የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

CAPACITY BUILDING TRAINING FOR TVT TRAINERS ON INNOVATIVE PEDAGOGY AND DIGITAL INTEGRATION

PART II: DIGITAL INTEGRATION

August 2024

የኢፌዲሪ የቴክኒክና ሙያ ስልጠና ኢንስቲትዩት
FDRE TECHNICAL & VOCATIONAL TRAINING INSTITUTE

ኢንተርፕረነርሺፕ ልማት ኢንስቲትዩት
Entrepreneurship Development Institute®

Outline

1. Introduction to Digital Literacy
2. Accessing Relevant Information over the Internet
3. Managing Online Resources using Web Browsers
4. **Using productivity Applications**
5. **Online Communication and collaboration**
6. **Online Security and Privacy Control**



Unit 4

Using productivity Applications

Using productivity Applications



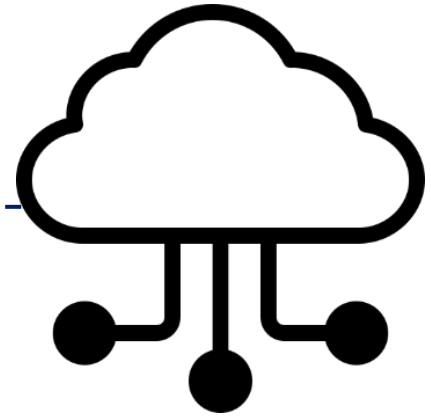
- Productivity applications are essential tools for TVET trainers to **create and modify a variety of digital resources**
- These applications offer a range of features to **support content development, from basic text editing to complex multimedia creation**

Online Productivity Tools

- Online productivity tools, often cloud-based, provide accessible and collaborative platforms for creating and modifying digital resources
- These tools are particularly useful for trainers working remotely or collaboratively with colleagues



Benefits and Risks of Online Productivity



Benefits of Cloud Computing

- Reduced cost
- Enhanced mobility
- Scalability
- Automatic Updates



Risks of Cloud Computing

- Dependence on provider
- Data protection and control
- Potential loss of privacy

Accessibility: Access documents and collaborate with others from any device with internet access

Real-time collaboration: Multiple users can work on the same document simultaneously

Automatic saving: Changes are saved automatically, reducing the risk of data loss

Integration: Many online tools integrate with other applications and services

Popular Online Productivity Tools





Google Workspace : This suite includes tools like Google Docs, Sheets, Slides, and Forms, allowing for document creation, data analysis, presentations, and surveys

Microsoft 365: Similar to Google Workspace, Microsoft 365 offers Word, Excel, PowerPoint, and OneNote for various content creation needs

Canva: A user-friendly graphic design platform for creating social media graphics, presentations, and other visual content

Adobe Creative Cloud: A comprehensive suite of design and creativity tools, including Photoshop, Illustrator, and InDesign, for advanced graphic design and multimedia production

- Trainers can use the following Google Workspace tools in various ways to enhance their activities:



How to access the google Workspace?

Offline Productivity Tools



Offline productivity tools are installed on a local computer and do not require an internet connection



These tools are suitable for trainers who prefer to work offline or in environments with limited internet access

Common Offline Productivity Tools

Office



Creative Cloud Photoshop Illustrator Lightroom InDesign Premiere After Effects and more...

Microsoft Office Suite: Includes Word, Excel, PowerPoint, and Outlook for various content creation and management tasks

OpenOffice/LibreOffice: Free open-source alternatives to Microsoft Office with similar functionalities

Adobe Creative Suite: A comprehensive suite of design and creativity tools for offline use

Video editing software: Tools like Adobe Premiere Pro, Final Cut Pro, or DaVinci Resolve for creating video content

Audio editing software: Tools like Audacity or Adobe Audition for creating and editing audio content

Benefits of Offline Productivity Tools

Independence: Work without relying on an internet connection

Control: Full control over software and data on the local computer

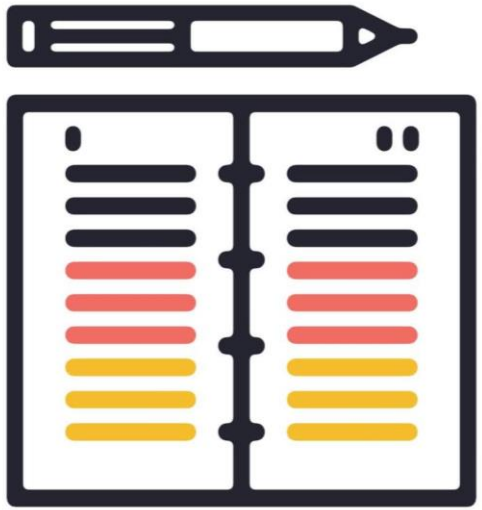
Performance: Often offer better performance compared to online counterparts for resource-intensive tasks

Best Practices for Using Productivity Applications in Training Development

- Effective utilization of productivity applications can significantly enhance the quality and efficiency of training material development
- Here are some best practices

Best Practices in Content Creation (Microsoft Word):

1. Content Creation



Document Formatting:

- Use of styles for headings and paragraphs
- Customizing fonts, sizes, and colors
- Applying themes and templates

Page Layout:

- Using columns, page breaks, and section breaks

Tables and Charts:

- Inserting and formatting tables
- Creating and embedding charts

References and Citations:

- Inserting footnotes and endnotes
- Managing bibliographies and citation styles
- Using cross-references and bookmarks

Best Practices in Content Creation (Microsoft Word):

1. Content Creation



Graphics and Media:

- Inserting and formatting images, shapes, and SmartArt
- Adding and customizing text boxes and word art

Accessibility:

- Ensure created materials are accessible to all learners by following accessibility guidelines (e.g., using alternative text for images).

Collaboration:

- Track changes and comments for reviewing documents
- Using co-authoring features and sharing documents online

Version Control:

- Maintain multiple versions of training materials to track changes and revert if necessary.

Proofreading:

- Thoroughly proofread all materials for errors in grammar, spelling, and content accuracy.

Digital Storage:

- Store training materials in a centralized location (e.g., cloud storage or shared network drive) for easy access.



