DIGCITY

Spolufinancovaný Európskou úniou

GAME-BASED DIGITAL CITIZENSHIP

Príručka o zručnostiach digitálneho občianstva

LogoPsyCom PENS digiQ YuzuPulse

Táto príručka je súčasťou zdrojov **projektu DigiCity**.

Viac informácií nájdete na webovej stránke projektu: **https://projectdigicity.eu/**

Koordinátor projektu

Omladinski savez udruženja ‘OPENS’ (Srbsko)

Partnerské organizácie

Digitálna Inteligencia (Slovensko)

YuzuPulse (Francúzsko)

Logopsycom (Belgicko)

Obsah

I. ÚVOD

V dnešnom prepojenom svete je digitálne prostredie rovnako dôležitou súčasťou nášho každodenného života ako to fyzické. Od platforiem sociálnych médií až po vzdelávacie pomôcky – internet ponúka nekonečné možnosti na komunikáciu, učenie a tvorivosť. Orientácia v tomto rozsiahlom a dynamickom priestore si však vyžaduje viac než len technické zručnosti; vyžaduje si súbor hodnôt, správania a vedomostí, ktoré sú známe pod pojmom digitálne občianstvo.

Cieľom tejto príručky je vybaviť mladých ľudí základnými zručnosťami digitálneho občianstva, ktoré im umožnia zodpovedne, eticky a efektívne sa zapájať do digitálneho sveta. Venuje sa kľúčovým témam, ako je súkromie online, zodpovedné používanie sociálnych médií, dezinformácie a ako ich rozpoznať a čo sú to digitálne stopy. Nie sú to len zručnosti, ale aj životné lekcie, ktoré pomôžu mladým ľuďom prosperovať v čoraz viac digitálnej spoločnosti.

Cieľ a význam tejto príručky

Príručka o zručnostiach digitálneho občianstva slúži ako základný pilier na dosiahnutie cieľa, ktorým je výchova informovaných a zodpovedných digitálnych občanov. Systematicky sa v nej uvádzajú rozhodujúce aspekty digitálneho občianstva, ktoré musia školitelia a mládežnícke organizácie uchopiť. Tým, že táto príručka ponúka komplexný prehľad tém, ako je ochrana súkromia online, zodpovedné používanie sociálnych médií a rozlišovanie dezinformácií, vybavuje školiteľov a pedagógov základnými vedomosťami na efektívne vedenie mladých učiacich sa ľudí.

Prostredníctvom praktických tipov a inkluzívnych aktivít zdôrazňuje táto príručka kritické myslenie, etické správanie a zodpovednú digitálnu komunikáciu. Vytvára teoretický rámec vymedzením kľúčových pojmov a poskytnutím realizovateľných stratégií na začlenenie zásad digitálneho občianstva do vzdelávacích postupov.

Význam digitálneho občianstva

Internet je dôležitý nástroj, ale jeho používanie môže prinášať aj ťažkosti. Mladí ľudia sa často stretávajú s problémami, ako sú kyberšikana, dezinformácie, narušenie súkromia a dlhodobé dôsledky ich konania na internete. Bez správneho vedenia môžu tieto problémy brániť nielen ich osobnému, ale aj akademickému a profesionálnemu rastu.

Cieľom tejto príručky je preklenúť túto priepasť poskytnutím praktických tipov a pútavých aktivít, ktoré sú prístupné pre všetkých. Dôrazom na kritické myslenie, etické správanie a zodpovednú komunikáciu chce príručka pomôcť mladým študentom prijímať informované rozhodnutia a podporiť pozitívne interakcie v digitálnom priestore.

Pre koho je táto príručka určená?

- **Mladých ľudí** – pomáha im vybudovať si sebadôveru a schopnosti bezpečne a zodpovedne sa pohybovať v digitálnom svete.
- **Pedagógov a školiteľov** – poskytuje im nástroje a stratégie na podporu mladých ľudí pri rozvíjaní silných zručností v oblasti digitálneho občianstva.
- **Mládežnícke organizácie** – rozširuje ich vzdelávacie postupy tým, že do svojich programov začlenia zásady digitálneho občianstva.

Čo od príručky očakávať?

Príručka je rozdelená do prehľadných kapitol, z ktorých sa každá zameriava na jeden z dôležitých aspektov digitálneho občianstva:

- **Digitálne občianstvo** – úvod do zásad a hodnôt, ktoré charakterizujú zodpovedné zapojenie sa do digitálneho sveta.
- **Digitálne kompetencie – základné zručnosti** – prehľad najdôležitejších zručností potrebných pre efektívne a bezpečné zapojenie sa do digitálneho prostredia.
- **Mediálna gramotnosť – porozumenie, rozpoznávanie a práca s klamlivými a zavádzajúcimi informáciami** – nástroje a stratégie na identifikáciu dôveryhodných zdrojov a zabránenie šíreniu nepravdivých informácií.
- **Zodpovedné používanie sociálnych médií – pozitíva, negatíva a e-reputácia** – nahliadnutie do zodpovedného používania sociálnych médií, ktoré vyvažujú ich výhody a potenciálne riziká.
- **Digitálne stopy a ich kontrola** – odporúčania, ako online aktivity formujú individuálnu reputáciu jednotlivca a tým jeho nasledujúce príležitosti.
- **Ochrana súkromia online** – praktické rady na ochranu osobných údajov a spravovanie nastavení ochrany súkromia.
- **Slovník pojmov** - užitočná referenčná časť definujúca kľúčové pojmy a koncepty súvisiace s digitálnym občianstvom.

Príručka je navrhnutá tak, aby bola náučná a zároveň praktická a aby zabezpečila, že zásady digitálneho občianstva sa dajú uplatniť v každodenných situáciách.

Čo chceme (prostredníctvom príručky) dosiahnuť?

Táto príručka je viac než len nástroj na vzdelávanie; symbolizuje odhodlanie vychovávať generáciu premýšľajúcich, etických a zodpovedných digitálnych občanov. Spoločne môžeme vytvoriť bezpečnejšie a inkluzívnejšie digitálne prostredie, v ktorom má každý možnosť učiť sa, rásť a spájať sa.

Vydajme sa na túto cestu k digitálnemu občianstvu spoločne a umožnime mladým študentom stať sa lídrami v digitálnom veku.

II. DIGITÁLNE OBČIANSTVO

Digitálne občianstvo sa vzťahuje na zodpovedné a primerané používanie technológií každým, kto sa zapája do digitálneho prostredia. Zahŕňa rôzne spôsoby správania, zručnosti a vedomosti, ako je ochrana osobných údajov, rešpektujúca komunikácia a pozitívne prispievanie do online komunít, ktoré sú potrebné na bezpečnú a efektívnu orientáciu v digitálnom svete.

Koncepcia digitálneho občianstva je v dnešnom svete kľúčová, nakoľko digitálne interakcie sú významnou súčasťou každodenného života. Digitálne občianstvo môže významne ovplyvniť ľudské správanie na internete viacerými spôsobmi, ako napríklad povzbudiť k zodpovednému správaniu na internete prostredníctvom rešpektujúcej komunikácie. Online používatelia, ktorí sa častejšie zapájajú do slušných a ohľaduplných interakcií, sa menej často stretávajú s prípadmi kyberšikany a online obťažovania. Digitálne občianstvo taktiež podporuje etické vytváranie a zdieľanie obsahu, pretože si jednotlivec lepšie uvedomuje zákony o autorských právach a práva duševného vlastníctva.

Dodržiavaním zásad digitálneho občianstva si lepšie uvedomíte bezpečnosť z hľadiska ochrany svojho súkromia a naučíte sa spravovať svoju digitálnu stopu, ďalej chrániť si osobné údaje, čím znížite riziko krádeže identity a zneužitia online. Digitálni občania sú lepšie pripravení identifikovať a vyhnúť sa online podvodom, dezinformáciám a potenciálne škodlivému obsahu.

Na druhej strane vzdelávanie v oblasti digitálneho občianstva zlepšuje celkovú digitálnu gramotnosť rozvíjaním zručností, ako je napríklad kritické myslenie. Naučíte sa kriticky vyhodnocovať informácie v online priestore, čo vedie k informovanejším rozhodnutiam a názorom, a tak k vedomejšiemu a ľahšiemu rozhodovaniu.

Na druhej strane vzdelávanie v oblasti digitálneho občianstva zlepšuje celkovú digitálnu gramotnosť rozvíjaním zručností, ako je napríklad kritické myslenie. Naučíte sa kriticky vyhodnocovať informácie v online priestore, čo vedie k informovanejším rozhodnutiam a názorom, a tak k vedomejšiemu a ľahšiemu rozhodovaniu.

Práva a povinnosti digitálnych občanov

Jedným zo základných práv digitálnych občanov je ochrana osobných údajov. Všeobecné nariadenie o ochrane údajov (GDPR), ktoré Európska únia zaviedla v roku 2018, je prelomovým nariadením, ktorého cieľom je chrániť súkromie a osobné údaje jednotlivcov v EÚ.

GDPR stanovuje vysoké štandardy ochrany údajov a súkromia, posilňuje práva digitálnych občanov a je vzorom pre ostatné regióny.

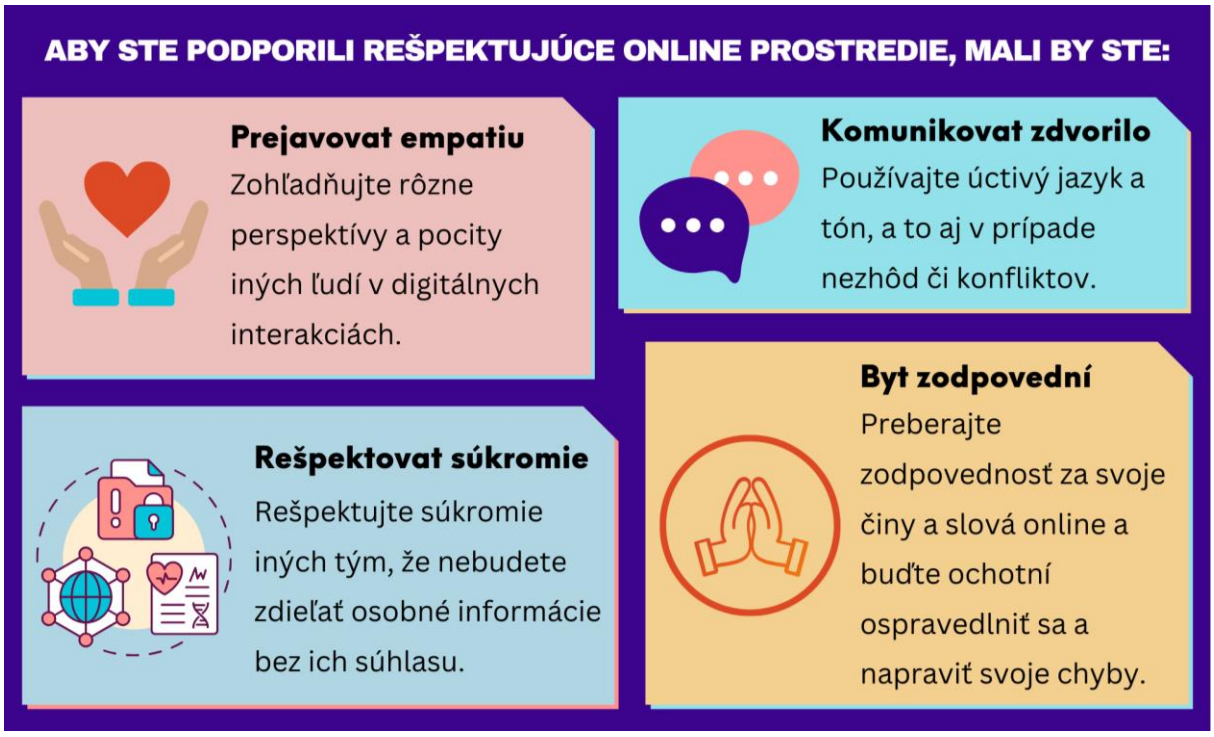
Viac informácií na stránke **GDPR.eu „What is GDPR, the EU's new data protection law?" (Wolford B, n.d.)**

Digitálni občania môžu pri problémoch na internete hľadať pomoc a podporu viacerými spôsobmi:

- **Online podporné komunity** – pripojenie sa k fóram a skupinám, kde si jednotlivci vymieňajú skúsenosti a rady týkajúce sa riešenia digitálnych problémov.
- **Linky pomoci a tiesňové linky** – využívanie špecializovaných liniek pomoci pre prípady kyberšikany, online obťažovania alebo digitálnej závislosti.
- **Mechanizmy nahlasovania** – používanie nástrojov na nahlasovanie na platformách sociálnych médií a webových stránkach na označenie nevhodného alebo škodlivého obsahu.
- **Vzdelávacie pomôcky** – prístup k online kurzom a školeniam na zvýšenie digitálnej gramotnosti a pochopenia práv v oblasti digitálnych technológií.

