

MODUL 09

MEDIÁLNA GRAMOTNOSŤ A ONLINE BEZPEČNOSŤ

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 ňom. Každá časť predstavuje určitý pojem a prepája ho s praktickou aktivitou. Aktivity sú určené pre dospelých začiatočníkov. Nevyžadujú pokročilé technické znalosti. Cieľom je osvojiť si užitočné návyky: zastaviť sa pred zdieľaním, overovať zdroje, chrániť účty, kontrolovať nastavenia súkromia a v prípade potreby požiadať o pomoc.

Modul obsahuje aj časť Učenie hrou. Nejde o prílohu, ale o praktickú súčasť modulu, v ktorej účastníci uplatňujú teóriu prostredníctvom krátkych úloh zameraných na rozhodovanie, inšpirovaných skutočnými kvízmi z oblasti mediálnej gramotnosti a kybernetickej bezpečnosti.

Na konci modulu účastníci dokončia integrovanú aktivitu: analyzujú online obsah, overia jeho dôveryhodnosť a pripravia krátky plán bezpečnosti online.



Sagrada Família, Španielsko

INFORMÁCIE O MODULE

 Číslo modulu 09	 Úroveň Začiatocník
 Téma Bezpečnosť online a mediálna gramotnosť	 Forma Hybridné vzdelávanie
 Trvanie 3 hodiny	 Hlavný výstup Plán bezpečnosti online

O tomto module

Táto e-kniha sprevádza DREAM Modul 9, ktorý je venovaný mediálnej gramotnosti a bezpečnosti online. Jej cieľom je pomôcť účastníkom používať digitálne médiá uvedomelejšie, chrániť sa online a prijímať lepšie rozhodnutia pri čítaní, zdieľaní alebo publikovaní informácií.

Mediálna gramotnosť nie je len o rozpoznávaní falošných správ. Zahŕňa pochopenie toho, kto vytvoril určité posolstvo, prečo bolo vytvorené, ako sa k nám dostáva, aké dôkazy ho podporujú, aké emócie vyvoláva a aké riziká vznikajú pri jeho zdieľaní.

S tým súvisí aj bezpečnosť online. Človek, ktorý dokáže hodnotiť informácie, musí zároveň vedieť chrániť svoje účty, rozpoznať podvody, spravovať svoje súkromie, reagovať na škodlivé správanie a vedieť, kde požiadať o pomoc.

V rámci projektu DREAM tento modul podporuje digitálnu participáciu, prácu s kultúrnym dedičstvom a komunitné projekty. Účastníci môžu využívať online platformy na zdieľanie miestnych príbehov, obrázkov, videí, modelov alebo vzdelávacích materiálov. Je potrebné, aby to robili kriticky, bezpečne a s rešpektom.



Ciele vzdelávania

- Pochopiť, čo sú digitálne nástroje a prečo sú dôležité pre samostatnosť.
- Identifikovať základné súčasti počítača a ich funkcie.
- Rozlišovať medzi hardvérom, softvérom, operačným systémom, aplikáciou a súborom.
- Správne zapnúť, vypnúť, uspať, reštartovať a uzamknúť počítač.
- Rozpoznať pracovnú plochu, okná, ponuky, ikony a panel úloh.
- Používať základné funkcie klávesnice, myši a touchpadu.
- Vytvárať, ukladať, kopírovať, presúvať, premenovávať, odstraňovať a obnovovať súbory a priečinky.
- Používať webový prehliadač a vykonávať základné vyhľadávanie spoľahlivých informácií.
- Uplatňovať základné návyky v oblasti bezpečnosti, ochrany súkromia a správy hesiel.
- Sťahovať, inštalovať a odinštalovať aplikácie z oficiálnych zdrojov.
- Pripraviť súbor na odoslanie e-mailom alebo zdieľanie v cloude.
- Dokončiť integrovanú praktickú aktivitu súvisiacu so skutočnou potrebou.

Obsah

1. Čo je mediálna gramotnosť	3
2. Prečo je mediálna gramotnosť dôležitá pre DREAM	5
3. Fakt, názor, interpretácia a reklama	7
4. Ako sa k nám dostávajú online informácie	9
5. Nepravdivé informácie, dezinformácie a manipulácia	11
6. Zvyky pri hodnotení zdrojov a overovaní faktov	12
7. Obrázky, videá a obsah generovaný umelou inteligenciou	14
8. Súkromie, digitálna stopa a osobné údaje	16
9. Základy online bezpečnosti: účty, heslá a zariadenia	18
10. Odporúčania INCIBE a dôveryhodné zdroje pomoci	20
11. Have I Been Pwned a kontroly úniku údajov	21
12. Bezpečnosť zdieľaných súborov: Telegram, priame stiahnutia a komprimované archívy	23
13. Online podvody, phishing a sociálne inžinierstvo	26
14. Kyberšikana, nenávistné prejavy a úctivá účasť	28
15. Bezpečné zverejňovanie v komunitných a pamiatkových projektoch	30
16. Učte sa hrou: Úlohy z mediálnej gramotnosti a kyberbezpečnosti	32
17. Záverečná aktivita	34
18. Tip pre digitálnu pohodu	36
19. Základný slovník	37
20. Záverečná časť modulu	38
Bibliografia	39

1. Čo je mediálna gramotnosť

Mediálna gramotnosť je schopnosť zodpovedne pristupovať k mediálnym správam, rozumieť im, hodnotiť ich, vytvárať ich a zdieľať. Vztahuje sa na správy, príspevky na sociálnych médiách, videá, obrázky, podcasty, výsledky vyhľadávania, reklamu, webové stránky a obsah generovaný umelou inteligenciou. Mediálne gramotný človek neverí všetkému hneď, ale ani všetko automaticky neodmieta. Umením je klaŕ lepšie otázky: kto to vytvoril, aké dôkazy sú uvedené, čo chýba, komu to prospieva a čo by som mal skontrolovať pred zdieľaním?

Mediálna gramotnosť zahŕňa aj pochopenie toho, že mediálne správy sú konštruované. Nadpis, fotografia, výber hudby, štýl úpravy alebo miniatúra môžu ovplyvniť to, aký máme názor na danú tému ešte predtým, ako si prečítame podrobnosti.



