INTRODUCTION TO ORGANIZATIONAL CYBER RESILIENCE MANAGEMENT

INTRODUCTION TO CYBERSECURITY SUPPORT IN ORGANIZATIONS

EVERYDAY CYBERSECURITY IN ORGANIZATIONS

MORE INFORMATION
http://cs.unu.edu
This workshop aims to provide managers and directors of third sector organizations with the basic understanding of Information and Communication Technology (ICT) management in organizations. It describes the resources, processes, roles, and responsibilities associated with effective use of ICT towards organizational goals. It introduces organizational risk management and presents frameworks to help managers understand the risks that are faced by their organizations as well as tools for managing those risks. The workshop also introduces basic ICT concepts, organizational cybersecurity threats and countermeasures, and the local cybersecurity landscape - in terms of the legalities and compliance requirements as well as key cybersecurity stakeholders.

**CONTENT OUTLINE**

**ICT Management**
- Role of ICT in organizations
- ICT roles, responsibilities, and functions
- Organizational ICT ecosystem

**Risk Management**
- Organizational resilience
- Business continuity planning
- Risk management frameworks

**Cybersecurity risks management**
- Cybersecurity goals
- Organizational cybersecurity domains
- Cybersecurity frameworks and standards
- Common cybersecurity threats, vulnerabilities, countermeasures, and impacts

**Local cybersecurity landscape**
- Legalities and compliance
- Key cybersecurity stakeholders
- Cyber threat landscape
This workshop is designed to provide a foundation understanding of information and communication technology (ICT) and the cybersecurity domains. It is targeted at non-technical personnel who are responsible for or involved in providing ICT support within the organizations. As an introductory module, it aims to equip the participants with the basic awareness of cybersecurity threats, vulnerabilities, countermeasures, and impacts. It also aims to equip the participants to be able to provide basic support within the organizations and to handle relevant incident escalation.

**CONTENT OUTLINE**

**Foundational Information Technology**

**Cybersecurity risks management**
- Cybersecurity goals
- Organizational cybersecurity domains
- Cybersecurity frameworks and standards

**Cyber threats**
- Common cybersecurity threats
- Threat actors
- Threat killchain
- Impact on organizations

**Cybersecurity countermeasures**
- Cyber resilience phases
- Proactive security
- Top organizational countermeasures

**Cybersecurity incident response**
- Local cybersecurity ecosystem and stakeholders
- Incident reporting
This workshop aims to provide basic cybersecurity awareness and understanding for individuals working within organizations. The goal of the workshop is to enhance the ability of individuals to practice good cyber hygiene and to use cyber resources safely and securely. It focuses on the interrelated areas of computer security, mobile security, web security, social media security, and data security. It will also highlight the cybersecurity role and responsibilities of individuals within organizations.

**CONTENT OUTLINE**

**Introduction to Information Technology and Cybersecurity**
- Basic IT concepts
- Cybersecurity goals
- Cybersecurity harms and impacts

**Being cyber-secure**
- Cyber threat landscape
- Technical and non-technical cyber threats
- Key countermeasures for individuals
- Cyber hygiene
- Incident handling and reporting

**Being secure at work**
- The weakest link in cybersecurity
- Individuals' roles and responsibilities
- Common policies and guidelines

**Specific cybersecurity domains**
- Computer security
- Mobile security
- Web security
- Social media security
- Data security

**Cybersecurity culture and attitudes**
"Enhancing the cyber resilience of the civil society in smart digital futures"

Smart Citizen Cyber Resilience