Data Analysis (Microsoft Excel):

1. **Data Entry and Management:**
   - Efficient data entry techniques and shortcuts
   - Sorting and filtering data
   - Using data validation to ensure accuracy

2. Formulas and Functions:

- Basic arithmetic operations
- Common functions like SUM, AVERAGE, COUNT, MIN, MAX
- Advanced functions like VLOOKUP, HLOOKUP, INDEX, MATCH
- Logical functions like IF, AND, OR



Analysis (Microsoft Excel):

3. Data Analysis Tools:

- PivotTables and PivotCharts for summarizing data
- Conditional formatting for visual data analysis
- Data visualization using charts and graphs

4. Data Organization:

- Using tables to manage and analyze data
- Grouping and outlining data

Content Creation and Presentation:



1. **Slide Design and Layout:**
   - Using themes and templates for professional slide design
   - Customizing slide layouts with placeholders
2. **Text and Graphics:**
   - Adding and formatting text boxes, images, shapes, and SmartArt
   - Using icons and illustrations for visual enhancement
3. **Multimedia:**
   - Inserting and customizing audio and video clips
   - Creating and embedding animations and transitions



Content Creation and Presentation:

4. Charts and Tables:

- Creating and formatting charts and tables
- Importing charts from Excel

5. Slide Master and Templates:

- Creating and modifying slide master layouts for consistent formatting
- Using custom templates for brand consistency

6. Interactive Elements:

- Adding hyperlinks and action buttons for interactive presentations
- Embedding live data from Excel

Content Creation and Presentation:



7. Presenter Tools:

- Using presenter view for notes and slide previews
- Setting up and using slide show options effectively

8. Exporting and Publishing:

- Exporting presentations as PDFs or video files
- Publishing presentations to the web or sharing on platforms like Microsoft Stream



Unit 5

Online communication and collaboration



Discussion

- How do you primarily use email in your work?
- What, in your opinion, constitutes good email etiquette in a professional setting?
- Are there any specific email etiquette guidelines or best practices you follow regularly?

Using Online Digital tools for communication and collaboration



- In the modern educational landscape, online digital tools are essential for effective communication and collaboration
- For trainers, these tools provide platforms to interact with colleagues, students, and industry experts, fostering a more connected and collaborative learning environment
- They enable the sharing of ideas, resources, and feedback in real-time, enhancing the overall educational experience



- Online communication tools are digital platforms that enable users to **exchange messages, hold discussions, and share information over the internet.**
- These tools are crucial for maintaining clear and consistent communication in **educational settings.**

Key Tools and Features



Email: Email is a fundamental communication tool that allows users to send and receive messages electronically



Instant Messaging: Messaging apps provide real-time text communication, often with additional features such as voice and video calls, file sharing, and group chats



Video Conferencing: Applications such as Zoom, Google Meet, and Skype facilitate face-to-face meetings and virtual classrooms through video calls



Social Media Platforms: Social media platforms allow users to connect, share content, and engage with others online

Application for Trainers



Student Interaction:

Trainers can use email and instant messaging to communicate with students, providing support, answering questions, and sharing resources



Virtual Meetings:

Video conferencing tools enable trainers to conduct virtual classes, hold meetings with colleagues, and participate in professional development webinars



Quick Updates:

Instant messaging platforms allow trainers to send quick updates and reminders to students and colleagues, ensuring everyone stays informed



- Email is a fundamental tool for facilitating efficient and formal communication with students, collogues, and stakeholders
- It provides a reliable platform for sharing updates, discussing requirements, sending documents, and maintaining a written record of communications
- To use email in a professional setting you should refer **to set of guidelines and principles prepared by your institute**

This Photo by Unknown Author is licensed under CC BY



- **Email etiquette** in a professional setting refers to the **set of guidelines and principles** that individuals should follow when using email for business or work-related communication.

- Adhering to proper email etiquette is crucial for maintaining a positive, respectful, and effective online communication environment.

Here are Some common principles of email etiquette in a professional setting:

Use a Professional Email Address:	Your email address should reflect your professionalism, typically using your name or a variation of it, and be associated with your organization if applicable
Clear and Informative Subject Lines:	Use clear, concise subject lines that accurately describe the content of your email
Greeting and Salutation:	Start your email with a polite greeting, such as "Dear " or "Hello ." Use the recipient's name when possible
Concise and Relevant Content:	Keep your emails clear and to the point
Professional Tone:	Maintain a professional and respectful tone in your emails
Grammar and Spelling:	Proofread your emails to ensure they are free from grammatical and spelling errors

Email Etiquette

Use Cc and Bcc Judiciously:	Only use the "Cc" and "Bcc" fields when necessary
Replying and Forwarding:	When replying to or forwarding emails, trim the previous message to include only relevant information
Label and attach:	Attachments: Clearly label and attach files, and be cautious not to overload the recipient with large attachments
Respond:	Respond to emails promptly, especially if it's related to work tasks or time-sensitive matters
Respect Privacy:	Always respect the privacy of email recipients
Signature:	Include a professional email signature with your name, title, contact information, and any relevant disclaimers or confidentiality notices

Email etiquette

Use Out-of-Office Messages	: If you will be away from your email for an extended period, set up an out-of-office message to inform senders when they can expect a response
Avoid Using Email for Emotional	Avoid Using Email for Emotional or Controversial Discussions: Email is not the best medium for emotional or contentious discussions
Follow Company Policies:	Adhere to your organization's specific email policies and guidelines, which may include rules for data security, email retention, and acceptable use



Key Email Skills

- Developing strong email skills is essential for Trainers to communicate effectively and professionally
- Here are some key skills you need to develop

How ?

- **Setting up a Gmail account:**
- **Sending Email**
- **Using Cc and Bcc:**
- **Adding Attachments:**
- **Replying and Forwarding:**
- **Using Labels and Filters:**
- **Setting Up an Email Signature:**
- **Out-of-Office Autoreply (vacation Replay):**

Conferencing and Virtual Meetings



- Video conferencing tools have become integral in education, allowing educators and leaders to connect with students, colleagues, and stakeholders from anywhere.
- Platforms like Zoom, Microsoft Teams, and Google Meet enable virtual meetings, webinars, and interactive sessions. This topic will cover the use of these tools for effective online meetings.

Conferencing tools .





- **Google Meet:** Google Meet is a video conferencing tool, which is valuable for virtual meetings, lectures, and webinars. Educators can host virtual discussions, engage with students or staff, and conduct training sessions.
- **Zoom Meeting App:** Zoom is a popular video conferencing and online meeting platform that provides a range of services for hosting and participating in virtual meetings, webinars, and collaborative sessions. Zoom has gained immense popularity for its user-friendly interface, robust features, and cross-platform compatibility.