Hlavné pojmy

Mediálna gramotnosť: schopnosť kriticky a zodpovedne pristupovať k mediálnemu obsahu, rozumieť mu, hodnotiť ho, vytvárať ho a zdieľať.

Zdroj: osoba, organizácia, publikácia, webová stránka alebo iný pôvod, z ktorého pochádza informácia alebo mediálny obsah.

Posolstvo: hlavná myšlienka, informácia alebo dojem, ktorý mediálny obsah sprostredkúva svojmu publiku.

Dôkaz: informácia použitá na podporu tvrdenia alebo výroku, napríklad fakty, údaje, dokumenty, fotografie, odborné poznatky alebo iný overiteľný materiál.

Publikum: ľudia, ktorých má mediálne posolstvo osloviť alebo ktorých pravdepodobne osloví.

Účel: dôvod, prečo bolo mediálne posolstvo vytvorené, napríklad s cieľom informovať, vysvetľovať, presviedčať, zabávať, niečo propagovať alebo podnietiť ľudí k činnosti.



Praktická úloha

Vyber si jeden online príspevok a odpovedz:

- kto ho vytvoril?
- čo sa ťa snaží prinútiť myslieť si alebo urobiť?
- aké dôkazy poskytuje?

Malá rada: Nepýtajte sa len na to, či je správa pravdivá; spýtajte sa, ako sa vás snaží ovplyvniť.

2. Prečo je mediálna gramotnosť dôležitá pre DREAM

Účastníci programu DREAM môžu používať digitálne nástroje na dokumentovanie miestneho dedičstva, zverejňovanie výsledkov projektov, zdieľanie školiacich materiálov alebo účasť v online komunitách. Tieto aktivity si vyžadujú dôveru a zodpovednosť. Keď komunitný projekt zverejní obsah online, stáva sa súčasťou informačného prostredia. Nesprávne uvedenie zdroja obrázku, prehnané tvrdenie, zavádzajúca štatistika alebo nebezpečná publikácia môžu poškodiť dôveryhodnosť.

Mediálna gramotnosť pomáha účastníkom stať sa lepšími účastníkmi, nielen lepšími spotrebiteľmi. Naučia sa vyhľadávať, porovnávať, interpretovať, vytvárať a zdieľať s rozvahou.

V oblasti kultúry a kultúrneho dedičstva mediálna gramotnosť chráni aj kontext. Príbeh, predmet alebo obrázok by nemali byť vytrhnuté zo svojho významu ani použité spôsobom, ktorý mátie publikum.



Hlavné pojmy

Digitálna participácia: Zapájanie sa do digitálneho priestoru prostredníctvom prispievania informáciami, nápadmi, vedomosťami alebo obsahom, namiesto toho, aby človek informácie iba prijímal.

Pamäť komunity: Príbehy, fotografie, skúsenosti, tradície a vedomosti, prostredníctvom ktorých si komunita pamätá svoju minulosť a rozumie jej.

Dôveryhodnosť: Miera, do akej možno informáciu alebo obsah považovať za dôveryhodnú. Dôveryhodnosť posilňuje presnosť, spoľahlivé zdroje, správne uvedenie autorstva a transparentnosť v prípade neistoty.

Kontext: Základné informácie potrebné na správne pochopenie niečoho, napríklad kto to vytvoril, odkiaľ a z akého obdobia to pochádza, čo to predstavuje a prečo je to dôležité.

Zodpovedné publikovanie: Kontrola obsahu pred jeho zdieľaním a zohľadnenie presnosti, zdrojov, povolení, súkromia, uvedenia autorstva a možných dôsledkov pre zapojené osoby alebo komunitu.



Praktická úloha

Uveď tri typy obsahu, ktoré by projekt DREAM mohol publikovať online, a jedno riziko pre každý z nich.

Malá rada: Dobrý digitálny projekt nie je len viditeľný, ale je aj dôveryhodný.

3. Fakt, názor, interpretácia a reklama

Fakt sa dá overiť na základe dôkazov. Názor vyjadruje určitý pohľad na vec. Interpretácia vysvetľuje, čo niečo môže znamenať. Reklama sa snaží presvedčiť ľudí, aby niečo kúpili, klikli, prihlásili sa na odber alebo niečo podporili. Online obsah často mieša tieto kategórie. Video môže obsahovať fakty, osobné názory, sponzorované produkty a emotívne rozprávanie príbehov. Príspevok na sociálnych médiách môže vyzeráť ako informácia, ale v skutočnosti slúži ako reklama. Študenti by sa mali naučiť oddeľovať tvrdenie od emócií. Ak správa hovorí, že niečo je šokujúce, naliehavé alebo zrejmé, čitateľ by sa mal aj tak opýtať, aké dôkazy to potvrdzujú.



Hlavné pojmy

Fakt: Tvrdenie, ktoré možno overiť a podložiť spoľahlivými dôkazmi.

Názor: Osobný pohľad, presvedčenie alebo úsudok. Názor môže vychádzať z faktov, ale nemožno ho dokázať rovnakým spôsobom ako faktické tvrdenie.

Interpretácia: Vysvetlenie toho, čo môže znamenať informácia, udalosť, obrázok alebo zdroj. Rôzni ľudia môžu ten istý materiál interpretovať odlišne, preto by mali byť dôvody a dôkazy, na ktorých je interpretácia založená, jasné.

Reklama: Obsah vytvorený na propagáciu produktu, služby, organizácie alebo aktivity a na podnietenie ľudí ku konkrétnej činnosti, napríklad k nákupu, návšteve alebo registrácii.

Sponzorovaný obsah: Obsah, ktorý bol zaplatený alebo inak podporený spoločnosťou alebo organizáciou. Mal by byť jasne označený, aby ho publikum mohlo odlíšiť od nezávislého redakčného alebo informačného obsahu.

Dôkaz: Informácia použitá na podporu alebo overenie tvrdenia, napríklad oficiálny dokument, fotografia, súbor údajov, záznam, odborný zdroj alebo iný spoľahlivý materiál.



Praktická úloha

Označ tri vety z online článku ako fakt, názor, interpretáciu alebo reklamu.

Malá rada: Predtým, ako zareagujete, zistite, aký druh správy čítate.

