

MODUL 07

DIGITÁLNE OBČIANSTVO

DIGITAL RURAL EUROPEAN ART
AND MEMORY



Partneri projektu





Spolufinancovaný
Európskou úniou

Informácie o projekte:

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

Financované Európskou úniou. Vyjadrené názory a stanoviská sú však výlučne názormi autora alebo autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie ani SAAIC. Európska únia ani orgán poskytujúci grant za ne nenesú zodpovednosť.



Ako používať túto e-knihu

Tento materiál si môžete prečítať pred vzdelávacím stretnutím, počas neho alebo po jeho skončení. Najskôr preskúmate, čo znamená digitálne občianstvo a prečo samotný prístup k technológiám nezaručuje začlenenie. Následne si prakticky vyskúšate, ako overovať informácie verejnej správy, rozpoznávať riziká a bezpečnejšie používať digitálnu identitu. Potom vytvoríte praktickú kartu postupu pre skutočnú verejnú službu a overíte, či by podľa nej dokázala postupovať aj iná osoba.

Každá časť obsahuje krátku praktickú alebo reflexívnu úlohu. Tieto úlohy vám pomôžu prepojiť jednotlivé pojmy so situáciami z každodenného života. V žiadnom momente nemusíte používať skutočné heslá, identifikačné čísla ani osobné dokumenty. Keď sa úloha týka verejnej služby, skončíte pred skutočným odoslaním žiadosti a pracujte iba s verejne dostupnými informáciami.

Na konci e-knihy nájdete komplexnú záverečnú aktivitu, kontrolný zoznam na vzájomné hodnotenie, tip pre digitálnu pohodu, slovník pojmov a zoznam použitej literatúry. Záverečným výstupom je Karta postupu verejnou službou – jasný, bezpečný a komunitne orientovaný návod, ktorý môže inej osobe poslúžiť ako východiskový bod.

INFORMÁCIE O MODULE

 Číslo modulu 07	 Úroveň Začiatocník
 Téma Bezpečné a sebavedomé zapájanie sa do digitálneho verejného života	 Forma Hybridné vzdelávanie
 Trvanie 3 hodiny	 Hlavný výstup Karta postupu verejnou službou

O tomto module

Verejný život sa čoraz viac presúva do digitálneho prostredia. Ľudia vyhľadávajú oficiálne informácie, rezervujú si termíny, podávajú žiadosti, získavajú dokumenty, kontaktujú inštitúcie a zapájajú sa do komunitného rozhodovania prostredníctvom webových stránok a online portálov. Tieto služby môžu šetriť čas a znižovať potrebu cestovania. Ich používanie však môže byť náročné, ak sú informácie nejasné, spôsob overenia totožnosti je neznámy alebo nie je zjavné, na koho sa možno obrátiť so žiadosťou o pomoc. Digitálne občianstvo zahŕňa prístup, bezpečnosť, práva a participáciu. Patrí sem aj schopnosť pomôcť inej osobe porozumieť postupu využitia verejnej služby, požiadať inštitúciu o podporu a zapájať sa do rozhodnutí, ktoré ovplyvňujú miestne miesta, tradície a spoločnú pamäť. Vo vidieckych komunitách, kde môžu vzdialenosť a obmedzené možnosti podpory vytvárať ďalšie prekážky, dokážu jasné usmernenia a spolupráca zvýšiť zmysluplnosť a inkluzívnosť digitálnych služieb.

Cieľom tohto modulu je pomôcť vám pohybovať sa v digitálnom verejnom priestore bezpečnejšie, sebavedomejšie a samostatnejšie. Modul prepája praktické digitálne zručnosti s kritickým úsudkom, povedomím o ochrane súkromia a komunitnou participáciou. Zameriava sa na pochopenie toho, kto danú službu poskytuje, ako overiť dôveryhodnosť informácií, ako chrániť osobné údaje a čo robiť, keď digitálny postup nefunguje. Cieľom nie je zapamätať si všetky národné portály ani systémy digitálnej identifikácie. Cieľom je osvojiť si všeobecne využiteľný postup: určiť zodpovednú inštitúciu, nájsť oficiálnu cestu k službe, overiť zdroj, pochopiť jednotlivé kroky, chrániť osobné údaje, nájsť pomoc a jasne vysvetliť celý postup inej osobe.



Ciele vzdelávania

- Chápať digitálne občianstvo ako prístup, bezpečnosť, práva a účasť v online a offline komunitách.
- Rozpoznať právne, sociálne a praktické rozmery občianstva.
- Vysvetliť, prečo prístup k zariadeniu alebo internetovému pripojeniu nevedie automaticky k zmysluplnému digitálnemu začleneniu.
- Nájsť oficiálne webové stránky, portály, oznámenia a kontaktné miesta verejných služieb.
- Skontrolovať či sú verejné informácie aktuálne, dôveryhodné a prepojené so zodpovednou inštitúciou.
- Pri hodnotení neznámej stránky aplikovať laterálne čítanie a overenie z dvoch zdrojov.
- Rozlišovať zastarané informácie, dezinformácie, nepravdivé informácie a podvody.
- Rozpoznať bežné varovné signály správ, ktoré napodobňujú verejný orgán.
- Zmapovať fázy postupu online verejnej služby vrátane pomoci a alternatívnych trás.
- Vytvoriť a vzájomne recenzovať kartu trasy verejnej služby.