FREE PLAN COMPARISON ZOOM VS. GOOGLE MEET

Features	zoom	Meet
Participant capacity	100	100
Group Meeting Length	40 mins	60 mins
Number of meetings	Unlimited	Unlimited
Mobile App	Yes	Yes
Live closed captions	Yes	Yes
Share your screen and present	Yes	Yes
Adjustable layouts	Yes	Yes
Customer Support	Ticket	Self-help and community support
Encryption	Yes	Yes
Storage	No	15 GB Free drive storage
Virtual background	Yes	
Group Chat	Yes	Yes
Private chat	Yes	No
Breakout room	Yes	No
Co-Annotation on screen share	Yes	No

Skills needed in setting a virtual meeting

How ?

- Set Up Meeting
- Join a Zoom Meeting
- Schedule Meetings
- share screen
- Record Meetings



Discussion

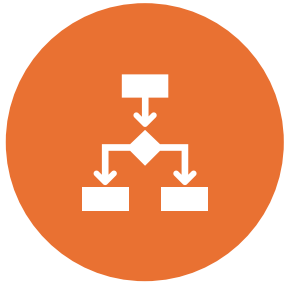
- How do you primarily work collaboratively with your teams in your workplace?
- What digital tools you use for collaborative projects?
- Do you prefer to store your files in cloud storages? Which cloud storage platforms you use?

Online Collaboration



- Collaboration refers to **the joint effort of individuals or groups** working together to achieve a common goal.
- Online collaboration tools are **digital platforms that allow multiple users to work together** on projects, share documents, and coordinate tasks in real-time.
- These tools are essential for fostering **teamwork and enhancing productivity** in educational environments.

The following are Key Characteristics of Online Collaborative Tools in common:



Multiple users: Multiple users can access, work and contribute on the same document or projects



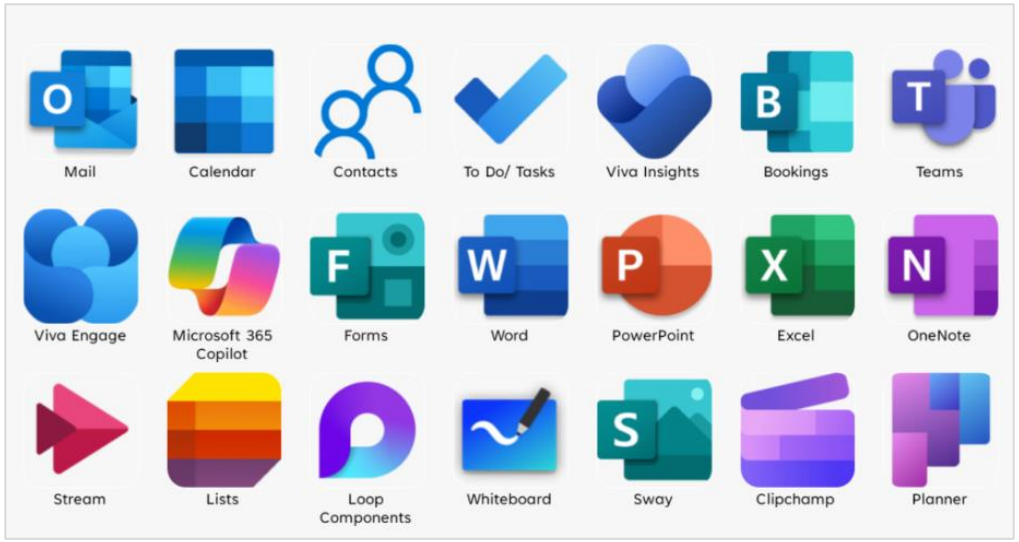
Real-time: Responses, editing and updates are shown immediately, thus saving time for all involved

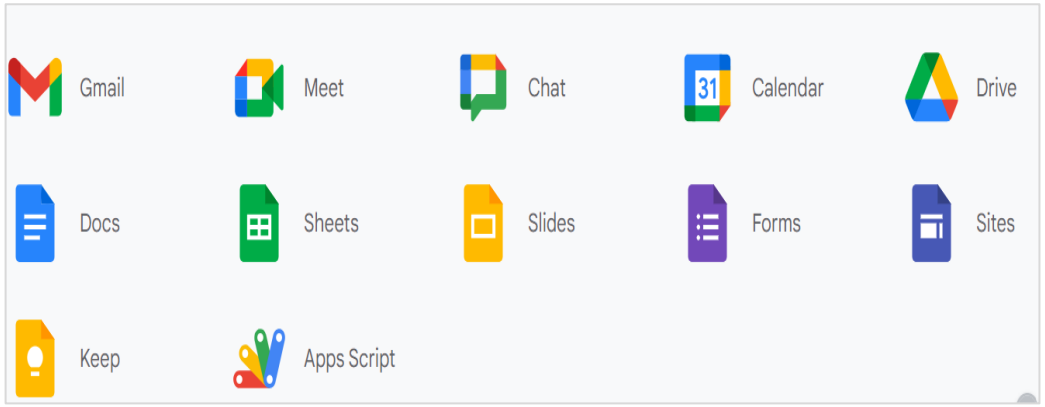


Global reach: Most online collaborative tools can be utilized from any location with the right set-up and Internet connection



Concurrent access: Concurrent multiple user access allows for faster editing and decision making on tasks





- Nowadays a variety of web apps such as word processors, spreadsheets, and presentation applications can be accessed using almost any browser

Key Tools and Features

- **Document Collaboration:** Platforms like Google Workspace and Microsoft 365 enable real-time co-authoring and editing of documents
- **Project Management:** Tools like Trello, Asana, and Monday.com help manage projects by organizing tasks, setting deadlines, and tracking progress
- **File Sharing:** Services such as Dropbox, Google Drive, and OneDrive provide cloud storage for easy sharing and access to files from any device
- **Collaborative Whiteboards**: Applications like Miro and Microsoft Whiteboard offer virtual whiteboards for brainstorming, sketching ideas, and visual collaboration

Application for Trainers



Lesson Planning: Trainers can collaborate with colleagues on lesson plans, curriculum development, and educational resources using document collaboration tools



Student Projects: Project management tools facilitate the organization and monitoring of group projects, ensuring that students collaborate effectively and meet deadlines



