BASIC UNDERSTANDING OF CYBER SECURITY FOR SHIP OPERATIONS – UG LEVEL

Micro Credit Course
on
Basic Understanding of Cyber Security for Ship Operation
Indian Maritime University Navi-Mumbai Campus
T.S. Chanakya, Navi-Mumbai.

Developed by Capt. Mihir Chandra, ASP, SNS

BASIC UNDERSTANDING OF CYBER SECURITY FOR SHIP OPERATIONS – UG LEVEL

Course Information

Course	BASIC UNDERSTANDING OF CYBER THREATS AND SECURITY FOR SHIP OPERATIONS
Academic year	DNS / BSc
Credit	1- [15 HRS]

Lecturer(s)

Lecturer

Coordinator

Contact

General Learning Objectives [GLOs]

* 1. Introduction to Cyber Security
* 2. Awareness of various types of attacks and management
* 3. Dangers associated with cyberattacks
* 4. Case Study
* 5. Presentation by students

Specific Learning Objectives (SLO)

Upon completion of the course, students should be able to:

1.1 Acknowledge cybersecurity awareness,
1.2 Know National cybersecurity policy 2013,
1.3 Understand National Cyber Safety and Security Standards,
1.4 Learn about the National Cyber Defence Research Centre & Information Technology Act.

2.1 Cybersecurity and safety management
2.2 Ransomware, Malware, viruses and spyware, identification of theft and compromise of classified data
2.3 Dangers associated with emails - Phishing
2.4 Risks regarding removable media - USB stick dangers
2.5 File sharing and copyright issues

3.1 Dangers of unsecured wireless networks
3.2 Risks of social networking
3.3 Unauthorized system access
3.4 Characteristics of a strong password

4.1 Case study and presentation on cybersecurity incidents and framework

BASIC UNDERSTANDING OF CYBER SECURITY FOR SHIP OPERATIONS – UG LEVEL

Content Synopsis

Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security.

It is important because the government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing business, and cybersecurity describes the discipline dedicated to protecting that information and the systems used to process or store it.

The most difficult challenge in cybersecurity is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cybersecurity resources on perimeter security to protect only their most crucial system components and defend against known threats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cybersecurity. Shipping Industry is much more demanding and is a means to last end connectivity for stakeholders with digital, automated and innovative advancements.

Therefore awareness of cybersecurity is a clarion call and IMO has rightly put great emphasis on industry to derive mechanism and adopt a policy for the cyber-safe industry.

Course Delivery	Lecture Tutorial
Instructional method	Guided Self-Study

Course Assessments	Projects/Tests (30%)	
	--------→	Total 40% FORMATIVE-'F'
[Weightage]→	Presentations (10%)	

End course SUMMATIVE 'S' ASSESSMENT- Total weightage 60%

GRAND TOTAL- 100%

Suggested Literature - Appendix-I

Mandatory - Appendix - II

BASIC UNDERSTANDING OF CYBER SECURITY FOR SHIP OPERATIONS – UG LEVEL

Notes:

- Attendance can be through direct contact or online mode.
- Course attendance (100%) has to be completed within the stipulated time.
- Attendance to be maintained by Student & Lecturer.
- Students are encouraged to attend equivalent Courses (e.g., NPTEL; Swayam; AICTE; Coursera; etc.) for their benefit.

Timetable

Hours		Type	Topic	Reading(s)	Remarks
Week 1					
2		Lecture	GLO UNIT-1 &2	APPENDIX II	
2		Tutorial	GLO UNIT 2	APPENDIX I	
1 to 2		Presentations /Questions	GLO UNIT1-2		
Week 2					
2		Lecture	GLO UNIT 2-3	APPENDIX II	
2		Tutorial	GLO UNIT3	APPENDIX I	
1 to 2		Presentations /Questions	GLO UNIT 3		
Week 3					
2		Lecture	GLO UNIT 4		
2		Tutorial	REVISION UNITS-1-2-3-4		
1 to 2		Presentations /Questions	GLO UNIT 4		
Week 4					
		Assessments: Presentations /Project work			

Appendix-I

Suggested Literature

Part-A: MOOCs

1. Computer Science and Engineering - NOC: Introduction to Information Security I
2. Cyber Security Fundamentals - Rochester Institute of Technology
3. Cyber Security Basics - IBM
4. Cyber Security Basics: A Hands-on Approach - Universidad Carlos III de Madrid

Part-B: YouTube

1. https://www.youtube.com/watch?v=inWWhr5tnEA&list=PLEiEAq2VkUUJfPOj5nRounXvf3n17PCft
2. Cyber Security Full Course for Beginner
3. Cyber Security Training for Beginners

Part-C: Additional Links

1. What are malware, viruses, Spyware, and cookies, and what differentiates them? | DigiCert
2. Can PDF files be dangerous? Protect your email!
3. What's the risk in downloading a .pdf from a phishing email? - Information Security Stack Exchange
4. Dangers of Opening Unknown Email Attachments
5. Computer Security - Terminologies
6. NATIONAL CYBER SAFETY AND SECURITY STANDARDS(NCSSS) || NATIONAL CYBER DEFENCE RESEARCH CENTRE(NCDRC) - ncdrc.res.in
7. Cyber Crime Case Studies Ahmedabad:: Cyber Fraud In India
8. Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - Media, Telecoms, IT, Entertainment - India
9. National Cyber Security Policy 2013

Appendix-II

Mandatory

Part-A: Policy & Laws

1. National Cyber Security Policy - 2013.pdf
2. National Cyber Security Strategy 2020 DSCI submission.pdf
3. National Cyber Crime Reference Handbook.pdf
4. FVFv
5. VvVd

Part-B: Case Study

6. SHIP-SECURITY-BRIDGE-VULNERABILITY-STUDY.pdf
7. Cyprus-Shipping-Chamber-Cyber-Security-Case-Study.pdf
8. Ship security challenges in high-risk areas.pdf
9. Case Studies in Cyber Supply Chain Risk Management.pdf
10. Risk-based ship security analysis - an approach based on civilian and military methods.pdf
11. PORT SECURITY-Threats and Vulnerabilities.pdf
12. The Guidelines on Cyber Security Onboard Ships-2021-version-4.pdf

Part-C: Books

13. Cyber Security Book.pdf
14. Cybersecurity Best Practices Guide.pdf
15. Dangers Phishing Avoid Lure Cybercrime ebook.pdf

Part-D:

16. Email Security: An Overview of Threats and Safeguards.pdf
17. Risk Management of Email and Internet Use in the Workplace.pdf
18. Internet spam threats and email exploitation - A scuffle with inbox attack.pdf
19. Copyright Infringement due to Online File Sharing.pdf
20. The Dark Sides of Social Networking Sites: Understanding Phishing risks.pdf
21. Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques.pdf
22. Public Wi-Fi Security risks.pdf
23. Security Issues in Wireless Systems.pdf
24. Peer-to-Peer File Sharing and Copyright Law: A Primer for Developers.pdf
25. Copyright, Intellectual Property, and Illegal File-Sharing.pdf
26. Cyber Security Awareness Booklet for Citizens.pdf