



Co-funded by
the European Union

MODULE 07

DIGITAL CITIZENSHIP

DIGITAL RURAL EUROPEAN ART
AND MEMORY



Project partners



Project DREAM
Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122



Co-funded by
the European Union

Project information:

DREAM - Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122

Funded by the European Union. However, the views and positions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or SAAIC. Neither the European Union nor the granting authority can be held responsible for them.



How to use this E-book

You can read this material before, during or after the learning session. First, you will explore what digital citizenship means and why access alone does not guarantee inclusion. Next, you will practice how to verify public information, recognize risks and use digital identity more safely. You will then create a practical route card for a real public service and test whether another person could follow it.

Each section includes a short practical or reflective task. These tasks are designed to help you connect the concepts with everyday situations. You do not need to use real passwords, identification numbers or personal documents at any point. When a task involves a public service, stop before any real submission and work only with publicly available information.

At the end of the e-book you will find an integrated final activity, a peer-review checklist, a digital wellbeing tip, a glossary and a reference list. The final output is a Public Service Route Card: a clear, safe and community-oriented guide that another person could use as a starting point.

MODULE INFORMATION

 Module number 07	 Level Beginner
 Topic Safe and confident participation in digital public life	 Format Hybrid learning
 Duration 3 hours	 Main output Public Service Route Card

About this module

Public life is increasingly digital. People search for official information, make appointments, submit requests, obtain documents, contact institutions and participate in community decisions through websites and online portals. These services can save time and reduce travel, but they can also feel difficult when the information is unclear, the identification process is unfamiliar or there is no obvious person to ask for help. Digital citizenship includes access, safety, rights and participation. It also includes the ability to help another person understand a public procedure, to ask institutions for support and to take part in decisions affecting local places, traditions and shared memory. In rural communities, where distance and limited support can create additional barriers, clear guidance and cooperation can make digital services more meaningful and inclusive.

The purpose of this module is to help you move through digital public life more safely, confidently and independently. It combines practical digital skills with critical judgement, privacy awareness and community participation. The focus is on understanding who provides a service, checking whether information can be trusted, protecting personal data and knowing what to do when a digital route does not work. The aim is not to memorise every national portal or identification system. The aim is to learn a transferable method: identify the responsible institution, locate the official route, verify the source, understand the steps, protect personal data, find help and explain the process clearly to another person.



Learning Objectives

- Understand digital citizenship as access, safety, rights and participation in online and offline communities.
- Recognise the legal, social and practical dimensions of citizenship.
- Explain why access to a device or internet connection does not automatically lead to meaningful digital inclusion
- Find official public-service websites, portals, notices and contact points.
- Check whether public information is current, trustworthy and connected to the responsible institution.
- Apply lateral reading and two-source confirmation when evaluating an unfamiliar page.
- Distinguish outdated information, misinformation, disinformation and scams.
- Recognise common warning signs of messages that imitate a public authority.
- Map the stages of an online public-service procedure, including help and alternative routes.
- Create and peer-review a Public Service Route Card.

Index

0. Before You Begin: My Starting Point	3
1. What is Digital Citizenship?	4
2. Three Connected Dimensions of Digital Citizenship	6
3. Access, Inclusion and Rural Communities	7
4. European Digital Rights and Principles	7
5. Digital Public Services and the Service Journey	9
6. Finding Official Public Information	11
7. Verifying Sources Through Lateral Reading	12
8. Outdated Information, Misinformation, Disinformation and Scams	13
9. Personal Data, Authentication and Safe Access	16
10. Digital Citizenship and Cultural Participation	17
11. Final Activity: Public Service Route Card.....	18
12. Share and Peer Review	23
13. Digital Wellbeing Tip	24
14. Basic Glossary	25
15. Module Closing.....	26
Bibliography	27

0. Before You Begin: My Starting Point

Before starting the module, rate each statement from 1 to 5. Use 1 when you cannot do the task yet and 5 when you can do it independently. This is not a test. It is a way to notice your starting point and later recognise your progress.

