DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 3: NETWORK SECURITY

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.

EXECUTIVE SUMMARY

This module introduces network security as a fundamental part of cybersecurity and an essential competence area for VET students, educators and institutions. It explains how secure networks protect communication, data, digital services and institutional operations in increasingly connected learning environments.

The module focuses on practical understanding. Learners explore key concepts, risks, protection principles, tools and realistic scenarios that help them recognise vulnerabilities and propose basic mitigation measures.

INTRODUCTION

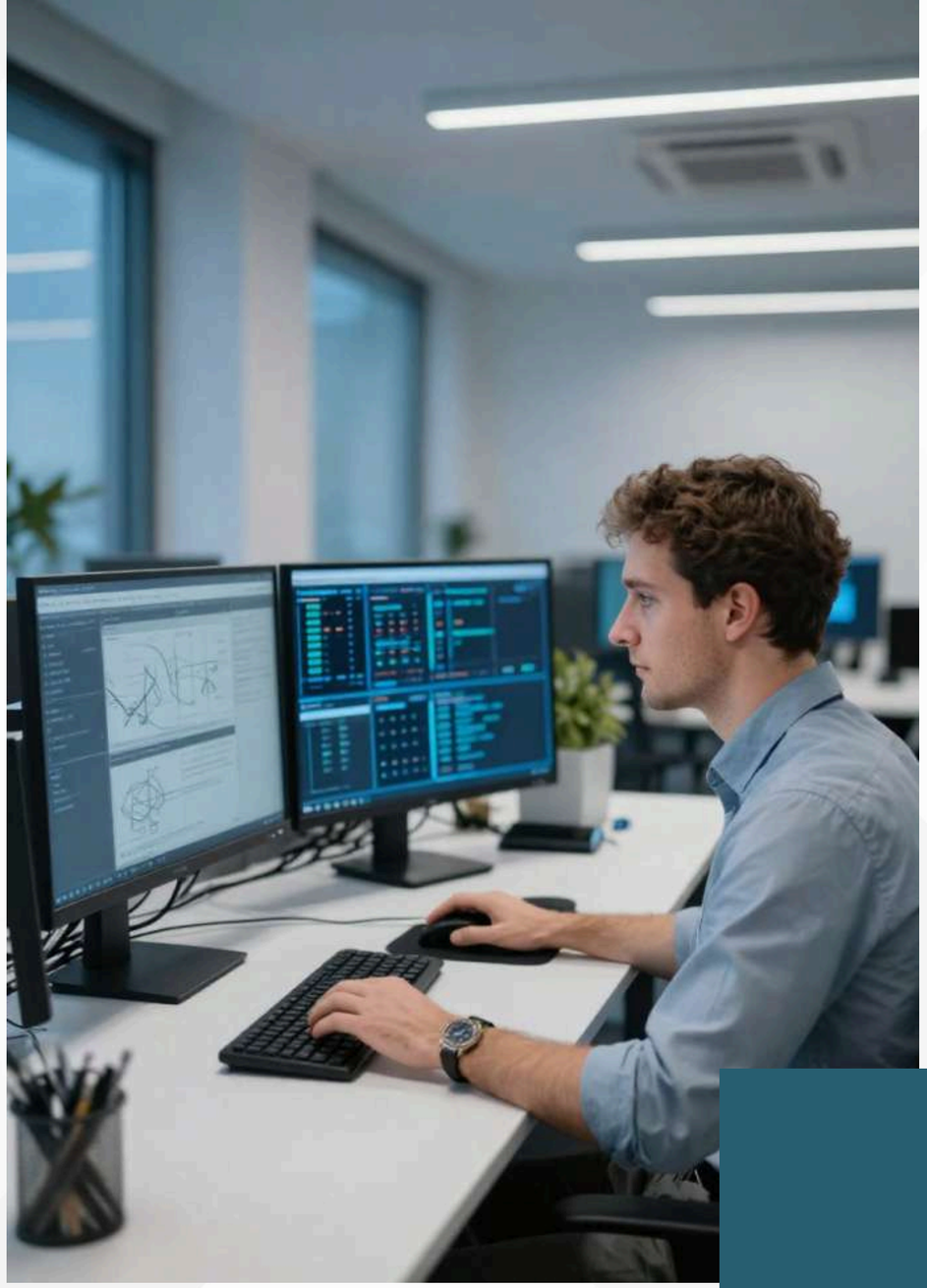
VET institutions rely on digital systems for teaching, administration, communication and cooperation. Learning platforms, Wi-Fi networks, computer laboratories, cloud services and digital registers are now part of everyday institutional work.

Because of this dependence, network security is no longer only a technical issue. It is also connected to trust, learning continuity, data protection and responsible behaviour from students, teachers and staff.

