities.

- Understand the role of cybersecurity in defending against cyber scams and fraud.
- Become familiar with the latest tools and techniques used by criminals to perpetrate cyber scams and fraud.
- Become aware of best practices in terms of cyber security and cyber hygiene.
- Understand the different types of phishing attacks, their techniques, and the potential harm they can cause.
- Be able to recognize the signs of a phishing attack and know how to respond if they receive a suspicious email.
- Learn best practices for avoiding phishing attacks, including identifying malicious links and emails, and how to protect personal data.
- Understand the importance of reporting phishing emails and taking appropriate action.
- Develop the skills necessary to educate their colleagues on the dangers of phishing attacks and how to protect against them.
- Learn how to create a security policy for their company or organization to help protect against phishing attacks.
- Gain an understanding of the legal and ethical implications of phishing attacks and their potential to harm individuals and organizations.

- Develop an understanding of the different tools and technologies available to defend against phishing attacks.
- Develop an understanding of the different methods used by attackers to exploit users and organizations.
- Learn how to develop effective strategies to respond to and mitigate a phishing attack.
- Understand the concept of social engineering and its potential impact on organizations.
- Recognize the tactics used by social engineers to gain access to confidential information and assets.
- Identify common techniques used by social engineers, such as pretexting, phishing, and tailgating.
- Develop methods to identify and mitigate social engineering attacks.
- Learn methods of recognizing and responding to potential social engineering attacks.
- Create a plan for training and educating users on social engineering threats.
- Understand the importance of user education and security policies in preventing social engineering attacks.

- Develop an understanding of how the human factor can be leveraged to increase the security of an organization.
- Learn the techniques used by social engineers to gain access to confidential information and assets.
- Understand the role of security awareness training in preventing social engineering attacks.
- Gain an appreciation of the importance of implementing a comprehensive security strategy in order to protect against social engineering attacks.
- Develop strategies for detecting and responding to possible social engineering attacks.
- Understand the legal implications of social engineering attacks and the importance of adhering to information security policies.
- Learn how to assess the effectiveness of security policies and procedures in preventing social engineering attacks.
- Develop an understanding of the different types of social engineering attacks and their potential impacts.
- Introduce participants to the basics of Instant Messaging (IM) and its role in cyber security.

- Explain the different types of IM tools, their features and how they can be used to communicate securely.
- Teach participants the importance of creating strong passwords, setting up two-factor authentication, and other important security measures.
- Explain the different methods of encryption and how they can be used to protect IM conversations.
- Discuss the potential risks and dangers of using IM and the steps that can be taken to minimize them.
- Describe the basics of social engineering and how it can be used to target IM users.
- Show how IM can be used to communicate securely with colleagues and contacts.
- Explain the importance of using secure IM practices when communicating with customers and other third-parties.
- Teach participants how to determine when IM conversations should be kept private, and when they should be shared with others.
- Demonstrate how to use IM securely and responsibly.
- Develop an understanding of the threats of smishing and vishing in the cyber security environment.

- Learn how to identify smishing and vishing messages and recognize malicious links.
- Understand the techniques used by attackers to deceive victims via smishing and vishing messages.
- Develop an understanding of the countermeasures to protect against smishing and vishing attacks.
- Learn how to respond to smishing and vishing incidents.
- Learn how to report smishing and vishing incidents to proper authorities.
- Develop an understanding of the legal implications of smishing and vishing attacks.
- Understand the importance of user education and awareness in preventing smishing and vishing attacks.
- Develop strategies to create an effective security awareness training program.
- Learn how to use simulated smishing and vishing attacks to educate users.
- Learn how to create a culture of security awareness within an organization.
- Understand the need for ongoing security awareness training for users.
- Explain the concept of ransomware and its impact on organizations.

- Identify common types of ransomware and malicious software.
- Describe preventive measures that can be employed to reduce the risk of a ransomware attack.
- Identify the signs of a ransomware attack and the steps to take should an attack occur.
- Develop strategies for restoring systems and data in the event of a ransomware attack.
- Explain the importance of user awareness and education in protecting against ransomware.
- Analyze the current security landscape and how it affects ransomware protection.
- Identify and implement effective measures to protect against ransomware.
- Develop best practices for effective incident response in the event of a ransomware attack.
- Learn how to effectively manage and monitor ransomware detections.
- Understand the importance of developing and maintaining a secure backup strategy.
- Understand the importance of log monitoring and data integrity.
- Educate users about the risks of ransomware attacks and how to protect against them.
- Understand the importance of security controls, such as encryption and authentication.
- Utilize antivirus and anti-malware software to reduce the risk of ransomware attacks.