Informácie o dostupných zdrojoch vám umožnia efektívne riešiť a vyriešiť problémy online. Viac informácií nájdete na **Find a Helpline**.

Základom digitálneho občianstva je rešpekt.



Uplatňovaním týchto zásad prispievate k pozitívnej a rešpektujúcej digitálnej komunite.

Digitálni občania sú tiež zodpovední za rozpoznávanie a reagovanie na diskrimináciu a škodlivé správanie online. To zahŕňa:

Aktívnym odporom proti diskriminácii a škodlivému správaniu online pomáhate vytvárať bezpečnejší a spravodlivejší digitálny priestor pre všetkých používateľov.

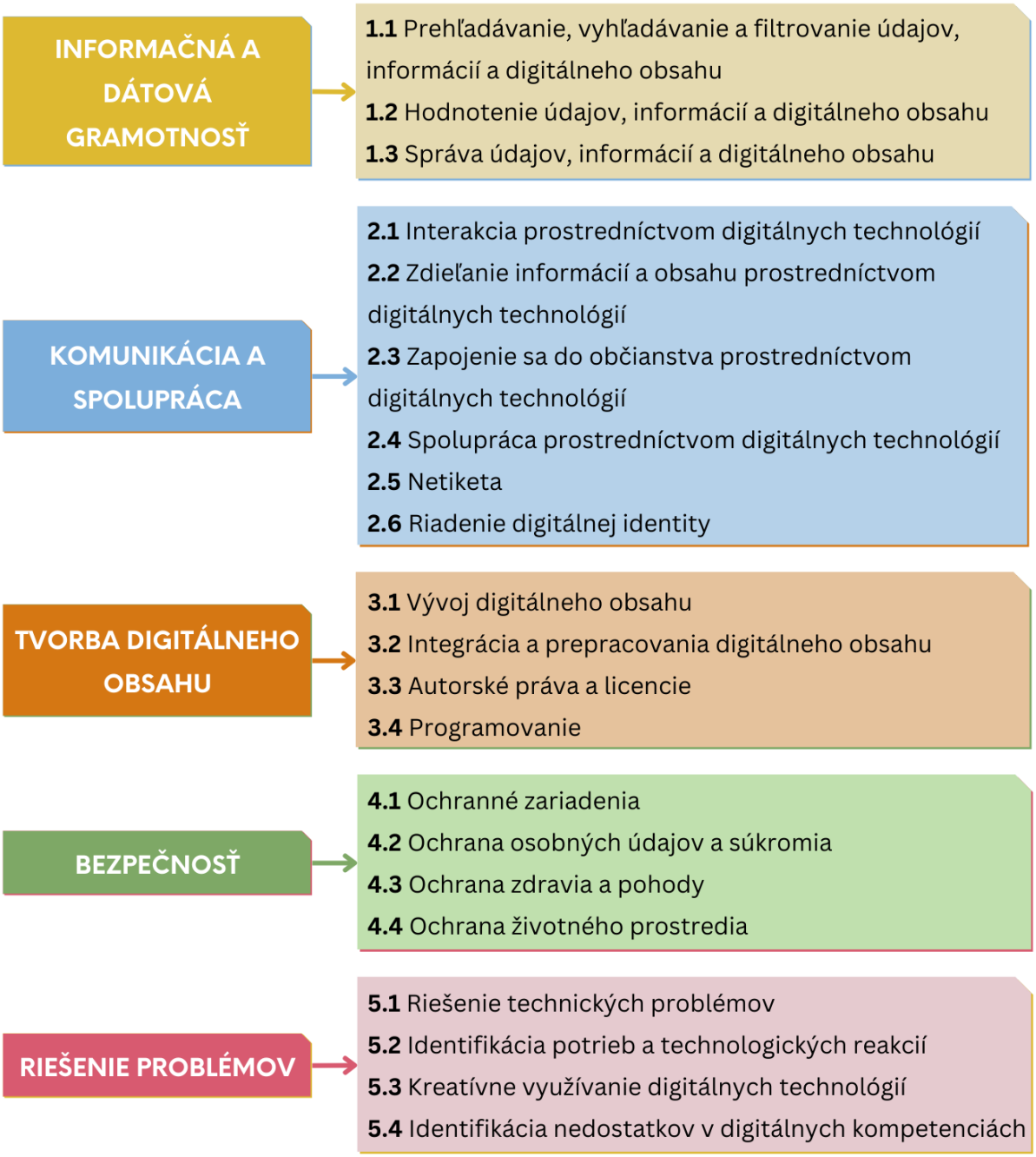
III. DIGITÁLNE KOMPETENCIE – ZÁKLADNÉ ZRUČNOSTI

Definícia digitálnych kompetencií

Podľa definície rámca digitálnych kompetencií pre občanov (**DigComp**) Európskej komisie sú digitálne kompetencie nevyhnutné pre sebavedomé, kritické a zodpovedné zaobchádzanie s digitálnymi technológiami v rôznych kontextoch, vrátane vzdelávania, zamestnania a osobného života. Zahŕňajú široké spektrum zručností, od základnej počítačovej gramotnosti až po pokročilé schopnosti v oblasti etického používania technológií a riešenia digitálnych problémov.

Rámce ako DigComp poskytujú štruktúrovaný prístup k pochopeniu mnohostrannej povahy digitálnych kompetencií. Zdôrazňujú dôležitosť dostupnosti, čím sa zabezpečuje, že digitálne kompetencie sú inkluzívne a použiteľné pre všetkých občanov bez ohľadu na ich pôvod alebo schopnosti.

Zdroj: DigComp 2.2: Rámec digitálnych kompetencií pre občanov, Európska komisia



Informačná gramotnosť a kritické myslenie

Vyhľadávanie a práca s informáciami

Informačná gramotnosť zahŕňa nielen vyhľadávanie informácií, ale aj hodnotenie ich kvality a relevantnosti. Techniky, ako je používanie pokročilých operátorov vyhľadávania Google a kritické hodnotenie ich výsledkov, ako aj rozpoznávanie dôveryhodných zdrojov, sú nevyhnutné na orientáciu v rozsiahlom množstve údajov dostupných na internete. Nástroje ako **Google**

Scholar, akademické databázy a renomované spravodajské portály sú príkladmi zdrojov, ktoré môžete použiť na získanie spoľahlivých informácií.

Okrem toho sa manažment informácií vzťahuje aj na vedomosti o tom, ako ukladať, vyhľadávať a chrániť svoje údaje. To zahŕňa používanie digitálnych nástrojov na organizovanie informácií, ako sú napríklad riešenia na ukladanie informácií na cloudovom úložisku, poznanie zásad správy údajov, ako sú napríklad pravidlá pomenovania súborov a jednotlivé stratégie zálohovania údajov. Zahŕňa aj uvedomenie si etických dôsledkov používania údajov, ako je rešpektovanie práv duševného vlastníctva a súkromia.

Hodnotenie zdrojov

Nepravdivé a zavádzajúce informácie sú na internete veľmi rozšírené, a preto by ste si mali osvojiť schopnosť kriticky posudzovať zdroje informácií, s ktorými sa stretávate. To si žiada preskúmanie referencií a hodnovernosti autora (obsah, kvalitu, hodnovernosť a zdroje jeho publikácií), presnosť informácií a prítomnosť prípadných predsudkov. Čítanie s porozumením, overovanie faktov z viacerých zdrojov a používanie nástrojov, ako sú webové stránky na overovanie faktov (napr. **Snopes**, **FactCheck.org**) sú praktické stratégie, ktoré vám pomôžu v tomto procese vyhodnocovania.

Okrem toho je dôležité pochopiť vplyv algoritmov – na základe predchádzajúceho správania a preferencií užívateľov v online svete sa digitálnym občanom zobrazuje personalizovaný obsah, ktorý má následne výrazný vplyv na skreslené vnímanie informácií. Poznanie vplyvu algoritmov na vaše informačné prostredie vám môže umožniť vyhľadávať rôzne perspektívy a vyhnúť sa takzvaným komorám ozvien (v angličtine *echo chambers*).

Riešenie online problémov a kritická evaluácia

Riešenie problémov v digitálnom kontexte je viac než len technické riešenie problémov; vyžaduje si kritické hodnotenie a adaptívne myslenie. Zručnosti v oblasti riešenia digitálnych problémov zahŕňajú identifikáciu digitálnych potrieb, analýzu potenciálnych riešení a výber najúčinnejších stratégií.

Napríklad, keď čelíte online bezpečnostnej hrozbe, ako je *phishing*, musíte posúdiť situáciu, rozpoznať hrozbu a prijať vhodné opatrenia, ako je napríklad nahlásenie incidentu a posilnenie bezpečnostných opatrení.

Vzdelávacie metódy, ktoré zahŕňajú digitálne simulácie, hranie rolí a interaktívne aktivity zamerané na riešenie problémov, môžu pomôcť mladým ľuďom rozvíjať tieto kompetencie pútavým a praktickým spôsobom. Poskytovaním reálnych scenárov, ktoré si vyžadujú kritické vyhodnocovanie a rozhodovanie, môžu pedagógovia lepšie pripraviť svojich študentov na zložitosť digitálneho sveta.

Komunikácia a tvorba obsahu

Zručnosti v oblasti digitálnej komunikácie

Digitálna komunikácia zahŕňa zručnosti potrebné na efektívnu interakciu v rôznych online prostrediach, čo z nej robí základ digitálnych kompetencií. Efektívni digitálni komunikujúci dokážu prispôsobiť svoje myšlienky svojmu publiku, vybrať vhodné komunikačné kanály a zachovať profesionalitu a rešpekt v digitálnych kontaktoch.

Súčasťou osvojovania si digitálnych komunikačných zručností je aj skúmanie konceptu „netikety“, to znamená usmernení pre zdvorilé a úctivé správanie sa na internete. Zahŕňa aj diskusie o digitálnej stope a trvalosti online aktivít, pričom sa zdôrazňuje, aké dôležité je premýšľať pred zverejnením príspevku a pochopiť dlhodobý vplyv digitálnej komunikácie.

Nástroje online spolupráce

Spolupráca je kľúčovou súčasťou moderného pracovného a vzdelávacieho prostredia; uľahčujú ju digitálne nástroje, ktoré umožňujú ľuďom spolupracovať bez ohľadu na ich fyzickú polohu. Online nástroje na

spoluprácu, ako napríklad **Slack**, **Trello**, a **Asana**, ponúkajú platformy na komunikáciu tímov, zdieľanie súborov a riadenie projektov v reálnom čase. Ovládanie týchto nástrojov sa považuje za súčasť digitálnych kompetencií, pretože sa široko používajú vo vzdelávacom aj profesionálnom prostredí na zvýšenie produktivity a podporu tímovej práce.