Resource Sharing: File sharing services allow trainers to distribute instructional materials, assignments, and multimedia content to students and colleagues



Interactive Learning: Collaborative whiteboards can be used in virtual classrooms for interactive activities, brainstorming sessions, and visual learning exercises

Online storage







- Online storage is a file hosting service that allows you to upload, store, and access your files online
- It is also referred to as a cloud storage service, an online file storage provider, or cyberlocker
- Google Docs, One Drive and Dropbox are examples of file storage and sharing services, aimed at allowing users to upload and share all types of files across all the devices they use

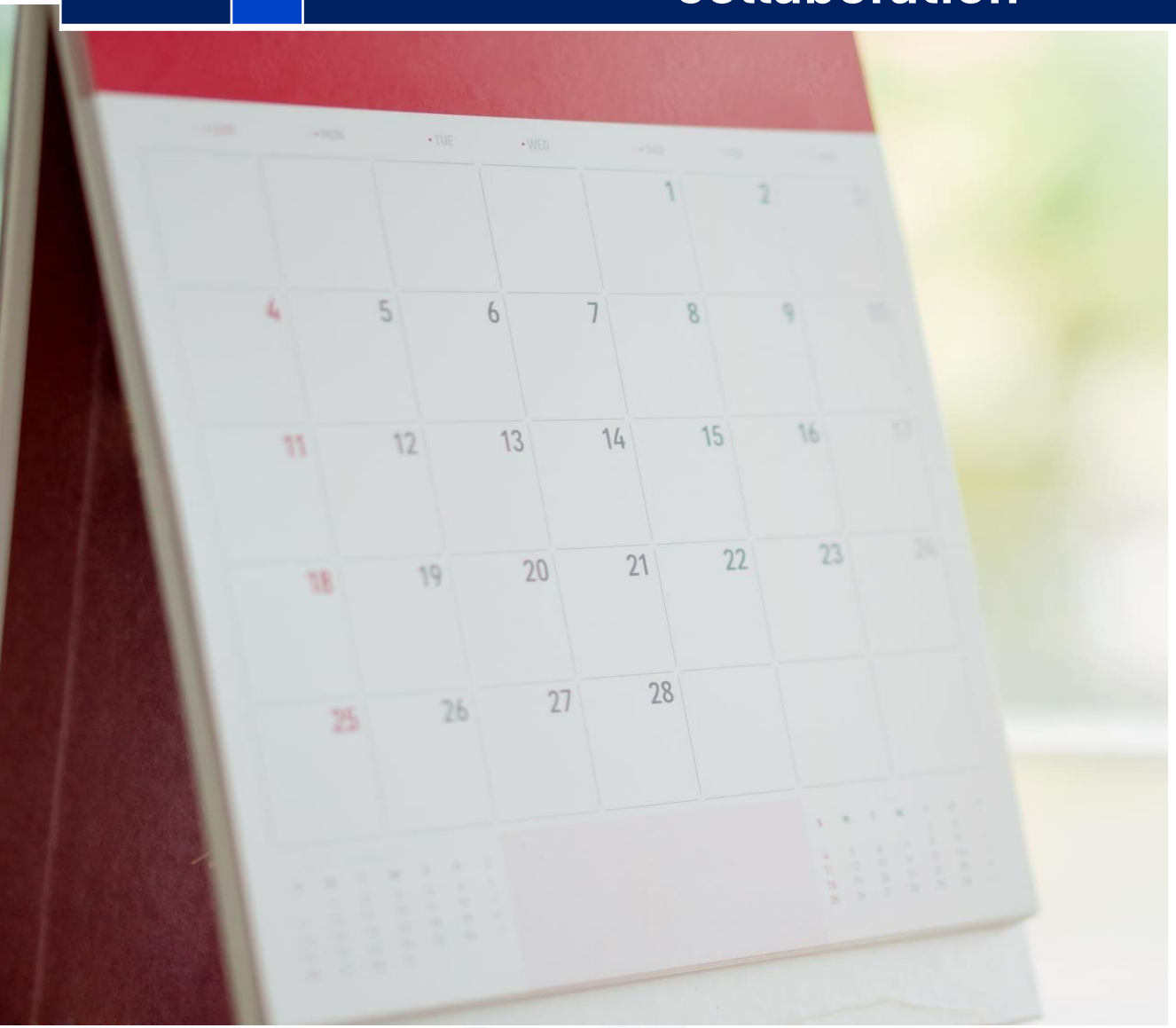
Google Drive



Document Storage: Managers can use Google Drive to store and organize important documents, Managing Files and Folders, Upload a File and automatically sync local files.



File Sharing: Managers can share files and folders with team members, clients, or partners, allowing for easy information dissemination and collaboration on projects



Online Calendars

- An online calendar allows you to keep track of your events and activities
- Google Calendar simplifies scheduling and event management
- The calendar can also integrate with other apps to send event reminders



Schedule Management: you can use Google Calendar to create, manage, and organize your schedules

Event Coordination: Google Calendar allows you to schedule meetings, set reminders, and invite participants

Sharing Calendars: Trainers can share their calendars with their collogues, helping everyone stay aware of each other's schedules and reducing scheduling conflicts

Integration: Google Calendar can be integrated with other tools like Gmail, making it easier for trainers to create events directly from emails

Productivity applications



- Google Docs, Google Sheets, and Google Slides are part of Google Workspace, which is a suite of productivity applications offered by Google
- Each of these tools serves a distinct purpose

Google Docs



Real-time collaboration: Multiple users can work on the same document simultaneously and see each other's edits in real-time

Access from any device: Documents are stored in the cloud, making them accessible from any device with an internet connection

Version history: Google Docs saves versions of documents, enabling users to track changes and revert to previous versions if needed

Template library: Users can choose from a variety of templates for different types of documents, such as resumes, reports, and newsletters



Real-time collaboration: Like Google Docs, Google Sheets enables multiple users to collaborate on a single spreadsheet simultaneously

Cloud storage: Spreadsheets are stored in the cloud, ensuring easy access from anywhere and automatic saving

Import and export data: Google Sheets supports importing and exporting data in various formats, making it compatible with other spreadsheet software



Collaboration: Multiple users can collaborate on a presentation in real-time, allowing for group input and feedback

Template gallery: Users can choose from a variety of presentation templates to create professional-looking slideshows

Real-Time Collaboration skills on Documents and Projects

How ?