Index

0. Predtým, ako začnete: Môj východiskový bod	3
1. Čo je digitálne občianstvo?	4
2. Tri prepojené rozmery digitálneho občianstva	6
3. Prístup, inklúzia a vidiecke komunity	7
4. Európske digitálne práva a zásady	7
5. Digitálne verejné služby a cesta používateľa službou	9
6. Vyhľadávanie oficiálnych verejných informácií verejnej správy	11
7. Overovanie zdrojov pomocou laterálneho čítania	12
8. Zastarané informácie, misinformácie, dezinformácie a podvody	13
9. Osobné údaje, overenie totožnosti a bezpečný prístup	16
10. Digitálne občianstvo a kultúrna participácia	17
11. Záverečná aktivita: Karta postupu verejnou službou	18
12. Zdieľanie a vzájomné hodnotenie	23
13. Tip pre digitálnu pohodu	24
14. Základný glosár	25
15. Záver modulu	27
Bibliografia	28

0. Predtým, ako začnete: Môj východiskový bod

Pred začatím modulu ohodnoťte každé tvrdenie na stupnici od 1 do 5. Hodnotenie **1** použite vtedy, ak danú úlohu zatiaľ neviete vykonať, a hodnotenie **5**, ak ju dokážete zvládnuť samostatne. Nejde o test. Cieľom je uvedomiť si svoju východiskovú úroveň a neskôr rozpoznať vlastný pokrok.

- Viem nájsť oficiálnu webovú stránku verejnej služby.
- Dokážem overiť, či sú informácie verejnej správy aktuálne a dôveryhodné.
- Rozumiem tomu, kedy a prečo služba vyžaduje digitálnu identifikáciu.
- Dokážem rozpoznať podozrivé správy, ktoré napodobňujú verejný orgán.
- Dokážem inej osobe vysvetliť hlavné kroky online úradného postupu.

Svoje hodnotenia si uchovajte. K týmto tvrdeniam sa vrátite na konci modulu.

1. Čo je digitálne občianstvo?

Občianstvo možno chápať viacerými navzájom prepojenými spôsobmi. Ako právne postavenie vyjadruje formálny vzťah medzi jednotlivcom a štátom vrátane uznaných práv a povinností. Ako pocit spolupatričnosti označuje vzťah ku komunite, miestu, kultúre alebo spoločnému politickému priestoru. Ako praktické konanie znamená zapájať sa do verejného života, spolupracovať s ostatnými, klásť otázky, vyžadovať od inštitúcií zodpovednosť a prispievať k riešeniu spoločných záležitostí.



Kľúčové pojmy

Občianstvo ako právny status: Formálny vzťah medzi jednotlivcom a štátom, ktorý zahŕňa uznané práva a povinnosti.

Občianstvo ako pocit spolupatričnosti: Pocit prepojenia s komunitou, miestom, kultúrou alebo spoločným politickým priestorom.

Občianstvo ako praktické konanie: Zapájanie sa do verejného života prostredníctvom spolupráce, kladenia otázok, vyžadovania zodpovednosti a prispievania k riešeniu spoločných záležitostí.

Digitálne občianstvo: Uplatňovanie prístupu, práv, povinností, úsudku a participácie v digitálnom prostredí.

Digitálne občianstvo prenáša tieto práva, povinnosti a formy účasti do digitálneho prostredia. Predstavuje schopnosť aktívne, sústavne a zodpovedne sa zapájať do komunit online aj offline prostredníctvom kompetentného a pozitívneho využívania digitálnych technológií. Digitálny občan nerobí iba to, že ovláda zariadenie. Dokáže využívať príležitosti, posudzovať informácie, chrániť svoje práva, rešpektovať ostatných a zapájať sa do verejného a komunitného života.

Digitálne občianstvo sa preto neobmedzuje iba na slušné správanie na internete. Zahŕňa aj informačnú gramotnosť, kritické myslenie, participáciu, etiku a schopnosť postaviť sa proti vylúčeniu alebo manipulácii. Tento pojem prepája praktické zručnosti s úsudkom a zodpovednosťou. Človek môže vedieť, ako sa preklikať webovou stránkou, no napriek tomu môže potrebovať podporu pri posudzovaní, či je stránka oficiálna, či je požiadavka primeraná

alebo či je služba prístupná a spravodlivá (Rada Európy, 2019, 2025; Richardson a Milovidov, 2022; Európska komisia, Spoločné výskumné centrum, 2025).



Reflexia

Spomeňte si na jednu nedávnu digitálnu aktivitu súvisiacu s verejným alebo komunitným životom. Mohlo ísť o vyhľadávanie informácií, dohodnutie si stretnutia, kontaktovanie obce, prečítanie verejného oznámenia, účasť na konzultácii alebo pomoc inej osobe s online formulárom. Ktorý aspekt občianstva bol prítomný: právny status, príslušnosť, prax alebo viac ako jeden?

2. Tri prepojené rozmery digitálneho občianstva

Rada Európy (2019) opisuje digitálne občianstvo prostredníctvom troch navzájom prepojených rozmerov: byť online, online pohoda a online práva. Tieto rozmery sa navzájom prekrývajú. Človek potrebuje prístup a zručnosti, ale aj bezpečnosť, rešpekt, súkromie a zmysluplné možnosti zapájať sa.

Byť online: Tento rozmer zahŕňa prístup, inklúziu, vzdelávanie, kreativitu a mediálnu gramotnosť. V každodennom verejnom živote to môže znamenať napríklad nájsť správny oficiálny portál a porozumieť informáciám, ktoré sú na ňom uvedené.