- I can find the official website for a public service.
- I can check whether public information is current and trustworthy.
- I understand when and why a service asks for digital identification.
- I can recognise suspicious messages that imitate a public authority.
- I can explain the main steps of an online public procedure to another person

Keep your ratings. You will return to the same statements at the end of the module.

1. What is Digital Citizenship?

Citizenship can be understood in several connected ways. As a legal status, it describes the formal relationship between a person and a state, including recognised rights and responsibilities. As belonging, it describes a sense of connection to a community, place, culture or shared political space. As practice, it means taking part in public life, cooperating with others, asking questions, holding institutions accountable and contributing to common concerns.



Key Concepts

Citizenship as legal status: A formal relationship between a person and a state, including recognised rights and responsibilities.

Citizenship as belonging: A sense of connection to a community, place, culture or shared political space.

Citizenship as practice: Participation in public life through cooperation, questions, accountability and contribution to shared concerns.

Digital citizenship: The application of access, rights, responsibilities, judgement and participation in digital environments.

Digital citizenship applies these rights, responsibilities and forms of participation in digital environments. It is the capacity to participate actively, continuously and responsibly in communities online and offline through competent and positive engagement with digital technologies. A digital citizen does more than operate a device. They can access opportunities, evaluate information, protect rights, respect others and participate in public and community life.

For this reason, digital citizenship is not limited to polite online behaviour. It also includes information literacy, critical thinking, participation, ethics and the ability to challenge exclusion or manipulation. The concept connects practical skills with judgement and responsibility. A person may know how to click through a website but still need support to decide whether the page is official, whether a request is appropriate or whether a service is

accessible and fair (Council of Europe, 2019, 2025; Richardson & Milovidov, 2022; European Commission, Joint Research Centre, 2025).



Reflection

Think about one recent digital action connected to public or community life. It may have involved searching for information, making an appointment, contacting a municipality, reading a public notice, joining a consultation or helping another person with an online form. Which aspect of citizenship was present: legal status, belonging, practice or more than one?

2. Three Connected Dimensions of Digital Citizenship

The Council of Europe (2019) describes digital citizenship through three connected dimensions: being online, well-being online and rights online. These dimensions overlap. A person needs access and skills, but also safety, respect, privacy and meaningful opportunities to participate.

Being online: This includes access, inclusion, learning, creativity and media literacy. In everyday public life, it may mean finding the correct official portal and understanding the information provided there.

Well-being online: This includes safety, health, empathy and responsible use. It may mean avoiding pressure, recognising scams, limiting unnecessary sharing of personal data and asking for support when a process becomes overwhelming.

Rights online: This includes participation, privacy, consumer awareness and democratic rights. It may mean using a public service, giving feedback, joining a consultation or requesting information from an institution.

These dimensions show why digital citizenship is both personal and social. The individual needs confidence and skills, while institutions need to provide understandable, safe and accessible services. Communities also play a role when people share knowledge, support one another and identify barriers that should be addressed.



Practical Task

Choose one digital public action, such as booking an appointment or finding information about a cultural programme. Write one example of what the person needs in each dimension: being online, well-being online and rights online. Identify which dimension is most likely to create a barrier.

3. Access, Inclusion and Rural Communities

Digital citizenship involves access, judgement and action. A person may have a smartphone and an internet connection but still be excluded if a service is difficult to understand, requires unfamiliar identification, uses complex language or provides no human support. Digital inclusion therefore has several levels: access to technology, skills to use it and the ability to achieve a meaningful result (Correa & Pavez, 2016; Morte-Nadal & Esteban-Navarro, 2025).

Digital public services can be especially valuable in rural communities because they can reduce travel, waiting time and dependence on office opening hours. At the same time, slow connections, mobile-only access, limited transport, unfamiliar systems and fewer local support points can make the same services harder to use. Confidence, trust, clear information and the possibility of asking a person for help strongly influence whether someone completes a procedure or gives up.



Practical Task

Imagine that a resident must use an online service but has only a smartphone and an unstable connection. Identify one barrier related to access, one related to skills and one related to achieving the final result. For each barrier, suggest a form of support that protects the person's independence and privacy.

