Прирачник

за дигитална писменост и безбедност

Сè што треба да знаеш за побезбедно, покритичко и поодговорно движење низ дигиталниот свет



Institute for Good Governance and Euro Atlantic Perspective

Република Северна Македонија
Министерство за социјална политика, демографија и млади

Содржина

ЗА ПРОЕКТОТ „САЈБЕР БРАНА“	3
ЗОШТО ДИГИТАЛНАТА ПИСМЕНОСТ Е ВАЖНА?	5
КАКО ДА ПРЕПОЗНАЕШ ДЕЗИНФОРМАЦИЈА?	7
FACT-CHECKING ВО ПРАКСА	11
НАЈЧЕСТИ ОНЛАЈН ИЗМАМИ	14
ПАМЕТНИ ДИГИТАЛНИ НАВИКИ	18
ДИГИТАЛНА МЕНТАЛНА ХИГИЕНА	21
ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И DEEPFAKE СОДРЖИНИ	24
КАКО ФУНКЦИОНИРААТ АЛГОРИТМИТЕ?	26
ДИГИТАЛНО ГРАЃАНСТВО	28
„САЈБЕР БРАНА“ ГАЛЕРИЈА	30
МОЈА ЛИЧНА САЈБЕР БРАНА	36
ЗАВРШНА ПОРАКА	37

За проектот „Сајбер Брана“



Живееме во време кога секојдневно сме опкружени со океан од информации. И додека дел од нив се точни и проверени, постојат и такви кои се лажни, манипулативни или имаат цел да нè измамат. Социјалните мрежи, вештачката интелигенција и дигиталните платформи отвораат многу можности, но носат и нови предизвици. Затоа, денес не е доволно само да знаеме како да користиме интернет - важно е да знаеме како да го користиме безбедно, одговорно и критички.

Токму со таа цел беше реализиран проектот **„Сајбер Брана – креативна младинска иницијатива за дигитална писменост и безбедност“**. Преку работилници, едукативни содржини, креативен конкурс, изложба, квиз и онлајн кампања, проектот ги поттикна младите да размислуваат критички, да препознаваат дезинформации и да ги заштитат своите лични податоци и дигитален идентитет.

Во рамки на проектот, младите следеа обуки за дигитална и медиумска писменост, сајбер хигиена и креативно користење на дигиталните алатки, како и обука за графички дизајн и креирање визуелни содржини. Низ овој процес, тие не беа само публика, туку активни учесници и одговорни креатори. Преку постери, мемиња, инфографици, фотографии и видеа, младите ги преточија пораките за дигитална безбедност, критичко размислување и препознавање дезинформации во содржини блиски до нивната генерација.

Проектот „Сајбер Брана“ покажа дека младите не треба да бидат гледани само како корисници на интернет, туку и како важни сојузници во градењето побезбедна, поодговорна и покритичка дигитална средина.



Овој **прирачник** е еден од трајните резултати на проектот. Во него се собрани практични совети, примери и алатки кои ќе ти помогнат полесно да препознаеш дезинформации, да избегнеш најчести интернет измами, безбедно да ги користиш социјалните мрежи и да се снајдеш во дигиталниот свет.

Се надеваме дека овие страници ќе ти помогнат да стекнеш навики кои ќе те направат побезбеден, поодговорен и посамоуверен дигитален граѓанин.

Запомни: Твојата најсилна „Сајбер Брана“ не е во електронскиот уред што го користиш, туку во знаењето што го носиш со себе.

Секој клик е избор. Нека твоите избори бидат информирани, безбедни и одговорни.

Зошто дигиталната писменост е важна?



Речиси секој ден донесуваме десетици одлуки на интернет. Читаме вести, гледаме видеа, кликнуваме на линкови, разговараме на социјалните мрежи, користиме апликации и сè почесто комуницираме со алатки базирани на вештачка интелигенција.

Но, дали секоја информација што ја гледаме е точна? Дали секој профил и корисничка сметка се вистински? Дали секој линк е безбеден?

Токму затоа дигиталната писменост денес е една од најважните животни вештини. Таа не значи само да знаеш како да користиш телефон, компјутер или социјални мрежи. Таа значи да умееш критички да размислуваш, да препознаеш кога некој се обидува да те манипулира, да ги заштитиш своите лични податоци и безбедно да се движиш низ дигиталниот свет.

Да се биде дигитално писмен значи да знаеш...
✔️ да препознаеш дезинформација и манипулативна содржина;
✔️ да провериш дали информацијата доаѓа од доверлив извор;
✔️ да ги заштитиш своите профили и лични податоци;
✔️ да препознаеш интернет измама пред да стане проблем;
✔️ одговорно да комуницираш и да придонесуваш за поздрава дигитална средина.