- Evaluate and recommend security solutions for ransomware protection.
- Demonstrate an understanding of the security risks involved in using search engines.
- Identify malicious websites, phishing scams, and other malicious content.
- Research and identify safe search engine practices to protect user data.
- Understand the importance of using secure search engines to protect personal information.
- Demonstrate how to access, use, and assess secure search engine features and settings.
- Understand the importance of using strong passwords and two-factor authentication.
- Utilize search engine privacy settings to protect personal information.
- Identify and use secure search engine tools, such as secure search and web filtering.
- Evaluate the effectiveness of secure search engine tools.
- Utilize secure search engine tools to protect private data.
- Analyze the impact of search engine usage on personal data security.
- Implement best practices for securely using search engines.
- Use secure search engine tools to protect against malicious content.
- Utilize search engine tools to investigate suspicious activity.

- Identify and secure potential risks associated with using search engines.
- Understand the importance and value of antivirus software in protecting computers, networks, and data from malicious attacks.
- Learn the different types of antivirus software and the various features and benefits of each.
- Identify the various threats posed by viruses and the need to protect against them.
- Install, configure, and manage antivirus software to ensure optimal protection.
- Monitor and update antivirus software regularly to ensure ongoing protection.
- Understand the importance of user education in recognizing malicious threats and protecting against them.
- Analyze threats and respond to them appropriately.
- Understand the importance of regular virus scans and the need for manual intervention to ensure optimal protection.
- Develop and implement policies and procedures for antivirus software use and maintenance.
- Learn how to create and implement an effective antivirus management plan.
- Understand the basic principles and benefits of using a password manager in cybersecurity.

- Learn how to set up and use a password manager for both personal and business use.
- Develop an understanding of why passwords are such an important part of cybersecurity.
- Learn about the different types of password managers available and the features that make them effective.
- Develop strategies for creating and managing strong passwords.
- Understand the importance of using unique passwords for each online account.
- Learn how to securely store and share passwords with others.
- Understand the risks associated with weak passwords and how to protect yourself against them.
- Develop the ability to recognize phishing and other social engineering attacks.
- Learn how to use two-factor authentication (2FA) to further secure online accounts.
- Understand the need to regularly update passwords and other credentials.
- Develop the ability to recognize and respond to suspicious activity on online accounts.
- Learn how to securely back up and restore passwords.
- Understand the importance of using secure protocols when accessing online accounts.

- Learn best practices for using a password manager in the workplace.
- Understand the concept of two-factor authentication and its importance in cybersecurity awareness.
- Learn how two-factor authentication works and identify common methods of two-factor authentication.
- Identify the benefits of two-factor authentication and how it can improve security.
- Learn about different types of two-factor authentication, including SMS, biometrics, and hardware tokens.
- Understand the different methods of implementing two-factor authentication and the security considerations associated with each.
- Analyze the vulnerabilities of two-factor authentication and identify best practices for securing user accounts.
- Understand the guidelines for implementing two-factor authentication in the workplace.
- Identify strategies for educating users on the importance of two-factor authentication and its security benefits.
- Assess the usability and user experience of two-factor authentication systems.

- Discuss the legal aspects of two-factor authentication and how it can be used to comply with data privacy regulations.
- Introduce students to the concept of web browser security and explain its importance in the context of cybersecurity awareness.
- Educate students on the potential threats that can arise from inadequate web browser security.
- Discuss the various tools and features available to enhance web browser security such as browser extensions, two-factor authentication, password managers, etc.
- Demonstrate the different settings and configurations that can be used to improve web browser security.
- Show how to properly configure web browsers to ensure that they are up-to-date with the latest security updates and patches.
- Explain the different methods of malware detection and removal and how to use them to protect web browsers.
- Introduce students to the different types of malicious code and discuss how to identify and remove them.

- Demonstrate the secure browsing habits that should be adopted to protect web browsers from potential security threats.
- Explain the importance of using encrypted connections when browsing the web and demonstrate the different methods of setting up encryption.
- Teach students to recognize phishing attempts and other social engineering attacks and how to avoid them.
- Show how to properly configure web browsers to block malicious websites and downloads.
- Educate students on the different ways to deploy secure web browsers and the implications of their use in a corporate environment.
- Demonstrate how to use a virtual private network (VPN) to protect web browsers from malicious activity.
- Discuss the importance of using strong passwords and two-factor authentication when accessing web applications and websites.
- Explain the importance of using browser sandboxing to protect web browsers from malicious code.
- Provide guidance on how to detect and respond to malicious activity on web browsers.