4. European Digital Rights and Principles

The European approach to digital transformation is human-centred. Technology should serve people, strengthen participation and respect the same rights online that apply offline. The *European Declaration on Digital Rights and Principles* presents a shared direction for a digital transformation that is fair, safe and inclusive.



Key Concepts

- People and their rights should be at the centre of digital transformation.
- No one should be left behind.
- Everyone should be able to gain the skills needed to participate.
- People should have access to key digital public services.
- Digital spaces should support informed choice, participation, safety and sustainability.

These principles are relevant when evaluating a public service. A service may be technically available but still exclude people through inaccessible language, unclear procedures, poor mobile design or lack of support. Digital rights therefore concern both protection from harm and the positive ability to participate (European Parliament, Council of the European Union, & European Commission, 2023; European Commission, 2026a).



Reflection

Choose one digital service you know. Which principle does it support well? Which principle could be strengthened? Base your answer on a concrete feature, such as accessibility, clear instructions, privacy information, human assistance or an offline alternative.

5. Digital Public Services and the Service Journey

Digital public services allow people to obtain information, submit requests, make appointments, provide evidence, receive decisions or communicate with public institutions online. The *EU Digital Decade* treats digital public services as one of the four main areas of Europe's digital transformation (European Parliament & Council of the European Union, 2022; European Commission, 2026b).

A public service should be understood as a journey rather than a single webpage. The user first needs to find the correct route, then understand the service, prepare what is required, identify securely, complete the action, confirm that it was received and know where to get help. A clear route includes all of these stages.



Key Concepts

Find: Where is the official information or portal?

Understand: Who can use the service and what result does it provide?

Prepare: Which documents, data, fees and deadlines are required?

Authenticate: Is a digital identity, password, code or electronic signature required?

Act: Which form, upload, appointment, payment or other action is involved?

Confirm: How will the user know that the action was received or completed?

Get help: Where can the user ask a question, correct an error, appeal or use another channel?

This journey provides a practical structure for analysing almost any digital public procedure, even when national portals and identification systems differ (European Parliament & Council of the European Union, 2018; Morte-Nadal & Esteban-Navarro, 2025).



Practical Task

Choose a familiar public service and describe its journey using the seven stages above. You do not need to open an account or submit anything. Note which stage is easiest to understand and which stage would be most difficult to explain to another person.

6. Finding Official Public Information

Search engines, social media posts, news articles and private advice pages may help you discover a topic, but they should not replace information from the institution responsible for the service. Search summaries can also remove context, show outdated details or place unofficial pages above official results.

Official public information normally includes information published by the responsible public institution; a national, regional, municipal or European portal linked by that institution; a complete official notice, law, form, procedure or guidance document; or an authorised assistance service or contact point (European Parliament & Council of the European Union, 2018; European Commission, Joint Research Centre, 2025).



Key Concepts

The central question is not simply: *“Does this page look official?”*

The better question is: *“Who is responsible for this service, and can I confirm that this page belongs to or is authorised by that institution?”*

This shift from appearance to responsibility is essential because designs, logos and familiar colours can be copied.

7. Verifying Sources Through Lateral Reading

A professional-looking page is not automatically trustworthy. Country domains differ, so there is no single ending such as .gov that proves a page is official everywhere. Verification requires several checks: identify the institution named on the page, read the complete web address, look for contact and legal information, and confirm that the institution is actually responsible for the service (McGrew, 2024; Moore & Hancock, 2022; European Commission, Joint Research Centre, 2025).

Professional fact-checkers often use a method called **lateral reading**. Instead of remaining inside an unfamiliar page and studying only its design or wording, they open another tab and search for information about the source, organisation or claim. They find the institution's official homepage or legal notice, check whether the service is linked from another trusted public source and return to the original page only after confirming who is behind it (Brodsky et al., 2021; McGrew, 2024).