Tieto nástroje sa dajú integrovať aj do aktivít v triede, aby sa študenti naučili projektovému manažmentu, komunikácii a spolupráci v digitálnom priestore. Práve skupinové projekty, ktoré si vyžadujú, aby študenti používali nástroje na digitálnu spoluprácu, im môžu pomôcť rozvíjať praktické zručnosti v oblasti riadenia úloh, efektívnej komunikácie a spolupráce na dosiahnutí spoločného cieľa.

Základy tvorby obsahu

Tvorba digitálneho obsahu zahŕňa vytváranie rôznych foriem digitálnych médií, ako sú texty, obrázky, videá a interaktívny obsah. Táto kompetencia sa neobmedzuje len na technické zručnosti, ale zahŕňa aj kreativitu, porozumenie potrieb publika a uplatňovanie etických aspektov, ako je dodržiavanie autorských práv a vyhýbanie sa plagiátorstvu. Základné zručnosti v oblasti tvorby obsahu zahŕňajú používanie digitálnych nástrojov na úpravu, navrhovanie a publikovanie obsahu, ako aj pochopenie princípov digitálneho *story-tellingu*.

Mali by ste experimentovať s rôznymi platformami na tvorbu obsahu – od blogovania až po tvorbu videa, aby ste si vybudovali zručnosti a vyjadrili svoje myšlienky. Pochopenie základov tvorby obsahu zahŕňa aj uvedomenie si úlohy vizuálneho dizajnu a používateľského zážitku, ktoré sú nevyhnutné na to, aby bol digitálny obsah pútavý a prístupný. Okrem toho by ste sa mali dozvedieť o význame prístupnosti digitálneho obsahu a zabezpečiť, aby vaše výtvory boli inkluzívne a aby ich mohlo používať rôzne publikum.

IV. MEDIÁLNA GRAMOTNOSŤ

Definícia mediálnej gramotnosti

Mediálna gramotnosť vám umožní získať prístup k mediálnemu obsahu, analyzovať ho, hodnotiť, vytvárať a pracovať s ním na rôznych platformách. Zahŕňa pochopenie povahy mediálnych informácií, procesov mediálnej produkcie a úlohy, ktorú médiá zohrávajú pri formovaní spoločnosti. Mediálna gramotnosť zahŕňa aj rozpoznanie dynamiky moci vo vlastníctve médií a ekonomických, politických a kultúrnych vplyvov, ktoré riadia mediálny obsah.

Rozsah mediálnej gramotnosti sa v digitálnom veku výrazne rozšíril a zahŕňa tradičné médiá, ako sú noviny a televízia, ako aj digitálne médiá, ako sú sociálne siete, podcasty, blogy a streamovacie služby. S nástupom nových technológií, ako je umelá inteligencia a virtuálna realita, sa rozsah mediálnej gramotnosti naďalej vyvíja a vyžaduje si neustále vzdelávanie a adaptáciu. Tento širší rozsah poukazuje na potrebu komplexného prístupu, ktorý integruje vzdelávanie v oblasti mediálnej gramotnosti do rôznych predmetov a aspektov každodenného života.

Porozumenie správam v médiách

Schopnosť porozumieť mediálnym správam si vyžaduje schopnosť kriticky analyzovať, ako médiá konštruujú realitu. Informácie v médiách nie sú neutrálne; odrážajú úmysly a predsudky ich tvorcov, ktoré môžu ovplyvniť spôsob, akým informácie vnímate a interpretujete. Tvorcovia médií používajú rôzne techniky, ako je *framing*, výber zdrojov, vizuálne zobrazenie a emocionálne stimuly, aby formovali svoje posolstvá a ovplyvňovali vaše vnímanie.

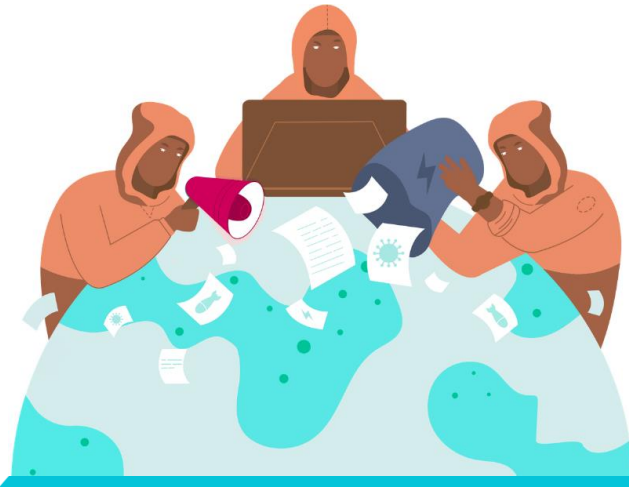
Napríklad použitie dramatických vizuálnych prvkov v spravodajstve môže posilniť emocionálny vplyv príbehu, čo môže viesť k zvýšenému znepokojeniu alebo panike verejnosti. Podobne môže vynechanie určitých perspektív alebo hlasov zmeniť chápanie problému a prezentovať jednostranný pohľad. Ak sa naučíte dekonštruovať tieto správy, môžete identifikovať základné predpoklady a predsudky, čo vedie k diferencovanejšiemu chápaniu mediálneho obsahu.

Rozvoj týchto analytických zručností možno podporiť prostredníctvom aktivít, ktoré zahŕňajú porovnávanie rôznych mediálnych zobrazení tej istej udalosti, diskusiu o vplyve vlastníctva médií na spravodajstvo a skúmanie toho, ako reklamné stratégie formujú správanie spotrebiteľov.

Rozpoznanie a správne narábanie s mizinformáciami

Dezinformácie sú v dnešnom mediálnom prostredí, kde rýchlosť a dosah digitálnej komunikácie môžu posilniť nepravdivé alebo zavádzajúce informácie, všadeprítomným problémom. Na rozpoznanie a riadenie vplyvu dezinformácií je dôležité, aby ste rozumeli ich rôznym typom:

- **Vyfabulovaný obsah -** zahŕňa úplne nepravdivé informácie vytvorené s cieľom oklamať. Napríklad falošný spravodajský článok, ktorý klamlivo tvrdí, že nejaká celebrita zomrela, sa môže rýchlo šíriť na sociálnych sieťach a spôsobiť zmätok a nepokoj v spoločnosti.
- **Clickbait -** označuje senzačné alebo zavádzajúce titulky, ktorých cieľom je prilákať kliknutia a zvýšiť tak návštevnosť webových stránok, často na úkor pravdivosti. Napríklad titulok „Neuveríte, čo urobil tento politik!“ môže viesť k článku, ktorý zveličuje alebo skresľuje fakty, aby prilákal čitateľov.
- **Deepfake -** zmanipulované videá alebo obrázky vytvorené pomocou umelej

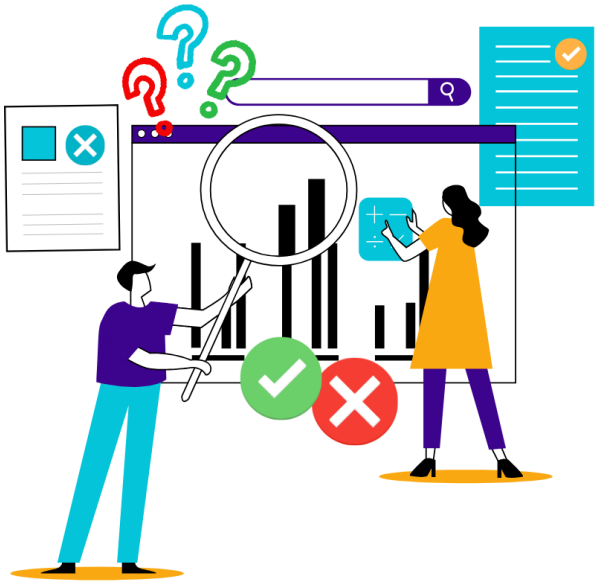


inteligencie, ktoré zobrazujú ľudí hovoriacich alebo robiacich veci, ktoré nikdy nerobili. Príkladom môže byť deepfake video, na ktorom verejne známa osoba, napríklad politik, urobí vyhlásenie, ktoré v skutočnosti nikdy neurobil, čo sa môže použiť na šírenie nepravdivých naratívov alebo na zdiskreditovanie danej osoby.

- **Zavádzajúci obsah -** informácie, ktoré skresľujú realitu alebo prezentujú fakty zavádzajúcim spôsobom. Napríklad použitie fotografie z nesúvisiacej udalosti na prezentáciu aktuálnych správ môže divákov oklamať, aby si mysleli, že súvisí s príbehom, o ktorom sa informuje.
- **Nepravdivý kontext -** skutočné informácie prezentované v zavádzajúcom kontexte, ktorý mení ich pôvodný význam. Príkladom je stará fotografia, ktorá sa použije na prezentáciu aktuálnej udalosti, čím sa u divákov vytvorí dojem, že situácia trvá alebo je väčšia ako v skutočnosti je.
- **Fingovaný obsah -** zahŕňa obsah, ktorý sa vydáva za skutočné zdroje. Napríklad falošné webové stránky napodobňujú vzhľad renomovaných spravodajských portálov s cieľom šíriť falošné správy, čo čitateľom sťažuje rozlišovanie medzi skutočnými a falošnými správami.
- **Satira alebo paródia -** satirický obsah, napríklad články z webových stránok ako **The Onion**, ktorých primárnym cieľom je pobaviť, ale ak si publikum neuvedomuje ich satirickú povahu, môžu byť mylne považované za faktické spravodajstvo.
- **Falošná atribúcia -** pripísanie časti obsahu alebo citátu nepravdivému alebo neexistujúcemu zdroju. Napríklad priraďovanie vymysleného citátu známemu vedcovi alebo verejnej osobnosti s cieľom dodať tvrdeniu neoprávnenú dôveryhodnosť.
- **Fámy a hoaxy -** neoverené informácie, ktoré sa šíria prostredníctvom sociálnych sietí a často vytvárajú falošné dojmy alebo paniku. Klasickým príkladom je virálne šírenie hoaxov o stiahnutí výrobkov z trhu alebo falošných zdravotných rád, ako je napríklad mýtus, že pitie horúcej vody môže zabrániť šíreniu COVID-19.

Fact-checking a overovanie informácii

Overovanie faktov a verifikácia údajov zahŕňajú systematické hodnotenie presnosti a spoľahlivosti informácií prostredníctvom analýzy viacerých zdrojov, skúmania dôkazov a používania verifikačných nástrojov. Kľúčové kroky pri efektívnom overovaní faktov sú:



- **Posudzovanie zdrojov -** začnite kontrolou dôveryhodnosti zdroja. Renomované zdroje majú zvyčajne transparentné redakčné normy, poskytujú údaje o autoroch a zverejňujú prípadné konflikty záujmov.
- **Krížové porovnávanie -** porovnajte informácie s inými overenými zdrojmi. Konzistentnosť vo viacerých dôveryhodných zdrojoch zvyšuje pravdepodobnosť, že informácie sú pravdivé.
- **Používanie overovacích nástrojov -** nástroje, ako je Google reverzné vyhľadávanie obrázkov, môžu pomôcť overiť autenticitu obrázkov, zatiaľ čo rozšírenia prehliadača, ako je **NewsGuard**, poskytujú hodnotenia dôveryhodnosti spravodajských webových stránok.
- **Overenie odbornosti autora -** posúďte, či je autor kvalifikovaný na vyjadrovanie sa k danej téme. Odborníci alebo uznávané autority v danej oblasti s väčšou pravdepodobnosťou poskytnú spoľahlivé informácie.
- **Analýza faktov -** vyhľadajte podporné dôkazy, ako sú údaje, výsledky výskumu alebo priame citácie odborníkov. Spoľahlivé informácie sú zvyčajne dobre podložené dôkazmi, ktoré možno nezávisle overiť.