Интернетот е едно од најмоќните места за учење, комуникација и креативност. Но, исто како и во реалниот живот, важно е да знаеш кому му веруваш, што споделуваш и како ги носиш своите одлуки.

Дигиталната писменост не е предмет што се учи само еднаш. Таа е вештина што се развива секој ден – со секој клик, секоја проверена информација и секоја одговорна одлука што ќе ја донесеш.

Како да препознаеш дезинформација?

Дезинформацијата не секогаш изгледа како очигледна лага. Понекогаш е напишана убедливо, има фотографија, звучи „логично“ или ја споделил некој што го познаваш. Токму затоа е важно да не реагираме веднаш, туку прво да застанеме, да провериме и да размислиме.



Лажни вести

Лажните вести се содржини што намерно шират неточни или измислени информации. Тие често се објавуваат за да предизвикаат паника, гнев, страв или недоверба.

Внимавај ако веста звучи премногу шокантно, нема наведени извори, не ја објавил ниту еден релевантен медиум или се повикува на „тајни информации“ без докази.

Манипулативни наслови

Насловот е првото нешто што го гледаме. Затоа дезинформациите често користат сензационалистички и манипулативни наслови за да нè натераат да кликнеме, да се вознемириме или да ја споделиме содржината без да ја прочитаме.



Примери за предупредувачки наслови се:

„Нема да верувате што се случи...“
„Ова го кријат од јавноста!“
„Шокантна вистина што никој не сака да ја знаете!“

Ако насловот звучи како да сака да те исплаши или налути, прочитај внимателно и провери дали текстот навистина го потврдува тоа што го тврди насловот.

Проверка на извори

Едно од најважните прашања е: Кој ја објавува оваа информација?

Провери дали станува збор за познат медиум, официјална институција, стручна организација или непозната страница без јасни податоци за авторот. Доверливите содржини најчесто имаат наведени автори, датуми, извори и линкови до дополнителни информации.

Ако текстот се повикува на „експерти“, „истражувања“ или „сведоци“, но не кажува кои се тие, тоа е знак за претпазливост.



Наведувачка содржина

Некои содржини не мора да бидат целосно лажни за да бидат манипулативни. Понекогаш се користат вистински факти, но се прикажуваат само делумно или во погрешен контекст.

На пример, може да се користи стара фотографија како да е од нов настан, да се извади изјава од контекст или да се прикаже само една страна од приказната.

Затоа, секогаш прашај се: *Што недостасува во оваа содржина? Дали има и друга страна на приказната?*

Поларизирачки и ексклузивен наратив

Дезинформациите често се обидуваат да создадат поделби. Тие користат јазик што ги дели луѓето на „*ние*“ и „*тие*“, ги претставува сите што мислат поинаку како непријатели или тврди дека само една група ја знае „вистината“.

Внимавај на содржини што користат изрази како:

„Само ние ја кажуваме вистината“
„Сите други медиуми лажат“
„Тие сакаат да ве замолчат“
„Ако не го споделиш ова, ти си дел од проблемот“

Таквиот јазик често има цел да предизвика силна емоција, а не да информира.

Недоволни или тешко проверливи податоци

Доверливата информација треба да може да се провери. Ако во текстот има големи тврдења, но нема бројки, документи, линкови, изјави, датуми или јасни извори, треба да бидеш внимателен/на.

Посебно внимавај кога содржината користи формулации како:

„се зборува дека... /се шпекулира дека... “
„според неофицијални информации...“
„многумина тврдат...“
„експертите предупредуваат...“

Овие изрази не се секогаш проблем, но ако нема дополнителни докази, не треба веднаш да се земаат како сигурна информација.

Пред да споделиш, провери!

Пред да споделиш некоја содржина, постави си три прашања:

1. *Кој ја објавил информацијата?*
2. *Дали има докази и извори?*
3. *Дали содржината ме тера да реагирам веднаш, без да размислам?*

Ако одговорот не е јасен, подобро е да не споделиш веднаш.

Проверувањето не значи недоверба кон сè. Тоа значи одговорност кон себе и кон другите.



Fact-checking во пракса

Не мора да бидеш новинар или истражувач за да провериш дали една информација е точна. Постојат едноставни чекори што секој може да ги направи пред да поверува или да сподели некоја содржина.



1. Провери ја фотографијата

Фотографиите лесно можат да бидат извадени од контекст или повторно искористени за сосема друг настан.

Затоа користи Reverse Image Search - алатка што покажува каде и кога фотографијата претходно била објавена.

Најпознати алатки се: **Google Images (Search by Image)**, **Google Lens**, **TinEye** и други.

Ако фотографијата е објавена пред неколку години, а некој тврди дека е од вчера, најверојатно станува збор за манипулација.