- Provide an understanding of the various data privacy laws and regulations that apply to organizations and how to comply with them.
- Educate participants on the importance of protecting personal data, as well as the potential repercussions of failing to do so.
- Develop an understanding of the security risks associated with the use of social media platforms.
- Identify potential threats and vulnerabilities related to social media usage.
- Develop an awareness of the importance of maintaining a secure online presence.
- Learn how to protect personal and corporate data from malicious actors.
- Understand the legal and ethical implications of using social media.
- Develop the skills needed to securely navigate social media platforms.
- Learn best practices for creating and managing secure social media accounts.
- Recognize and respond quickly to potential security threats.
- Develop an understanding of the security implications of sharing sensitive content on social media.
- Learn how to create secure passwords and employ two-factor authentication.

- Develop an understanding of the potential impact of malicious content on social media.
- Comprehend the importance of monitoring social media accounts regularly.
- Learn how to identify and report suspicious activity on social media.
- Develop an understanding of how to protect data from unauthorized access.
- Understand the implications of data privacy and protection laws.
- Develop an understanding of the types of Fake News and its impact on society.
- Identify the motivations behind Fake News and how it is spread.
- Understand the techniques used to create Fake News and how to spot it.
- Learn about the legal implications of Fake News and how to protect against it.
- Understand the importance of fact-checking and developing critical thinking skills when consuming media.
- Recognize the potential consequences of spreading Fake News and how to avoid it.
- Explore the ethical implications of Fake News and its effects on society.
- Develop strategies to counter Fake News, including identifying and reporting it.
- Discover the potential for using technology to combat Fake News.

- Understand the importance of media literacy and how to be a responsible consumer of information.
- Educate participants on the growing threat of identity theft and the importance of being aware of the risks.
- Provide an overview of the types of identity theft, such as online, financial, and medical identity theft.
- Provide an understanding of the methods criminals use to gain access to personal information, such as phishing and malware.
- Explain the legal and financial implications of identity theft and the steps that can be taken to protect oneself.
- Equip participants with the knowledge needed to recognize potential red flags, such as suspicious emails or websites.
- Help participants understand the importance of using strong passwords and other strategies for staying secure online.
- Discuss the importance of monitoring activity related to one's personal information, such as credit card statements.

- Provide guidance on how to respond to a suspected case of identity theft, such as alerting the authorities and financial institutions.
- Demonstrate how to prevent identity theft by using secure networks, practicing good online safety habits, and being aware of the latest scams.
- Highlight the resources available to those affected by identity theft, such as credit monitoring services and identity theft protection plans.
- Develop a comprehensive understanding of the causes, effects, and social implications of cyberbullying.
- Explain the legal ramifications of cyberbullying and the consequences of engaging in such behavior.
- Identify the signs and symptoms of cyberbullying.
- Understand the psychological and emotional impact of cyberbullying on both the victim and the offender.
- Examine best practices for responding to and preventing cyberbullying.
- Explore effective strategies for addressing cyberbullying in school and workplace settings.
- Learn how to create an effective cyberbullying policy for an organization.

- Develop skills for effective communication with parents, teachers, administrators, and other stakeholders regarding cyberbullying.
- Review the various resources and services available to help those affected by cyberbullying.
- Examine the role of technology in facilitating cyberbullying and learn how to use technology safely and responsibly.
- Provide a comprehensive overview of encryption and its role in cybersecurity awareness.
- Explain the different types of encryption and how they are used to protect data.
- Discuss the importance of encryption in protecting data and networks from unauthorized access.
- Explain the importance of encryption for secure communication and data storage.
- Discuss the legal and ethical considerations of encryption and its implications for privacy and security.
- Provide an understanding of the best practices for using encryption to protect data.
- Identify the various tools and technologies available for implementing encryption.
- Understand the fundamentals of encryption and its role in cybersecurity.
- Learn the different types of encryption and their implementations.

- Recognize the importance of encryption in protecting data and systems.
- Understand the principles of public-key and symmetric-key cryptography.
- Learn how to use cryptography to protect data in transit and at rest.
- Learn how to use encryption to protect emails, messages, and other forms of communication.
- Learn how to use encryption to authenticate users and verify identities.
- Understand the security features available in Windows 10 and how to use them to protect data and systems from malicious attacks.
- Explain the importance of patching and patch management in Windows 11.
- Describe the various types of malware and how to identify and eliminate them.
- Explain network security principles and how they apply to Windows 11 systems.
- Outline the security principles of authentication and authorization and how they apply to Windows 10 systems.
- Demonstrate how to implement user access controls in Windows 11.
- Describe how to use the Windows Firewall to protect data and systems.