Etická konzumácia médií

Etická konzumácia médií zahŕňa uvedomenie si výberu médií a ich vplyvu na jednotlivcov a spoločnosť. Vyžaduje si to kritický prístup k výberu a zdieľaniu

mediálneho obsahu, pričom sa zohľadňujú faktory, ako je presnosť, zaujatosť, reprezentácia a potenciálny vplyv na verejnú diskusiu. Etickí konzumenti médií aktívne vyhľadávajú rôzne perspektívy, spochybňujú zámery mediálnych správ a vyhýbajú sa šíreniu neovereného alebo škodlivého obsahu.

Na etickú konzumáciu médií je dôležité pochopiť aj vplyv algoritmov na médiá, s ktorými sa stretávame. Algoritmy na sociálnych platformách a vo vyhľadávačoch často personalizujú obsah na základe vášho správania, čím vytvárajú komory ozveny (tzv. *echo chambers*), ktoré posilňujú vaše existujúce presvedčenia a obmedzujú prístup k odlišným názorom. Ak si uvedomíte tieto vplyvy, môžete podniknúť kroky na diverzifikáciu svojej mediálnej konzumácie, napríklad sledovať zdroje s rôznymi perspektívami, používať nástroje na sledovanie zaujatosti médií alebo zámerne vyhľadávať obsah, ktorý spochybňuje vaše predpoklady.

Zodpovedná tvorba obsahu

Ako tvorca online obsahov by ste mali mať na pamäti potenciálny vplyv svojich výstupov a zvážiť, ako by mohli ovplyvniť rôzne publiká, najmä zraniteľné alebo marginalizované skupiny. To zahŕňa vyhýbanie sa jazyku alebo obrazom, ktoré upevňujú stereotypy, uistenie sa, že sa vyjadrujete presne, a rešpektovanie súkromia a súhlasu jednotlivcov pri zobrazovaní v médiách. Napríklad pri vytváraní obsahu, v ktorom vystupujú skutočné osoby, je dôležité získať ich súhlas a poskytnúť kontext, aby sa predišlo skresleniu.

Mediálna gramotnosť je základným súborom zručností, ktoré sú nevyhnutné na to, aby sa vám darilo v dnešnom zložitom mediálnom prostredí. Podporou schopnosti kriticky sa zaoberať mediálnymi správami, rozpoznať a zvládnuť dezinformácie či vytvárať obsah eticky, môžete sebe aj ostatným umožniť pohybovať sa v mediálnom prostredí so sebavedomím a integritou. Keďže médiá sa naďalej vyvíjajú, zásady mediálnej gramotnosti budú mať naďalej zásadný význam pri podpore inkluzívnej, spravodlivej a kritickej spoločnosti.

V. ZODPOVEDNÉ POUŽÍVANIE SOCIÁLNYCH SIETÍ

Podľa údajov používalo v roku 2023 internet denne približne 97 % ľudí vo veku 16 – 29 rokov v EÚ a 83 % využívalo sociálne siete (Eurostat, 2023). Keďže používanie digitálnych platforiem je medzi mladými ľuďmi značne rozšírené, mali by si uvedomiť výhody a nevýhody používania sociálnych médií.

Výhody sociálnych sietí

Online kultúra umožňuje spojenie a komunikáciu s ostatnými digitálnymi občanmi a budovaním sociálneho kapitálu môžu platformy sociálnych médií zlepšiť duševnú pohodu. Poskytuje tiež prostredie na rozvíjanie záujmov, vedomostí a zručností, ako aj na zábavu a poskytnutie podpory.

Okrem toho vám tiež pomáha byť informovaným o dianí vo svete. Mnohé spravodajské kanály majú na sociálnych platformách svoje profily, na ktorých zdieľajú tie najdôležitejšie správy v stručnej a zrozumiteľnej forme, čo uľahčuje udržať si prehľad o aktuálnom dianí.

Sociálne médiá môžu byť obzvlášť užitočné pre mladých ľudí v núdzi – online prostredie zjednodušuje prístup k odbornej pomoci a zároveň umožňuje zachovať anonymitu. Okrem toho prostredníctvom priateľov a spriaznených osôb v online skupinách môžete získať okamžitú emocionálnu podporu. Sociálne médiá tiež znižujú pocit osamelosti a izolácie. Mimoriadne cenné sú aj online komunity, ktoré sú moderované odborníkmi na duševné zdravie – vytvárajú bezpečné prostredie na zdieľanie emócií a prijímanie vzájomnej podpory. Zároveň aj niektorí blogeri a influenceri hovoria o problémoch duševného zdravia a ponúkajú priestor na svojich online profiloch, kde sa jednotlivci môžu podeliť o svoje svedectvá. Sledovanie niečieho príbehu o prekonávaní ťažkostí vám môže dodať odvahu prekonávať svoje problémy.

Riziká a nástrahy sociálnych sietí

Hoci výhody sociálnych médií sú nepopierateľné, je dôležité, aby si mladí ľudia boli vedomí aj rôznych nástrah na internete, ktoré môžu predstavovať riziko, ba priam hrozbu. Štatisticky platí, že výška potenciálneho rizika rastie úmerne s frekvenciou a intenzitou aktivity jednotlivca v online priestore. Úroveň zraniteľnosti voči rizikám a ich dôsledkom ovplyvňuje celý rad faktorov vrátane veku, pohlavia, vzdelania a kultúrneho prostredia.

So zvýšeným používaním komunikačných nástrojov, sociálnych médií a herných platforiem hrozí riziko online obťažovania, kyberšikany, kybernetického prenasledovania, *flamingu*, nenávistných prejavov, *groomingu*, ako aj krádeže identity. Virtuálny svet obsahuje aj rôznorodý škodlivý obsah násilnej alebo sexuálnej povahy, dezinformácie, rasizmus, antisemitizmus a mnohé ďalšie, čo má vážne dôsledky na duševné zdravie mladej demografickej skupiny a celej spoločnosti.

V tejto súvislosti sú dospievajúce dievčatá obzvlášť zraniteľné na internete kvôli spoločenskému porovnávaniu fyzickej príťažlivosti a falošným štandardom krásy. Sociálne médiá sú preplnené fotografiami, na ktorých jednotlivci používajú skrášľujúce filtre a retušovanie na vytvorenie nerealistických obrazov dokonalých tiel a tvárí. V dôsledku intenzívneho vystavenia sa takémuto obsahu sú ženy zraniteľné z hľadiska nespokojnosti s vlastným telom a negatívneho vnímania samých seba, čo ďalej súvisí s nízkym sebavedomím a možnosťou vyústenia až do problémov s duševným zdravím alebo porúch príjmu potravy.

V kontexte digitálneho priestoru nemožno opomenúť, že atraktívne príspevky z podujatí, dovoleniek a festivalov môžu vyvolať strach z toho, že ste o niečo

prišli alebo že niečo premeškáte v budúcnosti (koncept známy pod anglickou skratkou FOMO – *fear of missing out*), a pocity závisti a vlastnej nedostatočnosti. Často zabúdame brať do úvahy, že mnohé z týchto príspevkov sú naaranžované a často neodrážajú skutočný život používateľov.

Online platformy umožňujú „únik" z reálneho sveta a zábava na nich aktivuje dopamín (tzv. „neurotransmiter potešenia"). Tieto aspekty často vedú k závislosti na rôznych platformách, nakoľko sa ľudia v snahe o doplnenie dopamínu začnú až príliš venovať online obsahom a strávia veľa času online. Online závislosť je časovo vyčerpávajúca a má negatívny vplyv na fyzické zdravie, sociálne vzťahy, koncentráciu a produktivitu, čo môže viesť k slabým študijným alebo pracovným výsledkom. Zároveň to spôsobuje psychickú nepohodu a zdravotné následky. Sociálne médiá sú často spájané aj s poruchami spánku a úzkosťou.

Okrem toho si treba uvedomiť, že nie všetko na internete je pravda a že mnohé profily zdieľajú zavádzajúce informácie alebo dokonca dezinformácie, ktoré môžu byť veľmi nebezpečné, ak sa berú vážne.

Ambivalencia sociálnych sietí: Rola algoritmov

Algoritmy predstavujú súbor pravidiel, výpočtov a rozhodovacích procesov, ktoré platformy používajú na triedenie, odporúčanie a prezentáciu obsahu používateľom. Algoritmy sú navrhnuté tak, aby uprednostňovali obsah, s ktorým budú používatelia s najväčšou pravdepodobnosťou interagovať, a to na základe predchádzajúcich údajov o správaní, ako sú lajky, zdieľania a čas strávený pri konkrétnom obsahu.

Jedným z pozitívnych aspektov algoritmov sociálnych médií je vylepšený používateľský zážitok, pretože obsah je personalizovaný, čím sa znižuje informačné preťaženie a podporujú sa relevantné informácie pre používateľa. Algoritmy vám napríklad pomáhajú nájsť komunity a informácie prispôsobené vašim záujmom, čím sa platformy stávajú používateľsky prívetivejšie.

Jednou z hlavných obáv je však posilnenie komôr ozvien, v ktorých ste vystavení predovšetkým obsahu, ktorý sa zhoduje s vašimi existujúcimi názormi. Algoritmy uprednostňujú senzačný obsah, posilňujú zavádzajúce a klamlivé informácie, pretože zvyšujú zapájanie sa užívateľov. Ak si tieto manipulácie neuvedomujete, môžete sa ľahko dostať do komôr ozveny, ktoré posilňujú predsudky a podporujú dezinformácie, čo môže viesť až k radikalizácii a polarizácii.

Psychologické účinky týchto algoritmov sú tiež hlboké. Neustále vystavenie emocionálne nabitému obsahu môže viesť k úzkosti, depresii a pocitu izolácie. Okrem toho návyková povaha platforiem riadených algoritmami prispieva k nadmernému používaniu sociálnych médií, keď sa ocitnete v nekonečných cykloch „scrollovania“ bez toho, aby ste si uvedomili, akú emocionálnu daň si to vyberá.

Účinky európskej legislatívy týkajúcej sa digitálnych služieb, ktorá vyžaduje, aby platformy zverejňovali svoje odporúčacie algoritmy, sa ešte len prejavia v budúcnosti.

Klikajte s rozvahou: Tipy pre zodpovedné používanie sociálnych sietí

Online priestor by mal byť bezpečný a každý používateľ by sa v ňom mal cítiť pohodlne. Ľudia často využívajú sociálne platformy na socializáciu, vytváranie profesionálnych kontaktov alebo aktivizmus, ale spôsob, akým sa angažujú online, môže trvale ovplyvniť nielen ich osobný život, ale aj celú spoločnosť. V rámci digitálneho občianstva sú pre používanie sociálnych médií nevyhnutné kompetencie, ako je kritické

myslenie, empatia či digitálna, mediálna a informačná gramotnosť. Ak sa chcete stať zodpovednými digitálnymi občanmi, mali by ste sa riadiť nasledovnými radami:

- **Zamyslite sa, skôr než niečo zverejníte -** sociálne médiá často nabádajú k impulzívnemu zverejňovaniu. Príspevky uverejnené v hneve alebo frustrácii môžu zle odrážať vašu povahu a ostatní by si ich mohli zle vysvetliť. Uvedomelý prístup k zdieľaniu môže zabrániť nedorozumeniam alebo poškodeniu vašej elektronickej reputácie.
- **Uvedomujte si dôsledky zdieľania osobných informácií** - zdieľanie osobných údajov, ako sú PII (z anglického *Personal Identifiable Information*), poloha, cestovné plány alebo citlivé názory, vás môže ohroziť. Tieto príspevky môžu byť použité na sledovanie vašich aktivít, ohroziť vaše súkromie alebo dokonca viesť ku krádeži identity.
- **Buďte si vedomí potenciálnych kriminálnych aktivít -** je nevyhnutné byť ostražitým voči technologickým aj medziľudským rizikám v digitálnom priestore. Rozpoznajte pokusy o phishing a krádež identity, ako aj kybernetické útoky a vyhnite sa im. Vyhýbajte sa klikaniu na neznáme alebo podozrivé odkazy a sťahovaniu súborov z nedôveryhodných zdrojov.
- **Pred zdieľaním obsahu si overte fakty -** pred zdieľaním článkov alebo príspevkov sa uistite, že pochádzajú z dôveryhodných zdrojov. Mali by ste rozvíjať schopnosti kritického myslenia, aby ste dokázali rozoznať faktický obsah od poplašných správ alebo clickbaitov. Nepresné alebo zavádzajúce príspevky nielenže poškodzujú vašu dôveryhodnosť, ale prispievajú aj k spoločenským škodám.
- **Zachovávajte rešpekt a empatiu v online interakciách -** sociálne médiá môžu byť priestorom pre zdravý a konštruktívny dialóg. Vyhnite sa hádkam alebo osobným útokom online, pretože tie sa často rýchlo stupňujú a zanechávajú trvalé negatívne pocity. Uplatňujte digitálnu empatiu a s rešpektom si vypočujte opačné názory, pretože to podporuje pozitívne online prostredie.
- **Uplatňujte aktívnu a pozitívnu angažovanosť -** svoju digitálnu reputáciu môžete zlepšiť prostredníctvom premyslených príspevkov. Či už na

odborných fórach alebo v sociálnych médiách, prispievanie cennými postrehmi a praktizovanie digitálnej empatie môže pomôcť formovať silnú, pozitívnu digitálnu identitu. Patrí sem zapájanie sa do hodnotných diskusií, zdieľanie zmysluplného obsahu alebo podpora iniciatív, ktoré propagujú inklúziu a sociálnu zodpovednosť online.