OVERVIEW

Network security refers to the tools, policies and techniques used to protect networks and the data that moves through them. It helps ensure that digital communication remains safe, reliable and available when needed.

Effective network security combines several elements: protected devices, secure software, strong access control, monitoring, clear procedures and user awareness. These elements work together to create a layered defence.



IMPORTANCE OF THE TOPIC

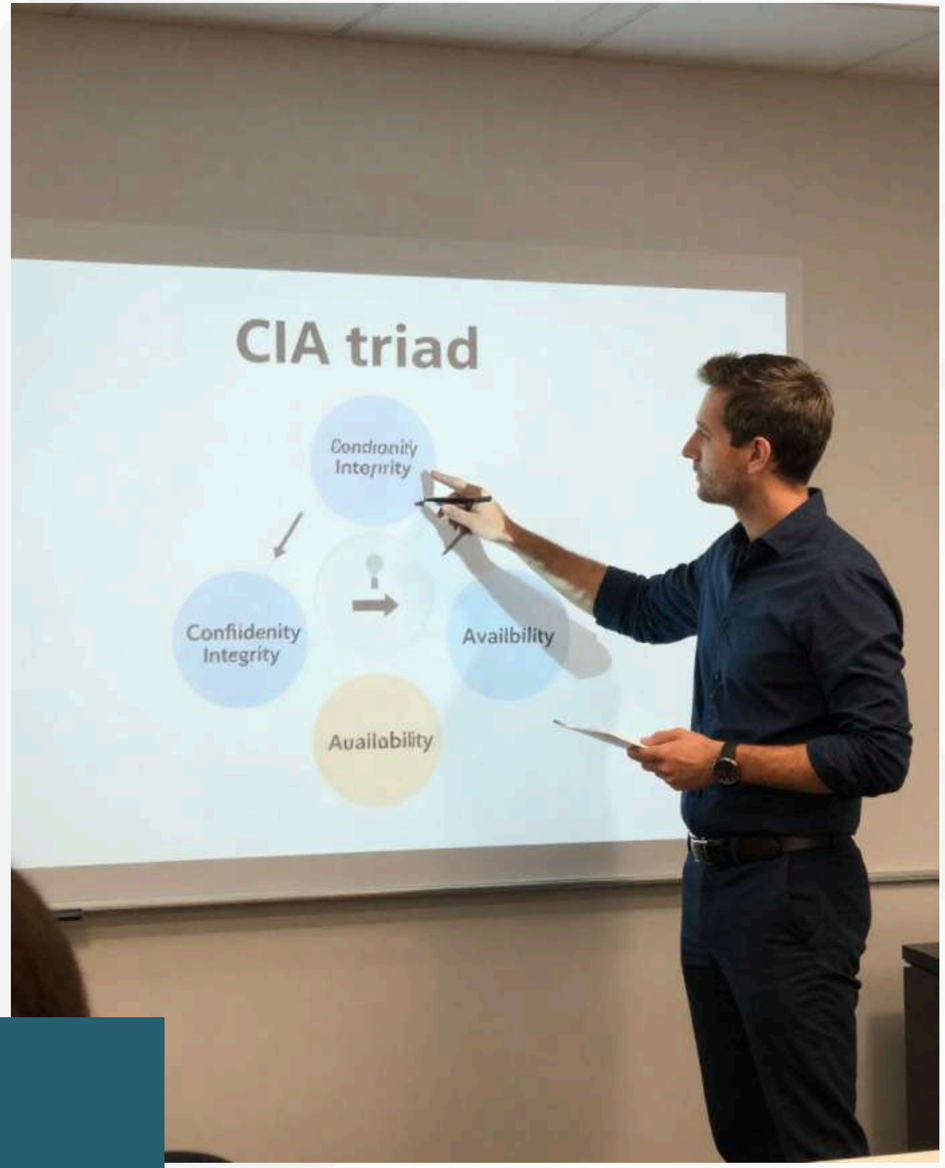
A single network weakness can create serious consequences for an educational institution. It can expose personal data, interrupt teaching, block access to learning platforms or damage the reputation of the organisation.

In the VET context, secure networks support both daily operations and practical learning. They help protect students, staff, institutional data and cooperation with external partners.

LEARNING OBJECTIVES

By the end of this module, learners should be able to:

- Explain the meaning and purpose of network security
- Identify common network threats, vulnerabilities and risks
- Understand key principles such as defence-in-depth, least privilege and segmentation
- Recognise the role of firewalls, IDS/IPS, VPNs, encryption and monitoring tools
- Analyse simple VET-based scenarios and suggest protection measures
- Understand the ethical use of network security tools



KEY CONCEPTS AND DEFINITIONS

The module introduces the basic vocabulary needed to understand network security. The most important foundation is the CIA Triad: confidentiality, integrity and availability.

