25 Years
Committed to Human Rights
In Special Consultative Status with UN ECOSOC
Honorary of the UN Human Rights Prize 2023

DIGITAL LITERACY

Prepared by: Mohamed Abuazzoum
Member, International Relations Unit (IRU)
Coordinator, Digital Youth Rights Unit

Supervised by : Amal Shamoun

Date: 17 September 2025

25/26

Table of Content

01

Foundations of Digital Literacy

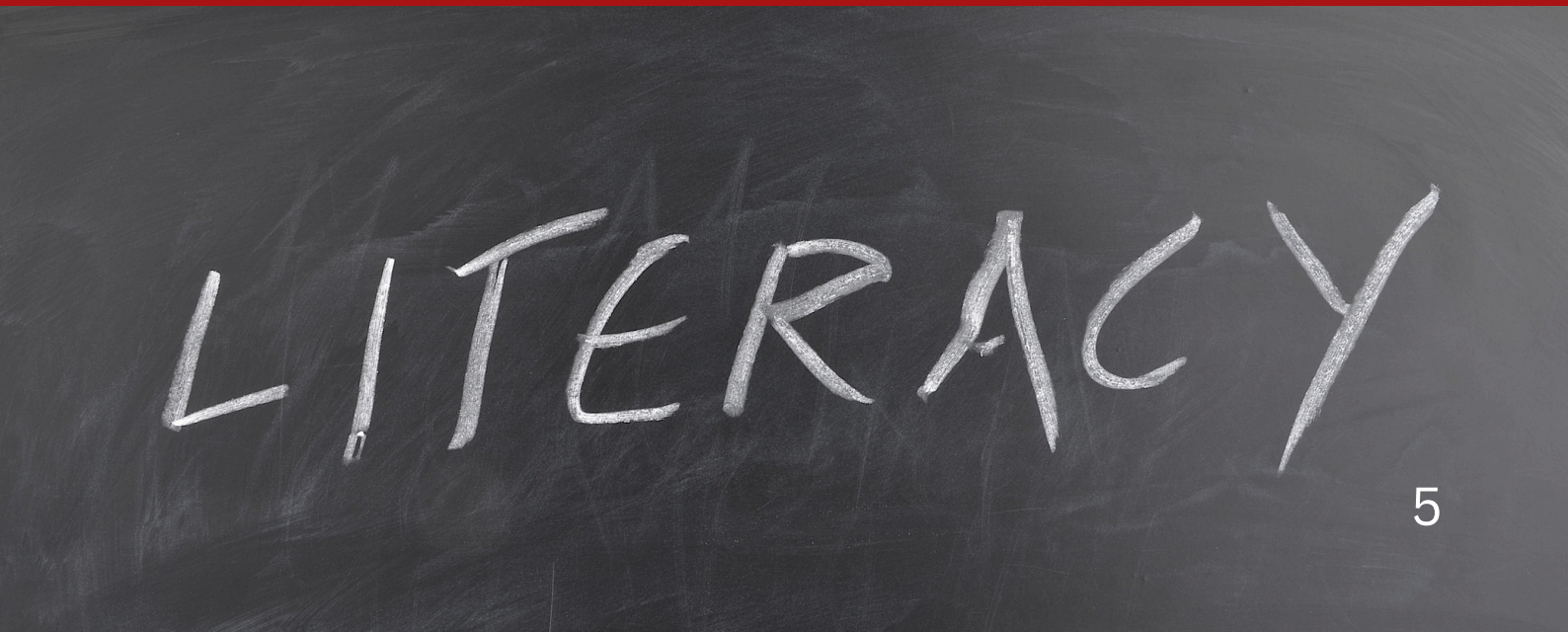
INTRODUCTION

In the current digital era, technology and the internet are pervasive in practically every part of our lives, from how we connect and amuse ourselves to how we learn and work. Effectively navigating this digital environment, however, calls for more than simply gadget and app proficiency. It entails comprehending the fundamental ideas underlying how digital systems function, such as data collection, algorithmic content selection, and the significance of digital rights. (UNESCO, 2018)

This unit will help you become a self-assured and responsible digital citizen by guiding you through these fundamental ideas in an understandable manner.