- **Create a new file on Google Docs**
- **Share a file with a group of users**
- **Adding and replying to comments**
- **Using Suggestion mode to track changes**
- **Reviewing changes**



Learning Activities

Scenario:

- Assume You are a group of four students working on a group project for your history class.
- Your project is about creating a presentation on "The Industrial Revolution."
- Each team member has specific tasks to complete, and you need to collaborate using Google Drive to create a cohesive and well-organized presentation.



Learning Activities

Instructions:

Step 1: Set Up the Project Folder

1. Create a new Google Drive folder for your project and name it "Industrial Revolution History Project."

Step 2: Share the Folder

Share the folder with your team members:

- Click on the folder.
- Click the "Share" button in the upper-right corner.
- Enter your team members' email addresses and set their permissions to "Can edit."

Step 3: Create Subfolders

Inside the project folder, create subfolders for each major section of your project, such as "Research," "Images," "References," and "Presentation."

Step 4: Organize Tasks

In the "Research" subfolder, create **a Google Docs document** for each team member to write their respective sections of the project. Assign each team member a specific section, like "Causes," "Effects," "Innovations," and "Impact."



Learning Activities

Activity 5 Collaborative Academic Project Using Google Drive

Instructions:

Step 5: Collaborative Document Editing

Each team member should:

- Open their assigned Google Docs document.
- Add their research and content to their document.
- Comment and suggest edits in each other's documents to ensure consistency and accuracy.

Step 6: Collecting Visuals

In the "Images" subfolder, each team member should upload relevant images, graphs, and charts that complement their research.

Step 7: Creating References

In the "References" subfolder, create a Google Sheets document for collecting and citing your sources. Each team member should add their sources and properly format citations.

Step 8: Presentation

In the "Presentation" subfolder, create a Google Slides presentation. Each team member can work on a specific section of the presentation and incorporate the content from their Google Docs documents.

Step 9: Regular Updates and Communication

Use the comment feature in Google Docs, Sheets, and Slides to communicate with team members, ask questions, and provide feedback.



Online Security and Privacy Control



Discussion

- What is Security ? What are the Reasons for Protecting Personal Information online?
- What is Privacy? and how we can control It ?
- What is digital Identity? Can you mention Examples of a digital identity.

Why we Protect Personal Information ?

- Nowadays, more and more people are using the Internet and mobile devices for online shopping, banking, business, communication and other activities.
- Making information easier to access through the Internet also exposes businesses to some security issues.
- Hackers are able to take advantage of vulnerabilities in the transmission of data online to gain unauthorized access to systems and networks.
- There have been many reports of data breaches and identity theft in the past few years. Cybercriminals often steal personal information such as banking records, credit card details, usernames and passwords for financial gain (Smith J. R., 2020).



- **Security** refers to the measures and practices that protect data, systems, and resources from unauthorized access, damage, disruption, or theft.
  - It encompasses strategies and tools to ensure the confidentiality, integrity, and availability of information and resources, often involving authentication, encryption, firewalls, and other protective mechanisms (Smith & Johnson, 2022).



- **Privacy** is the right and practice of controlling personal information and data, determining who has access to it, and how it is used.
  - It involves protecting individuals from unwarranted intrusion into their personal lives, ensuring that data collection and processing are transparent, and obtaining consent for the collection and use of personal information (Smith & Johnson, 2022).



Discussion

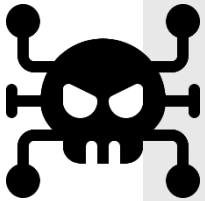
What is a threat?

Can you mention some potential threats to computers, devices, and data.



- Maintaining data security is a vital for individuals, small businesses and large corporations.
- Ensuring that data is kept secure is essential in avoiding disaster, both personally and professionally, but unfortunately it can be a difficult task due to malicious or unintentional behavior (Garcia & Martinez, 2020).
- There are many potential threats to computers, devices and data, including malware, the risk of unauthorized access, theft, and accidental damage.
- It is important to understand these threats to plan appropriately to reduce the likelihood of them affecting you.

- This is malicious software typically designed to install itself on a computer or device without consent in order to damage files or steal information (Garcia & Martinez, 2020).
- Malware is an umbrella term used to refer to viruses, worms, Trojans, spyware, adware, and other forms of malicious code.



Virus:

An intrusive program that infects computer files and may cause damage.



Worm:

Self-replicating malware that uses a computer network to send copies of itself to other computers.



Trojan:

A destructive program that masquerades as an application.



Spyware:

Malware that collects information on user browser habits without their consent.

Unauthorized access

- Accessing computers, devices or data without permission, whether the intention is malicious or not, may have negative consequences such as the alteration, loss or theft of data (Mitchell & Turner, 2018).



- Damage from accidents such as breakages, fires or floods may result in the destruction, alteration or loss of computers, devices and data (Mitchell & Turner, 2018).





- An offence that involves using the Internet or a computer to carry out illegal activities, often for financial or personal gain.
- Examples include :
  - Identity theft and
  - Social engineering.



- Social engineering is a way to manipulate or influence people with the goal to illegally obtain sensitive data (for example, passwords or credit card information) (Roberts & Parker, 2020).
- Social engineers research and learn about the personal environment of their target and fake their identity to obtain confidential information from the victim.
- In most cases, they infiltrate third-party computer systems to spy on sensitive data.

Methods of Social Engineering

- **Phone calls:**
  - One of the most common methods social engineers use in their attacks is conducted via the phone.
  - The attacker may impersonate a person of authority, a person representing a person of authority or a service provider to extract information from an unsuspecting user.
  - For example, a person claiming to be the CEO of the company calls someone on the helpdesk, requesting for his password, which he claims to have forgotten.



Methods of Social Engineering

- **Phishing:**
  - A type of social engineering attack wherein the perpetrator sends an e-mail that appears to come from a legitimate source (for example, a banks).
  - The e-mail usually requests for verification of information, sometimes warning of dire consequences if the recipient fails to comply. A phishing e-mail usually includes links to fraudulent web pages which are made to look very similar to legitimate web pages, including logos and content.







Methods of Social Engineering

- **Pharming**
  - In a pharming scam, a victim's computer or server is infected with malicious code that re-directs them to bogus websites.
  - in Pharming, the victim is re-directed to a bogus site even if they have entered the correct web address.