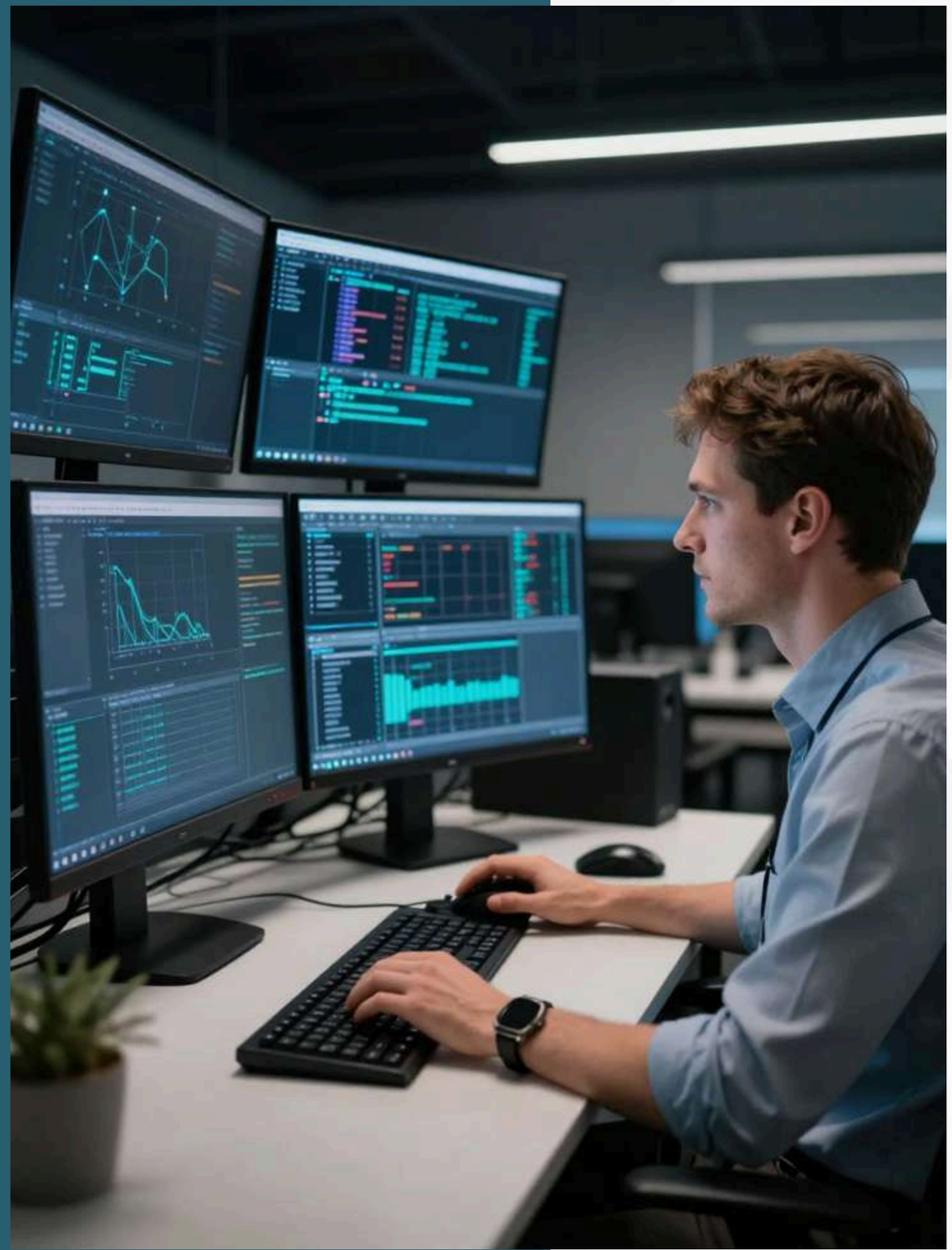
Confidentiality means that data is accessible only to authorised users. Integrity means that data remains accurate and unchanged. Availability means that systems and data are accessible when needed.

Other key terms include threat, vulnerability, risk, encryption, authentication and access control.

CONTEXT AND BACKGROUND

Educational networks have become more complex because they combine physical infrastructure, cloud platforms, remote access, personal devices and third-party services. This creates more opportunities for learning, but also more possible entry points for attackers.

In VET institutions, the risk is especially important because computer laboratories, workshops and project platforms may imitate real workplace environments. Students must therefore learn not only how networks function, but also how they can be protected responsibly.