WHAT IS DIGITAL LITERACY?

Digital literacy refers to the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship. It includes skills such as computer literacy, ICT literacy, information literacy and media literacy which aim to empower people, and in particular youth, to adopt a critical mindset when engaging with information and digital technologies, and to build their resilience in the face of disinformation, hate speech and violent extremism.



DIGITAL LITERACY FROM A HUMAN RIGHTS PERSPECTIVE

From a human rights standpoint, digital literacy encompasses more than technological proficiency. It equips individuals with the knowledge and resources they need to safeguard and exercise their fundamental rights online. This comprehensive approach highlights several key dimensions:

Understanding Digital Rights	**Awareness of the rights to information access, privacy, freedom of expression, and protection from online discrimination.**
Protecting Personal Data	**Recognizing how personal data is collected and used, while learning to manage and safeguard one's digital footprint.**
Freedom of Expression and Access to Information	**Exercising the right to express opinions and participate in public discourse while respecting the rights of others.**
Access and Inclusion	**Ensuring equal access to the internet regardless of location, income, gender, or ability.**
Resisting Online Harm	**Identifying and responding to digital threats such as censorship, disinformation, surveillance, and online abuse.**
Empowering Civic Engagement	**Using digital tools to participate in democratic processes, remain informed, and advocate for positive change.**

WHAT DOES IT MEAN TO BE "ONLINE"?

In the digital age, being "online" goes beyond merely connecting to the internet. Each interaction through a device whether a smartphone, computer, or tablet creates data that contributes to your digital footprint. This footprint is essentially a record of your online activities and is categorized into two main types:

Active Digital Footprint

information deliberately shared by the user. These actions are intentional and often visible to others.
Examples include:

- Posting on social media platforms.
- Submitting reviews or comments.
- Filling out online forms or surveys.
- Signing up for newsletters or services.
- Sending emails or messages.

Passive Digital Footprint

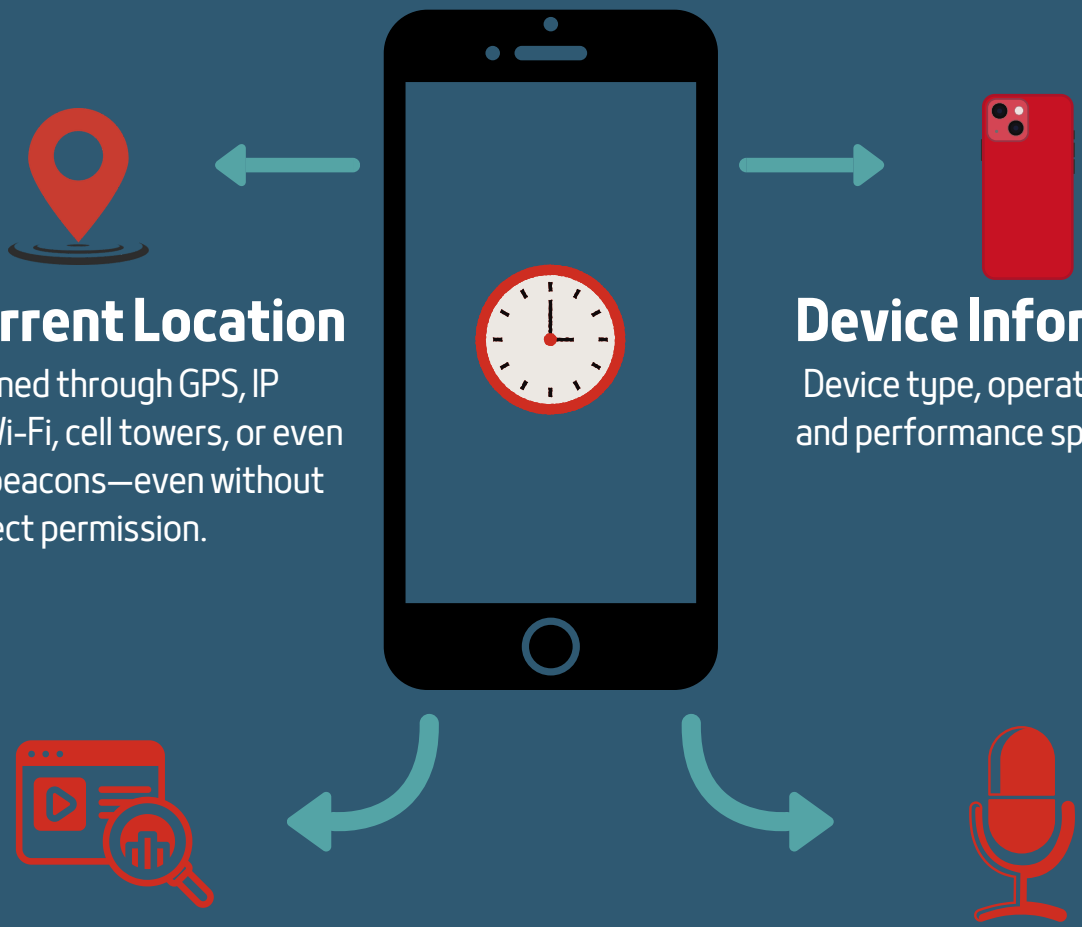
information collected automatically, often without the user's awareness. Websites, apps, advertisers, and governments may gather this data. Examples include:

- Tracking cookies stored in browsers.
- IP addresses and device types .
- Geolocation and time zone.
- Logs of browsing history & app usage.

HOW DO APPS COLLECT INFORMATION ABOUT YOU?

Apps like Facebook, Instagram, and TikTok collect far more data than many users realize. This data collection powers their business models, allowing them to deliver personalized content and highly targeted advertisements.

Common Data Points Collected by Apps:



Your Current Location

Determined through GPS, IP addresses, Wi-Fi, cell towers, or even Bluetooth beacons—even without direct permission.

Device Information

Device type, operating system, and performance specifications.

Engagement Data

Time spent on features, posts you like, share, or comment on, and your browsing habits.

Sensitive Permissions (if granted)

Access to contacts, call history, microphone, or camera recordings.

WHAT ARE ALGORITHMS AND HOW DO THEY WORK?

Algorithms are a series of computational steps that transform input into output. In apps and social media, they decide what content to show you based on your behavior and data.

How Algorithms Learn from You:

+ **Engagement**

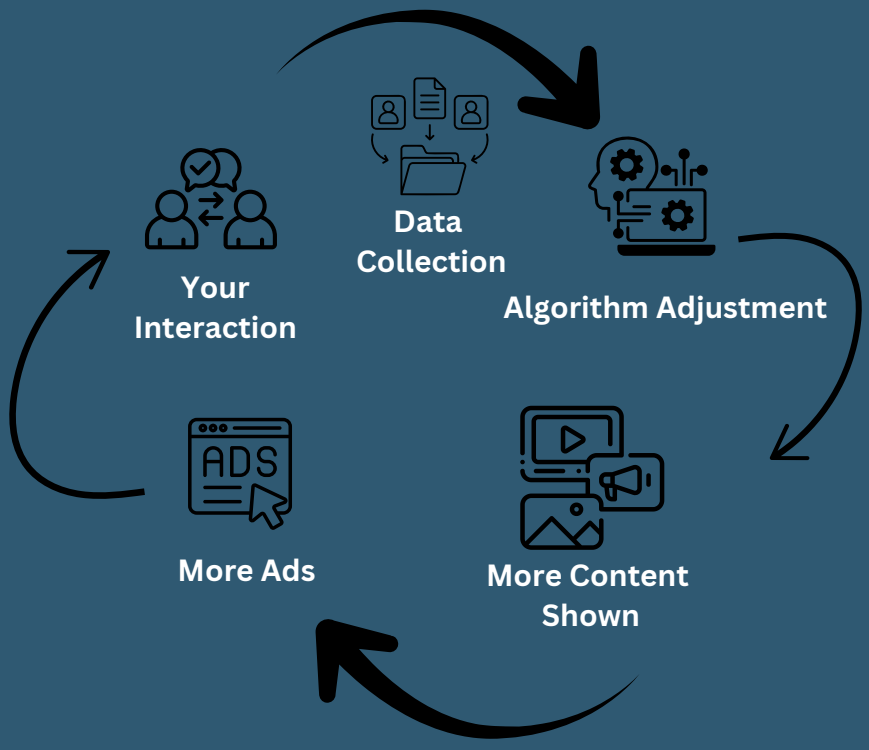
  Likes, comments, shares, and saves = more of that content. Quick scrolls = less of that content.