Online pohoda: Tento rozmer zahŕňa bezpečnosť, zdravie, empatiu a zodpovedné používanie technológií. Môže to znamenať odolávať nátlaku, rozpoznávať podvody, obmedzovať zbytočné zdieľanie osobných údajov a požiadať o pomoc, keď sa určitý postup stane príliš náročným.

Online práva: Tento rozmer zahŕňa participáciu, ochranu súkromia, spotrebiteľské povedomie a demokratické práva. Môže znamenať využívanie verejnej služby, poskytovanie spätnej väzby, zapojenie sa do verejnej konzultácie alebo požiadanie inštitúcie o informácie.

Tieto rozmery ukazujú, prečo má digitálne občianstvo osobnú aj spoločenskú rovinu. Jednotlivec potrebuje sebadôveru a zručnosti, zatiaľ čo inštitúcie musia poskytovať zrozumiteľné, bezpečné a prístupné služby. Dôležitú úlohu zohrávajú aj komunity, keď ľudia zdieľajú vedomosti, navzájom si pomáhajú a upozorňujú na prekážky, ktoré je potrebné odstrániť.



Praktická úloha

Vyberte si jednu digitálnu verejnú činnosť, ako napríklad rezerváciu stretnutia alebo vyhľadanie informácií o kultúrnom programe. Napíšte jeden príklad toho, čo daná osoba potrebuje v každom rozmere: trávenie času online, online pohoda a online práva. Identifikujte, ktorý rozmer s najväčšou pravdepodobnosťou vytvorí bariéru.

3. Prístup, inklúzia a vidiecke komunity

Digitálne občianstvo zahŕňa prístup, schopnosť posudzovať informácie a konať. Človek môže mať smartfón aj internetové pripojenie, no napriek tomu môže byť vylúčený, ak je služba ťažko zrozumiteľná, vyžaduje neznámy spôsob identifikácie, používa zložitý jazyk alebo neposkytuje možnosť ľudskej podpory. Digitálna inklúzia má preto niekoľko úrovní: prístup k technológiám, zručnosti potrebné na ich používanie a schopnosť dosiahnuť zmysluplný výsledok (Correa & Pavez, 2016; Morte-Nadal & Esteban-Navarro, 2025).

Digitálne verejné služby môžu byť mimoriadne prínosné pre vidiecke komunity, pretože môžu znižovať potrebu cestovania, skracovať čakanie a obmedzovať závislosť od otváracích hodín úradov. Zároveň však môže pomalé internetové pripojenie, prístup iba prostredníctvom mobilného telefónu, obmedzená doprava, neznáme systémy a nedostatok miestnych kontaktných miest sťažiť využívanie týchto služieb. Sebadôvera, dôvera v službu, jasné informácie a možnosť požiadať niekoho o pomoc výrazne ovplyvňujú, či človek daný postup dokončí alebo sa ho vzdá.



Praktická úloha

Predstavte si, že obyvateľ musí používať online službu, ale má iba smartfón a nestabilné pripojenie. Identifikujte jednu bariéru súvisiacu s prístupom, jednu súvisiacu so zručnosťami a jednu súvisiacu s dosiahnutím konečného výsledku. Pre každú bariéru navrhните formu podpory, ktorá chráni nezávislosť a súkromie danej osoby.

4. Európske digitálne práva a zásady

Európsky prístup k digitálnej transformácii je zameraný na človeka. Technológie by mali slúžiť ľuďom, posilňovať ich účasť na spoločenskom živote a rešpektovať rovnaké práva online, aké platia aj offline. *Európska deklarácia o digitálnych právach a zásadách* predstavuje spoločný smer digitálnej transformácie, ktorá je spravodlivá, bezpečná a inkluzívna.



Kľúčové koncepty

- Ľudia a ich práva by mali byť stredobodom digitálnej transformácie.
- Nikto by nemal zostať pozadu.
- Každý by mal mať možnosť získať zručnosti potrebné na účasť.
- Ľudia by mali mať prístup ku kľúčovým digitálnym verejným službám.
- Digitálne priestory by mali podporovať informovaný výber, účasť, bezpečnosť a udržateľnosť

Tieto zásady sú dôležité aj pri hodnotení verejnej služby. Služba môže byť technicky dostupná, no napriek tomu môže niektorých ľudí vylučovať pre nezrozumiteľný jazyk, nejasné postupy, nevhodný dizajn pre mobilné zariadenia alebo nedostatok podpory. Digitálne práva sa preto týkajú nielen ochrany pred ujmom, ale aj reálnej možnosti zapájať sa a zúčastňovať sa na verejnom živote (European Parliament, Council of the European Union, & European Commission, 2023; European Commission, 2026a).



Reflexia

Vyberte si jednu digitálnu službu, ktorú poznáte. Ktorý princíp dobre podporuje? Ktorý princíp by sa dal posilniť? Svoju odpoveď založte na konkrétnej vlastnosti, ako je prístupnosť, jasné pokyny, informácie o ochrane súkromia, ľudská asistencia alebo offline alternatíva.

5. Digitálne verejné služby a cesta používateľa službou

Digitálne verejné služby umožňujú ľuďom získavať informácie, podávať žiadosti, dohodnúť si termíny, predkladať potrebné doklady, prijímať rozhodnutia alebo komunikovať s verejnými inštitúciami online. Program *Digitálna dekáda EÚ* považuje digitálne verejné služby za jednu zo štyroch hlavných oblastí digitálnej transformácie Európy (Európsky parlament a Rada Európskej únie, 2022; Európska komisia, 2026b).