MAIN THEMES

Network security is based on several connected themes. These themes help learners understand how different protection measures work together.

The module focuses on:

- Secure communication protocols
- Protection of routers, switches and access points
- Network segmentation and zoning
- Monitoring and detection of suspicious activity
- Incident response and resilience
- Ethical use of cybersecurity tools

CORE PRINCIPLES

A secure network is built on clear principles that guide everyday decisions. Defence-in-depth means that several layers of protection are used together, so that one failed control does not expose the whole system.

Least privilege means that users should have only the access they need for their role. Segmentation separates users, systems and services into zones, reducing the possibility that an incident spreads across the whole institution.

DEFENCE-IN-DEPTH AND LEAST PRIVILEGE

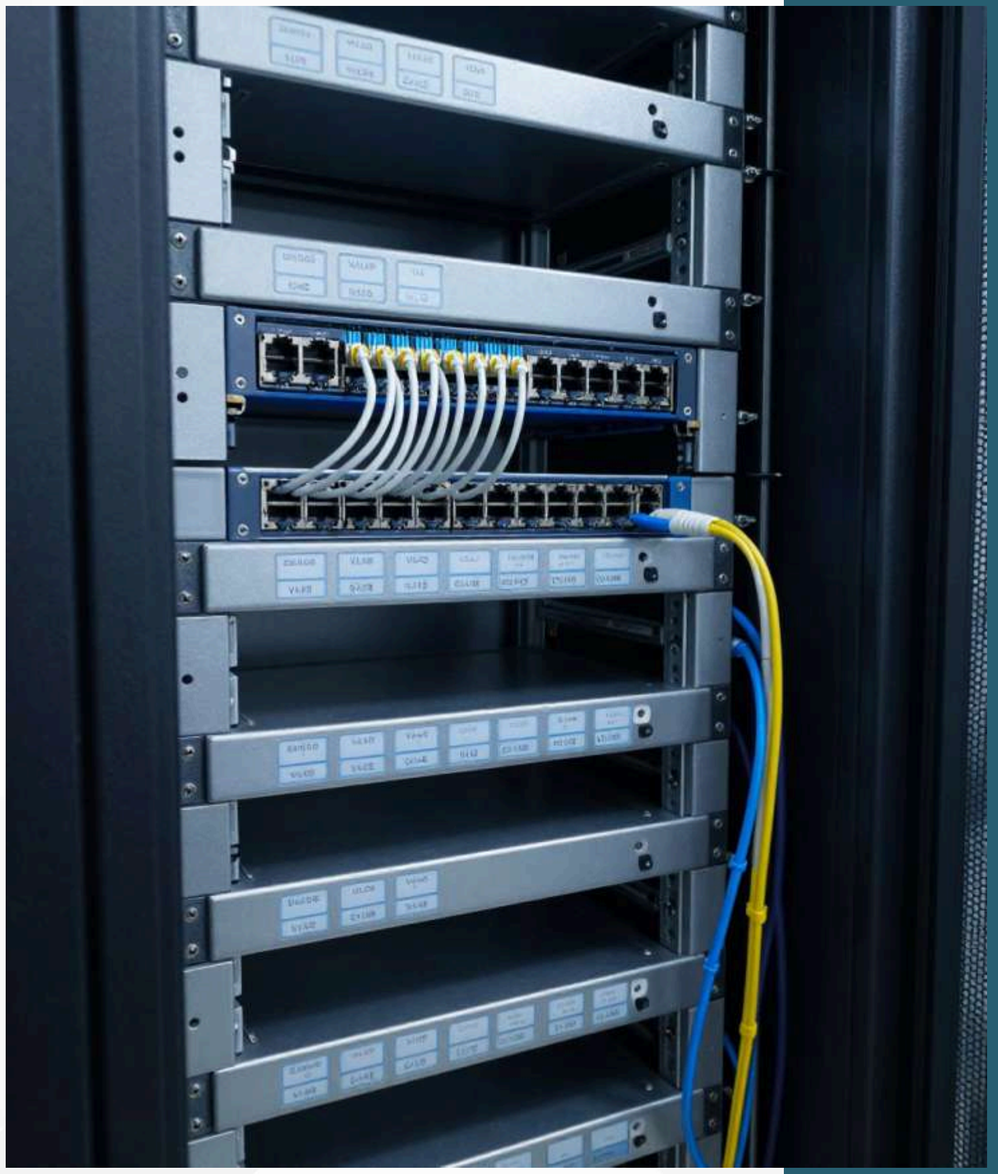
Defence-in-depth and least privilege are two of the most important principles for reducing damage. They help institutions avoid depending on one single security measure.