+ **Time Spent**

  Even without clicking, stopping longer on a post signals strong interest.

+ **Similar Users**

  If people like you engage with something, it's recommended to you too.



WHAT IS A "FILTER BUBBLE"?

A filter bubble is a digital space created by algorithms that selectively show users information based on their previous actions (clicks, likes, shares, searches, and time spent on content).

The term was introduced by Eli Pariser (2011) to describe how personalization algorithms isolate people from opposing viewpoints and reinforce pre-existing beliefs.

Platforms like Facebook, YouTube, TikTok, Instagram, and Google Search are the main drivers of these bubbles through algorithmic personalization.

How Filter Bubbles Work

You interact with content	**Algorithms track your likes, comments, shares, and time spent.**
Protecting Personal Data	**User behavior (time spent, network connections, engagement) is gathered.**
The algorithm adjusts	**Prioritizes similar material, filtering out content it predicts you'll ignore or dislike.**
Your feed becomes personalized	**You see fewer opposing views and more of the same type of content.**
Your perspective narrows	**Over time, your worldview is shaped by a limited set of ideas, reinforcing existing beliefs.**

02

Digital Privacy and Safety

INTRODUCTION

Our personal information is at greater risk as we depend more on the internet for socialising, working, studying, and communicating. Every picture we send, message we send, or form we complete adds to a digital footprint that, if not adequately safeguarded, could be exploited. This unit covers the definitions of digital privacy and security, their implications for your everyday life and rights, and doable precautions you can take to keep safe online.

WHAT IS DIGITAL PRIVACY?

Digital privacy is your ability to control your personal data—what you share, who can see it, and how it is used. It is recognized as a fundamental human right under international law, specifically affirmed in Article 12 of the Universal Declaration of Human Rights, which states:
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence..." (United Nation, 1948).
Online privacy includes everything from your phone number and photos to your conversations and location.

Simple examples of personal data:


Your name and date of birth


Your address or school


Photos you post online


Messages exchanged with friends


Your browsing habits

WHAT IS DIGITAL SECURITY?

Digital security, also called cybersecurity, refers to the practices and tools used to protect your devices, data, and personal identity from threats such as account hacking, phishing scams, malware, spyware, and data breaches. Without digital security, private information can be exposed or stolen, leading to serious consequences such as financial loss or identity theft (OHCHR, 2022). At its core, digital security means using tools and good habits to prevent unauthorized access to your information. This includes setting strong passwords, enabling two-factor authentication, avoiding suspicious links, and keeping your software updated.

Common Digital Threats:

Account hacking

Unauthorized access to your account, often used to steal data or impersonate you.

Malware and Spyware

Malicious apps or software that damage devices, track activities, or steal data..

Phishing Scams

Fake websites or messages that trick you into revealing personal information.

Data Breaches

When confidential data stored by organizations or platforms is leaked or exposed.

CC AND BCC IN EMAIL SECURITY

In the world of email communication, understanding the difference between CC (Carbon Copy) and BCC (Blind Carbon Copy) is essential for maintaining digital security and privacy.

(BCC) Blind Carbon Copy

- Sends to multiple email addresses without showing the recipients' name
- Protects the privacy of the recipients
- Simplifies the look of the email
- Prevents any replies to be sent to other recipient

Examples: Mailing list, newsletter, farewell messages

(CC) Carbon Copy

- Referred to as "courtesy copy"
- Allows to send to multiple email addresses
- Allows recipients to stay informed
- Recipients are not required to reply