2. Провери го датумот

Честа практика е старите вести повторно да се споделуваат како да се нови.

Провери:

✔️ кога е објавен текстот;
✔️ дали фотографијата или видеото се од истиот период;
✔️ дали информацијата е сè уште актуелна.

Понекогаш и вистинска информација може да стане дезинформација ако е претставена во погрешен временски контекст.

3. Провери го авторот и изворот

Запрашај се:

• *Кој ја објавил информацијата?*
• *Дали медиумот е познат и транспарентен?*
• *Дали е наведен автор?*
• *Дали има линкови до официјални извори?*

Ако не можеш да најдеш кој стои зад информацијата, има причина да бидеш внимателен.

4. Размислувај критички

Критичкото размислување не значи да не веруваш никому. Тоа значи да поставуваш прашања. Прашај се:

- Дали има докази?
- Дали оваа информација е потврдена и од други извори?
- Дали текстот се обидува да ме исплаши, налути или изненади?
- Дали реагирам емотивно наместо рационално?

Најголемата предност на дезинформациите е нашата брза реакција.

5. Провери ја информацијата онлајн

Пред да поверуваш или споделиш нешто, побарај дали истата информација ја објавиле и други релевантни медиуми или институции.

Ако станува збор за голема вест, речиси секогаш ќе можеш да ја најдеш и на официјални веб-страници, кредибилни медиуми или проверувачи на факти.

6. Развивај медиумска и ВИ писменост

Денес не е доволно само да знаеме да користиме интернет. Потребно е да знаеме и како функционираат медиумите и вештачката интелигенција.

AI може да создаде фотографии, видеа и гласови што изгледаат убедливо, но не се вистински.

Затоа секогаш проверувај:

✔️ дали содржината изгледа премногу совршено;
✔️ дали има официјална потврда;
✔️ дали истата информација постои и на други доверливи извори.

Запомни:

Не проверувај затоа што не веруваш никому. Проверувај затоа што сакаш да бидеш сигурен дека информацијата е точна.

Во дигиталниот свет, неколку минути проверка можат да спречат ширење на дезинформации и да те заштитат од измама.

Најчести онлајн измами

Интернетот ни овозможува полесна комуникација, учење и забава, но истовремено е простор каде измамниците постојано смислуваат нови начини да дојдат до лични податоци, лозинки или финансиски информации. Најчесто тие ја користат нашата љубопитност, доверба или брза реакција.

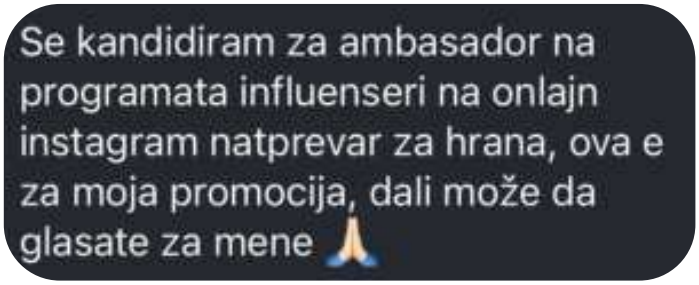
Добрата вест е дека повеќето измами можат лесно да се препознаат ако знаеш на што да обрнеш внимание.

„Гласај за мене“

Една од најчестите измами на социјалните мрежи започнува со порака од пријател или познаник:

„Те молам гласај за мене, многу ми значи.“

Пораката обично содржи линк до страница што изгледа како вистински сајт за гласање. Но, кога ќе го отвориш, од тебе се бара да се најавиш со Instagram, Facebook или друга сметка. Во моментот кога ќе ги внесеш податоците, тие завршуваат кај измамниците, кои можат да го преземат твојот профил и да ја испратат истата порака до сите твои контакти.



← Пример од порака која се праќа на социјалната мрежа Инстаграм и има за цел да ги уркаде податоците за сметката на корисниците

Како да се заштитиш?

✔️ Никогаш не внесувај лозинка за социјални мрежи преку линк добиен во порака.
✔️ Провери ја добро веб-адресата пред да одлучиш да се најавиш.
✔️ Ако нешто изгледа сомнително, контактирај го пријателот преку порака на друга социјална мрежа или јави му се.

Лажни наградни игри

„Освој нов телефон!“
„Ти си среќниот добитник!“
„Само денес добиваш подарок!“

Ваквите објави често изгледаат како да доаѓаат од познати компании, но нивната цел е да те натераат да оставиш лични податоци, да кликнеш на сомнителен линк или да ја споделиш измамата со други.

