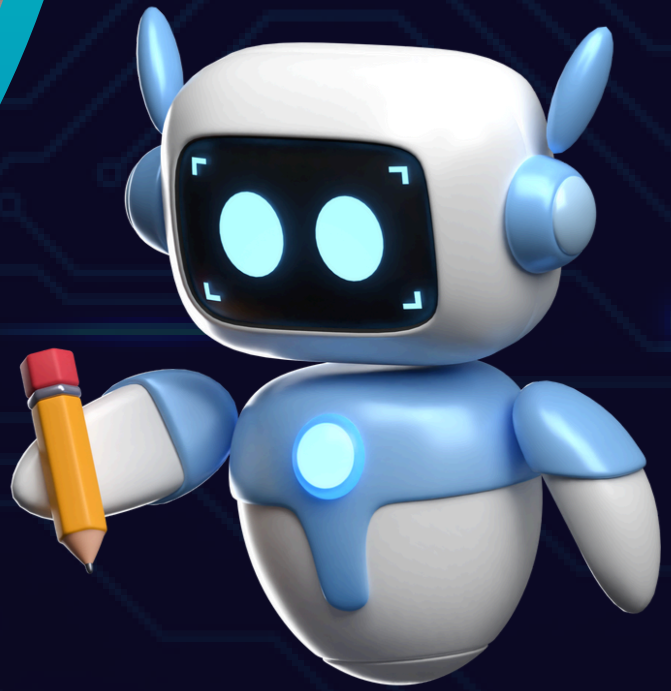
TALENTO TECH

TIC

REGIÓN 3

CAUCA - NARIÑO

LESSON 1



Universidad Tecnológica de Pereira

faceIT

Lesson 1: Warm-Up Activity: "Digital Habits Brainstorm"

Objective: To engage participants and introduce the concept of digital hygienethrough a relatable discussion.

Instructions:

1. **Opening Question:** Ask students "Whatdaily habits do you followto stay healthy, like washing hands or exercising?". Writetheir answers on a shared board or in the chat.

2. **Transition to Digital Hygiene:**

- Say: "Justlike physical hygienekeeps us healthy,digital hygiene keepsour online lives safe. What habits do you already follow to protect your devices or online accounts?"
- Allow them to share simple actions like using passwords, avoiding suspicious links, or updating software.

3. **Interactive Brainstorm:**

- Divide students into small groupsand ask them to come up with 3-5 habitsthey think are essential for staying secure online.
- Groups share their ideas briefly on a padlet https://padlet.com/dashboard/make?mobile_page=LayoutPicker

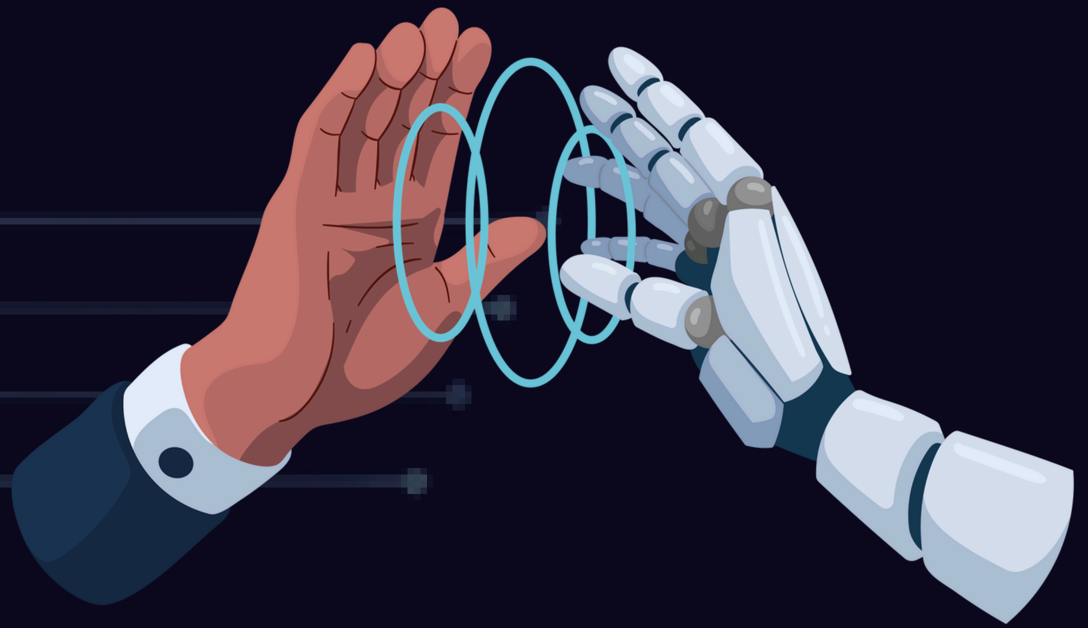
Wrap-Up: Highlight that this session will dive into key habits for "digital hygiene" to strengthen their online security and awareness.

2) **Watch the video Computer Basics:** Protecting Your Computer
https://www.youtube.com/watch?v=6mMZFoXbKqI

3) True or false questionsabout the video Computers Basics:Protecting Your Computer
https://view.genially.com/6762bf0942aa2fef03579612/interactive-content-true-or-false-quiz-p rotecting-your-computer

4) Useful terminology before reading
Go to https://www.baamboozle.com/study/1459795

The students will learn and review vocabulary related to the topic



5) Reading: Cybersecurity best practices

Software and systemsupdate: avoid exploitable vulnerabilities.

What are patches?

Patches are operating system (OS) and software updates that fix security flaws in a product or program. Updatesmay be released by softwarecompanies to addressperformance issues and add more security features.

How Do Vulnerabilities Work?

A vulnerability is a defect in a system's or program's code. These vulnerabilities can be used by hackers to install malicioussoftware, obtain unauthorized access, or steal data. Exploitable weaknesses have the potential to become serious dangers such as:

Data breaches: Private data may be taken.
Ransomware Attacks: Hackers may encrypt your data anddemand money.
Network Damage: When a device is compromised, it can causeproblems for the entire company.

The Role of Updates in Cybersecurity

1. **Patching SecurityGaps:** Developers releaseupdates to fix security flaws as soon as they are identified.

2. **Enhancing Compatibility:** Updates ensure your system is compatible with the latest security protocols.

3. **Preventing Zero-DayAttacks:** These attacksexploit vulnerabilities beforea patch is available. Updating regularly reduces this risk.

To ensure your digital devicesare protected againstpotential attacks, installsoftware updates as soon as possible. Vendors typically post updates on their websites, and some softwarewill automatically check for updates. If automatic options are available, the Cybersecurity and Infrastructure Security Agency (CISA) recommends taking advantage of them. If not, periodically check the vendor's websitesfor updates. Only download softwareupdates from trusted websites, avoid links in email messages, and be cautious of attachments claiming to have software updates. Apply automatic updates from trusted network locations and avoid updating softwarewhile connected to untrusted networks. If updates must be installed over an untrusted network, use a Virtual Private Network connection.

Best Practices for Updating Software

To ensure your systems remainsecure:

1. **Enable AutomaticUpdates:** This ensuresthat your softwarereceives the latest patches as soon as they are released.

2. **Regularly Check for Updates:** For software that doesn't update automatically, periodically check for and install updates manually.

3. **Prioritize CriticalUpdates:** Security updatesshould be installed promptly to mitigate potential risks.

4. **Maintain Backup Copies:** Before updating,back up important data to prevent loss in case of any issues during the update process.

Keeping your softwareand systems updatedis a fundamental aspect of digital hygiene.By staying current with updates, you protect your devices from exploitable vulnerabilities and ensure optimal performance.