4. Ako sa k nám dostávajú online informácie

Ľudia nevidí online informácie náhodne. Vyhľadávače, sociálne siete, videoplatformy a odporúčacie systémy rozhodujú o tom, čo sa zobrazí ako prvé, čo sa opakuje a čo sa javí ako populárne. **Algoritmy** môžu byť užitočné, pretože pomáhajú filtrovať obrovské množstvá obsahu. Môžu však tiež vytvárať úzke informačné návyky, opakovať podobné názory a uprednostňovať emocionálny alebo extrémny obsah.

Pozornosť ovplyvňujú aj influenceri, online komunity a dizajn platforiem. Lajky, zdieľania, komentáre, notifikácie a sekcie trendov môžu spôsobiť, že obsah pôsobí dôležito, aj keď nie je spoľahlivý.



Hlavné pojmy

Algoritmus: Súbor pravidiel alebo výpočtov, ktoré digitálny systém používa na spracovanie informácií a rozhodovanie o tom, aký obsah alebo výsledky zobrazí.

Odporúčanie: Obsah navrhnutý používateľovi na základe signálov, ako sú predchádzajúca aktivita, záujmy, popularita alebo pravidlá platformy.

Kanál príspevkov: Neustále aktualizovaný tok príspevkov, videí, správ alebo iného obsahu zobrazovaného na platforme.

Influencer: Osoba, ktorá si vybudovala publikum online a môže ovplyvňovať to, čomu jej sledovatelia venujú pozornosť, o čom diskutujú, čomu dôverujú alebo čo kupujú.

Dizajn platformy: Spôsob, akým je digitálna platforma usporiadaná, vrátane tlačidiel, oznámení, rozloženia a funkcií, ktoré môžu ovplyvniť správanie ľudí a to, čo vidia.

Pozornosť: Obmedzená mentálna kapacita, ktorú ľudia venujú informáciám. Mnohé digitálne platformy sú navrhnuté tak, aby upútali a udržali pozornosť čo najdlhšie.



Praktická úloha

Porovnaj prvé výsledky pre rovnakú tému na dvoch platformách. Sú podobné alebo odlišné?

Malá rada: To, čo vidíte online, je vyberané, nie je to neutrálne.

5. Nepravdivé informácie, dezinformácie a manipulácia

Mylné informácie sú nepravdivé alebo nepresné informácie zdieľané bez nutne zlomyseľného úmyslu. **Dezinformácie** sú nepravdivé alebo zavádzajúce informácie vytvorené alebo šírené zámerne s cieľom oklamať.

Manipulácia môže využívať skutočné fakty zavádzajúcim spôsobom. Príspevok môže obsahovať starú fotografiu, vynechať kontext, preháňať štatistické údaje, uvádzať falošného odborníka alebo prezentovať jediný príklad tak, akoby potvrdzoval všeobecné pravidlo.

Clickbait využíva zvedavosť, strach alebo hnev, aby prinútil ľudí kliknúť. Emocionálna manipulácia je silná, pretože ľudia často zdieľajú obsah skôr, ako si ho overia, ak tento obsah potvrdzuje to, čo už cítia.



Praktická úloha

Nájdí nadpis, ktorý využíva silné emócie. Prepíš ho neutrálnym spôsobom.

Malá rada: Silné emócie sú signálom, aby ste spomalili, a nie aby ste zdieľali ešte rýchlejšie.

Učte sa hrou: po tejto časti vyskúšajte Úlohu 3, Laboratórium falošných správ, v časti 16. Premení techniky šírenia dezinformácií na krátku aktivitu zameranú na rozhodovanie.

6. Zvyky pri hodnotení zdrojov a overovaní faktov

Základná kontrola zdroja začína jednoduchými otázkami: kto to uverejnil, kedy, kde, na základe akých dôkazov a s akým účelom? Ak je zdroj nejasný, s informáciami by sa malo zaobchádzať opatrne. **Krížová kontrola** znamená porovnanie tvrdenia s inými spoľahlivými zdrojmi. Pomôcť môžu oficiálne inštitúcie, uznávané médiá, akademické zdroje, špecializované organizácie a orgány overujúce fakty, ale aj tak by sa mali čítať kriticky.

Overovanie faktov nie je len úlohou novinárov. Študent si môže osvojiť malé návyky: čítať viac ako len nadpis, skontrolovať dátum, vyhľadať to isté tvrdenie inde, skontrolovať URL, hľadať pôvodný zdroj a vyhnúť sa zdieľaniu snímok obrazovky bez kontextu.



Hlavné pojmy

Zdroj: Osoba, organizácia, dokument, webová stránka alebo iný materiál, z ktorého informácia pochádza.

Dôveryhodnosť: Miera, do akej možno zdroj alebo informáciu považovať za dôveryhodnú na základe faktorov, ako sú odbornosť, transparentnosť, presnosť a dôkazy.

Dôkaz: Informácia, ktorá podporuje alebo pomáha overiť tvrdenie, napríklad dokumenty, údaje, fotografie, záznamy, výskum alebo iné spoľahlivé zdroje.

Krížové overovanie: Porovnávanie rovnakého tvrdenia alebo informácie s inými nezávislými zdrojmi s cieľom zistiť, či ich potvrdzujú, vyvracajú alebo dopĺňajú o ďalší kontext.

Pôvodný zdroj: Najstarší alebo primárny zdroj, z ktorého pochádza informácia, obrázok, citát, štatistika alebo tvrdenie, na rozdiel od neskoršieho opätovného zverejnenia, zhrnutia alebo kópie.

Overovanie faktov: Proces kontroly správnosti tvrdenia prostredníctvom skúmania dôkazov, identifikovania pôvodného zdroja a porovnávania spoľahlivých informácií.

Malá rada: Ak nemôžete zistiť, odkiaľ tvrdenie pochádza, nepomáhajte mu šíriť sa ďalej.

Učte sa hrou: po tejto časti vyskúšajte úlohu č. 3, Fake News Lab, v *časti 16* a pred výberom odpovede využite návyky overovania zdrojov.

7. Obrázky, videá a obsah generovaný umelou inteligenciou

Obrázky a videá pôsobia presvedčivo, pretože vyzerajú priamočiaro. Môžu však byť upravené, vytrhnuté z kontextu, naaranžované, generované umelou inteligenciou alebo opätovne použité z inej udalosti. Užitočným zvykom je **reverzné vyhľadávanie** obrázku, overenie, či sa tá istá fotografia neobjavila skôr, hľadanie vizuálnych nezrovnalostí a overenie, či je zdroj obrázku spoľahlivý.