Lateral reading is useful because a page can provide convincing information about itself. Independent confirmation is stronger. A second official source may be another government portal, the institution's homepage, an official contact page, an authorised help service or a published notice that links to the same procedure.

A Simple Verification Routine

1. Name the institution that should be responsible for the service.
2. Check the complete web address rather than only the page title.
3. Open a new tab and search for the institution separately.
4. Find the official homepage, contact page or legal notice.
5. Confirm the service through a second official source or contact point.
6. Return to the original page only after the source has been verified.

8. Outdated Information, Misinformation, Disinformation and Scams

When using digital public services, finding information online is only the first step. You also need to decide whether the information is **current**, **accurate** and **trustworthy**. A page can look professional and still contain outdated information, while a message that appears to come from an official institution may actually have been created to deceive you. Not every incorrect or harmful piece of information is the same. Understanding the type of problem helps you decide what to check and how to respond.



Key Concepts

Outdated information: The source may once have been correct, but a date, form, fee or deadline has changed. The correct response is to find the current official version.

Misinformation: False or misleading information may be shared without an intention to deceive. Verify it before acting or sharing it.

Disinformation: False or manipulated information is deliberately created or spread. Check the evidence and report it where appropriate.

Scam or impersonation: A person imitates an authority to obtain money, credentials or personal data. Stop, do not click or pay, and contact the authority through an independently found official route.

These problems can sometimes **overlap**. A fraudulent message may contain disinformation, imitate a public institution and direct the user to a fake website. This is why it is important to check not only what a message says, but also who sent it, where the link leads and what the message asks you to do.

Figure 1

Example of bank phishing email

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.ameribank7.com/reset-password>

Thank you,

Bank America

Note. From Example bank phishing email [Vector graphic], by Isochrone and Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_bank_phishing_email.svg). CC BY 4.0.

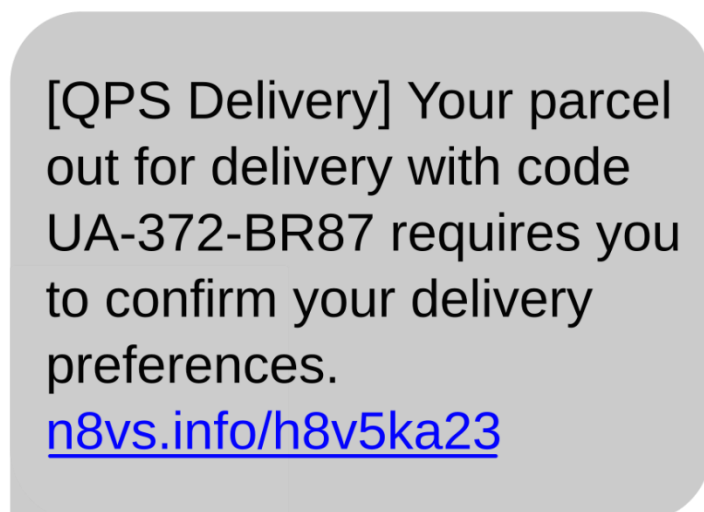
Public-service scams often create pressure so that the recipient acts before checking. They may copy official logos, use a sender name similar to a real institution or claim that a benefit, fine, account or document is at immediate risk.

Common Warning Signs

- Unexpected urgency, such as a demand to act immediately or lose a benefit.
- A request for passwords, full access codes or remote control of the device.
- Payment through gift cards, cryptocurrency or an unusual private account.
- A shortened, misspelled or unrelated web address.
- A message that asks the user to log in through a link instead of the official portal.
- A sender name that does not match the email address or telephone number.
- A threat or instruction that discourages checking with the institution.

Figure 2

Example of Phishing SMS



Note. Image showing a fictional example of a parcel delivery SMS phishing message. From Example phishing SMS [Vector graphic], by Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_phishing_SMS.svg). CC0 1.0.

9. Personal Data, Authentication and Safe Access

Personal data is information that identifies a person or can be connected to them, such as a name, identification number, address, photograph, location or account information. Under the GDPR, personal data should be collected for a clear purpose and limited to what is necessary for that purpose (European Parliament & Council of the European Union, 2016).