In a VET institution, this means that students should not access administrative systems, guest users should not reach internal servers, and administrator rights should be limited. Sensitive systems should use individual accounts and multi-factor authentication.

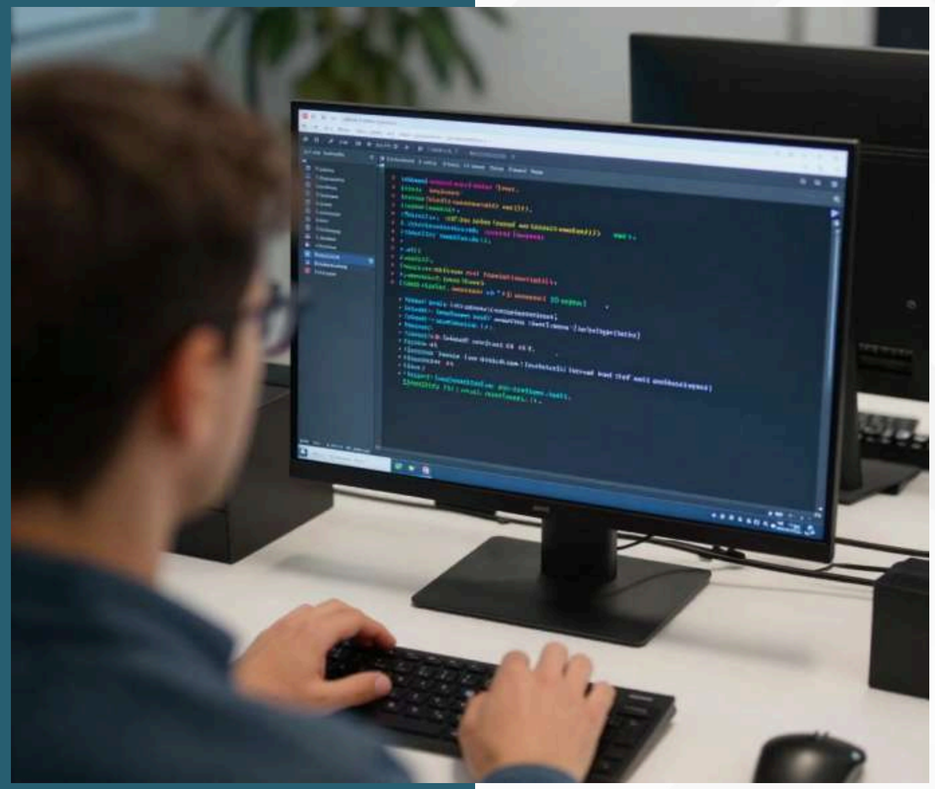
NETWORK SEGMENTATION

Network segmentation divides a network into separate zones with different access rules. This is especially useful in schools and VET centres because students, teachers, guests, administrative staff and external partners do not need the same level of access.

Possible zones include the administrative network, teacher network, student learning network, computer laboratory network, guest Wi-Fi and server or cloud access zone. Segmentation limits lateral movement if one device or account is compromised.



SECURE CONFIGURATION AND AUTHENTICATION



Many network incidents begin with simple weaknesses such as default passwords, outdated firmware, unnecessary services or shared accounts. Secure configuration helps reduce these risks from the beginning.

Important practices include changing default credentials, disabling unused services, updating devices, restricting remote administration and using secure protocols. Strong authentication and multi-factor authentication provide additional protection for sensitive systems.

