

XXX

▶ TALENTO TECH

REGIÓN 3

CAUCA - NARIÑO

MODULE 1- UNIT 2



TIC

UTP
Universidad Tecnológica
de Pereira

faceIT



TIC

UNIT 2: COMMON THREATS AND RISK MANAGEMENT

GENERAL OBJECTIVES:



Identify common digital threats and risks and understand how to manage them.



Identify malware, its types and impact on valuable information and resources.



TIC



01

Linguistic competence: Build up the skill to spot and comprehend basic vocabulary, concepts, and phrases about cybersecurity, threats and risks.

02

Pragmatic competence: Understand effectively written phrases and text related to cybersecurity, scientific articles, or instructions.

03

Sociolinguistic competence: Relate and contextualize cybersecurity vocabulary and concepts within the real-world experiences making it possible to enhance the ability to relate linguistic forms to their practical uses in the field of cybersecurity.

Competencie
s to Develop



TIC

Time available: 4 hours

Lesson cybersecurity

Learning materials.

- 1) Socialize the technology idiom of the day.
 - 2) Warm-up activity: "Spot theRisk"
 - 3) Socialize the following terms related to malware. Matching activity
 - 4) Read the text: "What is malware? and types of malware."
 - 5) Quizizz game: Multiple choice questions reading: What Is cybersecurity and Why Does It Matter?
 - 6) Video: Different Types of Malware Explained | How does Anti-malware Detects them?
 - 7) Multiple choice activity based on the previous video.
 - 8) Reading 2: Phishing: The Most Common Scam in Emails and Messages
 - 9) Kahoot game
 - 10) Reading: "Vulnerability, Threat, and Risk Management"
 - 11) True and false activity about the previous reading
- Practice activity: "Phishing hunt"

<https://www.youtube.com/watch?v=HuasitV4lcw>

<https://create.kahoot.it/details/1ad0066b-fe79-40ab-b992-fe18a2ac8552>

UNIT 2: Common threats and risk management

1) Idiom of the day "BACKDOOR"

A "backdoor" is a hidden pathway into a computer system that avoids standard security checks. It can be deliberately designed for legitimate access or unintentionally left open, potentially compromising the system's security.

2) WARM-UP ACTIVITY: "Spot the Risk"

Objective: Engage students in identifying common threats and introduce the concept of risk management through a simple and interactive exercise.



Materials

- A slide or image showing a workplace or home environment with visible cybersecurity risks (e.g., a person sharing a password, a sticky note with login details on a computer, an open laptop in a café).
- Alternatively, describe scenarios if visuals are not available.

Instructions

1. Begin by asking: "What do you think are some common risks in the digital world?" Let a few students share their thoughts briefly. Write down key ideas if possible (e.g., weak passwords, phishing emails).
2. Show the image or describe a scenario, and ask students: "Can you identify any risks or threats in this situation? What would you do to manage or reduce them?"

Example Scenario:

- A person is typing their password in a public place where others can see.
- Someone receives an email asking for personal details from an unknown sender.
- A laptop is left unattended and unlocked in a coffee shop.
- 3. Briefly summarize the importance of recognizing risks:

"Common threats often come from simple mistakes or oversights. Risk management helps us identify and fix these vulnerabilities before they cause harm. Let's explore this further today."



TIC





TIC



Optional Variation:

Turn it into a competition! Divide students into small groups, give them different scenarios or images, and see who can identify the most risks in a short time.