Methods of Social Engineering

- **Shoulder Surfing:**
  - This includes direct observation techniques, such as looking over someone's shoulder, to get information.
  - It is commonly used to obtain passwords, ATM PINs and security codes.



Identify Theft



- Identity theft is when someone deliberately impersonates and uses another person's identity.
- This is usually done for financial gain or to obtain credit and/or other benefits using someone else's name:
  - E.g, when someone uses another person's identity to obtain a driver's license.
- An initial implication of identity theft is the amount of time and money needed to re-establish your identity and credit history and to clear your name.

Methods of Identify Theft

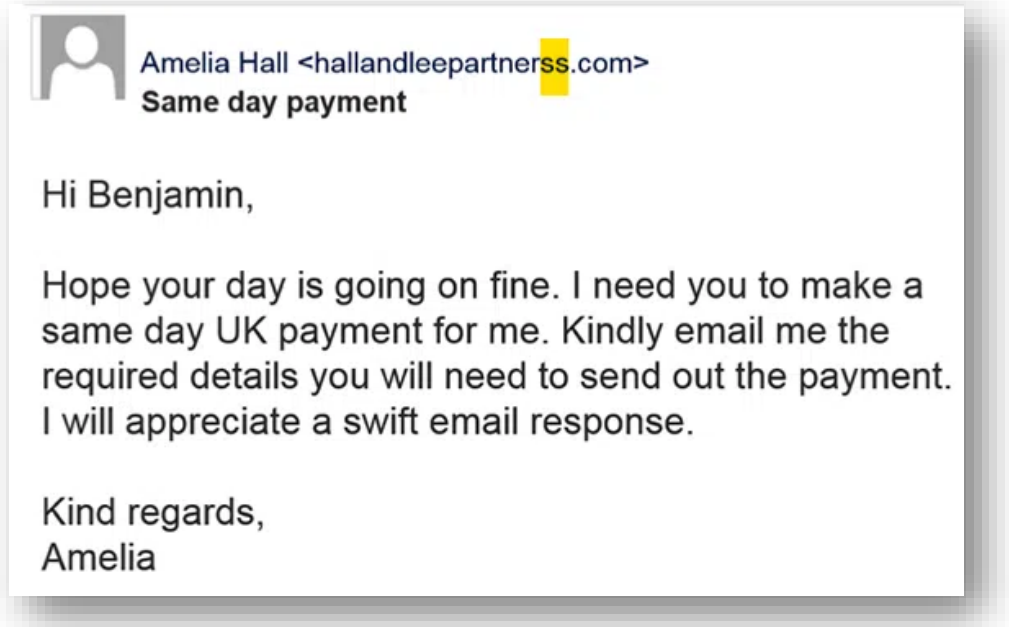
- **Information Diving:**
  - Also known as Dumpster Diving, it is a method of obtaining personal or private information by digging through a dumpster or trash bin for discarded documents or material such as utility bills or credit card statements.



Methods of Identify Theft

- **Skimming:**
  - Identity thieves use skimming as a method of capturing a victim's personal data by using a small electronic device.
  - A skimmer is a device that is usually attached to an ATM machine's card slot.
  - A victim may unwittingly slide his card into the skimmer, which then reads and stores all the information from the card's magnetic strip.





Methods of Identify Theft

- **Pretexting:**
  - This involves creating and using an invented scenario (the pretext) to engage a targeted victim.
  - The pretext increases the chance the victim will revel information or perform actions that would be unlikely in ordinary circumstances – for example, someone pretending to be from a company that provides you with a service might persuade you to share your bank account details with them.



Discussion

Discuss Different kinds of attacks or threats you have experienced locally in your work environment or privately.



Discussion

How we can protect our devices and data from authorized access?

List different mechanisms you use to protect your self online.

Methods to Protect Personal and Institutional Data



- Protecting personal and institutional data is essential to ensure confidentiality, integrity, and availability. It involves implementing security measures to prevent unauthorized access, data breaches, and loss of sensitive information.

Techniques include:

- Use safe browser settings
- Privacy Control in social media accounts
- Two-Factor Authentication (2FA)
- Regularly Back Up Data to Remote Location
- Setting up security policies

- Use anti-virus software
- Regularly update Software
- Download programs from known sources
- Use Strong passwords
- Use Encryption
- Securing equipment

Use anti-virus software



- Anti-virus software is used to scan files to identify and eliminate malware.
- There are numerous free and paid anti-virus software packages available.
- Norton, McAfee, windows defender, Kaspersky, AVG and Avast Antivirus are the popular antiviruses.
- But the popularity and effectiveness of antivirus software can change over time, It is important to research the available options.
- This are some tips when you use Anti- virus software:
  - Use anti-virus software to detect viruses and stop them from being installed or removing them.
  - Regularly update anti-virus, application and operating system software to detect new viruses, fix known problems and security risks.
  - You can use antivirus software to scan external drives and downloaded software.



Learning Activities

Activity 1 — To perform a quick scan in Windows Defender Security Center:

Instructions:

1. Open Windows Defender by clicking the search tool on the taskbar and entering Windows Defender.
2. Select Windows Defender Security Center.
3. Select Virus & threat protection.
4. In the Virus & threat protection page, select Quick Scan to begin a quick scan.
5. Windows Defender runs the quick scan.

Regularly update Software



- Software developers often release software updates to address problems or fix security vulnerabilities in their products.
- These updates help prevent or fix problems or enhance and improve how your computer works.
- Therefore, it is important to regularly check for updates to your software, such as your anti-virus, application and operating system software.



Discussion

How strong is your password? What will you do to make your password Strong?

Do you think using the same password for every platform a good practice?

Learning Activities

Activity 2 To test how secure your password is

Instructions:

- Go to http://howsecureismypassword.net/ to test how secure your password is:
- Tested it with different sample passwords of your own or write “password”.