Obsah generovaný umelou inteligenciou prináša nové výzvy. Text, obrázky, hlasy a videá môžu napodobňovať skutočných ľudí alebo reálne udalosti. Riešením nie je panika, ale overovanie: skontrolujte kontext, zdroj, dôkazy a či dôveryhodné zdroje informujú o tej istej udalosti.



Hlavné pojmy

Upravený obrázok: Obrázok, ktorý bol po nasnímaní alebo vytvorení zmenený.

Kontext: Informácie súvisiace s obrázkom alebo posolstvom, ktoré nám pomáhajú pochopiť, čo skutočne zobrazuje alebo znamená.

Spätné vyhľadávanie: Spôsob vyhľadávania na internete pomocou obrázka namiesto slov, ktorý umožňuje zistiť, kde inde sa daný obrázok nachádza.

Deepfake: Falošný alebo pozmenený obrázok, video alebo zvuk vytvorený pomocou umelej inteligencie tak, aby pôsobil alebo znel ako skutočný.

Obsah generovaný AI: Text, obrázky, video alebo zvuk vytvorené čiastočne alebo úplne umelou inteligenciou.

Overovanie: Kontrola toho, či je informácia, obrázok alebo tvrdenie pravdivé, presné a dôveryhodné.



Praktická úloha

Porovnaj dva obrázky s rovnakou témou a urči, aký kontext každý z nich poskytuje alebo skrýva.

Malá rada: Realistický obrázok nie je to isté ako spoľahlivý dôkaz.

Učte sa hrou: po tejto časti vyskúšajte úlohu č. 2, „Skutočné alebo umelá inteligencia?“, v časti 16. Úloha vyzýva študentov, aby si obrázky a videá najprv prezreli, než im uveria.

8. Súkromie, digitálna stopa a osobné údaje

Súkromie znamená mať pod kontrolou osobné informácie a vedieť, kto ich môže vidieť, ukladať, používať alebo zdieľať. **Digitálna stopa** je stopa, ktorú zanechávajú účty, príspevky, fotografie, komentáre, vyhľadávania, údaje o polohe a zdieľané súbory.

Mali by ste sa vyvarovať zverejňovania citlivých informácií, ako sú doklady totožnosti, heslá, súkromné adresy, osobné telefónne čísla, informácie o zdravotnom stave alebo fotografie iných ľudí bez ich súhlasu. Nastavenia súkromia sú dôležité, ale nie sú zázračné. Súkromný príspevok sa stále dá skopírovať. Vymazaný príspevok mohol byť uložený. Zdieľaná zložka môže byť preposlaná. Bezpečné správanie je spoľahlivejšie ako spoliehanie sa výlučne na nastavenia.



Hlavné pojmy

Súkromie: Mať kontrolu nad tým, kto môže vidieť alebo používať informácie o tebe.

Osobné údaje: Informácie, podľa ktorých ťa možno identifikovať, napríklad tvoje meno, e-mailová adresa, telefónne číslo alebo fotografia.

Digitálna stopa: Informácie a stopy, ktoré po sebe zanechávaš pri používaní webových stránok, aplikácií alebo online služieb.

Súhlas: Jasné udelenie povolenia na to, aby sa niečo stalo, napríklad aby bola zdieľaná tvoja fotografia alebo osobné údaje.

Viditeľnosť: Kto môže vidieť tvoj profil, príspevky, fotografie alebo iné informácie online.

Nastavenia: Možnosti v aplikácii alebo na webovej stránke, ktoré ti umožňujú kontrolovať napríklad súkromie, oznámenia a to, kto môže vidieť tvoj obsah.



Praktická úloha

Prezri si vzorový profil na sociálnej sieti a identifikuj tri informácie, ktoré by nemali byť verejné.

Malá rada: Zdieľajte tak, ako keby sa obsah mohol šíriť ďalej, než očakávate.

9. Základy online bezpečnosti: účty, heslá a zariadenia

Mnohé problémy s online bezpečnosťou začínajú práve pri účtoch. Slabé heslo, opakované použitie hesla alebo nechránený e-mailový účet môžu útočníkom umožniť prístup k ďalším službám. Medzi dobré základné návyky patrí používanie dlhých jedinečných hesiel, ich ukladanie v správcovi hesiel, zapnutie viacfaktorovej autentifikácie, aktualizovanie zariadení, zamykanie obrazoviek a vyhýbanie sa neznámym súborom na stiahnutie.

Dôležité sú aj zálohy. Ak dôjde k strate, poškodeniu alebo infikovaniu zariadenia, zálohy môžu ochrániť dôležité súbory. Pri práci v komunite alebo na projekte by mali byť zálohy organizované a prehľadné, nie improvizované na poslednú chvíľu.



Hlavné pojmy

Správca hesiel: Nástroj, ktorý bezpečne uchováva tvoje heslá, aby si si ich nemusel/a všetky pamätať.

Viacfaktorové overovanie: Dodatočný bezpečnostný krok, ktorý vyžaduje viac než len heslo, napríklad kód odoslaný na tvoj telefón.

Aktualizácia: Novšia verzia softvéru, ktorá môže opraviť problémy, zlepšiť bezpečnosť alebo pridať nové funkcie.

Záloha: Uložená kópia dôležitých súborov, ktorú môžeš použiť, ak sa pôvodné súbory stratia alebo poškodia.

Zabezpečenie zariadenia: Kroky, ktoré podnikáš na ochranu svojho telefónu, tabletu alebo počítača pred neoprávneným prístupom, stratou alebo škodlivým softvérom.



Praktická úloha

Vytvor si osobný kontrolný zoznam bezpečnosti účtu bez toho, aby si uvádzal/a akékoľvek skutočné heslo.

Malá rada: E-mailový účet je často hlavným kľúčom; chráňte ho ako prvý.

10. Odporúčania INCIBE a dôveryhodné zdroje pomoci

INCIBE, Španielsky národný inštitút pre kyberbezpečnosť, je užitočným zdrojom informácií o online bezpečnosti v Španielsku. Poskytuje usmernenia, vzdelávacie zdroje a linku pomoci v oblasti kyberbezpečnosti pre občanov, odborníkov a organizácie.

