ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

Certified by Rocheston®

RCCS® Certification Program Guide

ROCHESTON

NEW YORK

DISTINGUISHED

About Rocheston

Rocheston, a young New York based internet technology start-up, despite being in its nascent stage, is a company that is raring to go. Rocheston has a worldwide presence, with its headquarters in New York. The company's technology development center is based out of Chennai, with reach offices in Singapore and Dubai.

The team at Rocheston consists of young, liberal, innovative and forward-thinking individuals **who want to make a difference and change the world. At its core, Rocheston is a next-generation innovation company**, with cutting-edge research and development in emerging technologies such as Cybersecurity, Internet of Things, Big Data and automation.

Rocheston Certified Cybersecurity Specialist (RCCS)

Securityone® will primarily provide you with a working knowledge of all the fundamental threats to cybersecurity in our everyday life, and how to deal with them. Every end user, that is almost every single one of us in today's world, who has a minimum digital footprint, is in need of being educated in the ways to secure their devices and systems.

Within the next few years, the **Cybersecurity** Specialist will become one of the most coveted positions in every organization, small or big, in every corner of the world. Our course is designed to meet the needs of this highly sought after job position, and to give individuals lacking technical expertise a solid foundation on cybersecurity.

ROCHESTON®

Current Market Trends in Cybersecurity

In the parlance of the dark web, attackers these days want to 'own' your entire system.

- Tom Kellermann, Carbon Black's Chief Cybersecurity Officer

- Fifty six percent incident response partners have faced attempted counter-incidents in the **first quarter of 2019.**
- **42% of employers** are worried they won't be able to find the talent they need.
- Approximately **three quarters (72.8%)** are struggling to find relevant candidates.
- **86% of the most qualified candidates** for your open positions are already employed and not actively seeking a new job.
- **40 % of employees surveyed** said they plan on changing jobs in 2019

Rocheston is a global leader in the cybersecurity space, setting benchmark standards and becoming torchbearers in a domain that is beyond a doubt, **the greatest challenge across industries in 2019.**

An authority in **cybersecurity, Rocheston leads the way, inspiring others to appreciate and understand the importance of training and certification in best practices in cybersecurity**, to address the need of the hour.

ROCHESTON®

What will you learn from RCCS Training?

ROCHESTON® CERTIFIED CYBERSECURITY SPECIALIST

- Identify the challenges
- Safeguard a company's/individual's privacy
- Save time, energy and money
- Be less anxious
- Become an expert yourself
- Defeat a threat

ROCHESTON®

Identify the challenges

First and foremost, of course, know the challenges in the cyber environment. Since every individual today, whether a school student or an office employee, or even a homemaker, is knee-deep in digitization, it is vital that all of us should at least possess basic awareness and knowledge to keep our systems and ourselves safe.

Safeguard a company's/individual's privacy

Being aware of the potential threats and knowing how to address them will add a layer of protection to the company's as well as the individual's data.

Save time, energy and money

Every attack on an organization's digital identity costs them valuable time and effort to respond to the breaches and of course, leads to heavy financial losses. Training in cybersecurity will help the organization keep their money, and be more productive.

Be less anxious

Institutions and companies can be less anxious about confidential data being breached, thus keeping customers happy and the company safe.

Become an expert yourself

The user no longer has to rely solely on technical expertise, but can enforce basic security controls without having to wait for support. The course will help regular people handle their digital footprint securely.

Defeat a threat

Regulate the threats and ensure that the system is not exposed to further risks. Learn the different ways and techniques to overcome threats and address the loopholes.

A cybersecurity specialist program will teach you to safeguard privacy

- Identify the threats in your environment that could be detrimental to cybersecurity
- Note if the threat is coming from users and human error
- Try to identify how, if at all, users are creating IT risks
- What are the potential vulnerabilities in your system and how can they be targeted, due to user misuse
- Note the gaps in the network
- Find ways to improve security infrastructure
- Educate your employees on the importance of cyber security

Who needs RCCS?

RCCS is for everybody! Any individual, organization, government agency, including schools and colleges, would benefit from the course. Most importantly, the course is designed for ordinary day to day users who do not have the advantage of specialized technical knowledge, i.e. for the rest of us.

The RCCS will primarily provide you with a working knowledge of all the fundamental threats to cybersecurity in our everyday life, and how to deal with them. Every end user, that is almost every single one of us in today's world, who has a minimum digital footprint, is in need of being educated in the ways to secure their devices and systems.

Join us:

Our endeavor is to enable a cyber secure life for everyone.

ROCHESTON®

Why RCCS?

The **RCCS course will provide you with credible recognition as a Cybersecurity Specialist.** Best practices in next generation cybersecurity would make the Cybersecurity Specialist the most coveted officer in all majorenterprises in the next few years.

Not only that, the course would be ideal even for **non-technical people, and for day to day activities ranging from that of school students and housewives, to front end users at offices and overall everyday users of digital technology who need to have their data protected.**

RCCS enables you to gain better control over your own devices and data, and puts you in a better position to face the challenges to cybersecurity

Target Audience

Securityone® is for everybody!

- Any individual, organization, government agency, from school students to homemakers
- Representatives from school and college administration
- Technically and non-technically inclined people
- Front office users
- Everyday users of digital technology

ROCHESTON®

Eligibility

The student should have passed their 10+2 exams, or the equivalent of the same, preferably in the science stream. Other backgrounds, for instance, arts and commerce, are also eligible to apply.