When a public service asks for information, read why the data is requested and who will receive it. Connect each requested item with the service purpose. Avoid sending identity documents through an unofficial message or email. Never reuse or share authentication codes. Confirmation messages and official receipts may be important, but they should be stored securely.

Transferable Safety Principles

- Start from the official service portal, not from a link in an unexpected message.
- Check which identification method the portal officially accepts.
- Use your own device where possible and close the session when finished.
- Never tell another person your password, PIN or full one-time code.
- Do not allow an unknown caller to guide you through identity verification.
- Ask the official service for assisted access when the process is unclear.

10. Digital Citizenship and Cultural Participation

Digital citizenship also includes cultural participation. *The Faro Convention* links cultural heritage with participation, shared responsibility and democratic life. Cultural heritage is not only something that institutions protect on behalf of residents. People can contribute knowledge, express concerns, participate in decisions and help shape how local places, traditions and memories are understood (Council of Europe, 2005, 2019).

Digital tools can help residents access cultural information, communicate with institutions and contribute to decisions about local heritage. A digital citizen may use official tools to request access to an archive, report damage to a monument, register for a cultural programme, submit a question, join a public consultation or contact the institution responsible for a heritage asset.



Practical Task

Identify one local place, tradition, collection, event or community concern that may involve a public institution. What information or service might a resident need? Name the likely responsible institution and the practical result the person would want to achieve.

11. Final Activity: Public Service Route Card

Working in pairs or small groups, prepare one clear route for accessing a real public service. The route should connect to local heritage or community life. The trainer may provide suitable national or local examples because public portals and identification systems differ between countries.



Possible Service Scenarios



Heritage or community examples *may include*

- reporting damage to a monument or public heritage place
- requesting access to a municipal or regional archive
- registering for a municipal cultural programme
- finding a public consultation on local development or heritage
- finding the official procedure for using public space for a community cultural activity



Everyday alternatives *may include*

- booking an official appointment
- obtaining a certificate or official document
- finding information about employment or social support
- submitting a question or complaint to an authority
- changing or correcting information in a public record

Remember: *The output is not a completed application and must not contain real personal information. It is a practical guide showing how a person can find, verify and understand the official process. Stop before any real submission, payment or identity verification.*

Route Card Project Sheet

Service and purpose: What the service does and why a person may need it.

Responsible institution: The authority that manages the service.

Verified official source: The official portal or document and how it was confirmed.

Eligibility and preparation: Who can use the service, required documents, fees and deadlines.

Steps: A short, numbered route from the entry page to confirmation.

Digital identity: Whether login, eID, electronic signature or another method is required.

Privacy and safety: Data requested, safe-login reminders and one relevant scam warning.

Help and alternatives: Official contact, assistance, accessibility or an offline option.

Participation link: How the service supports community or cultural participation.

Step 1: Define the Service Need

Complete the sentence: “A person in our community needs to _____ because _____.”

Name a specific person or group, choose one concrete service and explain the practical result the person needs. A focused need makes the route easier to verify and explain.

Step 2: Locate the Official Route

1. Search the service name together with the responsible municipality, region, ministry or EU institution.
2. Open the result that appears to belong to the responsible authority.
3. Check the full web address.
4. Find the institution’s homepage, contact page or legal notice.
5. Confirm the route through a second official source.

Step 3: Complete the Five-Point Verification Check

The Five-Point Verification Check combines source verification, assessment of information currency, awareness of personal-data requests and independent confirmation.

Responsible authority: Name the public institution, authority or authorised organisation responsible for the service.

Official web address: Copy or record the complete web address. Check that the domain belongs to the responsible institution or to an authorised public-service portal.

Current information: Record the publication date, update date, version, current deadline or another indication that the information is still valid.

Appropriate data request: Note what personal information the service asks you to provide. Consider whether the requested information is necessary and appropriate for the stated purpose.

Independent confirmation: Name a second official source or contact point that confirms that this is the correct route to the service.