Examples: Scheduling, inform about changes, introducing contacts

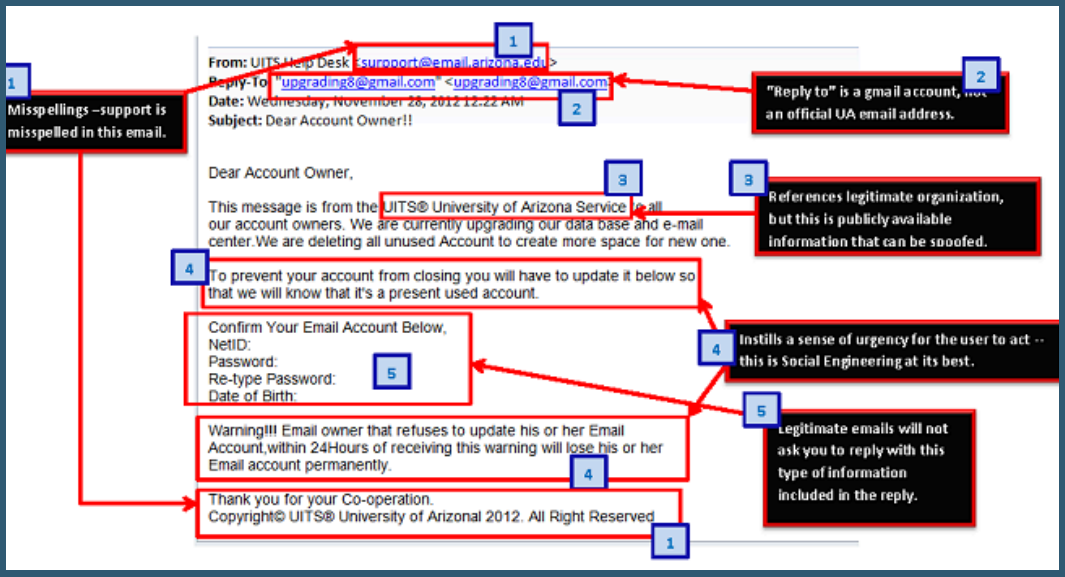
REAL-LIFE EXAMPLE: LEILA'S PHISHING INCIDENT

Leila, a university student, once received an email that appeared to come from her university's IT department.
The message warned her that her account would be suspended unless she clicked a link and logged in immediately.
Trusting it was real, she entered her credentials.

Soon after, Leila's account was hacked — the attacker used her account to send spam to her contacts. Because her contact list was exposed (similar to a CC misuse), others were also put at risk. Her sensitive documents and photos were accessed as well.

This incident could have been avoided if Leila had:

- Recognized the signs of phishing
- Used two-factor authentication (2FA)
- Ensured group emails used BCC to protect contact information



HOW CAN YOU PROTECT YOURSELF ONLINE?

Think of online safety like locking your doors at night — it's about protecting your data, identity, and privacy from digital threats. Here are practical strategies and tools to help you stay secure in the digital world.
Key resources and practices that can be helpful are as follows:

A. Secure and Distinct Passwords

Your password is the first line of defense.
A strong password should:

- Contain at least 12 characters.
- Mix numbers, uppercase/lowercase letters, and symbols (!, @, #).
- Avoid personal info (birthdays, names, "123456," or "password").
- Be unique for each account.

💡 Tip: Use a Password Manager (e.g., **LastPass, Bitwarden, 1Password**) to store and generate secure passwords.

📉 Avoid Credential Stuffing: When one password is leaked, hackers can access multiple accounts using that same login.

B. Two-Factor Authentication (2FA)

An extra layer of protection that requires a temporary code (sent via SMS, email, or authenticator app) in addition to your password.

Even if your password is stolen, attackers can't access your account without this code.

Enable 2FA in your account's Security Settings, it's simple and powerful.

C. Protecting Yourself from Phishing Scams

Phishing attempts often look like messages from trusted organizations asking for personal info.
How to Spot a Phishing Email:

- Suspicious sender or email address.
- Urgent tone ("Your account will be suspended!").
- Links with misspellings or strange domains.
- Grammar or spelling mistakes.

Rule: Don't click unfamiliar links — verify directly through the official website instead.

D. Keep Apps and Software Updated

Updates fix security bugs and improve performance.

- Turn on Automatic Updates to stay protected.
- Don't ignore update notifications — outdated software is a hacker's favorite target.

E. VPNs and Public Wi-Fi

Public Wi-Fi **(airports, cafés, libraries)** is convenient but risky hackers can intercept your data.

Using a VPN (Virtual Private Network) encrypts your connection, making your information unreadable to others.