MONITORING, DETECTION AND ENCRYPTION

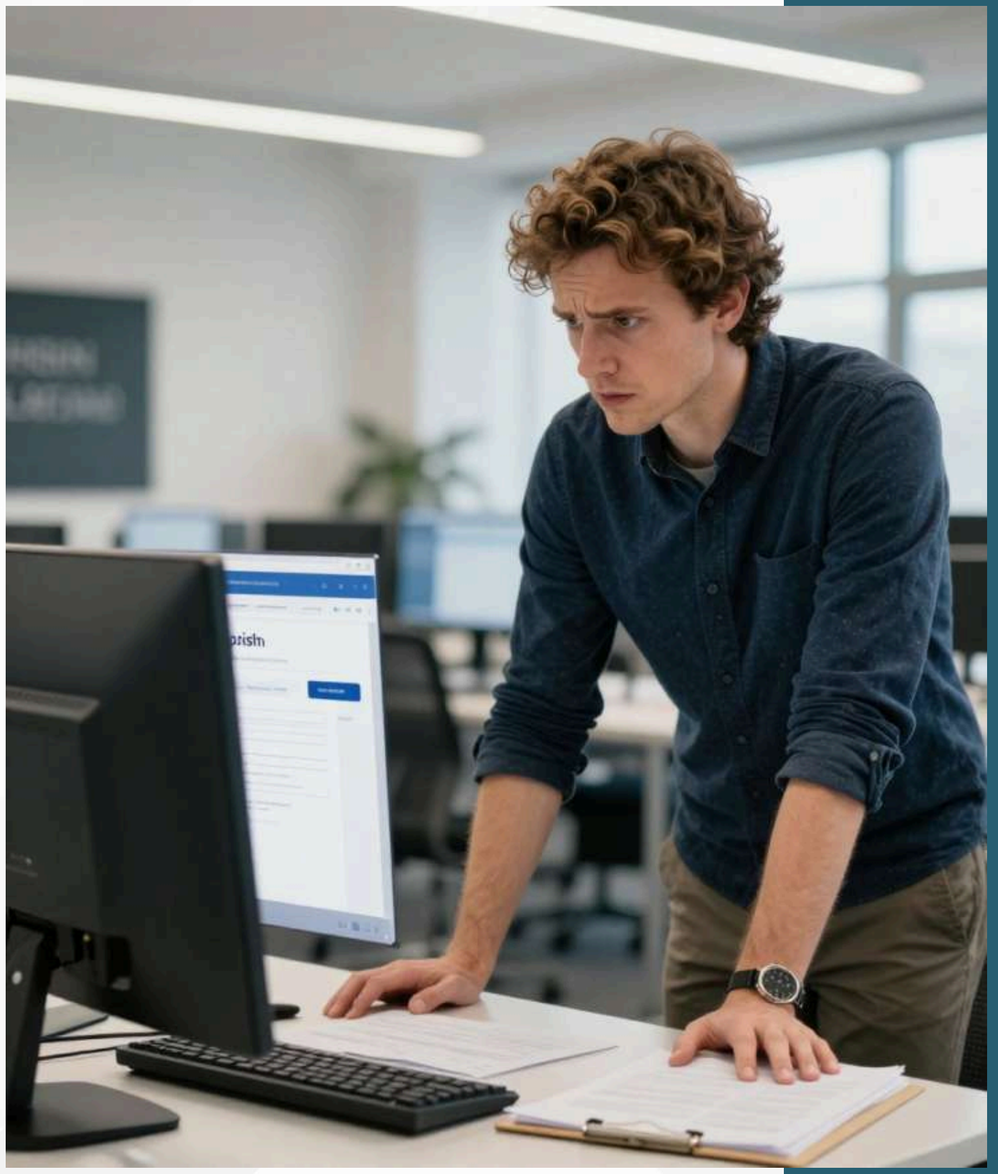
Monitoring helps institutions notice suspicious activity before it becomes a larger incident. Logs, firewall alerts, IDS/IPS tools and SIEM systems support early detection and better understanding of what happened.

Encryption protects communication from interception and manipulation. Secure protocols such as HTTPS, SSH, TLS and VPNs are essential when users access services remotely or exchange sensitive information.

CHALLENGES AND RISKS

Network security can be weakened by both technical and human factors. Even a well-designed system can become vulnerable if users ignore safe practices or if devices are not maintained properly.

Common risks include weak passwords, phishing, misconfigured devices, insecure Wi-Fi, malware infections, unpatched software, limited monitoring and low awareness. In education, limited budgets and staff capacity can make these risks more difficult to manage.