- Explain the benefits of using virtual private networks (VPNs) for secure remote access.
- Demonstrate how to configure and manage Windows Defender to detect and eliminate malicious threats.
- Explain the importance of data backup and recovery and how to back up data in Windows 11.
- Describe the role of intrusion detection and prevention systems (IDPS) in Windows 11.
- Outline the steps to respond to security incidents and breaches and how to recover from them.
- Introduce participants to the fundamentals of cybersecurity and its relevance in the macOS environment.
- Explain the importance of following best practices to secure macOS from malicious threats and attacks.
- Identify the various security policies, protocols, and tools available for macOS security.
- Demonstrate how to configure and use macOS built-in security features.
- Explain how to secure network connections and data transmissions in the macOS environment.

- Show how to use macOS tools to monitor system activity and detect suspicious activity.
- Discuss how to respond to security incidents and apply appropriate countermeasures.
- Explain the importance of regularly patching the system and keeping it up-to-date.
- Explore the use of third-party security products and services to enhance macOS security.
- Demonstrate how to create a secure backup and recovery plan for macOS systems.
- Understand the different types of mobile devices, including smartphones, tablets, and laptops.
-
- Identify the security risks associated with using mobile devices and the steps needed to secure them.
- Be aware of the common threats posed to mobile devices, such as malware, phishing, and data loss.
- Learn the best practices for securing mobile devices, such as using strong passwords, enabling encryption, and installing antivirus software.
- Understand the importance of keeping mobile devices updated with the latest security patches.

- Recognize the importance of using secure networks when accessing the internet.
- Learn how to protect sensitive data stored on mobile devices.
- Know how to respond to a mobile device security breach.
- Understand the implications of using mobile devices for work purposes.
- Understand the basics of iOS security, including the hardware and software security features and how to use them to increase security.
- Learn about the different threats and vulnerabilities to iOS devices, such as malicious applications, jailbreaking and data theft.
- Recognize the different types of attacks and methods used to exploit iOS devices.
- Understand the different security measures available to protect iOS devices and how to implement them.
- Explore best practices for setting up and managing mobile device security policies.
- Learn how to identify and remediate security issues on iOS devices.
- Understand the importance of device and data encryption and the methods available for achieving it.

- Gain an understanding of the importance of patch management and the tools available to manage patches.
- Learn how to secure wireless networks used by iOS devices and how to configure them for optimal security.
- Understand the different types of access control measures available for iOS devices and how to configure them.
- Learn about the different authentication methods available for iOS devices and how to configure them.
- Understand the importance of mobile device management (MDM) and how to configure it for iOS devices.
- Gain an understanding of the different types of malware and how to detect and mitigate them.
- Develop an understanding of the Android platform, its associated security concerns, and the techniques used to protect it.
- Learn about the Android security architecture and the various layers of protection it provides.
- Learn to identify potential security vulnerabilities and how to mitigate them.

- Understand the security implications of various Android versions, devices, and applications.
- Gain an understanding of the various security measures and tools available to secure Android devices.
- Develop an awareness of the security threats associated with cloud computing and the potential impact of a breach.
- Understand the importance of following best practices for securing cloud accounts, such as using strong passwords and two factor authentication.
- Learn how to manage, monitor and audit cloud security.
- Understand the role of encryption and key management in cloud security.
- Understand the basic principles of GDPR and how it affects organisations
- Understand the importance of data protection and privacy considerations when handling personal data
- Develop an understanding of the rights of individuals and their rights to privacy
- Develop an understanding of the legal framework and principles of GDPR

- Understand the implications of GDPR for organisations, such as data protection, data breach notifications and data retention requirements
- Introduce participants to the basic concepts of Virtual Private Network (VPN) technology, its purpose, and how it works.
- Demonstrate the importance of using a VPN to protect privacy and secure data while online.
- Show participants how to set up a VPN and manage it securely.
- Explain the potential risks associated with not using a VPN, such as data theft, identity theft, and malicious attacks.
- Educate participants on the different types of VPNs and the benefits of each.
- Demonstrate how to configure and use a VPN to access resources securely.
- Explain the implications of using a VPN for corporate and personal networks.
- Teach participants how to use a VPN to increase their security and privacy online.
- CASE STUDIES

Copyright 2023 Rocheston. All rights reserved.

Rocheston® is a registered trademark of Rocheston in the United States and/or other countries.