Внимавај ако:

✔️ профилот нема син знак за верификација или има многу малку следбеници;
✔️ се бара да внесеш лични или банкарски податоци;
✔️ наградата изгледа „предобра за да биде вистина“;
✔️ постојано те брзаат со пораки или објави како „последна шанса“ или „само денес“.

Phishing пораки

Phishing е обид некој да те измами претставувајќи се како банка, пошта, државна институција или позната компанија.

Најчесто ќе добиеш е-пошта, SMS или порака со текст дека мораш веднаш да потврдиш податоци, да платиш мала сума или да го ресетираш профилот.

Целта е да кликнеш на линкот и сам да ги внесеш своите податоци.



Објава во рамки на кампањата на проектот „Сајбер Брана – креативна младинска иницијатива за дигитална писменост и безбедност“.

Запомни:

Банките и институциите никогаш нема да бараат лозинки преку е-пошта или порака. Не отворај линкови ако не си сигурен од кого доаѓаат. Ако имаш сомнеж, отвори ја официјалната веб-страница рачно, наместо преку добиениот линк.

Лажни профили

Измамниците често креираат профили што изгледаат речиси идентично како профилите на вистински личности, компании или организации.

Нивната цел може да биде да бараат пари, да испраќаат сомнителни линкови, да шират дезинформации или да стекнат доверба за понатамошна измама.



Како да препознаеш лажен профил?

✔️ мал број објави или следбеници;
✔️ неодамна креиран профил;
✔️ чудни пораки со барање за пари или лични податоци;
✔️ граматички грешки и необичен начин на комуникација;
✔️ фотографии преземени од други профили.

Запомни

Најголемиот број интернет измами не се потпираат на сложена технологија, туку на човечка доверба и брзи реакции. Затоа, секогаш застани неколку секунди пред да кликнеш, да внесеш лозинка или да споделиш лични информации.

Неколку секунди проверка можат да спречат голема штета.

Паметни дигитални навики

Исто како што секојдневно се грижиме за личната хигиена, потребно е редовно да се грижиме и за нашата дигитална безбедност. Неколку едноставни навики можат значително да ја намалат можноста некој да ги злоупотреби твоите податоци или да добие пристап до твоите профили.

Користи силни и различни лозинки

Лозинката е првата линија на одбрана на секој профил.



Добрата лозинка треба:

✔️ да биде долга најмалку 12 знаци;
✔️ да содржи комбинација од големи и мали букви, бројки и специјални знаци;
✔️ да не содржи лично име, датум на раѓање или лесно препознатливи зборови;
✔️ да биде различна за секој профил.
Ако користиш иста лозинка на повеќе места, хакирањето на еден профил може да ги загрози и сите останати.

Вклучи двофакторска автентикација (2FA)

Двофакторската автентикација додава уште едно ниво на заштита.

Дури и ако некој ја дознае твојата лозинка, нема да може да се најави без дополнителниот код што го добиваш на телефонот или преку апликација за автентикација.

Секогаш кога е можно, вклучи 2FA на:

- Instagram
- Facebook
- Apple ID
- Microsoft
- банкарски и други важни профили.



Редовно ажурирај ги уредите и апликациите

Ажурирањата не носат само нови функции. Тие често ги поправаат безбедносните пропусти што можат да ги искористат сајбер-криминалците.



Затоа:

✔️ инсталирај ги новите ажурирања навреме;
✔️ користи лиценциран оперативен систем;
✔️ преземај апликации само од официјалните продавници.

Прави резервни копии (Backup)

Замисли да ти се расипе телефонот или компјутерот и да ги изгубиш сите фотографии, документи и контакти.

Редовното правење резервни копии ти овозможува лесно да ги вратиш податоците ако уредот се расипе, биде украден или биде погоден од малициозен софтвер.

Можеш да користиш:

- Cloud услуги (Google Drive, iCloud, OneDrive)
- Надворешен хард-диск или USB меморија.



Навики што прават голема разлика

✔️ Заклучувај го телефонот и компјутерот со PIN, лозинка или биометриска заштита.
✔️ Не оставај ги профилите најавени на јавни или туѓи уреди.
✔️ Одјави се по користење на јавен компјутер.
✔️ Не инсталирај апликации од непроверени извори.
✔️ Периодично проверувај кои уреди имаат пристап до твоите профили.

Дигитална ментална хигиена



Употребата на дигитални технологии може да игра важна улога за ментално здравје на децата и младите особено ако се користат неконтролирано и неправилно. Постојаната изложеност на информации, реакции и социјални интеракции онлајн влијае врз нашето расположение, себепочитување и концентрација. Дигиталните технологии и социјални мрежи може да предизвикаат и зависност што пак може да доведе до низа негативни емоции и однесувања кои можат да влијаат на менталната добросостојба кај младите како на пример анксиозност, замор, потешкотии во спиењето.