Verejnú službu treba chápať ako ucelenú cestu používateľa, nie iba ako jednu webovú stránku. Používateľ musí najprv nájsť správny spôsob prístupu k službe, potom pochopiť jej účel, pripraviť si požadované údaje a dokumenty, bezpečne overiť svoju totožnosť, vykonať potrebný úkon, potvrdiť si, že jeho podanie bolo prijaté, a vedieť, kde môže v prípade potreby získať pomoc. Zrozumiteľný postup zahŕňa všetky tieto fázy.



Kľúčové pojmy

Nájsť: Kde sa nachádzajú oficiálne informácie alebo portál?

Porozumieť: Kto môže službu používať a aký výsledok prináša?

Pripraviť: Ktoré dokumenty, údaje, poplatky a termíny sú potrebné?

Autentifikovať: Je potrebná digitálna identita, heslo, kód alebo elektronický podpis?

Konať: O aký formulár, nahranie, schôdzku, platbu alebo inú akciu ide?

Potvrdiť: Ako používateľ zistí, že akcia bola prijatá alebo dokončená?

Získať pomoc: Kde môže používateľ položiť otázku, opraviť chybu, odvolať sa alebo použiť iný kanál?

Táto cesta poskytuje praktickú štruktúru na analýzu takmer každého digitálneho postupu verejnej správy, a to aj v prípadoch, keď sa národné portály a systémy digitálnej identifikácie v jednotlivých krajinách líšia (Európsky parlament a Rada Európskej únie, 2018; Morte-Nadal a Esteban-Navarro, 2025).



Praktická úloha

Vyberte si známu službu verejnej správy a opíšte postup jej využitia podľa siedmich krokov uvedených vyššie. Nemusíte si vytvárať účet ani nič odosielať. Zamyslite sa nad tým, ktorý krok je najľahšie pochopiteľný a ktorý by sa vám najťažšie vysvetľoval inej osobe.

6. Vyhľadávanie oficiálnych verejných informácií verejnej správy

Internetové vyhľadávače, príspevky na sociálnych sieťach, spravodajské články a súkromné poradenské stránky vám môžu pomôcť zorientovať sa v určitej téme. Nemali by však nahrádzať informácie zverejnené inštitúciou, ktorá je za danú službu zodpovedná. Automaticky vytvorené súhrny vo výsledkoch vyhľadávania môžu navyše vynechať dôležitý kontext, zobrazovať zastarané údaje alebo uprednostniť neoficiálne stránky pred oficiálnymi zdrojmi.

Oficiálne verejné informácie zvyčajne zahŕňajú informácie zverejnené zodpovednou verejnou inštitúciou; národný, regionálny, obecný alebo európsky portál, na ktorý táto inštitúcia odkazuje; kompletne oficiálne oznámenie, zákon, formulár, postup alebo usmernenie; alebo autorizovanú asistenčnú službu či kontaktné miesto (Európsky parlament a Rada Európskej únie, 2018; Európska komisia, Spoločné výskumné centrum, 2025).



Kľúčové pojmy

Základná otázka neznie iba: „*Vyzerá táto stránka oficiálne?*“

Lepšie je opýtať sa: „*Kto je zodpovedný za túto službu a môžem si overiť, že táto stránka patrí danej inštitúcii alebo je ňou oficiálne poverená?*“

Tento posun od vzhľadu stránky k overeniu zodpovednej inštitúcie je veľmi dôležitý, pretože dizajn, logá aj známe farby možno jednoducho skopírovať.

7. Overovanie zdrojov pomocou laterálneho čítania

Profesionálne vyzerajúca stránka nemusí byť automaticky dôveryhodná. Domény verejných inštitúcií sa v jednotlivých krajinách líšia, preto neexistuje jediná koncovka, napríklad .gov, ktorá by všade spoľahlivo dokazovala, že stránka je oficiálna. Overovanie si vyžaduje niekoľko krokov: identifikovať inštitúciu uvedenú na stránke, skontrolovať úplnú webovú adresu, vyhľadať kontaktné a právne informácie a potvrdiť, že daná inštitúcia je skutočne zodpovedná za poskytovanie služby (McGrew, 2024; Moore & Hancock, 2022; Európska komisia, Spoločné výskumné centrum, 2025).

Profesionálni overovatelia faktov často používajú metódu nazývanú **laterálne čítanie**. Namiesto toho, aby zostali na neznámej stránke a posudzovali iba jej vzhľad alebo formulácie, otvoria si novú kartu a vyhľadajú informácie o danom zdroji, organizácii alebo tvrdení. Nájdu oficiálnu domovskú stránku inštitúcie alebo jej právne informácie, overia si, či na danú službu odkazuje aj iný dôveryhodný verejný zdroj, a k pôvodnej stránke sa vrátia až po potvrdení toho, kto za ňou stojí (Brodsky a kol., 2021; McGrew, 2024).

Laterálne čítanie je užitočné, pretože webová stránka môže sama o sebe uvádzať presvedčivé, no neoverené informácie. Nezávislé potvrdenie je spoľahlivejšie. Druhým oficiálnym zdrojom môže byť iný portál verejnej správy, domovská stránka príslušnej inštitúcie, jej oficiálna kontaktná stránka, poverená asistenčná služba alebo zverejnené oznámenie, ktoré odkazuje na rovnaký postup.

Jednoduchý postup overovania

1. Uveďte názov inštitúcie, ktorá by mala byť zodpovedná za službu.
2. Skontrolujte celú webovú adresu, nielen názov stránky.
3. Otvorte novú kartu a samostatne vyhľadajte danú inštitúciu.
4. Nájdite jej oficiálnu domovskú stránku, kontaktnú stránku alebo právne informácie.
5. Potvrďte službu prostredníctvom druhého oficiálneho zdroja alebo kontaktného miesta.
6. Na pôvodnú stránku sa vráťte až po overení zdroja.