- **Zvážte svoje publikum** - sociálne médiá sú často verejné alebo poloverejné a publikum tak môže byť širšie, než sa predpokladá. Príspevky určené pre vašich priateľov sa môžu ľahko dostať k budúcim zamestnávateľom, akademickým inštitúciám alebo nechceným divákom. Zachovanie reprezentatívneho, slušného a úctivého tónu a používanie netikety môže ochrániť vašu e-reputáciu.

- **Vyhnite sa nadmernej konzumácii sociálnych médií** - obmedzte konzumáciu sociálnych sietí tým, že si budete všímať váš čas strávený na obrazovke. Mnohé smartfóny teraz umožňujú používateľom nastaviť časové limity pre jednotlivé aplikácie vrátane sociálnych platforiem a po prekročení tohto limitu zašlú upozornenia. Táto funkcia pomáha manažovať čas strávený na obrazovke a podporuje uvedomenie si potenciálneho nadmerného používania.

E-reputácia: Ako sa prezentovať a komunikovať online?

Spôsob, akým ste vnímaní online, označovaný ako e-reputácia, je priamym odrazom vašej e-prítomnosti. E-reprezentácia úzko súvisí s bezpečnosťou online a etickým správaním vo virtuálnom prostredí. Online prítomnosť

presahuje pasívnu online účasť; zahŕňa aktívne kultivovanie digitálnej stopy prostredníctvom interakcií, tvorby obsahu a etického správania, pričom sa zdôrazňuje význam digitálnej gramotnosti a uvedomelej sebareflexie pri formovaní vašej verejnej osobnosti na internete.

Vaša online identita sa môže formovať úmyselne aj neúmyselne. Zámerné vytváranie identity zahŕňa profil, obrázky, príspevky a osobné informácie, ktoré sa rozhodnete umiestniť na internete. Neúmyselné prvky vašej identity vytvára niekto iný, kto o vás niečo nahrá, napríklad v prípade označenia vášho profilu na obrázku alebo v príspevku. V súčasnosti vám platformy oznamujú, že ste boli označení, a poskytujú možnosť odmietnuť alebo potvrdiť označenie. Táto možnosť vám poskytuje určitú úroveň kontroly nad vašou neúmyselnú online identitou.

Všetko, čo sa zdieľa online, zanecháva stopu. Preto je dôležité si rozmyslieť, čo sa bude zdieľať a aké to môže mať dôsledky. Digitálnu reputáciu, ktorú si vytvoríte, možno ľahko preskúmať prostredníctvom online vyhľadávania vášho mena alebo iných osobných údajov. Výsledky vyhľadávania môžu zahŕňať príspevky na sociálnych sieťach, komentáre, profesijné profily alebo akýkoľvek verejný obsah spojený s vašou identitou. Pozitívna online prítomnosť, ako napríklad zdieľanie kariérnych úspechov alebo konštruktívna účasť na fórach, zlepšuje vašu reputáciu. Na druhej strane negatívny obsah, ako napríklad nevhodné správanie v sociálnych médiách, kontroverzné komentáre alebo zdieľanie dezinformácií, môže poškodiť váš imidž a mať negatívny vplyv na budúce kariérne príležitosti. Napríklad uchádzači o zamestnanie a univerzitu môžu byť zamietnutí z dôvodu úvodnej kontroly uchádzačov na sociálnych sieťach.

VI. DIGITÁLNE STOPY A ICH KONTROLA

V dnešnom prepojenom svete zanechávajú naše online aktivity za sebou stopu údajov známu ako digitálna stopa.

Digitálna stopa sa vzťahuje na dátovú stopu, ktorú vytvárate pri používaní internetu. Zahŕňa všetky informácie o vašich online aktivitách, interakciách a prítomnosti na rôznych digitálnych platformách. Môžete sa stretnúť s dvoma typmi digitálnych stôp – aktívnymi a pasívnymi.

Aktívna digitálna stopa sa vzťahuje na údaje, ktoré zámerne zdieľate online, ktorých ste si vedomí a ktoré máte pod kontrolou. Patria sem všetky informácie, ktoré úmyselne zverejníte alebo odošlete, napríklad príspevky na sociálnych sieťach (ako sú Facebook, X alebo Instagram), online recenzie, ktoré napíšete na produkty alebo služby, a registrácie účtov vrátane informácií odoslaných pri vytváraní účtov na rôznych webových stránkach.

Pasívna digitálna stopa sú informácie, ktoré sa o vás zhromažďujú bez vášho bezprostredného pričinenia. Zahŕňa históriu prehliadania zaznamenanú webovými stránkami, záznamy o IP adresách, údaje o polohe z mobilných zariadení a údaje zhromaždené aplikáciami spustenými na pozadí.

Každá činnosť, ktorú vykonávate online, zanecháva stopy a niekedy môžu byť digitálne stopy tam, kde ich nečakáte. Tu je niekoľko príkladov digitálnych stôp, aby ste si ich mohli lepšie uvedomiť:

Prepojenie medzi digitálnou stopou a e-reputáciou je významné, pretože digitálna stopa tvorí jej základ. Ako sme uviedli vyššie, digitálna stopa zahŕňa všetky údaje a stopy, ktoré zanecháva jednotlivec pri svojich online aktivitách, a to úmyselných aj neúmyselných. Okrem iného sem patria príspevky v sociálnych médiách, komentáre, online nákupy a história prehliadania.

Digitálna stopa jednotlivca priamo ovplyvňuje jeho elektronickú reputáciu, pretože odráža jeho hodnoty, záujmy a správanie. Potenciálni zamestnávatelia, obchodní partneri a dokonca aj osobní známi často posudzujú e-reputáciu osoby na základe skúmania jej digitálnej stopy. Pozitívna digitálna stopa môže zlepšiť váš profesionálny a osobný imidž a vyzdvihnúť vaše odborné znalosti a spoľahlivosť. Naopak, negatívna digitálna stopa, napríklad nevhodný obsah alebo kontroverzné názory, môže poškodiť vašu dôveryhodnosť a spoľahlivosť, čo môže viesť k strate príležitostí.

Spravovanie vašej digitálnej stopy je kľúčové pre udržanie priaznivej e-reputácie. To zahŕňa obozretnosť pri zdieľaní obsahu online, využívanie nastavení ochrany súkromia a pravidelné monitorovanie vašej online prítomnosti, aby ste sa uistili, že je v súlade so želaným osobným a profesionálnym imidžom.

Potenciálne úskalia

Nespravovaná digitálna stopa môže okrem negatívnej e-reputácie viesť k rôznym rizikám:

- **Riziká ohrozujúce súkromie -** digitálne stopy vás môžu vystaviť rôznym rizikám ohrozujúcim súkromie, ako napríklad kybernetickému prenasledovaniu, obťažovaniu a dokonca aj fyzickým hrozbám. Osobné informácie zdieľané online môžu byť zneužité inými osobami, čo môže viesť k neželanej pozornosti a potenciálnej ujme.
- **Bezpečnostné hrozby -** kybernetickí útočníci môžu zneužiť digitálne stopy na krádež identity, phishingové podvody a falšovanie účtov. Odhalené osobné údaje, ako napríklad používateľské mená a heslá, môžu byť použité na získanie neoprávneného prístupu k vašim účtom, čo vedie k finančným stratám a iným škodám.
- **Cielená reklama a zneužívanie údajov -** spoločnosti používajú digitálne stopy na sledovanie správania a preferencií používateľov, čo umožňuje cielenú reklamu. Tento postup síce môže zlepšiť používateľský zážitok, ale zároveň vyvoláva obavy týkajúce sa ochrany osobných údajov a rozsahu, v akom sa osobné údaje používajú bez výslovného súhlasu.
- **Vplyv na životné prostredie -** ukladanie a spracovanie digitálnych údajov prispieva k spotrebe energie a emisiám uhlíka. Pozornosť venovaná digitálnej stope môže pomôcť zmierniť vplyv na životné prostredie.

Environmentálny aspekt

Ekologický rozmer digitálnej stopy je čoraz dôležitejším aspektom, pretože naše online aktivity sa neustále rozširujú. Digitálne aktivity si vyžadujú značnú spotrebu energie, pretože dátové centrá a siete, ktoré poháňajú online služby, predstavujú približne 1 % globálnych emisií skleníkových plynov súvisiacich s energiou.

Okrem toho je uhlíková stopa spotreby digitálneho obsahu značná. S rastom digitálnych služieb a technológií, ako sú hry na cloudovom úložisku,

blockchain a virtuálna realita, sa očakáva, že vplyv digitálnej stopy na životné prostredie prudko vzrastie. Na riešenie týchto environmentálnych problémov odborníci okrem iných stratégií odporúčajú podporovať postupy digitálnej triezvosti s cieľom znížiť zbytočnú digitálnu spotrebu.

Na záver možno konštatovať, že pochopenie a riadenie environmentálneho aspektu digitálnej stopy je kľúčové pre zabezpečenie udržateľnejšej digitálnej budúcnosti.

Ako môžeme znížiť riziká vyplývajúce z digitálnych stôp?

Manažment digitálnej stopy sa začína spravovaním vašich osobných údajov. Nasledujúce tipy vám pomôžu znížiť riziko úniku vašich osobných údajov:

Ďalším užitočným tipom je oboznámenie sa s nasledujúcimi nástrojmi a ich využitím:

- **Siete VPN (virtuálne súkromné siete)** – maskujú vašu IP adresu a šifrujú vaše online aktivity.
- **Blokátory reklám** – blokovaním obmedzujú sledovanie reklám a sledovacích zariadení.
- **Zabezpečené prehliadače -** používajte prehliadače so zabudovanými funkciami ochrany súkromia.
- **Vyhľadávače zamerané na ochranu súkromia -** vyberte si vyhľadávače, ktoré nesledujú vaše vyhľadávania.
- **Nástroje na odstraňovanie údajov -** používajte služby, ktoré pomáhajú odstrániť vaše osobné údaje z webových stránok sprostredkujúcich údaje.
- **Zabezpečené siete -** zabezpečte si ochranu domácej siete Wi-Fi, aby ste znížili riziko odhalenia.
- **Aktualizácie softvéru -** pravidelne aktualizujte softvér svojich zariadení a antivírusové programy.

Porozumením svojej digitálnej stope a zavedením týchto stratégií môžete lepšie chrániť svoju prítomnosť online a zmierniť tak potenciálne riziká spojené s vašimi digitálnymi aktivitami.