Оттука, дигиталната ментална хигиена е исклучително важна а се однесува на практики кои ни помагаат да ги управуваме емоциите, вниманието и дигиталните навики за да бидеме поздрави и поефикасни.

Како младите да ги подобрат овие состојби?

Правилно користење на социјалните медиуми, видео игрите и другите технологии.

Со цел да утврдат колку и на кој начин го поминуваат времето онлајн, да се запрашаат: *Колку време поминуваат на интернет? Дали ова влијае на нивните социјални активности, како што се вежбање, дружење со пријатели, читање и спиење? Каква содржина консумираат и како се чувствуваат? Дали се онлајн затоа што сакаат или чувствуваат дека мора да се присутни?*

Што да направат младите?	Прашање за себепроцена	Практичен совет
Ограничување на времето и содржините кои ги конзумираат во дигиталниот свет	Колку време навистина поминувам на телефонот/апликации? Дали тоа време ми го нарушува сонот, учењето или дружењето? Се чувствувам ли уморно или исцрпено по користење?	Постави реални дневни лимити и користи тајмери (Screen Time, Digital Wellbeing). Одреди „без екран“ периоди (на пр. 30–60 минути пред спиење). Направи 24-часовен дигитален дневник еднаш неделно и запиши апликации, време поминато онлајн и емоции.
Селекција на содржини	Каква содржина најчесто консумирам: информации, мемиња, долги видеа? Дали тие профили ме инспирираат или ме исцрпуваат?	Преферирај профили и канали што носат знаење или позитивност. Ограничувај пасивно „скролање“ избери 3 корисни канали и отфрли 5 што те исцрпуваат.

Што да направат младите?	Прашање за себепроцена	Практичен совет
Управување со емоции и реактивно однесување	Колку често реагирам брзо кога ќе се налутам или растажам од нешто онлајн? Дали потоа се каам?	Почекај 15–30 минути пред да одговориш („пауза-делувај“). Ако си вознемирен, запиши во дневник, јави се кај пријател или направи кратка прошетка пред да се вклучиш повторно.
Дозирање вести и социјални медиуми	Дали постојано проверувам вести? Дали нотификациите ме прекинуваат во учење/спиење?	Читај вести само во одредено време (на пр., 20–30 минути наутро и навечер). Исклучи нотификации за апликации што не се релевантни за тебе
Социјална поддршка и граници	Дали имам лице кому можам да кажам ако ме повредат онлајн? Дали контролираш кој ти пишува и кога?	Постави јасни онлајн граници (кажи кога не сакаш пораки, користи „mute“/„do not disturb“). Ако се соочуваш со сајбернасилство или анксиозност, побарај поддршка од пријател, родител, наставник или психолог.
Критичко размислување	Пред да споделам, дали сум сигурен дека информацијата е точна и безбедна за другите?	Практикувај „три прашања“ пред споделување: (1) Ова е точно? (2) Ова помага? (3) Може ли да наштети? Ако одговорот на некое прашање е „не“, не споделувај.
Паметни навики за сон и концентрација	Дали користењето екран пред спиење ми го нарушува сонот? Дали се прашувам колку време учам без прекини?	Никогаш не користи екран 30–60 минути пред спиење; вклучи ноќен режим/blue light filter ако мораш. Пробај„Помодоро“техника: 25 минути фокусирано учење, 5 мин пауза. Исклучи ги нотификациите и звукот.

Порака за младите:

Грижете се за својот дигитален простор исто како што се грижите за себе, поставувајте граници, бидете критични кон содржините и секогаш кога имате потреба,барајте поддршка. Престојувањето во природа, шетањето и разговорот овозможува полесна релаксација, не се оптоварувајте со непотребни мисли, намалете ја физичката тензија, и „дишете длабоко“ .

Вештачка интелигенција и deepfake содржини



- **AI фотографии** - Со помош на вештачката интелигенција денес брзо можат да се создадат фотографии кои изгледаат целосно реално, иако никогаш не постоеле. Затоа не треба автоматски да веруваме на сè што гледаме на интернет. Секоја фотографија треба да ја анализираме критички, да го провериме нејзиниот извор и да се запрашаме и да провериме дали постојат други докази кои ја потврдуваат нејзината автентичност.

- **AI видеа** - Видеото во дигиталната и ВИ ера веќе не претставува непобитен доказ за тоа дека нешто навистина се случило. Благодарение на алатките за видео обработка и едитирање, а особено со користење на алатки базирани на вештачка интелигенција можат да се создадат или изменат видеа во кои луѓето навидум кажуваат или прават нешто што никогаш не се случило. Затоа, пред да поверуваме или да споделиме ваква содржина, неопходно е да ја провериме преку повеќе релевантни и кредибилни извори.