8. Zastarané informácie, misinformácie, dezinformácie a podvody

Pri využívaní digitálnych verejných služieb je nájdenie informácií online iba prvým krokom. Musíte tiež posúdiť, či sú informácie **aktuálne**, **presné** a **dôveryhodné**. Stránka môže pôsobiť profesionálne a napriek tomu obsahovať zastarané informácie, zatiaľ čo správa, ktorá vyzerá, že pochádza od oficiálnej inštitúcie, mohla byť v skutočnosti vytvorená s cieľom oklamať vás. Nie každá nesprávna alebo škodlivá informácia je rovnaká. Pochopenie typu problému vám pomôže rozhodnúť sa, čo treba overiť a ako reagovať.



Kľúčové pojmy

Zastarané informácie: Zdroj mohol byť v minulosti správny, no dátum, formulár, poplatok alebo termín sa medzičasom zmenili. V takom prípade je potrebné nájsť aktuálnu oficiálnu verziu informácie.

Misinformácie: Nepravdivé alebo zavádzajúce informácie môžu byť šírené bez úmyslu niekoho oklamať. Predtým, ako sa podľa nich rozhodnete alebo ich budete ďalej zdieľať, si ich overte.

Dezinformácie: Nepravdivé alebo zmanipulované informácie sú vytvárané alebo šírené zámerne. Skontrolujte dôkazy a v prípade potreby ich nahláste.

Podvod alebo vydávanie sa za dôveryhodnú inštitúciu: Osoba alebo skupina sa môže vydávať za úrad či inú dôveryhodnú inštitúciu s cieľom získať peniaze, prihlasovacie údaje alebo osobné údaje. Zastavte sa, na nič neklikajte ani nič neplaťte a kontaktujte danú inštitúciu prostredníctvom oficiálneho kontaktu, ktorý ste si vyhľadali nezávisle.

Tieto problémy sa môžu niekedy **prekrývať**. Podvodná správa môže obsahovať dezinformácie, vydávať sa za správu verejnej inštitúcie a presmerovať používateľa na falošnú webovú stránku. Preto je dôležité overiť nielen to, čo správa uvádza, ale aj kto ju odoslal, kam vedie odkaz a čo od vás správa žiada.

Obrázok 1

Príklad bankového phishingového e-mailu

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

Poznámka. Z Example bank phishing email [Vector graphic], od Isochrone a Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_bank_phishing_email.svg). CC BY 4.0.

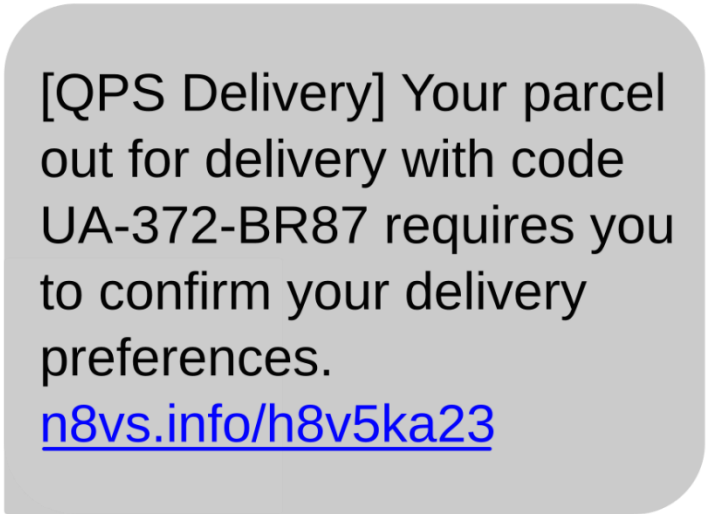
Podvody súvisiace s verejnými službami často vytvárajú tlak, aby príjemca konal skôr, než si informácie overí. Môžu kopírovať oficiálne logá, používať meno odosielateľa podobné názvu skutočnej inštitúcie alebo tvrdiť, že dávka, pokuta, účet či dokument sú bezprostredne ohrozené.

Bežné varovné signály

- Nečakaný časový nátlak, napríklad požiadavka okamžite konať, inak osoba príde o dávku alebo inú výhodu.
- Žiadosť o heslá, kódy na plný prístup alebo diaľkové ovládanie zariadenia.
- Požiadavka na platbu prostredníctvom darčekových kariet, kryptomeny alebo neobvyklého súkromného účtu.
- Skrátená, nesprávne napísaná alebo s danou službou nesúvisiaca webová adresa.
- Správa, ktorá žiada používateľa, aby sa prihlásil prostredníctvom odkazu namiesto oficiálneho portálu.
- Meno odosielateľa, ktoré sa nezhoduje s e-mailovou adresou alebo telefónnym číslom.
- Vyhrážka alebo pokyn, ktorý používateľa odrádza od overenia informácie priamo u príslušnej inštitúcie.

Obrázok 2

Príklad phishingovej SMS správy



[QPS Delivery] Your parcel
out for delivery with code
UA-372-BR87 requires you
to confirm your delivery
preferences.
n8vs.info/h8v5ka23

Poznámka. Obrázok zobrazujúci fiktívny príklad phishingovej SMS správy o doručení zásielky. Z Example phishing SMS [Vector graphic], od Belbury, 2025, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Example_phishing_SMS.svg). CC0 1.0.