Recommended VPNs: **WireGuard, OpenVPN, SoftEther**.
They offer strong encryption, privacy protection, and no data logs.

F. Messaging via Encryption

Use end-to-end encrypted apps like Signal or WhatsApp to ensure only you and the receiver can read your messages.
Why it matters:

- Prevents hackers or service providers from accessing your messages.
- Protects sensitive conversations.
- Keeps your digital footprint private.

G. Recognizing and Avoiding Online Threats

Cybercriminals often use fake links or malware.
Protect yourself by:

- Checking links before clicking (**hover on PC, long-press on mobile**).
- Using tools like VirusTotal to scan suspicious URLs.
- Avoiding oversharing personal data (**like date of birth or location**).
- Visiting only secure sites (**"https://" and lock icon**).

SOCIAL MEDIA THREATS: PROTECTING YOUR DIGITAL FOOTPRINT

In today's digitally connected world, social media has transformed the way we communicate, share, and connect. Yet, this convenience comes with hidden dangers that threaten our privacy, security, and online reputation. Understanding these threats is the first step toward safeguarding your personal data and maintaining control over your digital identity. Below are some of the key social media threats users should be aware of :

🔐 Identity Theft

Cybercriminals exploit personal information shared online —such as your full name, birthday, or contact details—to impersonate individuals, conduct financial fraud, or gain unauthorized access to private accounts.

Tip: Avoid posting identifiable details and use strict privacy settings to limit who can view your profile.

🎭 Fake Profiles and Social Engineering

Scammers often create convincing fake profiles to build trust, manipulate emotions, or trick users into revealing sensitive information.

These tactics rely on human psychology and can easily bypass traditional security measures.

Tip: Verify friend requests or messages from unfamiliar accounts before interacting.

📍 Oversharing and Privacy Breaches

Sharing too much—your daily routine, travel plans, or location—can expose you to stalking, harassment, or even physical harm.
Publicly available personal data also makes it easier for attackers to target you.

Tip: Think before you post — once something is online, it's hard to remove completely.

📊 Data Harvesting and Profiling

Social media platforms, advertisers, and data brokers continuously collect and analyze user data for marketing or political purposes—often without explicit consent.

This undermines digital privacy and personal autonomy.

Tip: Regularly review app permissions and adjust your privacy settings to minimize data collection.

⚠️ Platform Vulnerabilities and Cyber Attacks

Weak privacy controls or unpatched security flaws on social platforms can allow hackers to launch phishing campaigns, spread malware, or take over accounts.

Tip: Enable two-factor authentication (2FA) and keep your apps updated to strengthen your defense.

💬 Reputation Damage

Inappropriate posts, misinformation, or leaked private content can cause long-term harm to your personal and professional image.

Tip: Maintain a positive digital presence—think of your online footprint as part of your public identity.

SOCIAL MEDIA PRIVACY MANAGEMENT

Social media platforms are powerful tools for communication, collaboration, and connection.
However, they also collect vast amounts of personal data — often more than users realize.
Information shared innocently online can be exploited for identity theft, fraud, or targeted marketing.
Managing your privacy settings thoughtfully helps protect both your personal data and online reputation.

Take into account the following to keep control of your social media digital footprint:

Regularly Review and Adjust Privacy Settings

Most platforms — such as **Facebook**, **Instagram**, and **X** (formerly **Twitter**) — offer customizable privacy controls.

Review these settings frequently to determine who can view your posts, friend list, and location.
For example, switch visibility to "Friends Only" or adjust settings for each individual post.

Tip: Set a monthly reminder to check your privacy settings — platforms often update policies silently.

🔒 Limit Sharing of Sensitive Information

Avoid posting details such as your home address, phone number, daily routine, or vacation plans.
Oversharing increases risks of stalking, harassment, or physical theft.

Tip: When posting travel photos, wait until you return home.

👥 Be Cautious with Friend or Follow Requests

Not all connection requests come from real people.
Fake accounts are often used for data harvesting or phishing scams.

Tip: Connect only with people you know and trust — and report suspicious profiles immediately.

👁️ Control Visibility of Your Activity

Your likes, comments, and shared posts reveal more about you than you think.
Adjust settings to limit who can see your interactions and prevent unnecessary exposure.

