Cybersecurity: User Awareness

Overview course of 1 day - 7h
Ref.: SES - Price 2024: CHF950 (excl. taxes)

EDUCATIONAL OBJECTIVES

At the end of the training, the trainee will be able to:

Understand the types of IS security risks and their possible consequences

Identify measures to protect information and secure your workstation

Promote adherence to the company's IS security policy

THE PROGRAMME

last updated: 06/2022

1) Computer security: Understanding the threats and risks

- Introduction: general framework, what is meant by IT security (threats, risks, protection)?
- How can negligence create a disaster? Some examples. Responsibility.
- The components of an IS and their vulnerabilities. Client and server operating systems.
- Corporate networks (local, site-to-site, Internet access).
- Wireless networks and mobility. Applications at risk: Web, email, etc.
- Database and file system. Threats and risks.
- Sociology of hackers. Underground networks. Motivations.
- Types of risks. Cybercrime in France. Vocabulary (sniffing, spoofing, smurfing, hijacking, etc.).

2) Information protection and workstation security

- Vocabulary. Confidentiality, signature and integrity. Constraints of encryption.
- General overview of cryptographic elements. Windows, Linux or MAC OS: Which is the most secure?
- Management of sensitive data. The problem of laptops.
- What is the threat on the client workstation? What malicious code is.
- How do you deal with security breaches? The USB port. The role of the client firewall.

3) User authentication and access from outside

- Access controls: authentication and authorization.
- Why is authentication important?
- The traditional password.
- Authentication by certificates and tokens.
- Remote access via the Internet. Understanding VPNs.
- The value of strong authentication.

4) How can you get involved in IS security?

- Risk, vulnerability and threat analysis.
- Regulatory and legal constraints.
- Why does my organization need to meet these security requirements?
- Key people in security: understanding the role of the CISO and the Risk Manager.
- Acting for better security: social and legal aspects. The CNIL and legislation.
- Cyber-surveillance and privacy protection.
- The charter for the use of computer resources.
- Everyday security. The right reflexes. Execution.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

DATES

REMOTE CLASS
2024 : 05 Jul, 18 Nov