Materiály INCIBE pre občanov sa venujú praktickým témam, ako je bezpečné prehliadanie webu, zabezpečené pripojenia, základné nastavenia, antivírusové programy, firewally, aktualizácie, používateľské účty, zálohy, šifrovanie, heslá, škodlivý softvér, online podvody, phishing, smishing, vishing, ochrana súkromia, mobilné zariadenia a umelá inteligencia. INCIBE je cenným zdrojom, pretože prekladá kyberbezpečnosť do každodenných činností. Cieľom nie je stať sa technickým expertom, ale vedieť, čo robiť, keď dostanete podozrivú správu, pri ochrane účtu, pri online nakupovaní alebo pri konfigurácii zariadenia.

Jednoduchý kontrolný zoznam inšpirovaný iniciatívou INCIBE môže obsahovať:

- aktualizovať zariadenia
- používanie jedinečných hesiel
- aktivovať viacfaktorovú autentizáciu
- vytváranie záloh
- skontrolujte odkazy pred kliknutím
- nezdieľajte overovacie kódy
- skontrolujte nastavenia súkromia a požiadajte o pomoc, ak vám niečo nepripadá v poriadku



Praktická úloha

Použi zoznam tém INCIBE, vyber tri online riziká a ku každému napíš jedno preventívne opatrenie.

Malý tip: Súčasťou dobrej online bezpečnosti je aj vedieť, kde požiadať o spoľahlivú pomoc.

11. Have I Been Pwned a kontroly úniku údajov

Have I Been Pwned je služba, ktorá používateľom umožňuje skontrolovať, či sa ich e-mailová adresa nachádza v známych prípadoch úniku údajov. Môže sa použiť aj na pochopenie toho, prečo je opakované používanie hesiel nebezpečné. **Únik údajov** znamená, že informácie zo služby boli zverejnené. Môžu to byť e-mailové adresy, používateľské mená, heslá, telefónne čísla alebo iné údaje o účtoch. Ak sa heslo používa na viacerých účtoch, jeden únik môže ovplyvniť mnoho služieb.

Študenti by mali službu „Have I Been Pwned“ používať opatrne. Môžu skontrolovať e-mailovú adresu, nemali by však zadávať skutočné aktuálne heslá na náhodných webových stránkach. Pri správe hesiel by mali používať dôveryhodné správcovia hesiel alebo známe bezpečné kontrolné nástroje a riadiť sa oficiálnymi pokynmi. Ak sa e-mailová adresa objaví v zozname únikov, mali by reagovať pokojne a prakticky: zmeniť opakovane používané heslá, zabezpečiť, aby každé heslo bolo jedinečné, aktivovať viacfaktorovú autentizáciu, skontrolovať aktivitu na účtoch a dávať pozor na phishingové správy.



Hlavné pojmy

Únik údajov: Bezpečnostný incident, pri ktorom sa k súkromným alebo osobným údajom pristúpi bez povolenia alebo sa tieto údaje zverejnia.

Odhalená e-mailová adresa: E-mailová adresa, ktorá sa objavila v uniknutých alebo odcudzených údajoch a môže byť známa útočníkom.

Opakované používanie hesla: Používanie rovnakého hesla pre viac ako jeden účet.

Credential stuffing: Útok, pri ktorom sa odcudzené e-mailové adresy a heslá automaticky skúšajú na iných webových stránkach s cieľom zistiť, či fungujú aj tam.

Obnovenie prístupu k účtu: Proces opätovného získania prístupu k účtu, ak zabudneš heslo alebo stratíš prístup.



Praktická úloha

Nasimuluj plán reakcie na únik údajov. Čo by si urobil/a, keby sa tvoja e-mailová adresa objavila v úniku údajov?

Malá rada: Upozornenie na únik údajov neznamená koniec bezpečnosti; je to signál, aby ste si upratali svoje účty.

12. Bezpečnosť zdieľaných súborov: Telegram, priame stiahnutia a komprimované archívy

Mnohé riziká prichádzajú prostredníctvom súborov zdieľaných mimo oficiálnych kanálov: skupiny v aplikácii Telegram, neznáme cloudové priečinky, priame odkazy na stiahnutie, fóra, stránky s nelegálnym softvérom alebo skrátené URL adresy. Tieto cesty môžu byť právne sporné a technicky rizikové.

Najbezpečnejším odporúčaním je vyhnúť sa sťahovaniu súborov zo zdrojov s pochybnou zákonnosťou alebo nejasným pôvodom. Pirátsky softvér, cracknuté nástroje, neznáme inštalčné súbory a archívy chránené heslom sú bežnými spôsobmi distribúcie malvéru.

Pred otvorením stiahnutého súboru by si študenti mali položiť základné otázky:

Kto mi to poslal?

Čakal som ho?

Má zdroj dobrú povest'

Je používanie tohto súboru legálne? Zodpovedá názov súboru jeho obsahu?

Je príponou podozrivá?

Žiada ma to, aby som vypol antivírus alebo povolil makrá?

Komprimované súbory, ako sú ZIP, RAR alebo 7Z, by sa nemali otvárať naslepo. Najprv skontrolujte zdroj, skontrolujte archív antivírusovým programom, ak je to možné, prezrite si zoznam súborov bez ich rozbalenia a vyhnite sa archívom, ktoré obsahujú spustiteľné súbory, ako sú .exe, .scr, .bat, .cmd, .msi, .apk alebo podozrivé súbory skratiek.

Ak je súbor dôležitý, ale nie ste si istí, postupujte opatrnejšie: pred stiahnutím skontrolujte URL adresu, skontrolujte súbor aktualizovaným antivírusom, porovnajte hash hodnoty, ak ich oficiálny zdroj poskytuje, a zvážte využitie služieb s viacerými antivírusovými modulmi, ako je napríklad VirusTotal, pre verejné (nie súkromné) súbory

alebo URL adresy. Neodovzdávajte súkromné ani citlivé súbory do verejných skenovacích služieb.