Pro Tip: Review your activity log to monitor what others can see about you.

💡 Understand How Your Data Is Used

Most social media companies profit by selling user data or using it to tailor advertisements.
Understanding these practices empowers you to decide what information to share publicly.

Tip: Read privacy policies carefully and disable ad personalization features where possible.

03

Digital Rights, Freedom of Expression & Cybercrime Laws

OVERVIEW OF DIGITAL HUMAN RIGHTS

In today's interconnected world, digital human rights extend traditional human rights principles into the online environment — ensuring that individuals enjoy the same dignity, security, and freedoms in the digital space as they do offline.

These rights protect users from discrimination, surveillance, and censorship, while promoting freedom of expression, privacy, digital security, and access to information.

They are grounded in international legal frameworks such as:

- 🕊️ The Universal Declaration of Human Rights (UDHR)
- ⚖️ The International Covenant on Civil and Political Rights (ICCPR)
- 🌐 UN Mandates on Digital Freedom (OHCHR, UN Human Rights Office)

Together, these frameworks safeguard users' rights to participate, communicate, and thrive in the digital age.

MAJOR COMPONENTS OF DIGITAL HUMAN RIGHTS

Privacy: Protecting Personal Boundaries Online

Determined through GPS, IP addresses, Wi-Fi, cell towers, or even Bluetooth beacons—even without direct permission.

Access to Information: Empowering Participation

Access to digital information is a fundamental right that allows individuals to seek, receive, and share knowledge through any media platform including the internet.

Digital Security: The Foundation of Online Freedom

digital security underpins all digital rights. It involves protecting networks, systems, and personal data from unauthorized access and cyber threats — creating a safe environment for communication and self-expression.

Non-Discrimination: Equal Rights in the Digital Space

The principle of non-discrimination guarantees that everyone enjoys equal digital opportunities, regardless of gender, race, religion, disability, or background

FREEDOM OF EXPRESSION ONLINE

Freedom of expression is a cornerstone of human rights and democracy and it fully extends to the digital sphere. It ensures that individuals can share ideas, access information, and participate in discussions online without unjust restrictions. However, this freedom also comes with responsibilities and lawful boundaries to protect others and maintain social order.

Legal Foundations

The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) guarantee the right to freely seek, receive, and impart information and ideas through any medium oral, written, printed, artistic, or digital without borders.

Restrictions may only apply when they:

- Are clearly established by law.
- Pursue a legitimate goal such as national security, public order, or respect for the rights of others.
- Are proportionate and necessary in a democratic society.

Reasonable Restrictions

International frameworks outline limited situations where speech can be lawfully restricted:

- **Hate Speech:** Prohibited under Article 20(2) of the ICCPR for promoting hatred, discrimination, or violence.
- **Defamation:** Speech that unjustly harms someone's reputation may be subject to legal remedies.
- **Disinformation:** False or harmful content that poses threats to public safety or health can be regulated.

Threats to Digital Expression

New digital challenges complicate how expression functions online:

- **Vague Laws:** Ambiguous terms like "fake news" or "anti-national speech" are often used to silence dissent.
- **Unjustified Takedowns**: Platforms or governments may remove content without transparent justification.
- **Fear of Retaliation**: Online harassment, lawsuits, or surveillance discourage people from speaking freely.

Role of Digital Platforms

Private technology companies have immense influence over what users can see and say online.

- They determine what content stays or gets removed.
- Human rights organizations urge them to follow transparent, accountable policies consistent with international law.
- Independent oversight and appeal mechanisms are essential to ensure fairness.

CYBERCRIME LAWS IN THE MENA REGION

Overview

Governments across the Middle East and North Africa (MENA) have introduced or updated cybercrime laws to combat online fraud, misinformation, harassment, and digital threats.
These laws aim to:

- Strengthen cybersecurity infrastructure
- Enhance user protection
- Align with international standards

However, human rights organizations caution that broad definitions and limited oversight in some laws could open the door to censorship, privacy violations, and restrictions on free expression.