- **AI гласови** - Современите алатки за вештачка интелигенција можат многу верно да го имитираат нечиј глас со само неколку секунди аудио-снимка. Поради тоа, телефонските повици или гласовните пораки повеќе не треба автоматски да ги сметаме за доволен доказ дека навистина разговараме со одредена личност. Доколку добиеме необично барање, особено ако се однесува на пари, лозинки или лични податоци, секогаш треба дополнително да го провериме преку друг веродостоен комуникациски канал.

Секој твој личен податок и сè што претставува твој личен идентитет.

Во ерата на вештачката интелигенција, секој личен податок има вредност. Фотографиите, видеата, гласот, потписот, документите, па дури и нашиот лик, начинот на кој пишуваме или зборуваме, претставуваат дел од нашиот дигитален идентитет. Затоа е важно внимателно да размислуваме што објавуваме, бидејќи еднаш споделената содржина може да биде искористена на начини кои никогаш не сме ги очекувале.

Како функционираат алгоритмите?



Filter bubbles

Алгоритмите на социјалните мрежи не ни ја прикажуваат целата слика, туку најчесто содржините за кои проценуваат дека најмногу ќе нè задржат на платформата. ака постепено почнуваме да гледаме сè повеќе информации што се совпаѓаат со нашите интереси и ставови, а сè помалку различни перспективи.

Затоа е важно свесно да следиме различни извори на информации и критички да ги споредуваме, односно прифаќаме различните гледишта. Едноставно, излезете од вашиот дигитален „меур“ (bubble) и уживајте во различностите, бидејќи токму тие се богатство на секое општество и на целиот свет.

“Ехо комори“

Следствено на претходно кажаното, кога постојано комуницираме само со луѓе кои размислуваат исто како нас и следиме содржини што ги потврдуваат нашите ставови, лесно можеме да влеземе во таканаречени „ехо комори“. Во таква средина различните мислења речиси и не стигнуваат до нас, а поларизацијата дополнително се продлабочува.

Демократско општество се гради преку дијалог, почитување на различностите и аргументирана дебата. Не заборавајте дека секоја личност има еднакви права и еднакво достоинство како секој од нас, а емпатијата и почитувањето на правата и на „другите“ е единствениот правилен избор во секоја ера или епоха.



Зошто гледаме одредени содржини

Секоја интеракција што ја правиме на интернет остава дигитална трага. Лајковите, коментарите, споделувањата, пребарувањата и времето што го поминуваме на одредена содржина им помагаат на алгоритмите да одлучат што следно ќе ни прикажат. Затоа и самите сме активен дел од алгоритамот, а не само негови корисници. Или, кога некаде ќе прочитате дека веб-страницата користи или нуди „колачиња“, тоа не значи дека станува збор за оние што се јадат.

Дигитално граѓанство



ДА за одговорно коментирање

Културата на комуникација не завршува кога ќе се вклучиме на интернет. Пред да напишеме коментар, важно е да се запрашаме дали би го кажале истото и во директен разговор. Истовремено, уште поважно е да се запрашаме како би се чувствувале ако некоја друга личност го остави тој коментар за нас. Одговорната и инклузивна комуникација придонесува за поголема доверба, поквалитетен дијалог и дигитален простор кој еднакво припаѓа на сите луѓе. И запомни, не е неопходно за сè да имаш, а уште помалку јавно да изразиш личен став. Никој не го очекува или бара тоа од тебе.

НЕ за говорот на омраза

Говорот на омраза претставува чиста спротивност на слободата на изразување. Наједноставно кажано тоа е злоупотреба на слободата на изразување со цел навредување, дискриминација или поттикнување нетрпеливост кон поединци или групи. Запомни дека наместо да го шириме или охрабруваме говорот на омраза, секој од нас има одговорност да го пријави, да не учествува во неговото ширење и да придонесува за култура на почитување во онлајн просторот.

Почитување на различни ставови

Не мора да се согласуваме со личноста од другата страна на тастатурата или мобилниот телефон за да покажеме почит. Демократијата и дигиталното, односно ВИ општеството се темели на можноста различните мислења да се слушнат, аргументираат и почитуваат. Кога разговараме со факти, аргументи и меѓусебна почит, создаваме поквалитетен јавен простор за сите, каде доминира дебатата, квалитетот на мислењата, а нема простор за булингот, исмевањето, дискриминацијата и омаловажувањето.



Проверка пред споделување

Една од најважните дигитални навики денес е да провериме пред да споделиме. Неколку секунди потрошени за проверка на изворот, датумот, авторот и содржината можат да спречат ширење дезинформации, манипулации или измами. Во дигиталната и ВИ ера, секој од нас не е само корисник на информации, туку и нивен креатор, пренесувач и чувар на довербата во јавниот информативен простор.