9. Osobné údaje, overenie totožnosti a bezpečný prístup

Osobné údaje sú informácie, ktoré identifikujú konkrétnu osobu alebo ich možno s danou osobou prepojiť. Patria sem napríklad meno, identifikačné číslo, adresa, fotografia, údaje o polohe alebo informácie o účte. Podľa GDPR sa osobné údaje majú zhromažďovať na jasne stanovený účel a ich rozsah má byť obmedzený iba na údaje nevyhnutné na daný účel (Európsky parlament a Rada Európskej únie, 2016).

Keď verejná služba žiada o informácie, prečítajte si, prečo sa údaje požadujú a kto ich dostane. Spojte každú požadovanú položku s účelom služby. Vyhnite sa posielaniu dokladov totožnosti prostredníctvom neoficiálnej správy alebo e-mailu. Nikdy opakovane nepoužívajte ani nezdieľajte autentifikačné kódy. Potvrdzovacie správy a oficiálne potvrdenia môžu byť dôležité, ale mali by byť bezpečne uložené.

Zásady bezpečnosti

- Začnite na oficiálnom portáli služby, nie na odkaze v neočakávanej správe.
- Skontrolujte, ktorú metódu identifikácie portál oficiálne akceptuje.
- Ak je to možné, používajte vlastné zariadenie a po dokončení ukončíte reláciu.
- Nikdy nehovorte inej osobe svoje heslo, PIN kód ani celý jednorazový kód.
- Nedovoľte, aby vás neznámy volajúci sprevádzal overovaním totožnosti.
- Ak je postup nejasný, požiadajte oficiálnu službu o asistovaný prístup.

10. Digitálne občianstvo a kultúrna participácia

Digitálne občianstvo zahŕňa aj účasť na kultúrnom živote. *Dohovor z Faro* prepája kultúrne dedičstvo s participáciou, spoločnou zodpovednosťou a demokratickým životom. Kultúrne dedičstvo nie je iba niečo, čo inštitúcie chránia v mene obyvateľov. Ľudia môžu prispievať svojimi vedomosťami, upozorňovať na problémy, zapájať sa do rozhodovania a spoluvytvárať spôsob, akým sa miestne miesta, tradície a spomienky chápu a prezentujú (Rada Európy, 2005, 2019).

Digitálne nástroje môžu pomôcť obyvateľom získať prístup k kultúrnym informáciám, komunikovať s inštitúciami a prispievať k rozhodnutiam o miestnom dedičstve. Digitálny občan môže použiť oficiálne nástroje na požiadanie o prístup k archívu, nahlásenie poškodenia pamiatky, registráciu na kultúrny program, predloženie otázky, účasť na verejnej konzultácii alebo kontaktovanie inštitúcie zodpovednej za dedičstvo.



Praktická úloha

Vyberte si jedno miesto, tradíciu, zbierku, podujatie alebo záležitosť týkajúcu sa miestnej komunity, ktorá môže súvisieť s činnosťou verejnej inštitúcie. Akú informáciu alebo službu by mohol miestny obyvateľ potrebovať? Uveďte inštitúciu, ktorá je za danú oblasť pravdepodobne zodpovedná, a praktický výsledok, ktorý chce daná osoba dosiahnuť.

11. Záverečná aktivita: Karta postupu verejnou službou

Vo dvojiciach alebo malých skupinách pripravte jeden jasný postup využitia skutočnej verejnej služby. Vybraná služba by mala podľa možnosti súvisieť s miestnym kultúrnym dedičstvom alebo komunitným životom. Keďže sa verejné portály a systémy digitálnej identifikácie v jednotlivých krajinách líšia, lektor môže poskytnúť vhodné národné alebo miestne príklady.



Možné situácie využitia verejných služieb



Príklady z oblasti kultúrneho dedičstva a komunity

môžu zahŕňať

- nahlásenie poškodenia pamiatky alebo verejne prístupného miesta kultúrneho dedičstva
- požiadanie o prístup do obecného, mestského alebo regionálneho archívu
- prihlásenie sa na kultúrny program organizovaný obcou alebo mestom
- vyhľadanie informácií o verejnej konzultácii týkajúcej sa miestneho rozvoja alebo kultúrneho dedičstva
- vyhľadanie oficiálneho postupu na využitie verejného priestranstva na komunitnú kultúrnu aktivitu



Príklady z každodenného života

môžu zahŕňať

- rezervovanie termínu na úrade
- získanie potvrdenia alebo iného úradného dokumentu
- vyhľadanie informácií o možnostiach zamestnania alebo sociálnej podpory
- odoslanie otázky alebo sťažnosti príslušnému úradu
- zmenu alebo opravu údajov v úradnej evidencii

Pamätajte: Výstupom nemá byť vyplnená žiadosť a nesmie obsahovať skutočné osobné údaje. Má ísť o praktického sprievodcu, ktorý ukáže, ako môže človek nájsť, overiť a pochopiť oficiálny postup. Aktivitu ukončíte pred skutočným odoslaním žiadosti, uskutočnením platby alebo overením totožnosti.

Pracovný list ku karte postupu

Služba a jej účel: Čo služba umožňuje a prečo ju osoba môže potrebovať.

Zodpovedná inštitúcia: Orgán alebo inštitúcia, ktorá danú službu spravuje.

Overený oficiálny zdroj: Oficiálny portál alebo dokument a spôsob, akým bola jeho dôveryhodnosť potvrdená.

Oprávnenosť a príprava: Kto môže službu využiť, aké dokumenty sú potrebné a aké poplatky alebo termíny sa uplatňujú.