Jordan: Cybercrime Law No. 17 (2023)

- Replaced the 2015 law with expanded definitions and stricter penalties.
- Covers disinformation, online harassment, and financial fraud.
- Supporters say: It enhances accountability and online safety.
- Critics warn: Vague terms like "spreading fake news" or "provoking strife" could be used to silence legitimate voices.

United Arab Emirates: Federal Decree Law No. 34 (2021)

- Updated previous legislation on cybercrime and digital misinformation.
- Increased penalties for defamation and unauthorized data access.
- Added clauses criminalizing certain political or moral online content.
- Concerns: May suppress dissent or limit civic engagement.

Regional Context: Saudi Arabia, Egypt, Tunisia

Other MENA countries have enacted similar laws targeting online threats.
While these aim to promote digital safety, experts emphasize:

- Clear legal definitions
- Independent judiciary
- Transparency in enforcement
- Strong data protection policies

04

Do's and Don'ts for Safe and Responsible Digital Engagement

INTRODUCTION

The internet is an amazing environment for connecting, learning, and creating, but careless mistakes like a click of the wrong button or a hurried post on social media can have dire consequences for your safety, reputation, and opportunities. In previous units you learned how to navigate the online world using digital literacy skills, you learned ways to protect your privacy and security, and learned your rights and responsibilities under digital laws. This final unit brings everything together into a useful action guide of Do's and Don'ts actions that support safe habits, trust, and positive use of technology, and risky behaviour you want to avoid to mitigate threats and prevent harm.

THE DO'S POSITIVE DIGITAL PRACTICES

Having good digital habits protects your personal information and reputation online. If you embrace the good habits mentioned in this post, you will build trust and help create a safe digital world for yourself and everyone else. These Do's make it easier for you to use technology wisely and appropriately.

Protect Your Personal Information

- Create strong, unique passwords for every account.
- Never share personal details like your phone number or home address publicly.
- Enable Two-Factor Authentication (2FA) on all important accounts.
- Keep your device software and apps regularly updated.

Think Before You Click

- Verify the source of links, attachments, and downloads before opening them.
- Avoid clicking anything that looks suspicious or unexpected.
- Use safety tools such as antivirus, spam filters, or URL checkers:
  VirusTotal
  Cloudflare Radar

Be Kind and Professional Online

- Communicate clearly, respectfully, and politely.
- Avoid using offensive or inflammatory language.
- Treat every online conversation as if it were face-to-face.
- Build a positive digital reputation through empathy and respect.

Credit Your Sources

- Always acknowledge the creators of any content you use or share.
- Respect copyright and intellectual property laws.
- Add citations or attributions when reposting or remixing work.

Report Harmful or Illegal Content

- Use platform reporting tools for fake profiles, harassment, or illegal posts.
- Inform trusted adults or authorities if the situation is serious.
- Be a role model for positive digital behavior — encourage others to act responsibly.

THE DON'TS RISKY OR HARMFUL DIGITAL BEHAVIORS

Many risky online behaviors can be avoided to limit your chances of experiencing harm online, and also preserve your positive digital trail. These Don'ts are demonstrated for commonly poor choices that allow harmful or insecure behaviors and decisions to impact your security measures, legal issues, or interpersonal relationships. Be aware of your opportunities to make choices that can protect your positive digital well-being.

Don't Share Too Much Personal Information

- Don't divulge your exact location, activities, or personal information publicly.
- Don't disclose your financial matters or official documents online.
- Be wary to not mention sensitive things in photos or status updates.

Don’t Engage in Cyberbullying or Harassment

- Don't send threatening, hurtful, insulting or harmful messages.
- Don't participate in gossip or group chats that are negative.
- Follow the rules of others and report if you see/or hear abuse.

Don’t Ignore Privacy Settings

- Regularly go through your social media privacy controls and change them.
- You can control who sees your profiles, only have people that you trust.
- When not needed, shut down the location settings.

Don't Contribute to the Spread of Misinformation

- Before you share anything news or opinion based, ensure its facts.
- Don't forward messages and chains that are sensational or "fake."
- Use trusted news sources or communication that is official.

Don't Click on Links That Look Suspicious

- Don't click on links sent to you by unknown senders, don't visit strange websites.
- Don't download files from the sources you don't trust.
- Never trust pop-ups or offers that seem too good to be true.