„Сајбер Брана“ галерија

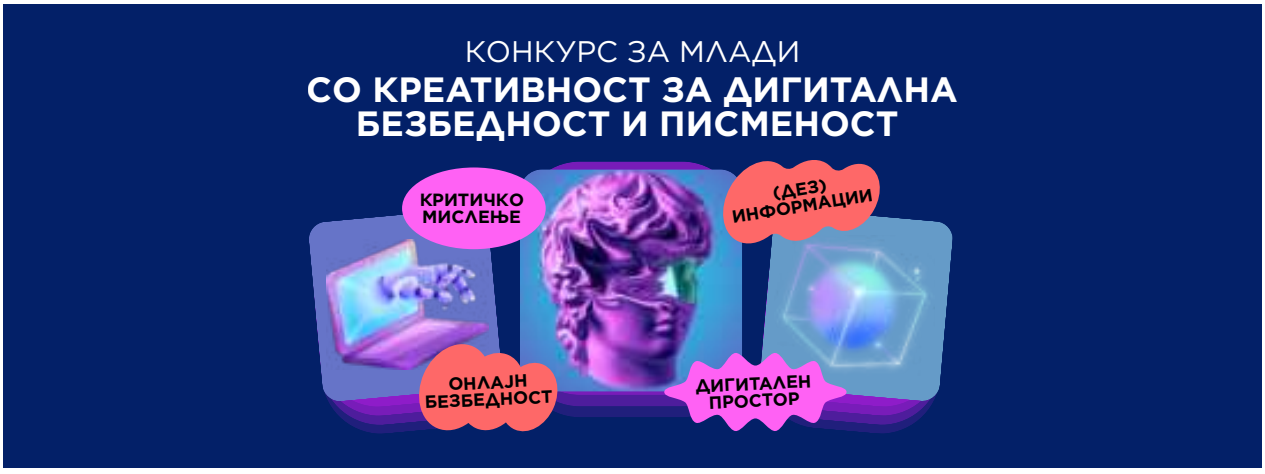
Во рамки на проектот „Сајбер Брана“ беше организиран конкурс за млади на тема дигитална писменост и безбедност, со цел преку креативен израз да се поттикне критичкото размислување и да се подигне свеста за предизвиците во дигиталниот свет.

По завршувањето на обуките за дигитална и медиумска писменост и графички дизајн, учесниците ги преточија своите знаења во оригинални постери, мемиња, инфографици, фотографии и видеа. Нивните дела обработуваа теми како препознавање дезинформации, заштита на личните податоци, интернет измами, сајбер хигиена и одговорно користење на социјалните мрежи.

Стручна комисија ги избра најдобрите трудови според нивната креативност, оригиналност, визуелна изведба и едукативна вредност.

Дел од нив се претставени на следните страници како потсетник дека најсилните пораки често доаѓаат токму од младите.

Видеата кои учествуваа на конкурсот, може да се погледнат на овие два линка: Линк 1 и Линк 2.