OPPORTUNITIES AND BENEFITS

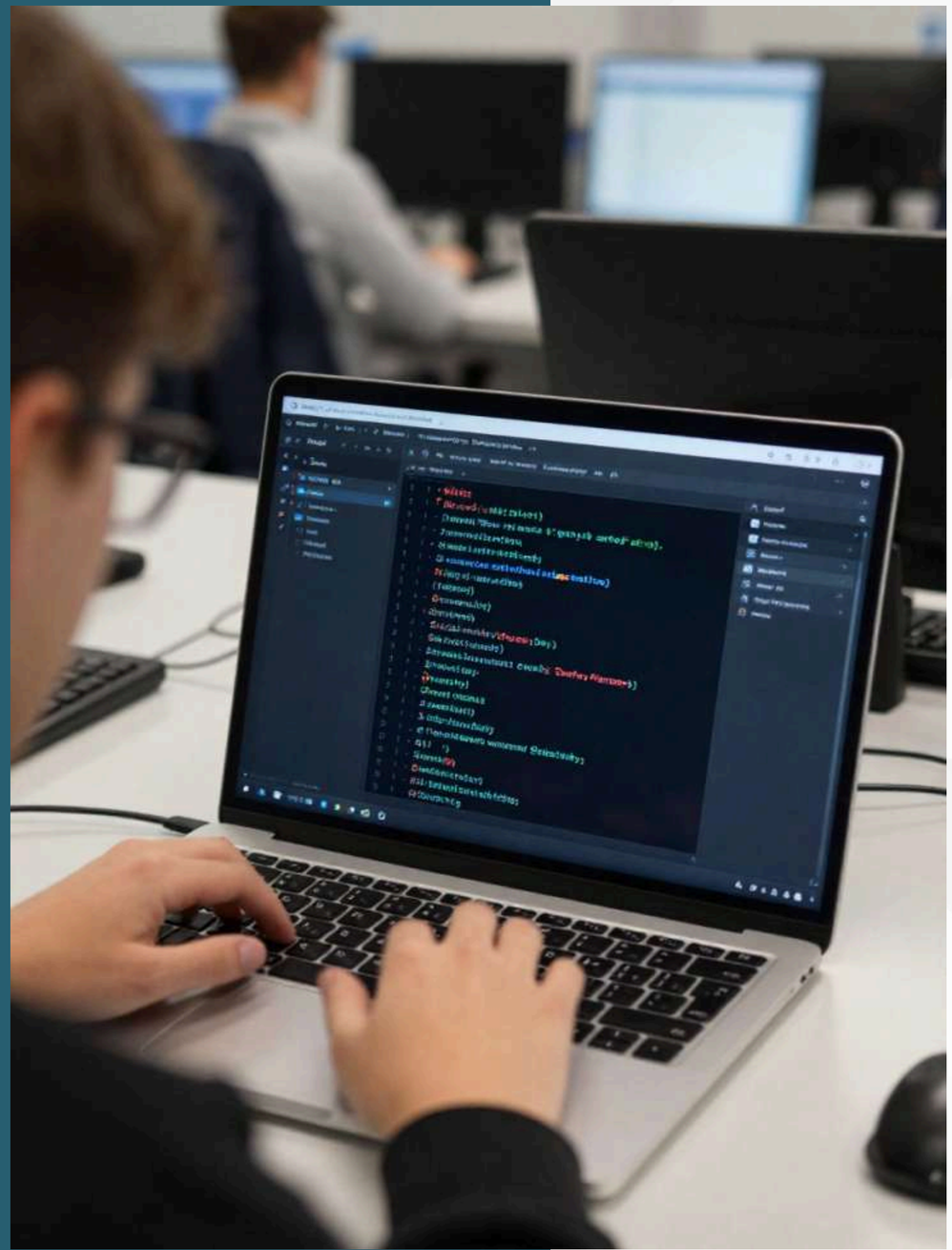
Good network security does not only prevent attacks. It also enables safer digital learning, stronger trust and more confident use of technology.

For VET institutions, secure networks protect personal and institutional data, reduce downtime, support compliance with data protection rules and improve cooperation with partners. They also provide realistic learning opportunities for students preparing for the digital labour market.

PRACTICAL APPLICATIONS

Network security becomes meaningful when it is connected to daily institutional practice. In a VET centre, it can be applied through secure Wi-Fi, protected computer laboratories, individual user accounts, safe remote access and monitoring of unusual traffic.

Students can also practise analysing simple network diagrams, identifying weak points, comparing secure and insecure configurations and proposing basic protection measures.



TOOLS AND METHODS

A wide range of tools and methods support network security. Some tools provide protection, while others help administrators and learners understand what is happening inside a network.

Examples include:

- Firewalls for controlling traffic
- IDS/IPS for detecting or blocking suspicious activity
- Vulnerability scanning for identifying weaknesses
- Packet analysis for observing network behaviour
- SIEM systems for collecting and analysing logs
- VPN, HTTPS, SSH and TLS for secure communication

All security tools must be used only in authorised and controlled environments.

CASE EXAMPLES / SCENARIOS

Scenario 1: Compromised Guest Wi-Fi
A guest network is not separated from the administrative network. A visitor connects to Wi-Fi and discovers internal devices and shared folders.

Scenario 2: Phishing and Remote Access
A teacher enters login details on a fake learning platform. The attacker uses the account to access institutional resources.

Scenario 3: Malware in a Computer Laboratory
A USB drive infects a lab computer, which later sends unusual traffic to an unknown external server.

INTERACTIVE ACTIVITIES

Network Risk Mapping
Learners analyse a simplified VET network diagram, identify possible technical, organisational and human-related risks, and propose mitigation measures.

Secure or Insecure?
Learners review everyday network practices and decide whether they are secure, insecure or acceptable only under certain conditions.

Incident Response Role Play
Learners take the roles of IT administrator, teacher, student, school manager and data protection officer to respond to suspicious network activity.