Kroky: Stručný očíslovaný postup od vstupnej stránky až po potvrdenie prijatia.

Digitálna identifikácia: Informácia o tom, či sa vyžaduje prihlásenie, elektronická identita, elektronický podpis alebo iný spôsob overenia totožnosti.

Súkromie a bezpečnosť: Požadované osobné údaje, pripomenutie zásad bezpečného prihlasovania a jedno relevantné upozornenie na možný podvod.

Pomoc a alternatívy: Oficiálny kontakt, dostupná asistencia, opatrenia na zabezpečenie prístupnosti alebo možnosť vybavenia služby osobne.

Prepojenie s participáciou: Spôsob, akým služba podporuje komunitnú alebo kultúrnu participáciu.

Krok 1: Definujte potrebu služby

Doplňte vetu: „Osoba v našej komunite potrebuje _____, pretože _____.“

Uved'te konkrétnu osobu alebo skupinu, vyberte jednu konkrétnu službu a vysvetlite praktický výsledok, ktorý daná osoba potrebuje. Jasne vymedzená potreba uľahčuje overenie a vysvetlenie celého postupu.

Krok 2: Nájdite oficiálny postup

1. Vyhľadajte názov služby spolu s názvom zodpovednej obce, mesta, regiónu, ministerstva alebo inštitúcie EÚ.
2. Otvorte výsledok, ktorý podľa dostupných údajov patrí zodpovednej inštitúcii.
3. Skontrolujte úplnú webovú adresu.
4. Nájdite domovskú stránku inštitúcie, kontaktnú stránku alebo právne informácie.
5. Potvrďte správnosť postupu prostredníctvom druhého oficiálneho zdroja.

Krok 3: Vykonajte päťbodovú kontrolu overenia

Päťbodová kontrola overenia spája overenie zdroja, posúdenie aktuálnosti informácií, kontrolu požadovaných osobných údajov a nezávislé potvrdenie správnosti postupu.

Zodpovedný orgán: Uved'te verejnú inštitúciu, orgán alebo poverenú organizáciu, ktorá je za službu zodpovedná.

Oficiálna webová adresa: Skopírujte alebo zaznamenajte úplnú webovú adresu. Skontrolujte, či doména patrí zodpovednej inštitúcii alebo autorizovanému portálu verejných služieb.

Aktuálne informácie: Zaznamenajte dátum publikácie, dátum aktualizácie, verziu, aktuálny termín alebo iný údaj o tom, že informácie sú stále platné.

Príslušná žiadosť o údaje: Zaznamenajte si, aké osobné údaje od vás služba žiada. Zvážte, či sú požadované informácie potrebné a vhodné na uvedený účel.

Nezávislé potvrdenie: Uveďte druhý oficiálny zdroj alebo kontaktný bod, ktorý potvrdí, že ide o správnu cestu k službe.

Päťbodová overovacia kontrola kombinuje overenie zdroja, posúdenie aktuálnosti informácií, povedomie o žiadostiach o osobné údaje a nezávislé potvrdenie.

Krok 4: Zmapujte postup

Zapíšte postup vo forme krátkych očíslovaných krokov. Začnite ešte pred prihlásením a skončíte pred skutočným odoslaním žiadosti.

1. Otvorte oficiálnu stránku služby.
2. Skontrolujte oprávnenosť a účel služby.
3. Pripravte požadované dokumenty alebo informácie.
4. Vyberte správnu identifikačnú alebo prístupovú metódu.
5. Vyplňte formulár, nahrajte ho, dohodnite si schôdzku alebo iný úkon.
6. Skontrolujte poplatky, termíny a očakávaný čas spracovania.
7. Uložte si potvrdzovacie alebo referenčné číslo.
8. Ak sa niečo pokazí, použite oficiálnu pomoc.

Karta by mala popisovať celý postup vrátane potvrdenia a podpory, nielen prvú stránku služby.

Krok 5: Identifikujte spôsob digitálneho overenia a požadované osobné údaje

Požiadavka na prihlásenie: Zaznamenajte, či sa prihlásenie nevyžaduje, vyžaduje sa len na odoslanie alebo sa vyžaduje od začiatku.

Spôsob overenia: Zaznamenajte si akceptovaný spôsob, ako je národné eID, peňaženka, mobilná aplikácia, heslo, kód, elektronický podpis alebo iný spôsob.

Požadované osobné údaje: Uveďte iba kategórie údajov, nikdy nie skutočné údaje účastníkov.

Účel údajov: Prepojte každú kategóriu údajov s účelom služby.

Informácie, ktoré sa nesmú zdieľať: Zahrňte heslá, PIN kódy, celé jednorazové kódy a dokumenty, ktoré nesúvisia s danou službou.

Krok 6: Nájdite pomoc, dostupnosť a alternatívy

Úplný postup zahŕňa aj informácie o tom, čo robiť, keď ideálny digitálny proces nefunguje.

Vyhľadajte:

- oficiálne telefónne číslo alebo e-mailovú adresu
- možnosť návštevy fyzického pracoviska alebo rezervovania termínu
- asistovanú digitálnu službu alebo poverené kontaktné miesto
- postup na opravu chyby, podanie sťažnosti alebo odvolanie

12. Zdieľanie a vzájomné hodnotenie

Vymeňte si kartu postupu s inou dvojicou alebo skupinou. Hodnotitelia by si mali kartu najprv prezrieť bez vysvetlenia jej autorov. Tým sa simuluje situácia, keď si člen komunity otvorí návod samostatne.