Nebezpečné môžu byť aj dokumenty. Súbory Office s makrami, PDF súbory z neznámych zdrojov, falošné faktúry a komprimované priečinky so skrytými spustiteľnými súbormi sú bežnými metódami útokov typu „“. Bezpečným zvykom je otvárať dokumenty v chránenom zobrazení, vyhýbať sa aktivácii makier a vždy, keď je to možné, používať oficiálne zdroje.

V prípade vzdelávacích prostredí by malo platiť jednoduché pravidlo: používajte oficiálne webové stránky, dôveryhodné repozitáre a legálne zdroje. Ak platforma alebo súbor žiada študentov, aby obišli platbu, deaktivovali ochranu, nainštalovali neznáme nástroje alebo ignorovali varovania, nie je vhodný na školenie.



Hlavné pojmy

Komprimovaný archív: Súbor, ktorý obsahuje jeden alebo viac súborov zabalených spolu, zvyčajne preto, aby sa dali jednoduchšie uložiť alebo odoslať. Bežným príkladom je ZIP.

Spustiteľný súbor: Súbor, ktorý po otvorení môže spustiť program alebo inštaláciu, napríklad súbor .exe.

Malvér: Škodlivý softvér, ktorý môže poškodiť zariadenie, ukradnúť informácie alebo k nemu získať prístup bez povolenia.

Hash: Digitálna hodnota, ktorú možno použiť na overenie, či bol súbor zmenený.

Antivírus: Softvér, ktorý pomáha vyhľadávať, blokovať a odstraňovať škodlivý softvér.

Priame sťahovanie: Sťahovanie súboru priamo z webovej stránky do zariadenia.

Cracknutý softvér: Softvér, ktorý bol nezákonne upravený s cieľom vyhnúť sa plateniu alebo odstrániť licenčné obmedzenia. Môže tiež obsahovať škodlivý softvér.

Chránené zobrazenie: Bezpečnostný režim, ktorý otvorí niektoré stiahnuté dokumenty so zakázanými úpravami, kým sa nerozhodneš, že je súbor bezpečný.



Praktická úloha

Prezri si vzorový scenár sťahovania súboru a rozhodni, či ho otvoriš, odstrániš, skontroluješ antivírusom, overíš u odosielateľa alebo ho znova stiahneš z oficiálneho zdroja.

Malý tip: Ak súbor pochádza z pochybného zdroja a žiada vás, aby ste mu rýchlo dôverovali, urobte opak: spomaľte a overte si ho.

Učte sa hrou: po tejto časti vyskúšajte Úlohu 4, Misia bezpečného sťahovania, v *časti 16*. Naučíte sa v nej rozhodovať o súboroch v aplikácii Telegram, priamom sťahovaní a komprimovaných archívoch.

13. Online podvody, phishing a sociálne inžinierstvo

Phishing je trik, ktorého cieľom je prinútiť ľudí prezradiť informácie alebo kliknúť na nebezpečný odkaz. Smishing využíva SMS alebo aplikácie na zasielanie správ. Vishing využíva telefonické hovory. Sociálne inžinierstvo využíva dôveru, naliehavosť alebo strach na ovplyvnenie správania.

Medzi bežné varovné signály patria naliehavé termíny, hrozby, výhry, neočakávané prílohy, žiadosti o overovacie kódy, podivné platobné pokyny, skrátené odkazy a správy, ktoré vyvíjajú tlak na ľudí, aby konali rýchlo.

Najbezpečnejšou reakciou je počkať. Nepoužívajte odkaz v správe. Prejdite priamo na oficiálnu webovú stránku alebo do aplikácie, kontaktujte organizáciu prostredníctvom známeho kanála a nikdy nezdieľajte heslá ani overovacie kódy.



Hlavné pojmy

Phishing: Falošná správa alebo webová stránka vytvorená s cieľom oklamať ňu a prinútiť ňu poskytnúť osobné údaje, heslá alebo peniaze.

Smishing: Phishing uskutočňovaný prostredníctvom textových správ alebo komunikačných aplikácií.

Vishing: Phishing uskutočňovaný prostredníctvom telefonického hovoru alebo hlasovej správy.

Podvod: Nečestný pokus oklamať niekoho, zvyčajne s cieľom ukradnúť peniaze, informácie alebo prístup k účtu.

Sociálne inžinierstvo: Manipulovanie ľudí, aby urobili niečo nebezpečné, napríklad zdieľali heslo alebo otvorili škodlivý odkaz.

Overovací kód: Dočasný kód používaný na potvrdenie tvojej identity pri prihlasovaní alebo pri vykonávaní citlivej zmeny v účte.



Praktická úloha

Analyzuj tri podozrivé správy a označ varovné signály.

Malá rada: Naliehavosť je jedným z najbežnejších nástrojov online podvodov.

Učte sa hrou: po tejto časti vyskúšajte úlohu č. 1 „Spoznajte phishing“ v *časti 16*. Funguje na rovnakom princípe ako interaktívne kvízy o phishingu: preskúmajte, rozhodnite sa a poučte sa zo spätnej väzby.

14. Kyberšikana, nenávistné prejavy a úctivá účasť

Bezpečnosť na internete nie je len technická záležitosť. Zahŕňa aj to, ako sa ľudia k sebe správajú. Kyberšikana, obťažovanie, nenávistné prejavy a ponižovanie môžu vážne ovplyvniť duševnú pohodu a účasť. Úctivá účasť znamená nesúhlasiť bez útokov, vyhýbať sa verejnému zosmiešňovaniu, nezverejňovať súkromné obrázky, hlásiť urážlivé správanie a podporovať ľudí, ktorí sú terčom takého správania.

V rámci vzdelávacích alebo komunitných projektov by sa skupiny mali dohodnúť na základných pravidlách ešte pred zverejňovaním alebo diskusiou online: kto môže komentovať, kto moderuje, čo je neprijateľné a ako sa budú riešiť problémy.



Hlavné pojmy

Kyberšikana: Opakované ubližovanie, zosmiešňovanie alebo vyhrážanie sa inej osobe pomocou digitálnych nástrojov.

Obťažovanie: Nežiaduce správanie, ktoré spôsobuje, že sa niekto cíti ohrozený, nepríjemne alebo nebezpečne.

Nenávistný prejav: Obsah, ktorý útočí na ľudí alebo podnecuje nenávisť voči nim pre ich vlastnosti, ako sú pôvod, náboženstvo, pohlavie alebo identita.