Ochrana osobných údajov a jej význam

Citlivé informácie, ako sú mená, adresy, identifikačné čísla, finančné údaje a dokonca aj osobné preferencie a zvyky, sa stali cenným tovarom nielen pre jednotlivcov, ale aj pre korporácie, subjekty tretích strán a nepochybne aj pre zločincov. Ochrana osobných údajov je veľmi dôležitá, aby sa predišlo narušeniu súkromia, akými sú krádeže identity a iné nekalé činnosti, ktoré vyplývajú z únikov údajov. Úniky údajov sú čoraz bežnejšie, čo znamená, že je potrebné rozumieť tomu, ako sa vaše osobné údaje zhromažďujú a uchovávajú, ako aj rizikám, ktoré sú spojené s ich nedostatočnou ochranou (Rada Európy 2019).

Právo na súkromie je základným ľudským právom a jeho význam sa v modernom digitálnom prostredí ešte zvýraznil. V roku 2018 bolo zavedené všeobecné nariadenie Európskej únie o ochrane údajov (GDPR), ktoré upravuje zhromažďovanie, uchovávanie a používanie osobných údajov (Sharma 2022). Táto legislatíva poskytuje ľuďom väčšie právomoci nad ich osobnými údajmi, čo im umožňuje efektívnejšie spravovať svoju digitálnu prítomnosť.

Riziká úniku osobných údajov

V mnohých prípadoch si používatelia neuvedomujú riziká, ktoré vyplývajú zo zdieľania údajov. Zdanlivo nevinné úkony, ako napríklad zverejnenie fotografie alebo zdieľanie polohy na sociálnych sieťach, môžu neúmyselne odhaliť viac, ako bolo zamýšľané, a tým vás vystaviť riziku.

Dôsledky úniku osobných údajov môžu byť rozsiahle a závažné. Jednou z významných hrozieb je krádež identity, keď niekto ukradne a použije citlivé osobné údaje, ako sú identifikačné čísla, prihlasovacie údaje alebo finančné informácie, na neoprávnené nákupy alebo otvorenie účtov v mene obete. Ďalším rizikom je, že niekto môže vytvoriť falošný profil na sociálnych sieťach, v ktorom sa vydáva za vás, čo má hneď niekoľko negatívnych dôsledkov. Podvodník môže vykonať niečo nezákonné, poškodiť vašu povesť alebo oklamať vašich priateľov, rodinu a kolegov. Okrem toho môžu takéto účty viesť k narušeniu súkromia, odhaleniu osobných informácií a kontaktov. Môže to tiež umožniť phishingové útoky alebo krádež identity, keď podvodník použije falošný profil na získanie neoprávneného prístupu k citlivým údajom, finančným účtom alebo iným online platformám, čo vám môže spôsobiť vážnu škodu.

Okrem toho môže únik osobných údajov viesť k poškodeniu dobrého mena, najmä ak sú osobné údaje zverejnené v nevhodnom kontexte alebo ich zneužijú tretie strany. Ak sa citlivé osobné údaje, ako sú súkromné správy, fotografie alebo videá zverejnia online, môžu sa zneužiť na poškodenie povesti jednotlivca, čo narúša osobné a profesionálne vzťahy, a môže to viesť napríklad aj k obťažovaniu alebo kyberšikane. V extrémnych prípadoch

môže únik osobných údajov prerásť až do hrozby v reálnom svete, napríklad do prenasledovania alebo vydierania.

Narušenie súkromia môže okrem toho spôsobiť emocionálne utrpenie, pretože obete sa cítia zraniteľné, zneužité a majú strach z možných následkov. Táto psychologická záťaž môže vážne ovplyvniť duševnú pohodu, zdravie a pocit bezpečia jednotlivcov. Narušenie súkromia často vedie k pocitom bezmocnosti, pretože obete si uvedomujú, že už nemajú kontrolu nad svojimi osobnými údajmi. Táto strata kontroly môže mať za následok zvýšenú úzkosť, stres a neustály strach z toho, čo sa môže stať ďalej. Obete môžu pociťovať nespavosť, paranoidné stavy alebo depresiu, pretože narušenie môže oslabiť ich dôveru v digitálne systémy a ostatných ľudí okolo nich. Tento stres sa ešte zintenzívni, keď sa prejavia dôsledky narušenia, ako napríklad finančné podvody alebo krádež identity. Pocit zraniteľnosti sa ešte zhorší, keď sú na internete vystavené citlivé informácie, ako napríklad súkromné fotografie alebo korešpondencia. Toto odhalenie môže viesť k poškodeniu reputácie, kyberšikane, obťažovaniu a dokonca k ohrozeniu fyzickej bezpečnosti. Môžu sa objaviť aj problémy s duševným zdravím, ako napríklad posttraumatická stresová porucha (PTSD), najmä ak sú vystavené citlivé údaje, ako napríklad lekárske záznamy alebo intímne fotografie.

Rozhodujúci je aj vplyv na pocit bezpečia. Osoby postihnuté narušením súkromia sa často necítia bezpečne v digitálnom ani fyzickom prostredí a obávajú sa ďalšieho zneužitia alebo poškodenia. Tento nedostatok bezpečnosti môže viesť k sociálnemu stiahnutiu, keďže obete sa vyhýbajú digitálnym priestorom a obmedzujú svoje interakcie, aby minimalizovali ďalšie vystavenie nepríjemnostiam. Psychologická záťaž sa preto neobmedzuje len

na okamih narušenia, ale môže siahať ďaleko za jeho hranice a ovplyvňovať rôzne aspekty každodenného života.

Aby sa predišlo takýmto následkom, je nevyhnutné uvedomiť si dôležitosť ochrany osobných údajov a prijať vhodné opatrenia na zmiernenie týchto rizík. Digitálni občania musia prijať účinné opatrenia, aby sa zabezpečilo, že ich súkromné osobné údaje nebudú neoprávnene sprístupnené a zneužité.

Zostaňte v bezpečí: Praktické tipy na ochranu vašich osobných údajov

Keďže osobné údaje sú neustále vystavované riziku odhalenia alebo zneužitia, je dôležité pochopiť a zaviesť účinné stratégie na ich ochranu. Prinášame základné postupy, ktoré jednotlivcom pomôžu chrániť ich súkromie v digitálnom priestore:

Obmedzte zdieľanie informácií a upravte nastavenia ochrany osobných údajov

Osobné údaje by sa mali zdieľať online veľmi opatrne. Nevedomky môžete zdieľať viac informácií, ako je potrebné, napríklad polohu v reálnom čase alebo osobné zvyky. Zníženie množstva zdieľaných osobných údajov, či už na sociálnych sieťach, alebo iných platformách, vám môže pomôcť chrániť sa pred rizikami, ako je kybernetické prenasledovanie alebo krádež identity. Vyhnite sa napríklad zverejňovaniu cestovných itinerárov alebo bežných noviniek z vášho života, ktoré by vás mohli urobiť zraniteľnými voči prenasledovaniu alebo iným nekalým aktivitám.

Úpravou nastavení ochrany súkromia môžete tiež kontrolovať, kto má prístup k vašim osobným údajom, čím sa zníži riziko neželaného odhalenia. Odporúča sa nastaviť profil ako súkromný a nedovoliť, aby vás sledovali neznáme osoby. Okrem toho vytvorenie zoznamu „blízkych priateľov“ na

platformách, ako je Instagram, alebo používanie nastavení ochrany osobných údajov na Facebooku na obmedzenie viditeľnosti príspevkov môže pomôcť zabrániť neželanému odhaleniu.

Pravidelne aktualizujte nastavenia ochrany osobných údajov

Vzhľadom na vývoj technológií a zásad ochrany osobných údajov je dôležité pravidelne kontrolovať a aktualizovať nastavenia ochrany osobných údajov v aplikáciách a online kontách. Tým sa zabezpečí, že osobné údaje budú poskytované v súlade s vašimi preferenciami. Mali by ste tiež vypnúť funkcie zdieľania polohy alebo zrušiť nepotrebné povolenia z aplikácií a služieb, ktoré už nepotrebujú prístup k vašim údajom.

Informujte sa o zákonoch upravujúcich ochranu osobných údajov

GDPR bolo zavedené s cieľom chrániť súkromie jednotlivcov tým, že sa zabezpečí, aby webové stránky pred zhromažďovaním osobných údajov získali výslovný súhlas používateľa. Informovanosť o týchto zákonoch vám umožní lepšie pochopiť svoje práva a prevziať kontrolu nad svojou digitálnou stopou. Nariadenie GDPR napríklad dáva používateľom právo požadovať, aby boli ich údaje vymazané alebo aby neboli zdieľané s tretími stranami.

Spravujte súbory cookies a nastavenia prehliadača

Súbory cookies, teda malé časti údajov uložené v elektronických zariadeniach používateľov, sú používané na väčšine webových stránok a vo webových prehliadačoch sú zvyčajne prednastavene povolené. Ich nastavenia môžete upraviť tak, aby ste súbory cookies prijali alebo odmietli.

Zatiaľ čo niektoré súbory cookies sú nevyhnutné pre funkčnosť webových stránok, iné môžu sledovať vašu aktivitu na rozličných stránkach. Správa nastavení súborov cookies v nastaveniach prehliadača vám pomôže kontrolovať, ktoré typy súborov cookies sú povolené, čím sa obmedzí nadbytočné a nežiadúce sledovanie. Okrem toho pravidelné vymazávanie súborov cookies a údajov o prehliadaní môže pomôcť zvýšiť súkromie.

Získajte základné technologické vedomosti

Pri ochrane súkromia online vám môžu pomôcť základné znalosti technologických pojmov, ako sú šifrovanie, IP adresa a súbory cookies. Napríklad znalosť princípu šifrovania vám pomôže pri výbere bezpečných komunikačných metód a znalosť v problematike IP adries vám pomôže uvedomiť si, ako môže byť vaša poloha sledovaná online. Informácie o technológiách na zlepšenie ochrany súkromia, ako sú siete VPN a bezpečné prehliadače, vám tiež umožnia účinnejšie chrániť vaše údaje a zvýšiť vašu anonymitu online. Zároveň povedomie o rôznych technológiách na zlepšenie ochrany súkromia, ako sú siete VPN a bezpečné prehliadače, vám tiež umožnia účinnejšie chrániť vaše údaje a zvýšiť vašu anonymitu online.

Buďte opatrní pri verejných Wi-Fi a zdieľaných zariadeniach

Hoci je verejná sieť Wi-Fi pohodlná, predstavuje značné bezpečnostné riziko, pretože nie je šifrovaná. To uľahčuje kyberzločincom zachytenie osobných údajov. Ak chcete zostať v bezpečí pri používaní verejnej Wi-Fi, vyhýbajte sa realizácii citlivých transakcií, ako je napríklad online bankovníctvo alebo nakupovanie. Bezpečnejšou alternatívou je používanie siete VPN, ktorá šifruje vaše internetové pripojenie a chráni vaše údaje pred zachytením inými osobami. Podobne predstavuje bezpečnostné riziko aj používanie verejných alebo zdieľaných elektronických zariadení, ako sú napríklad počítače v univerzitnej knižnici. Osobné údaje, ako sú prihlasovacie údaje alebo história prehliadania, sa môžu nedopatrením uložiť a sprístupniť ďalším používateľom.

Používajte silné heslá a dvojfaktorové overovania (2FA)

Jedným z najjednoduchších spôsobov ochrany online účtov je používanie silných a jedinečných hesiel. Silné heslo zvyčajne kombinuje veľké a malé písmená, číslice a špeciálne znaky. Je tiež veľmi dôležité vyhnúť sa opakovanému používaniu hesiel na rôznych

platformách. Dvojfaktorová autentifikácia (2FA) pridáva ďalšiu úroveň zabezpečenia, keďže vyžaduje druhú fázu identifikácie, ako je napríklad kód v textovej správe alebo autentifikačná aplikácia, čo výrazne znižuje pravdepodobnosť neoprávneného prístupu.