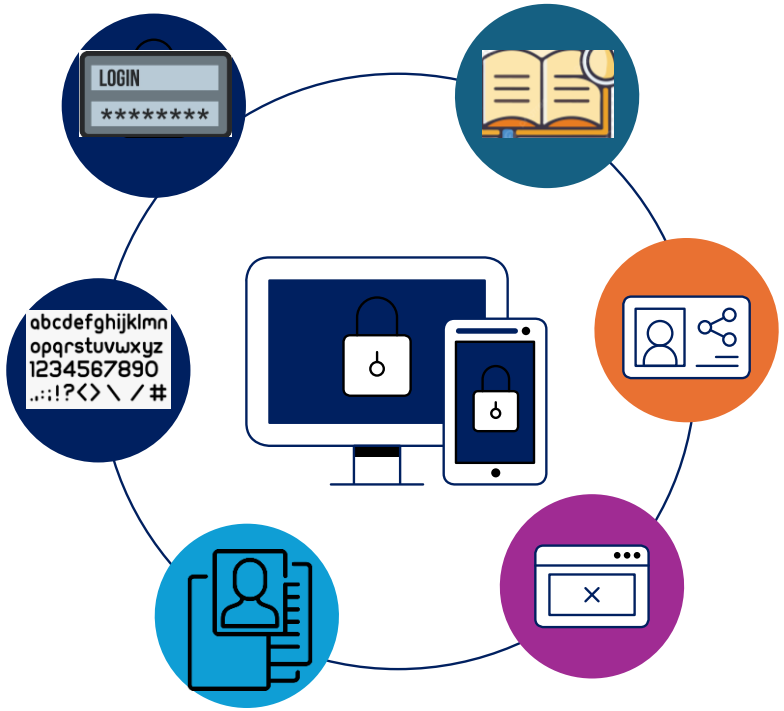




- Use strong passwords to prevent unauthorized access.
- These passwords can be required for access to computer systems, applications, shared files, networks, online forums, online shopping accounts and services, cloud storage, social media and email accounts etc.
- Password policies are guidelines or requirements on the creation and use of passwords.
- The following are some guidelines for password policies

Guidelines for password policies

- Create passwords with adequate length
- Create passwords with adequate character mix
- Avoid using passwords that include your personal information



- Avoid words found in the dictionary
- Do not share passwords
- Change regularly



- Encryption is a process that encodes data or information so that only authorized users can read the information.
- In the event that the data is intercepted by an unauthorized user, the interceptor will need to decrypt the data first before he is able to read it.
- Encryption is used to protect data as it's passed over a network.
- It is often used to prevent illegal access to or reproduction of information.



Learning Activities

Activity	3	To encrypt Microsoft Word document with password

Instructions:

1. Open Microsoft Word document and Click the FILE tab.
2. Click Info.
3. Click Protect Document.
4. Click Encrypt with Password.
5. In the Encrypt Document dialog box, type a password in the Password box.
6. Click OK.
7. In the Confirm Password dialog box, type the password again in the Reenter password box, and then click OK.
8. Save the file.

Regularly Back Up Data to Remote Location:



- Regularly back up data to a remote location to keep it safe in the event of problems such as network, hardware or software problems, theft or accidental damage.
- It is important to make regular backups as your files can be lost or destroyed accidentally; the hard disk may also develop problems.
- Thus, backups must be made to an external device such as CDs, DVDs, external hard disks or USB drives.
- Another option is to back up data on the Internet, using a “cloud” storage solution.



- ICT policies are usually implemented in a workplace to ensure safe and appropriate use of Internet services and connections.
- A company may issue a document to be signed by employees to comply with their regulations.
- When using ICT in an work environment it is good practice to set some rules for how it can be used by staff in order to protect everyone from potential risks.
- A good starting point is to create a document called an **acceptable use policy (AUP).**

An acceptable use policy (AUP)

- is a document that outlines what the school determines is acceptable in terms of behavior when using computers and the Internet
- In general, AUPs typically cover the appropriate use of e-mail, Internet, social media, network equipment, data, computers and mobile devices. Your AUP should be created with input from parents, students, teachers, and staff.
- It should be communicated to all students, staff and parents, and you should continually review and update your AUP to take account of continuous advances in technology.



- It includes Storing all equipment in a secure location.
- Mobile devices such as tablets and laptops are particularly easy to steal in a work environment because they are easy to carry and hide, and because devices are used by a number of different people it can be difficult to keep track of them.

1. **Digital Identity, Digital Footprint and Managing**
- **Privacy Settings**

- Some tips for keeping devices secure include:
  - Using laptop or tablet trolleys.
  - Locking them securely in safe storage facilities.
  - Using password controls.
  - Setting up remote tracking, locking, and wiping to be used in the event of loss or theft.



Discussion

- What is a Digital Identity ?
- What is Digital Footprint ?
- How to manage Managing Digital Identity Digital Footprint ?

What is Digital Identity?



- Digital identity refers to the collection of information about an individual that exists online.

This includes personal data, professional details, online behaviors, and the way an individual interacts with digital platforms.

Digital identity is formed through various online activities such as social media interactions, online purchases, email communications, and the use of online services.

key components of digital identity

Personal Information: Name, date of birth, address, and other identifying details.

Credentials Usernames, passwords, and authentication tokens used to access online accounts.

Professional Information: Employment history, professional affiliations, LinkedIn profiles, and other work-related data

Online Behaviors: Browsing history, social media activity, and online transactions.

What is Digital Footprint?



- A digital footprint is the trail of data that individuals leave behind when they use the internet.
- It includes all the information that can be traced back to a person as a result of their online activities.
- It includes your online activities, such as social media posts, emails, search history, and online purchases.
- This information can be accessed and analyzed by individuals, organizations, or even governments.

Example: Every time a TVET trainer posts a comment on a professional networking site, likes a page, or shares an article, they are contributing to their digital footprint.

- Digital footprints can be categorized into two types: active and passive.

1. Active Digital Footprint:

- This is the data that individuals intentionally leave online, such as social media posts, comments on blogs, and online reviews.
- Examples include uploading photos, tweeting, and sharing content on Facebook.

1. Passive Digital Footprint:

- This is the data that is collected without the individual's explicit knowledge, often by websites and apps that track user behavior.
- Examples include browsing history, location data, and online purchases.

- Impact of Digital Footprint:
  - **Privacy Concerns:** A large digital footprint can make individuals more vulnerable to privacy breaches, data mining, and cyberattacks.
  - **Reputation Management:** Everything that a person shares or that is shared about them online contributes to their public image and can have long-lasting effects.
  - **Data Control:** Managing a digital footprint involves controlling what information is shared online and being aware of how it is used by others.

- Managing Digital Identity and Footprint using Privacy settings
  - Privacy is the right to control information about oneself. It involves determining who can access, collect, use, and disclose personal information. In the digital age, privacy encompasses protecting personal data from unauthorized access, collection, and misuse. Social media platforms collect and use user data. To protect your privacy, it's crucial to manage your settings effectively.