Moderovanie: Proces kontroly online obsahu a správania a uplatňovania pravidiel komunity.

Nahlasovanie: Používanie nástrojov platformy na upozornenie na škodlivý, urážlivý alebo nevhodný obsah či správanie.



Praktická úloha

Napiš päť pravidiel komunity pre bezpečný online priestor projektu.

Malá rada: Bezpečný digitálny priestor potrebuje pravidlá, moderovanie a starostlivosť.

15. Bezpečné zverejňovanie v komunitných a pamiatkových projektoch

Pri zverejňovaní obsahu týkajúceho sa komunity alebo kultúrneho dedičstva by sa študenti mali zamyslieť nad súhlasom, kontextom a súkromím. Pred zdieľaním fotografie osoby, súkromného miesta alebo príbehu komunity môže byť potrebné získať povolenie. Bezpečné zverejňovanie tiež znamená overenie mediálnych práv, uvedenie zdroja, vyhýbanie sa zavádzajúcim popiskom a ochranu zraniteľných osôb alebo citlivých kultúrnych informácií.

Pred zverejnením môže projektový tím využiť krátke overenie: Je zdroj jasný? Je licencia jasná? Sú zobrazené osoby so súhlasom? Odhaľuje obsah súkromné údaje? Mohol by byť príbeh bez kontextu nesprávne pochopený?



Hlavné pojmy

Súhlas: Jasné povolenie od osoby pred použitím alebo zdieľaním jej fotografie, príbehu, hlasu alebo osobných údajov.

Uvedenie autorstva: Uvedenie osoby alebo zdroja, ktorý obsah vytvoril alebo poskytol.

Kontext: Základné informácie, ktoré pomáhajú ľuďom správne pochopiť príbeh, obrázok, predmet alebo tradíciu.

Bezpečnosť komunity: Zabezpečenie toho, aby publikovaný obsah nevystavoval ľudí, miesta alebo komunity zbytočnému riziku.

Citlivosť voči kultúrnemu dedičstvu: Zaobchádzanie s kultúrnym dedičstvom s ohľaduplnosťou a rešpektom, najmä ak zahŕňa osobné spomienky, tradície, posvätné miesta alebo citlivé informácie o komunite.

Kontrola pred publikovaním: Záverečná kontrola pred zdieľaním obsahu s cieľom uistiť sa, že je presný, rešpektujúci, správne označený zdrojmi a bezpečný na publikovanie.



Praktická úloha

Prezri si návrh príspevku o miestnom kultúrnom dedičstve a urči, čo by sa malo pred jeho zverejnením skontrolovať.

Malá rada: Zodpovedné zverejňovanie chráni tak publikum, ako aj komunitu, ktorú reprezentuje.

16. Učte sa hrou: Úlohy z mediálnej gramotnosti a kyberbezpečnosti

Táto časť premieňa pojmy mediálnej gramotnosti a online bezpečnosti na krátke úlohy zamerané na rozhodovanie. Študenti si prostredníctvom realistických scenárov s okamžitou spätnou väzbou precvičujú rozpoznávanie phishingu, obsahu generovaného umelou inteligenciou, dezinformácií a nebezpečných súborov.

Cieľom je učenie založené na praxi. Študenti si nielen prečítajú rady, ale robia rozhodnutia, porovnávajú signály, dostávajú vysvetlenia a zamýšľajú sa nad tým, čo by urobili v reálnom živote.

Navrhované bodovanie: každá úloha obsahuje 3 až 5 scenárov. Študenti získajú 1 bod za každé správne rozhodnutie a 1 bod navyše, ak dokážu vysvetliť varovný signál alebo overovací krok. Na konci môžu získať jednoduchý odznak: Pozorný kontrolór, Detektív zdrojov, Odhaľovateľ obrázkov generovaných umelou inteligenciou alebo Strážca kybernetickej bezpečnosti.

Úloha 1: Odhaľte phishing. Žiaci preverujú e-maily, SMS správy, priame správy alebo správy typu Telegram. Pozorujú odosielateľa, odkaz, tón, naliehavosť, prílohu, žiadosť o kódy a či ich správa vyzýva na použitie nebezpečného kanála. Inšpirácia: Kvíz o phishingu od Google/Jigsaw (<https://phishingquiz.withgoogle.com/>). Príklad rozhodnutia: kliknúť na odkaz, ignorovať ho, nahlásiť ho alebo prejsť priamo na oficiálnu webovú stránku.

Úloha 2: Skutočné alebo umelá inteligencia? Študenti analyzujú obrázky, krátke videá alebo snímky obrazovky a rozhodujú, či je obsah skutočný, generovaný umelou inteligenciou, upravený alebo chýba kontext. Hľadajú vizuálne nezrovnalosti, podivné ruky alebo text, neprirodzené odrazy, chýbajúci zdroj, staré obrázky opätovne použité ako nové udalosti a či dôveryhodné zdroje potvrdzujú tvrdenie. Inšpirácia: Detect Fakes od Northwestern University (<https://detectfakes.kellogg.northwestern.edu/>), hry na digitálnu gramotnosť Deepfakes Tracker (<https://deepfakestracker.org/digital-literacy-games/>), Real or AI (<https://whichoneisreal.com/real-or-ai/>) a Sightengine AI or Not (<https://sightengine.com/ai-or-not>).

Úloha č. 3: Laboratórium falošných správ. Študenti analyzujú titulky, príspevky alebo krátke články a identifikujú emocionálnu manipuláciu, slabé dôkazy, falošnú autoritu, clickbait, chýbajúci kontext, konšpiračné rámcovanie alebo zavádzajúce štatistiky. Inšpirácia: Bad News Game (<https://www.getbadnews.com/>), hry Inoculation Science (<https://inoculation.science/inoculation-games/>), NewsFeed Defenders a ABC Fake News Game. Príklad rozhodnutia: zdieľať, uložiť na neskôr, overiť v inom zdroji, preformulovať neutrálne alebo odmietnuť ako nedôveryhodné.

Úloha 4: Misia bezpečného sťahovania. Študenti dostanú realistické situácie zdieľania súborov: súbor ZIP v skupine na Telegrame, priamy odkaz na stiahnutie, súbor RAR chránený heslom, cracknutý inštalačný súbor, faktúru vo formáte PDF, skratku skrytú v archíve alebo súbor z neznámej cloudovej zložky. Rozhodnú sa, či súbor otvorí, vymaže, skontrolujú antivírusom, overia si to u odosielateľa, skontrolujú URL, porovnajú hash alebo stiahnu z oficiálneho zdroja.