Otázky na vzájomné hodnotenie

Vieme identifikovať službu a zodpovednú inštitúciu?

Sú kroky úplné a zoradené v logickom poradí?

Je spôsob overenia totožnosti vysvetlený bezpečne a zrozumiteľne?

Sú požadované dokumenty, poplatky a termíny jasne uvedené?

Dokážeme nájsť pomoc alebo alternatívny spôsob vybavenia služby?

Je bezpečnostné upozornenie relevantné?



Reflexia

Ktorá časť postupu sa vám vysvetľovala najľahšie? Vďaka ktorej úprave bola karta bezpečnejšia, zrozumiteľnejšia alebo prístupnejšia pre rôznych používateľov?

13. Tip pre digitálnu pohodu



Tip pre digitálnu pohodu

Jedna obrazovka, jedna úloha

Digitálne vzdelávanie môže byť vyčerpávajúce, keď o našu pozornosť súťaží príliš veľa otvorených kariet, správ a nástrojov. Sústredenie sa na jednu viditeľnú úlohu pomáha vytvoriť pokojnejšie a zvláduteľnejšie podmienky na učenie.

Vyskúšajte: Počas nasledujúceho krátkeho pracovného bloku zatvorte alebo minimalizujte všetko, čo práve nepotrebujete. Nechajte otvorenú iba úlohu, šablónu, súbor alebo webovú stránku, s ktorou momentálne pracujete.

Otázka na zamyslenie: Akú jednu digitálnu úlohu potrebujem práve teraz dokončiť?

Tento návyk je obzvlášť užitočný pri vybavovaní verejných služieb, pretože rozptýlenie môže viesť k prehliadnutiu pokynov, nechcenému zdieľaniu údajov alebo k nedokončeniu jednotlivých krokov.

14. Základný glosár

Prístupnosť: Navrhovanie informácií, služieb a nástrojov tak, aby ich mohli používať ľudia s rôznymi potrebami a schopnosťami.

Asistovaný digitálny prístup: Oficiálna podpora, ktorá pomáha osobe používať digitálnu službu bez toho, aby jej bola odobratá kontrola alebo súkromie.

Overenie totožnosti: Proces používaný na potvrdenie, že osoba je oprávnená pristupovať k účtu alebo službe.

Digitálne občianstvo: Aktívna, nepretržitá a zodpovedná účasť v online a offline komunitách prostredníctvom kompetentného používania digitálnych technológií.

Digitálna identita: Spôsob alebo súbor informácií používaných na preukázanie totožnosti v digitálnom prostredí.

Digitálna inklúzia: Schopnosť získať prístup k technológiám, používať ich s primeranými zručnosťami a dosiahnuť zmysluplný výsledok.

Dezinformácie: Nepravdivé alebo manipulované informácie zámerne vytvorené alebo šírené s cieľom klamať.

Elektronický podpis: Digitálny spôsob podpísania alebo schválenia dokumentu či úkonu.

GDPR: Všeobecné nariadenie EÚ o ochrane údajov, ktoré stanovuje pravidlá pre spracovanie a ochranu osobných údajov.

Laterálne čítanie: Opustenie neznámej webovej stránky a overenie nezávislých zdrojov s cieľom zistiť, kto za stránkou stojí a či sú jej tvrdenia dôveryhodné.

Misinformácia: Nepravdivá alebo zavádzajúca informácia, ktorá je zdieľaná bez nevyhnutného úmyslu niekoho oklamať.

Oficiálny zdroj: Informácia zverejnená alebo schválená verejnou inštitúciou zodpovednou za danú službu.

Osobné údaje: Informácie, ktoré identifikujú konkrétnu osobu alebo ich možno s touto osobou prepojiť.

Verejná služba: Informácie, pomoc alebo postup poskytovaný verejnou inštitúciou, ako sú napríklad stretnutia, dokumenty, žiadosti alebo konzultácie.

Podvod alebo vydávanie sa za inú osobu: Pokus napodobniť dôveryhodnú osobu alebo inštitúciu s cieľom získať peniaze, prihlasovacie údaje alebo osobné údaje.

Overenie prostredníctvom dvoch zdrojov: Overenie postupu alebo tvrdenia pomocou druhého nezávislého oficiálneho zdroja alebo kontaktného miesta.

Karta postupu verejnou službou: Zrozumiteľný návod, ktorý zaznamenáva oficiálny zdroj, jednotlivé kroky postupu, bezpečnostné upozornenia, možnosti pomoci a alternatívne spôsoby využitia verejnej služby.

15. Záver modulu

Digitálne občianstvo je schopnosť zapájať sa do digitálneho verejného života s potrebným prístupom, úsudkom, dôrazom na bezpečnosť a uvedomením si svojich práv. Nie je iba individuálnou zručnosťou. Závisí aj od zrozumiteľnej komunikácie inštitúcií, prístupných služieb a komunit, v ktorých môžu ľudia požiadať o podporu bez toho, aby stratili kontrolu nad svojimi súkromnými informáciami.

Po absolvovaní tohto modulu by ste mali vedieť vyhľadať a overiť oficiálne informácie verejnej správy, vysvetliť jednotlivé fázy postupu využitia verejnej služby, chrániť osobné údaje, rozpoznať bežné riziká a vytvoriť návod, podľa ktorého môže postupovať aj iná osoba. Karta postupu verejnou službou ukazuje nielen to, čo viete, ale aj to, ako môžu vaše vedomosti podporiť zapájanie ľudí do života komunity.

Bibliografia

- 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>