The Five-Point Verification Check combines source verification, assessment of information currency, awareness of personal-data requests and independent confirmation.

Step 4: Map the Procedure

Write the route as short, numbered actions. Begin before login and stop before any real submission.

1. Open the official service page.
2. Check eligibility and the purpose of the service.
3. Prepare the required documents or information.
4. Choose the correct identification or access method.
5. Complete the form, upload, appointment or other action.
6. Check fees, deadlines and expected processing time.
7. Save the confirmation or reference number.
8. Use the official help route if something goes wrong.

The card should describe the complete route, including confirmation and support, rather than only the first page.

Step 5: Identify Digital Identity and Personal Data

Login requirement: Record whether login is not required, required only for submission or required from the beginning.

Authentication method: Record the accepted method, such as national eID, wallet, mobile application, password, code, electronic signature or another method.

Personal data requested: List only data categories, never real participant data.

Purpose of the data: Connect each category with the service purpose.

Information that must not be shared: Include passwords, PINs, full one-time codes and unrelated documents.

Step 6: Find Help, Accessibility and Alternatives

A complete route includes what to do when the ideal digital process does not work. Look for:

- an official telephone number or email address
- a physical office or appointment option

- an assisted-digital service or authorised support point
- a procedure for correcting an error, making a complaint or appealing

12. Share and Peer Review

Exchange your route card with another pair or group. The reviewers should first examine the card without receiving an explanation from its creators. This simulates the situation in which a community member opens the guide independently.

Peer-Review Questions

Can we identify the service and the responsible institution?

Are the steps complete and in a logical order?

Is the authentication method explained safely?

Are the required documents, fees and deadlines clear?

Can we find help or an alternative route?

Is the safety warning relevant?



Reflection

What part of the route was easiest to explain? Which change made the card safer, clearer or more inclusive?

13. Digital Wellbeing Tip



Digital Wellbeing Tip

One Screen, One Task

Digital learning can feel exhausting when too many tabs, messages and tools compete for attention. Focusing on one visible task makes learning calmer and more manageable.

Try this: For the next short work period, close or minimise everything that is not needed. Keep only the task, template, file or webpage you are using now.

Reflection question: What is the one digital action I need to complete now?

This habit is particularly useful during public-service procedures, where distraction can lead to missed instructions, accidental sharing or unfinished steps.

14. Basic Glossary

Accessibility: The design of information, services and tools so that people with different needs and abilities can use them.

Assisted digital access: Official support that helps a person use a digital service without taking away their control or privacy.

Authentication: The process used to confirm that a person is authorised to access an account or service.

Digital citizenship: Active, continuous and responsible participation in online and offline communities through competent use of digital technologies.

Digital identity: A method or set of information used to prove identity in a digital environment.

Digital inclusion: The ability to access technology, use it with appropriate skills and achieve a meaningful result.

Disinformation: False or manipulated information deliberately created or spread to deceive.

Electronic signature: A digital method used to sign or approve a document or action.

GDPR: The EU General Data Protection Regulation, which sets rules for processing and protecting personal data.

Lateral reading: Leaving an unfamiliar page and checking independent sources to verify who is behind it and whether its claims are reliable.

Misinformation: False or misleading information shared without necessarily intending to deceive.

Official source: Information published or authorised by the public institution responsible for a service.

Personal data: Information that identifies a person or can be connected to them.

Public service: Information, assistance or a procedure provided by a public institution, such as appointments, documents, applications or consultations.

Scam or impersonation: An attempt to imitate a trusted person or institution in order to obtain money, credentials or personal data.

Service journey: The complete route from finding official information to preparation, authentication, action, confirmation and help.

Two-source confirmation: Verification of a route or claim through a second independent official source or contact point.

Public Service Route Card: A clear guide that records the official source, procedure, safety reminders, help options and alternatives for a public service.

15. Module Closing

Digital citizenship is the ability to participate in digital public life with access, judgement, safety and awareness of rights. It is not only an individual skill. It also depends on understandable institutions, accessible services and communities in which people can ask for support without losing control of their private information.