Reflexia

Ktorý varovný signál si takmer prehliadol/a a aký návyk ti pomôže všimnúť si ho nabudúce?

Malá rada: Dobrá úloha by mala pôsobiť ako skutočné rozhodnutie, nie ako test pamäti.

17. Záverečná aktivita

Záverečná aktivita spája mediálnu gramotnosť a bezpečnosť na internete. Študenti si vyberú online obsah súvisiaci s kultúrou, technológiami, miestnymi správami alebo komunitným životom a analyzujú ho, než sa rozhodnú, či by sa mal zdieľať.

Analytický hárok

Názov alebo téma	
Platforma	
Autor	
Dátum	
Hlavné tvrdenie	
Dôkazy	
Emocionálny jazyk	
Overenie zdroja	
Druhý zdroj	
Možný chýbajúci kontext	
Konečné rozhodnutie	

Bezpečnostný list

Dotknuté osobné údaje	
Riziká súvisiace so súkromím	
Varovné signály podvodu	
Opatrenia na zabezpečenie účtu	
Riziká súvisiace so sťahovaním súborov	
Môžu pomôcť usmernenia INCIBE?	
Bola by stránka „<i>Have I Been Pwned</i>“ užitočná na overenie, či som bol vystavený úniku údajov?	

Malá rada: Najlepší nástroj pre online bezpečnosť je chvíľka premýšľania pred konaním.

18. Tip pre digitálnu pohodu



Tip pre digitálnu pohodu

Spríjemni si používanie obrazovky

Príliš jasná obrazovka, príliš malý text alebo nepohodlná poloha pri sedení môžu spôsobiť, že digitálne aktivity budú únavnejšie, než je potrebné.

Vyskúšaj toto: Uprav jas obrazovky, v prípade potreby zväčši veľkosť textu a umiestni zariadenie tak, aby si ho mohol/a pohodlne používať. Ak sedíš dlhší čas, zmeň polohu alebo sa ponáhaj.

Otázka na zamyslenie: Existuje jedna malá zmena, ktorá by ti mohla spríjemniť používanie telefónu alebo počítača?

19. Základný slovník

Algoritmus: systém, ktorý vyberá alebo zoradí obsah podľa pravidiel a údajov.

Kyberšikana: opakované škodlivé správanie prostredníctvom digitálnych nástrojov.

Únik údajov: zverejnenie údajov o účte alebo osobných údajov zo služby.

Digitálna stopa: stopa informácií, ktorú osoba zanecháva online.

Dezinformácia: nepravdivé alebo zavádzajúce informácie šírené zámerne s cieľom oklamať.

Overovanie faktov: proces overovania tvrdenia na základe dôkazov a spoľahlivých zdrojov.

Hash: digitálny odtlačok používaný na porovnanie, či súbor zodpovedá očakávanej verzii.

Have I Been Pwned: služba slúžiaca na overenie, či sa e-mailová adresa nachádza v známych prípadoch úniku údajov.

INCIBE: Španielsky národný inštitút pre kyberbezpečnosť, dôveryhodný zdroj informácií a pomoci v oblasti kyberbezpečnosti.

Mediálna gramotnosť: schopnosť zodpovedne pristupovať k médiám, rozumieť im, hodnotiť ich, vytvárať ich a zdieľať.

Dezinformácia: nepravdivé alebo nepresné informácie, ktoré môžu byť zdieľané bez úmyslu ublížiť.

Viacfaktorová autentifikácia: ochrana účtu, ktorá vyžaduje dodatočný overovací krok.

Phishing: podvodná správa určená na krádež informácií alebo na to, aby používatelia klikli na nebezpečné odkazy.

RAR/ZIP/7Z: formáty komprimovaných archívov, ktoré môžu obsahovať jeden alebo viacero súborov.

Súkromie: kontrola a ochrana osobných údajov.

Zdroj: osoba, organizácia alebo platforma, ktorá zverejňuje informácie.

20. Záverečná časť modulu

Mediálna gramotnosť a bezpečnosť na internete sú každodenné zručnosti. Pomáhajú ľuďom aktívne sa zapájať do online prostredia bez toho, aby boli pasívni, nedbanliví alebo ľahko manipulovateľní. Tento modul ukázal, že spoľahlivá digitálna účasť si vyžaduje nielen kritické myslenie, ale aj praktickú ochranu. Študenti by mali overovať informácie, chrániť svoje účty, rešpektovať ostatných a zverejňovať príspevky s rozvahou.

Po absolvovaní tohto modulu by sa študenti mali vedieť na chvíľu zamyslieť pred zdieľaním, posúdiť zdroj, rozpoznať bežné riziká, využívať dôveryhodné zdroje pomoci, precvičovať si to prostredníctvom krátkych úloh a vytvoriť jednoduchý kontrolný zoznam bezpečnosti pre osobné použitie alebo pre potreby projektu.

Malá rada: Mysli kriticky, konaj bezpečne a zdieľaj zodpovedne.

Bibliografia

Európska komisia. (22. jún 2026). *Mediálna gramotnosť*. Formovanie digitálnej budúcnosti Európy. <https://digital-strategy.ec.europa.eu/en/policies/media-literacy>

Európska komisia. (23. jún 2026). *Boj proti dezinformáciám na internete*. Tvorba digitálnej budúcnosti Európy. <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

Grizzle, A., Wilson, C., & Gordon, D. (Eds.). (2021). *Občania s mediálnou a informačnou gramotnosťou: Mysli kriticky, klikaj múdro!* UNESCO. <https://www.unesco.org/en/articles/media-and-information-literate-citizens>

Instituto Nacional de Ciberseguridad. (b.d.). *Občianstvo*. Citované 28. augusta 2026 z <https://www.incibe.es/ciudadania>

Richardson, J., & Milovidov, E. (2022). *Príručka pre vzdelávanie v oblasti digitálneho občianstva: Byť online, pohoda online, práva online* (vydanie z roku 2022). Vydavateľstvo Rady Európy. Publikácia Rady Európy