Example: A TVET trainer can adjust their Facebook privacy settings to control who can see their posts, limit information shared with third-party apps, and review the data Facebook collects about them.

- Protecting Digital Identity:
  - **Strong Passwords:** Use complex, unique passwords for different accounts and change them regularly.
  - **Two-Factor Authentication:** Enable two-factor authentication (2FA) to add an extra layer of security.
  - **Privacy Settings:** Adjust privacy settings on social media and other platforms to limit who can see your information.
  - **Monitoring:** Regularly check online profiles, credit reports, and bank statements for any unusual activity.
  - **Be Selective with Sharing:** Think carefully before posting personal information, photos, or opinions online.
  - **Delete Old Accounts:** Close or delete accounts that are no longer in use to reduce the amount of data available online.
  - **Use Incognito Mode:** When browsing, use private or incognito mode to prevent the storage of cookies and browsing history.

- Best Practices in Protecting Digital Identity:
  - **Strong Passwords:** Use complex, unique passwords for different accounts and change them regularly.
  - **Two-Factor Authentication:** Enable two-factor authentication (2FA) to add an extra layer of security.
  - **Privacy Settings:** Adjust privacy settings on social media and other platforms to limit who can see your information.
  - **Monitoring:** Regularly check online profiles, credit reports, and bank statements for any unusual activity.
  - **Be Selective with Sharing:** Think carefully before posting personal information, photos, or opinions online.
  - **Delete Old Accounts:** Close or delete accounts that are no longer in use to reduce the amount of data available online.
  - **Use Incognito Mode:** When browsing, use private or incognito mode to prevent the storage of cookies and browsing history.

- Managing Privacy Settings on different Browsers There are some important web browser settings to consider.
-
  - **Cookies:** Configure cookie settings to manage how websites store and access data on your device. You can choose to block all cookies, allow cookies from visited sites, or create exceptions.
  - **Clear Browsing Data:** Regularly clear your browsing history, cookies, cache, and site data to maintain privacy and free up storage space.
  - **Pop-ups**: Block pop-up windows to prevent unwanted ads and potential security threats.
  - **Tracking:** Some browsers offer "Do Not Track" settings, which send a signal to websites requesting they not track your online activities. However, compliance is voluntary.



Learning Activities

Activity 3 Apply browser settings

Instructions:

- Open Google Chrome and perform the following activities:
  1. Allow / block cookies
  2. Delete your browser history, temporary Internet files, saved form data and saved passwords.
  3. Allow and block Pop-ups.

- Managing Privacy Settings on different Browsers
    - **Incognito or Private Browsing:** These modes prevent your browsing history from being saved on your device, but they don't guarantee complete anonymity.
    - **Safe Browsing:** Enable safe browsing to receive warnings when visiting potentially harmful or deceptive websites.
    - **Password Manager:** Use a built-in or third-party password manager to securely store and autofill your login credentials.
    - **Autofill:** Configure autofill settings for forms and payment information while ensuring the security of your data.



Discussion

Do you know what your current privacy settings are on each social media Platform?

Do you think everything what you will do on those platforms should be public?

- Managing Privacy Settings on different Social Medias

  - **Audience Controls:** Most platforms allow you to choose who can see your posts (public, friends, only you).
  - **Tagging:** Control who can tag you in photos or posts.
  - **Location Services:** Be mindful of sharing your location. Many apps allow you to turn off location services.
  - **Ad Settings:** Limit ad tracking by adjusting ad preferences.
  - **Data Sharing:** Review which apps and websites have access to your social media data and revoke unnecessary permissions.
  - **Privacy Checkups:** Many platforms offer privacy checkups to help you review and adjust your settings.



Learning Activities

Activity	4	Review and manage your privacy settings on Facebook:

Instructions:

- 1. Click your profile picture in the top right of Facebook.
- 2. Select Settings & privacy, then click Settings.
- 3. Click Privacy in the left column.
  - Walk through Privacy Checkup to make sure you're sharing your information with who you want.
  - Customize your Ad preferences to see ads that are more relevant to you.
  - Manage some of the content you share on Facebook, like posts, photos and videos, from the Manage Activity section of your activity log.
  - Learn how to manage what others can see about you.

Two-Factor Authentication (2FA):



- Two-Factor Authentication (2FA) is a security process that requires users to provide two different authentication factors to verify their identity.
- These factors typically include something the user knows (e.g., a password) and something the user has (e.g., a mobile device or security token).
- 2FA adds an extra layer of security to prevent unauthorized access even if the password is compromised.
- Different social media platforms offers 2FA to enhance the security of your account.



Learning Activities

Activity 5 Two-Factor Authentication Setup with Telegram:

Instructions:

Activity Steps:

1. **Accessing Account Settings:**
   - open the Telegram app on their mobile devices.
   - Navigate to the menu by tapping on the three horizontal lines in the top-left corner.
2. **Opening Account Settings:**
   - In the menu, select "Settings."
3. **Locating Privacy and Security:**
   - Within "Settings," find and tap on "Privacy and Security."
4. **Initiating Two-Step Verification:**
   - In "Privacy and Security," locate and tap on "Two-Step Verification."
5. **Setting a Password:**
   - tap on "Set Additional Password" to create 2FA password.
   - Emphasize the importance of choosing a strong and memorable password.
6. **Adding a Hint (Optional):**
   - add a hint for their 2FA password. However, not make it too explicit.
7. **Adding a Recovery Email (Optional):**
   - add a recovery email for account recovery if you forget your 2FA password.
8. **Verifying the Password:**
   - enter the newly created password to verify it.
9. **Confirmation and Completion:**
   - Once the password is verified, confirm that 2FA is successfully set up on their Telegram account.
10. **Testing the Two-Step Verification:**
    - log out of your Telegram account and attempt to log back in. They should experience the 2FA process by entering the password they just set.



Day 1 Discussion Points

- What are the key concepts and skills you have learned in the units discussed?
- How can the knowledge you gained help you improve your teaching Practice in your work environment?
- How can the lessons learned in this unit contribute to fostering a culture of digital literacy and responsible internet use among your students? What role do you see yourself playing in this cultural shift?
- Considering the rapid pace of technological change, how do you plan to keep your skills up to date? What resources or strategies will you use to continue learning in this area?


Thank you