Používajte zabezpečené webové stránky (HTTPS)

Pri zdieľaní osobných údajov alebo nakupovaní online sa vždy uistite, že je webová lokalita zabezpečená, a skontrolujte, či je v adrese URL uvedený prefix HTTPS. Písmeno „S“ v HTTPS označuje „*secure*“ (bezpečný), čo znamená, že webová lokalita používa šifrovanie na ochranu údajov pred zachytením tretími stranami. Ak chcete overiť, či je pripojenie zabezpečené, hľadajte vedľa adresy URL ikonu visiaceho zámku alebo prepínača.

Uplatnením týchto praktických tipov môžete výrazne zvýšiť svoje súkromie a bezpečnosť na internete, čo nie je len nevyhnutnosť, ale aj zodpovednosť. Kombináciou proaktívnej ochrany osobných údajov a technologického povedomia môžete minimalizovať riziká spojené so zdieľaním osobných údajov online.

VII. ZÁVER

Digitálny svet sa stáva čoraz dôležitejším prvkom nášho každodenného života, a preto je dôležité, aby si mladí ľudia osvojili zručnosti a hodnoty digitálneho občianstva. Podľa dát z Eurostatu (2023) 97 % jednotlivcov vo veku 16 až 29 rokov v EÚ denne používalo internet a 83 % bolo denne aktívnych na sociálnych sieťach. Tieto štatistické údaje poukazujú na všadeprítomnosť digitálnych technológií, ktoré formujú, akým spôsobom sa mladí ľudia učia, spájajú a zapájajú do diania vo svete.

Digitálny priestor slúži ako „okno do sveta“ a ponúka príležitosti na získavanie nových vedomostí a zručností. Aby však mladí ľudia mohli tieto príležitosti naplno využiť a zároveň sa vyhnúť potenciálnym rizikám, potrebujú pevné základy digitálneho občianstva. Táto príručka, ktorá je v súlade s rámcom digitálnych kompetencií pre občanov Európskej komisie, poskytuje tento základ tým, že zdôrazňuje kritické myslenie, etické správanie a základné kompetencie pre budúcnosť.

Digitálne občianstvo zahŕňa viac než len technické znalosti; ide o posilňovanie informovanej, rešpektujúcej a zodpovednej účasti v digitálnom prostredí. Táto príručka integruje zásady ochrany súkromia online, mediálnej gramotnosti, zodpovedného používania sociálnych médií a manažmentu digitálnych stôp a umožňuje žiakom prijímať uvážené rozhodnutia a pozitívne prispievať k digitálnej komunite.

Kompetencie uvedené v tejto príručke sú dôležité nielen pre orientáciu v dnešnom digitálnom prostredí, ale sú nevyhnutné aj pre budúci úspešný život v čoraz viac digitalizovanom svete. Keď pedagógovia, školitelia a organizácie zavedú tieto postupy, pomôžu formovať generáciu schopnú riešiť výzvy a maximalizovať príležitosti digitálneho veku.

Spoločne naďalej podporujme digitálne občianstvo ako základný kameň vzdelávania a zabezpečme, aby mladí ľudia mohli bezpečne, eticky a efektívne skúmať neobmedzené možnosti virtuálneho prostredia.

SLOVNÍK POJMOV

Autorské právo	Autorské právo je právny rámec, ktorý poskytuje tvorcom originálnych diel výhradné práva na používanie, reprodukciu, šírenie a adaptáciu ich výtvorov.
Autorské referencie	Autorské referencie vyjadrujú kvalifikáciu, skúsenosti, vzdelanie a odborné znalosti, ktoré má daná osoba v súvislosti s témou, o ktorej píše.
Dezinformácie	Dezinformácia je zámerne nepravdivá alebo zavádzajúca informácia, ktorá sa šíri s cieľom oklamať alebo manipulovať ostatných.
Digitálna (online) komunita	Digitálna (online) komunita je skupina ľudí, ktorí komunikujú, zdieľajú a spolupracujú prostredníctvom digitálnych platforiem a online priestorov.
Digitálna gramotnosť	Digitálna gramotnosť znamená schopnosť efektívne, bezpečne a zodpovedne používať digitálne technológie, nástroje a platformy na prístup k informáciám, ich hodnotenie, tvorbu a komunikáciu.
Digitálna stopa	Digitálna stopa je stopa údajov alebo informácií, ktoré osoba zanecháva pri používaní digitálnych zariadení, pri interakcii online alebo pri práci s technológiami.
Digitálna závislosť	Digitálna závislosť znamená nadmerné a nutkavé používanie digitálnych technológií, ako sú smartfóny, počítače, sociálne médiá, videohry alebo internet, do takej miery, že negatívne ovplyvňuje rôzne aspekty života človeka, ako sú vzťahy, práca, zdravie alebo celková duševná pohoda.

Digitálne nástroje	Digitálne nástroje označujú softvéry, platformy, aplikácie alebo zariadenia, ktoré využívajú digitálne technológie na vykonávanie úloh, riešenie problémov, komunikáciu alebo uľahčenie činností.
Digitálne občianstvo	Digitálne občianstvo predstavuje zodpovedné, etické a informované používanie technológií, najmä internetu, na efektívnu účasť v spoločnosti.
Digitálne obchodovanie	Digitálne obchodovanie (e-commerce) sa vzťahuje na nákup a predaj tovaru a služieb prostredníctvom internetu.
Digitálne práva	Digitálne práva sa zaoberajú právami a slobodami, ktoré majú jednotlivci v digitálnom svete, vrátane ich schopnosti používať, vytvárať a zdieľať digitálny obsah a informácie a zároveň chrániť svoje osobné údaje a súkromie.
Digitálne prostredie	Digitálne prostredie sa vzťahuje na akýkoľvek virtuálny priestor alebo ekosystém, v ktorom dochádza k digitálnym interakciám, činnostiam alebo procesom.
Digitálne zručnosti	Digitálne zručnosti zahŕňajú súbor zručností, vedomostí a postojov potrebných na efektívne a zodpovedné používanie digitálnych technológií v rôznych aspektoch života vrátane osobného, vzdelávacieho a pracovného kontextu.
Digitálny občan	Digitálny občan je osoba, ktorá využíva digitálne technológie a internet zodpovedne, eticky a efektívne, aby sa zapojila do života spoločnosti, politiky, vzdelávania a kultúry.

Digitálny priestor	Digitálny priestor označuje akékoľvek prostredie alebo platformu, ktorá existuje online alebo je poháňaná digitálnymi technológiami, kde používatelia interagujú, komunikujú a zapájajú sa do obsahu, služieb alebo medzi sebou navzájom.
Digitálny story-telling	Digitálny story-telling označuje používanie digitálnych nástrojov a platforiem na vytváranie a zdieľanie príbehov.
Digitálny svet	Digitálny svet označuje globálny ekosystém vytvorený digitálnymi technológiami, v ktorom sa informácie, komunikácia a činnosti uskutočňujú prostredníctvom elektronických a online prostriedkov.
Digitálny obsah	Digitálny obsah odkazuje na akékoľvek informácie alebo materiál, ktorý je vytvorený, uložený, distribuovaný alebo spotrebovaný v digitálnom formáte.
E-mail	E-mail (skratka pre elektronickú poštu) je spôsob výmeny digitálnych správ medzi ľuďmi pomocou elektronických zariadení, predovšetkým cez internet.
Empatia	Empatia je schopnosť pochopiť, zdieľať a vcítiť sa do pocitov, myšlienok alebo skúseností inej osoby.
Fact-checking	Fact-checking je proces overovania presnosti a pravdivosti informácií, tvrdení alebo výrokov, zvyčajne formou porovnávania so spoľahlivými a dôveryhodnými zdrojmi.
Flaming	Flaming označuje zverejňovanie alebo posielanie poburujúcich alebo urážlivých komentárov na internete s cieľom provokovať ostatných, podnecovať hnev alebo vyvolávať konflikty.

Grooming	Grooming je proces, pri ktorom si jednotlivec buduje vzťah s dieťaťom alebo inou zraniteľnou osobou s cieľom manipulovať s nimi, využívať ich alebo zneužívať.
Informačná gramotnosť	Informačná gramotnosť je schopnosť vyhľadávať, vyhodnocovať a používať informácie efektívne, účinne a eticky.
Inklúzia	Inklúzia znamená vytváranie prostredia, systémov a komunít, ktoré prijímajú rozmanitosť a zabezpečujú, aby všetci jednotlivci bez ohľadu na svoj pôvod, identitu alebo schopnosti mali rovnaký prístup k príležitostiam, občianskej participácii a rešpektu.
Komory ozveny	Komory ozveny odkazujú na prostredie, spravidla v rámci médií alebo sociálnych sietí, kde sú jednotlivci vystavení predovšetkým informáciám, názorom alebo myšlienkam, ktoré posilňujú ich existujúce presvedčenia alebo názory, namiesto toho, aby ich konfrontovali s rôznymi perspektívami.
Krádež identity	Krádež identity je neoprávnené získanie a použitie cudzích osobných údajov, zvyčajne na podvodné účely.
Kritické myslenie	Kritické myslenie je proces aktívnej a objektívnej analýzy, vyhodnocovania a syntézy informácií s cieľom prijímať odôvodnené a dobre informované rozhodnutia alebo úsudky.
Kritické posudzovanie	Kritické posudzovanie je proces starostlivého hodnotenia a analýzy niečoho – či už ide o myšlienku, argument, dielo, teóriu, alebo zdroj informácií – skúmaním jeho silných a slabých stránok, relevantnosti, presnosti a celkovej platnosti.

Kybernetické prenasledovanie	Kybernetické prenasledovanie znamená využívanie internetu, sociálnych médií alebo iných online platforiem na prenasledovanie alebo obťažovanie jednotlivca alebo skupiny.
Kyberšikana	Kyberšikana je využitie digitálnych technológií na obťažovanie, vyhrážanie sa, ponižovanie alebo ubližovanie.
Mediálna gramotnosť	Mediálna gramotnosť sa vzťahuje na schopnosť využívať, analyzovať, hodnotiť a vytvárať médiá v rôznych formách.
Mizinformácie	Mizinformácie odkazujú na nepravdivé alebo nepresné informácie, ktoré sa šíria bez ohľadu na úmysel oklamať.
Online aktivizmus	Online aktivizmus sa vzťahuje na používanie digitálnych nástrojov a platforiem na presadzovanie sociálnych, politických, environmentálnych alebo ekonomických cieľov.
Online obťažovanie	Online obťažovanie odkazuje na zneužívanie digitálnych platforiem a technológií na úmyselné poškodzovanie, zastrašovanie, vyhrážanie sa alebo ponižovanie jednotlivca alebo skupiny.
Online vykorisťovanie	Online vykorisťovanie označuje využívanie internetu alebo digitálnych platforiem na nekalé zneužívanie jednotlivcov, často prostredníctvom manipulácie, nátlaku alebo podvodu, s cieľom získať osobný, finančný alebo sexuálny prospech.
Osobné údaje alebo osobné	Osobné údaje sa vzťahujú na akékoľvek údaje alebo informácie, ktoré možno použiť priamo alebo nepriamo

identifikačné údaje (PII)	na identifikáciu, kontaktovanie alebo lokalizáciu jednotlivca.
Phishing	Phishing je typ kybernetického útoku, pri ktorom sa útočníci vydávajú za legitímne inštitúcie alebo jednotlivcov s cieľom vylákať od ľudí citlivé informácie, ako heslá, čísla kreditných kariet, čísla sociálneho a zdravotného poistenia alebo iné osobné údaje.
Podcast	Podcast je digitálny zvukový alebo obrazový program, ktorý sa dá streamovať alebo stiahnuť z internetu, zvyčajne v sérii epizód.
Práva duševného vlastníctva	Práva duševného vlastníctva sa zaoberajú právnou ochranou poskytovanou tvorcom a majiteľom duševného vlastníctva, ktoré zahŕňa nehmotné duševné výtvory.
Predpojatosť	Predpojatosť znamená tendenciu alebo preferenciu, ktorá ovplyvňuje úsudok, vnímanie alebo správanie jednotlivca spôsobom, ktorý je nespravodlivý, skreslený alebo neobjektívny.
Riešenie digitálnych problémov	Riešenie digitálnych problémov zahŕňa schopnosť používať digitálne nástroje, technológie a zdroje na identifikáciu, analýzu a hľadanie riešení problémov alebo výziev v rôznych kontextoch, ako je práca, osobný život alebo vzdelávanie.
Rovnosť	Rovnosť sa vzťahuje na zásadu čestnosti a spravodlivosti pri rozdeľovaní zdrojov, príležitostí a zaobchádzania, ktorá zabezpečuje, aby jednotlivci alebo skupiny dostali to, čo potrebujú na dosiahnutie rovnakých výsledkov.