What the course will consist of:

- A 2-day Training Program
- Time: 9:30 AM – 6 PM
- The provision of an active web portal
- Seminars conducted by qualified engineers
- Best in-class environment

Cost

For pricing in your region, please contact the local distributor.

RCCS Exam

- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.
- Multiple Choice Objective Questions
- Total count - approximately 90 questions
- Pass Percentage: 72%
- Retake Policy - You may retake the exam any time on an additional fee. For further details contact the exam coordinator.

The Cyberclass Web Portal

The access to an online e-learning platform will be given to attendants on registration. It will contain a series of study videos, pre-recorded lectures, white papers, educational animations and power point presentations. The Web Portal can be used to catch-up on a missed session or to view an attended session again.

http://cyberclass.rocheston.com

ROCHESTON®

Course Completion

- On completing the course and successfully passing the exam, the candidate will be provided with a RCCS certification.
- Candidates are free to use the logo as per the Terms & Conditions as a Rocheston Certified Professional.
- The candidate will also receive a Welcome Kit and login information to access the Members' Portal.
- The Members' Portal is an online forum for Certified RCCSs to interact.
- The certification is valid for two years and it can be renewed online.
- Contact the course coordinator for any enquiries about the renewal fee or downloading of the updated course material.

Course Objectives

In the RCCS program you will learn:

- Gain credible recognition as a Cybersecurity Specialist
- Best practices in fundamentals of cybersecurity
- Better control over your own devices and data
- Better privacy and security of personal information
- Best strategies to ensure secure payments on e-platforms
- Secure social media usage

Course Outline

Module 1: Securing Data and Privacy

- Macro and Micro Impact of Privacy Breach
- Policy Development and Privacy Management
- How to block a number on iOS and Android
- Setting up VPN for a smart TV
- Sharing VPN on Windows and OS X
- Going Incognito
- Securing online bank transactions

Module 2: How to Avoid Getting Scammed Online

- What are scams?
- What is online fraud?
- Types of Online Scams
- What to Keep in Mind to Avoid Getting Scammed
- How to Spot Online Fraud/Scam
- How to Prevent Getting Scammed
- What is Spoofing?

- Internal social engineering
- Internal online fraud protection
- Phishing protection
- Malicious antivirus identification
- Malware protection
- Malicious software scenario policies
- Verification standards for information seekers

Module 3: Securing Networks

- Securing Organizational Networks
- Securing Passwords
- Securing the Network
- Securing Wifi
- Securing sensitive data
- Updates and patches
- Internal update practices
- Third Party app update practices
- Update rollout
- Securing browsing
- Securing files
- File upload and sharing practices
- Securing remote access

Module 4: Securing Websites

- Authentication and cryptography
- Potential Threats
- How to secure websites
- Securing public web servers
- Training and development for web security
- Security management practices
- Standardized software configurations
- Server configuration
- Securing web server operations
- Securing Web Server Application
- Securing content

Module 5: Securing Emails

- Email security
- Email encryption
- Spam filter practices
- Responsible internal email usage
- Sensitive information sharing practices
- Retention policy
- Email usage policy

Module 6: Securing Mobile Devices

- Vulnerabilities in smartphone devices
- Cyber Threats to mobile devices
- Best practices for securing mobile devices
- Software security
- Effective Mobile Device Management
- What to do if mobile device is stolen or lost

Module 7: Securing Employees

- Background check policy in recruitment
- Background check policy for vendor and partners
- Access control
- What is a Human Firewall?
- Training employees in cybersecurity
- Sensitive information

Module 8: Securing Operations

- Security policy
- Identifying critical information
- Analyzing information
- Analyzing vulnerabilities
- Identifying potential exploitations
- Other steps to successfully implement OPSEC

Module 9: Securing Payments

- Securing customer payment
- Data storage policy
- Security tools and resources
- Access controls
- Security basics

Module 10: Incident Response and Reporting: A Guideline

- What is an incident?
- Types of breaches
- Physical breaches
- Network breaches

- Data breaches
- Incidence response
- Reporting an incident

Module 11: Social Media: Policy Development and Management

- Security roles and responsibilities
- Internal internet usage
- Social media policy

Module 12: Cybersecurity Basics

- Anti-Virus Software
- Application
- Authentication
- Authorization
- Backdoor
- Backup
- Bandwidth
- Blacklisting Software
- Brute Force Attack
- Clear Desk Policy
- Clear Screen Policy

- Cookie
- Cyberbullying
- Cybersecurity
- Cyber Threats
- Denial of Service Attack
- Dictionary Attack
- Digital Certificate
- Domain Hijacking
- Domain Name System (DNS)
- Dumpster Diving
- Electronic Infections
- Encryption
- End User License Agreement (EULA)
- File-Sharing Programs
- Firewall
- Flooding
- Grooming
- Hacker
- HTTPS
- Firewall
- Flooding
- Grooming
- Hacking

- HTTPS
- Hybrid Attack
- Instant Messaging (IM)
- IP (Internet Protocol) Address
- Internet Service Provider (ISP)
- Keystroke Logger
- Malware
- Man-In-the-Middle Attack
- Monitoring Software
- Network
- Operating System (OS)
- Password
- Password Cracking
- Password Sniffing
- Patch
- Peer-to-Peer (P2P) Programs
- Phishing
- Router
- Script
- Shoulder Surfing
- Skimming
- Sniffing
- Social Engineering

ROCHESTON