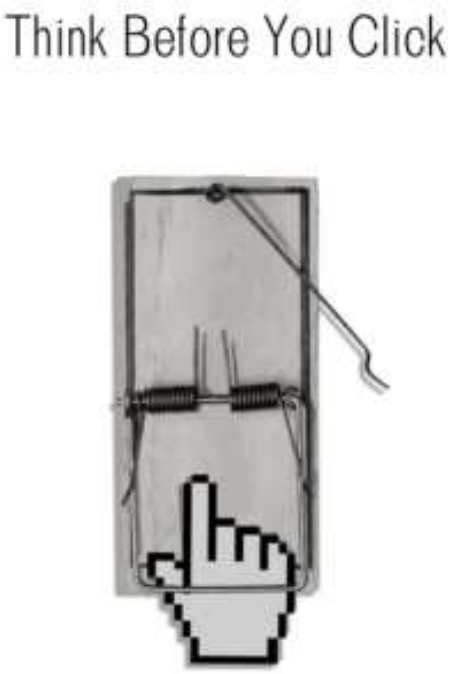




автор: **Симон Стоимилов**



автор: **Анита Андонова**



автор: **Стефани Здравковска**



автор: **Мартина Арсеска**



Скопје, 15 мај 2026

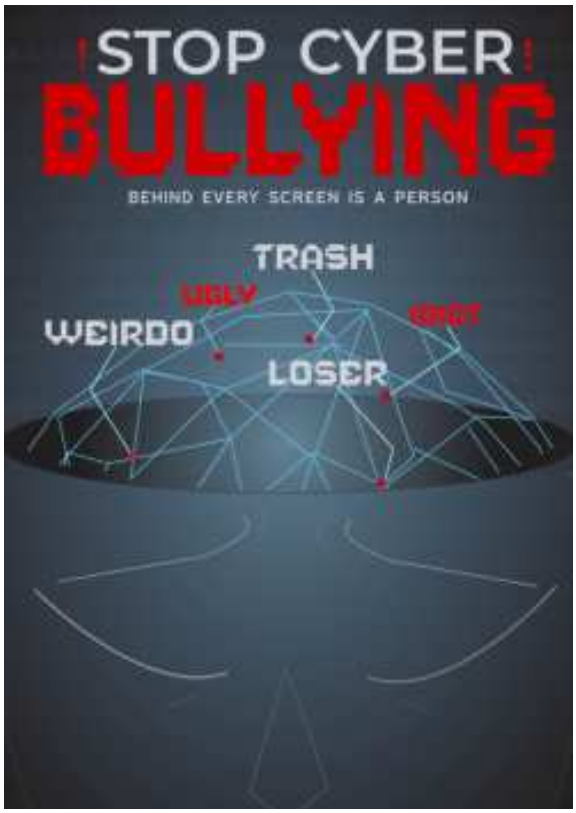
ДНЕВНА ХРОНИКА

УЖАС НА ВАРДАР: „ПАЦИЕНТОТ НУЛА" ГО ПОНЕСЕ ХАНТАВИРУСОТ ОД ЦЕНТАРОТ НА СКОПЈЕ?

ГУБРЕТО КАКО БИОЛОШКА БОМБА

Славниот град е под опсада на невидлив непријател.

автор: **Бојана Трајкова**



автор: **Марта Мијоски**



автор: **Благој Јованов**



автор: **Антонио Димески**



автор: **Деспина Козаровска**



автор: **Марта Петрушевска**



автор: **Ангела Зафировска**



автор: **Виктор Ристов**



автор: **Сара Јанкуловска**



автор: **Мартин Дамкоски**



автор: **Божанка Илиева**



автор: **Никола Гацов**



автор: **Кристијан Јордановски**



автор: **Стефан Вуловски Иванов**



автор: **Памела Павловска**

Моја лична Сајбер Брана

Проверувам дали...

□ Користам силни и различни лозинки за моите профили.
□ Имам вклучена двофакторска автентикација (2FA).
□ Редовно ги ажурирам телефонот, компјутерот и апликациите.
□ Правам резервни копии на важните податоци.
□ Не отворам сомнителни линкови и прилози.
□ Ја проверувам информацијата пред да ја споделам.
□ Го проверувам изворот, авторот и датумот на објавување.
□ Знам како да препознаам дезинформација и интернет измама.
□ Внимавам што споделувам на социјалните мрежи.
□ Не ја споделувам мојата лозинка со никого.
□ Знам што да направам ако некој ми го хакира профилот.
□ Размислувам критички пред да поверувам или да реагирам на содржина што ја гледам онлајн.
□ Одговорно користам алатки базирани на вештачка интелигенција и проверувам дали содржината е автентична.
□ Помагам и на другите да бидат побезбедни во дигиталниот свет.



Завршна порака

Интернетот е место на бескрајни можности за учење, комуникација, креативност и личен развој. Но, истовремено, тој бара од нас одговорност, критичко размислување и постојано учење.

Секој од нас има улога во создавањето побезбедна дигитална средина. Секој пат кога ќе провериш информација пред да ја споделиш, ќе препознаеш измама, ќе го заштитиш својот профил или ќе му помогнеш на некого да избегне дезинформација, придонесуваш интернетот да биде подобро место за сите.

Нека овој прирачник не биде последното нешто што ќе го прочиташ за дигиталната безбедност, туку почеток на навика секогаш да проверуваш, да размислуваш критички и да ги користиш дигиталните технологии одговорно.

Твојата најсилна „Сајбер Брана“ не е во уредот што го користиш, туку во знаењето што го носиш со себе.



Наслов:
Прирачник за дигитална писменост и безбедност

Проект:
„Сајбер Брана – креативна младинска иницијатива за дигитална писменост и безбедност“

Издавач:
Институт за добро управување и евроатлантски перспективи (ИДУЕП) во соработка со Студентарија.мк

Автори:
Гоше Николов
Билјана Кордалова
Бојан Кордалов

Година на издавање:
2026

Овој прирачник е изработен во рамки на проектот „Сајбер Брана – креативна младинска иницијатива за дигитална писменост и безбедност“ кој го спроведува Институтот за добро управување и евро-атлантски перспективи (ИДУЕП), во соработка со Студентарија, а е финансиски поддржан од Министерството за социјална политика, демографија и млади.