Rozšírená realita (AR)	Rozšírená realita (AR) je technológia, ktorá v reálnom čase prekrýva digitálne informácie, ako sú obrázky, zvuky alebo iné údaje do prostredia reálneho sveta.
Sociálne média	Sociálne médiá sú digitálne platformy a aplikácie, ktoré umožňujú používateľom vytvárať, zdieľať a vymieňať si obsah, myšlienky a informácie s ostatnými používateľmi vo virtuálnych komunitách a sieťach.
Spoločenský kapitál	Spoločenský kapitál je pojem, ktorý sa používa na opis hodnôt vyplývajúcich zo sociálnych interakcií a väzieb, ktoré majú ľudia v rámci svojich komunít, organizácií alebo spoločností.
Spoofing účtu	Spoofing účtu alebo aj falšovanie účtu znamená vydávanie sa za legitímny účet alebo identitu s cieľom oklamať ostatných.
Streamovacie služby	Streamovacie služby sú platformy alebo technológie, ktoré umožňujú používateľom prístup k mediálnemu obsahu (ako je hudba, videá, televízne programy, filmy a živé vysielanie) a jeho konzumáciu prostredníctvom internetu. Streamovanie prebieha v reálnom čase bez toho, aby sa obsah musel najprv stiahnuť.
Účasť	Účasť znamená aktívnu účasť alebo zapojenie jednotlivcov do činností, rozhodovacích procesov alebo udalostí.
Umelá inteligencia (AI)	Umelá inteligencia (AI) znamená simuláciu ľudskej inteligencie v strojoch, ktoré sú naprogramované tak, aby mysleli, učili sa a vykonávali úlohy, ktoré si zvyčajne vyžadujú ľudské poznanie, ako napríklad porozumenie

	jazyku, rozpoznávanie vzorov, riešenie problémov a rozhodovanie.
Virtuálna realita (VR)	Virtuálna realita (VR) je počítačom vytvorená simulácia prostredia, ktorá používateľov vtiahne do virtuálneho sveta, zvyčajne pomocou VR headsetu, senzorov a niekedy aj ďalšieho vybavenia, ako sú rukavice alebo ovládače.
Všeobecné nariadenie o ochrane údajov (GDPR)	GDPR je komplexný zákon o ochrane údajov, ktorý prijala Európska únia (EÚ). Účinnosť nadobudol 25. mája 2018 a jeho cieľom je regulovať spracovávanie osobných údajov fyzických osôb v rámci EÚ a Európskeho hospodárskeho priestoru (EHP).

BIBLIOGRAFIA

Všetky obrázky získané zo služby **Canva**.

Aboujaoude, E. (2022). "Protecting Privacy to Protect Mental Health: The New Ethical Imperative". *Journal of Medical Ethics*. **https://doi.org/10.1136/medethics-2018-105313**

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild". *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674-689. **https://dl.acm.org/doi/10.1145/2660267.2660347**

Baltacı, Ö., Bektas, M., & Kutlu, F. (2021). "Internet addiction, social anxiety, and coping strategies among university students: A cross-sectional study". *Journal of Research in Adolescence*, 31(3), 565-575.

Better Internet for Kids. (2020). *Insafe insights on...online reputation*. **https://www.betterinternetforkids.eu/practice/awareness/article?id=6668871**

Bucher, T. (2018). "If...Then: Algorithmic Power and Politics". *Oxford Studies in Digital Politics, New York, 2018; online edn, Oxford Academic*. **https://doi.org/10.1093/oso/9780190493028.001.0001**

Carrascal, J.P., et al. (2013). "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." *Computers in Human Behavior*, vol. 29, no. 2, 2013, pp. 340–349. **https://arxiv.org/abs/1112.6098**

Cataldo, I., Lepri, B., Neoh, M. J.-Y., & Esposito, G. (2021). "Social media usage and development of psychiatric disorders in childhood and adolescence: A review". *Frontiers in Psychiatry, 11*. **https://doi.org/10.3389/fpsyt.2020.508595**

Cyber Citizenship. (2023). *Digital Citizenship 101: Responsible Online Behavior*. **https://www.cybercitizenship.org/digital-citizenship-guide/**

ENISA. (2017). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. **https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines**

eSafety Commissioner. (2024). *Digital reputation*. **https://www.esafety.gov.au/key-topics/staying-safe/digital-reputation**

European Data Protection Supervisor. (2020). Guidelines on the Protection of Personal Data. **https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en**

Eurostat. (2024). *Young people - digital world.* **https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/39761.pdf**

Fardouly, J., Magson, N. R., Rapee, R. M., Johnco, C. J., & Oar, E. L. (2020). "The use of social media by Australian preadolescents and its links with mental health". *Journal of Clinical Psychology*, *76*(7), 1304–1326. **https://doi.org/10.1002/jclp.22936**

Gillespie, T. (2018). "Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media". *Yale University Press*. **http://dx.doi.org/10.12987/9780300235029**

Helberger, N. (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism*, *8*(6), 842–854. **https://doi.org/10.1080/21670811.2020.1773888**

Isin, E., & Ruppert, E. (2015). *Being Digital Citizens.* Rowman & Littlefield International, Ltd. ISBN/9781786614490. **https://rowman.com/WebDocs/Being_Digital_Citizens_Second_Ed_Open_Access.pdf**

Kaspersky. (2024). *What is a Digital Footprint?*. **https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint**

Kotobee Blog. (2024). *Game-Based Learning: What It Is and How to Apply It*. **https://blog.kotobee.com/game-based-learning/**

Kozyreva, A., Wineburg, S., Lewandowsky, S., Hertwig, R. (2022). "Critical Ignoring as a Core Competence for Digital Citizens." *Current Directions in Psychological Science* 32 (1): 81–88. Crossref. **https://journals.sagepub.com/doi/full/10.1177/09637214221121570**

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report 2009.* EU Kids Online Network. **http://eprints.lse.ac.uk/24372/**

McCrae, N., Gettings, S., & Purssell, E. (2017). "Social media and depressive symptoms in childhood and adolescence: A systematic review". *Adolescent Research Review*, 2, 315–330. **https://doi.org/10.1007/s40894-017-0053-4**

Netsafe. (2018). *From literacy to fluency to citizenship: Digital citizenship in education (2nd ed.)*. Wellington, NZ. **https://www.researchgate.net/publication/332886585**

Nolan, S., Hendricks, J., Ferguson, S., & Towell, A. (2017). "Social networking site (SNS) use by adolescent mothers: Can social support and social capital be enhanced by online social networks? – A structured review of the literature". *Midwifery*, 48, 24–31. **https://doi.org/10.1016/j.midw.2017.03.002**

OECD. (2022). *Is digital media literacy the answer to our disinformation woes?* The OECD Education Podcast. **https://www.oecd-ilibrary.org/education/is-digital-media-literacy-the-answer-to-our-disinformation-woes_326b63bf-en**

Oxford Dictionary. (n.d.). *Definition of 'digital citizenship.* **https://dictionary.cambridge.org/dictionary/english/digital-citizenship**

Popat, A., & Tarrant, C. (2023). "Exploring adolescents' perspectives on social media and mental health and well-being – a qualitative literature review". *Clinical Child Psychology and Psychiatry*, 28, 323–337. **https://doi.org/10.1177/13591045221092884**

Pretorius, C., Chambers, D., & Coyle, D. (2019). "Young People's Online Help-Seeking and Mental Health Difficulties: Systematic Narrative Review". *Journal of medical Internet research*, *21*(11), e13873, **https://doi.org/10.2196/13873**

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook*. Council of Europe. **https://rm.coe.int/16809382f9**

Ringrose, J., Gill, R., Livingstone, S. & Harvey, L. (2012). "A qualitative study of children, young people and 'sexting': A report prepared for the NSPCC". London: NSPCC. **https://www.researchgate.net/publication/265741962**

Sala, A., Porcaro, L., & Gómez, E. (2024). "Social Media Use and adolescents' mental health and well-being: An umbrella review". *Computers in Human Behavior Reports*, *14*, 100404. **https://doi.org/10.1016/j.chbr.2024.100404**

Scheinin, M. (2009). "Law and Security: Facing the Dilemmas". *SSRN Electronic Journal*. **http://dx.doi.org/10.2139/ssrn.1555686**

Secure Privacy. (2022). *The Ultimate Guide to Cookie Consent*. **https://secureprivacy.ai/blog/the-ultimate-guide-to-cookie-consent**

Senekal, J. S., Groenewald, G. R., Wolfaardt, L., Jansen, C., & Williams, K. (2023). "Social media and adolescent psychosocial development: A systematic review". *South African Journal of Psychology*, 53, 157–171. **https://doi.org/10.1177/00812463221119302**

Sharma, A. (2022). "Teaching Digital Privacy: Navigating the Intersection of Technology, Education, and Privacy." *Kanpur Historians*. Vol. IX, Issue II. **https://www.researchgate.net/publication/381952547_Teaching_Digital_Privacy_Navigating_the_Intersection_of_Technology_Education_and_Privacy**

Sheldon, R. (2023). *Navigating the Digital World: Online Reputation and Online Etiquette*. Igniyte. **https://www.igniyte.com/blog/navigating-the-digital-world-online-reputation-and-online-etiquette/**

Techopedia. (2023). *How to Protect Your Privacy Online*. **https://www.techopedia.com/how-to/how-to-protect-your-privacy-online**

Twenge, J. M., Haidt, J., Lozano, J., & Cummins, K. M. (2022). "Specification curve analysis shows that social media use is linked to poor mental health, especially among girls". *Acta Psychologica*, *224*, 103512. **https://doi.org/10.1016/j.actpsy.2022.103512**

UNICEF. (2023). *Digital civic engagement by young people*. **https://www.unicef.org/innocenti/reports/digital-civic-engagement-young-people**

G, V. (2024, July 31). *How can your digital footprint affect you in business opportunities?* Reputation Sciences. **https://www.reputationsciences.com/how-can-your-digital-footprint-affect-you/**

Vuorikari, R., Kluzer, S., Punie, Y., & Európska komisia. (2022). *DigComp 2.2: Rámec digitálnych kompetencií pre občanov*. Úrad pre vydávanie publikácií Európskej únie. **https://data.europa.eu/doi/10.2760/115376**

Webster, D., Dunne, L., & Hunter, R. (2021). „Association between social networks and subjective well-being in adolescents: A systematic review". *Youth & Society*, 53, 175–210. **https://doi.org/10.1177/0044118X20919589**

Wolford B, (n.d.), *What is GDPR, the EU's new data protection law?*, GDPR.eu, **https://gdpr.eu/what-is-gdpr/**

DIGICITY

GAME-BASED
DIGITAL CITIZENSHIP

www.projectdigicity.eu

Spolufinancovaný
Európskou úniou

Financované Európskou úniou. Vyjadrené názory a stanoviská sú však výlučne názormi autora/ autorov a nemusia sa zhodovať s názormi Európskej únie alebo národnej agentúry Tempus Foundation. Európska únia ani národná agentúra Tempus Foundation za ne nenesú zodpovednosť.

Kód projektu: 2023-2-RS01-KA220-YOU-000170562

LogoPsyCom PENS digiQ YuzuPulse