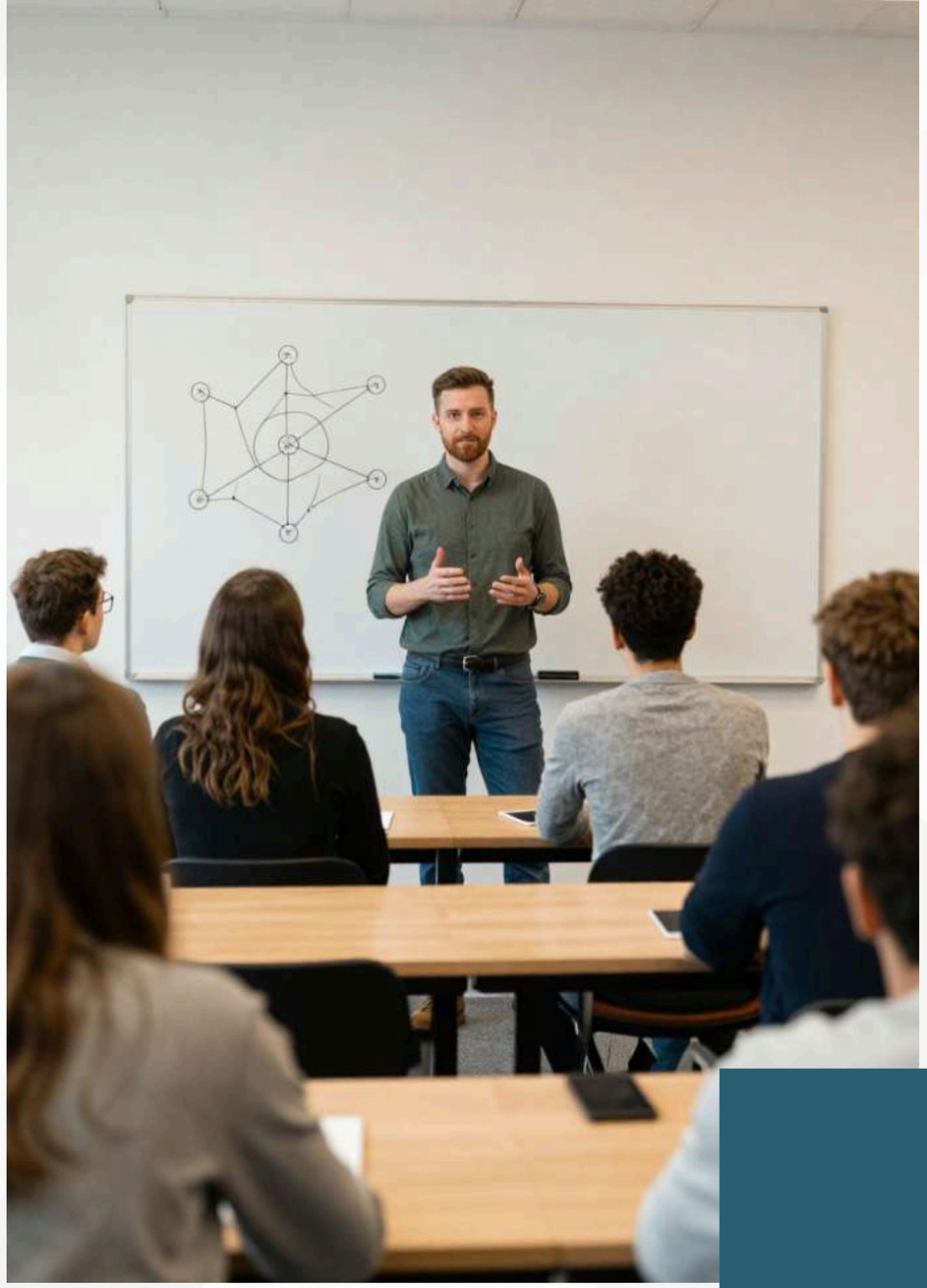
REFLECTION POINTS AND ASSESSMENT

Helping learners connect technical knowledge with responsible decision-making.

Discussion on which systems in the institution are most sensitive, why guest Wi-Fi should be separated, and how phishing can become a network security incident.

Assessment - multiple-choice questions focused on:

- Network segmentation
- Secure remote access
- Intrusion detection systems
- User awareness
- Defence-in-depth



CONCLUSION

Network security is a core pillar of cybersecurity and an essential competence area for VET education. It protects communication, data, services and institutional continuity.

A secure network requires layered protection, segmentation, authentication, encryption, monitoring and responsible user behaviour. By combining technology, policy, awareness and ethical practice, VET institutions can build safer, more resilient and more trustworthy digital learning environments.

DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 3: NETWORK SECURITY

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.