By the end of this module, you should be able to find and verify official public information, explain the stages of a public-service procedure, protect personal data, recognise common risks and create a route that another person can follow. The Public Service Route Card demonstrates not only what you know, but how that knowledge can support participation in your community.

Bibliography

- Belbury. (2025). Example phishing SMS [Vector graphic]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Example_phishing_SMS.svg
- Brodsky, J. E., Brooks, P. J., Scimeca, D., Todorova, R., Galati, P., Batson, M., ... & Caulfield, M. (2021). Improving college students' fact-checking strategies through lateral reading instruction in a general education civics course. *Cognitive research: principles and implications*, 6(1), 23. <https://doi.org/10.1186/s41235-021-00291-4>
- Correa, T., & Pavez, I. (2016). Digital inclusion in rural areas: A qualitative exploration of challenges faced by people from isolated communities. *Journal of Computer-Mediated Communication*, 21(3), 247-263. <https://doi.org/10.1111/jcc4.12184>
- Council of Europe. (2005). *Council of Europe Framework Convention on the Value of Cultural Heritage for Society* (CETS No. 199). <https://www.coe.int/en/web/culture-and-heritage/faro-convention>
- Council of Europe. (2019). *Digital citizenship education handbook*. Council of Europe Publishing. <https://book.coe.int/en/human-rights-democratic-citizenship-and-interculturalism/7851-digital-citizenship-education-handbook.html>
- Council of Europe. (2025). *Digital citizenship education*. <https://www.coe.int/en/web/education/digital-citizenship-education>
- Council of Europe. (2026). *Implementation of Recommendation CM/Rec(2019)10 on developing and promoting digital citizenship education: State of play*. Council of Europe Publishing.
- European Commission. (2022). *European Declaration on Digital Rights and Principles*. <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>
- European Commission. (2026a). *European Digital Rights and Principles*. <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>
- European Commission. (2026b). *Europe's Digital Decade*. <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

- European Commission. (2026c). *European Digital Identity*.
https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en
- European Commission, Joint Research Centre. (2025). DigComp 3.0: The Digital Competence Framework for Citizens. https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp/digcomp-30_en
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L 119, 1–88.
- European Parliament and Council of the European Union. (2018). Regulation (EU) 2018/1724 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services. Official Journal of the European Union, L 295, 1–38.
- European Parliament and Council of the European Union. (2022). Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030. Official Journal of the European Union, L 323, 4–26.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, L 2024/1183.
- European Parliament, Council of the European Union, & European Commission. (2023). European Declaration on Digital Rights and Principles for the Digital Decade. Official Journal of the European Union, C 23, 1–7.
- Isochrone, & Belbury. (2025). Example bank phishing email [Vector graphic]. Wikimedia Commons.
https://commons.wikimedia.org/wiki/File:Example_bank_phishing_email.svg
- Jurišić, I., & Bogataj, D. (2024). Enhancing digital government engagement among older adults: Literature review and research agenda. *IFAC-PapersOnLine*, 58(3), 256-261.
<https://doi.org/10.1016/j.ifacol.2024.07.160>

- Lee-Geiller, S. (2024). The moderating effect of digital literacy on the link between e-government effectiveness and trust in government. *Journal of Policy Studies*, 39(4), 77-101. <https://doi.org/10.52372/jps.e672>
- McGrew, S. (2024). Teaching lateral reading: Interventions to help people read like fact checkers. *Current Opinion in Psychology*, 55, 101737. <https://doi.org/10.1016/j.copsyc.2023.101737>
- Moore, R. C., & Hancock, J. T. (2022). A digital media literacy intervention for older adults improves resilience to fake news. *Scientific reports*, 12(1), 6008. <https://doi.org/10.1038/s41598-022-08437-0>
- Morte-Nadal, T., & Esteban-Navarro, M. Á. (2025). Recommendations for digital inclusion in the use of European digital public services. *Humanities and Social Sciences Communications*, 12(1), 273. <https://doi.org/10.1057/s41599-025-04576-7>