Шаблон за обука ИРЗ

|  |  |
| --- | --- |
| **Наслов** | Како да се идентификуваат информации што недостасуваат и лажни вести на интернет во културен контекст |
| **Област на обука** | *Ве молиме, одберете една или повеќе од следниве категории:*   |  |  | | --- | --- | | Online безбедност | X | | Културна и медиумска писменост |  | | Економски трансакции |  | | Заштита на лични податоци |  | | Дигитален идентитет и online репутација |  | |
| **Клучни зборови (мета-ознаки)** | безбедност на интернет, online сигурност, културен контекст, лажни вести, информации што недостасуваат. |
| **Овозможено од** | Институт за Развој на Заедницата - ИРЗ |
| **Јазик** | Англиски |
| **Резултати / цели / исходи од учењето** | |
| До крајот на овој модул ќе стекнете знаење за препознавање на лажни вести и информации што недостасуваат, како и безбедност на интернет во културен контекст.  Модулот се состои од четири единици кои обезбедуваат информации поврзани со темата во различни секции. Различни активности и знаења се поддржани со примери за подобро разбирање на материјалот, описни фотографии и корисни линкови за проширување на вашето знаење на темата.  Корисниците ќе имаат можност да се запознаат со безбедност на интернет во културен контекст како и со online сигурност. Можните online безбедносни закани ќе бидат претставени преку објаснувања за различните видови закани како што се: малициозен софтвер, фишинг, напади на лозинка итн.  Корисниците ќе можат да:  ● Да го разберат значењето на безбедноста и сигурноста на интернет;  ● Да направат разлика меѓу лажни вести, дезинформации и информации што недостасуваат;  ● Да користат различни совети во однос на онлајн безбедноста во културен контекст. | |
| **Опис** | |
| Дигиталните технологии го револуционизираа секој аспект од нашите животи. Тие имаат влијание врз вредностите на сите културни и креативни индустрии не само во однос на креативниот процес и неговото извршување, туку и во однос на работата на производи или уметнички производи и нивна промоција, дистрибуција, маркетинг и продажба.  Овој модул за обука ќе ги научи повозрасните дигитални корисници да откриваат потенцијални измами што би можеле да ги сретнат на интернет додека користат или бараат културни ресурси. Курсот ќе понуди конкретни примери на вообичаени измами поврзани со културни ресурси, како што се продажба на лажни билети, обиди за фишинг при нарачка преку Интернет итн.  Во денешната ера на технологија, лажните вести и информациите што недостасуваат се дел од секојдневната циркулација и информации на интернет. Корисниците ќе се запознаат со значењето на лажни вести и информации што недостасуваат, како да се препознаат лажните вести и важноста за правење разлика помеѓу лажни вести и информации што недостасуваат.  Зголемувањето на способноста за препознавање и заштита од информации што недостасуваат и лажни вести е единицата за учење која обезбедува информации и содржини во однос на способноста на корисниците да се заштитат на интернет. Понудени се совети и трикови, заедно со корисни примери и фотографии. | |

|  |  |
| --- | --- |
| **Содржина поделена во 3 модули** | |
| **1. ВОВЕД**  **2. СОДРЖИНА**  **Единица 1: Што е интернет безбедност?**  1.1 Што значи интернет безбедност и интернет сигурност?  1.2 Безбедност на интернет во културните содржини  **Единица 2: Најголеми закани за вашата безбедност на интернет**  2.1 Видови закани за безбедност на интернет  ● Малициозен софтвер  ● Човек во средината  ● Фишинг  ● Напади со лозинка  **Единица 3: Идентификување информации што недостасуваат, дезинформации, лажни информации и лажни вести во културен контекст**  3.1 Од каде доаѓаат лажните вести?  3.2 Како да препознаете лажни вести, дезинформации, лажни информации и информации што недостасуваат во културен контекст?  **Единица 4: Заштитете се од online безбедносни закани**  4.1 Заштитете се додека сте на интернет  4.2 Совети за online безбедност во културен контекст  **3. ЗАКЛУЧОК**  **Модул: Како да се идентификуваат информации што недостасуваат и лажни вести на интернет во културен контекст?**  **1. ВОВЕД**  Дигиталните технологии го револуционизираа секој аспект од нашите животи. Тие имаат влијание врз вредностите на сите културни и креативни индустрии не само во однос на креативниот процес и неговото извршување, туку и во однос на работата на производи или уметнички производи и нивна промоција, дистрибуција, маркетинг и продажба. Како што продолжува дигиталната промена, се повеќе уметници, филмски работници , продуценти, музичари и така натаму дигитално ги дистрибуираат своите производи. До крајот на овој модул ќе стекнете знаење и препознавање на лажни вести и информации што недостасуваат, како и online безбедност во културен контекст.  Во свет каде што хакерски напад се случува приближно на секои 39 секунди, безбедноста на интернет повеќе не може да се сфаќа несериозно. Во спротивно, сите ваши лични податоци може да бидат во опасност.  Но, што е тоа online безбедност, поточно? Какви закани има на интернет и што можете да направите за да се заштитите од нив? Заканата за безбедноста на интернет се однесува на секој можен малициозен напад кој има за цел незаконски пристап до податоци, нарушување на дигиталните операции или оштетување на информациите. Сега, повеќе од кога било културната содржина е широко достапна, таа е отворена и за online закани, ширење информации што недостасуваат, лажни информации, дезинформации и лажни вести и може да го оштетат искуството на една личност додека ужива и се информира за културни активнисти или настани.  **Единица 1: Што е интернет безбедност?**  **Секција 1.1 Објаснување на интернет безбедност и интернет сигурност**  Безбедноста на Интернет се состои од низа безбедносни тактики за заштита на активностите и трансакциите што се вршат online преку Интернет. Овие тактики се наменети да ги заштитат корисниците од закани како што се хакирање на компјутерски системи, е-пошта или веб-локации. Интернет-безбедноста е специфичен аспект на пошироките концепти како што се сајбер-безбеднос и компјутерска безбедност, фокусирајќи се на специфичните закани и ранливости на online пристапот и користењето на интернет.  Безбедноста на интернет ги штити луѓето кои користат интернет од штета преку свесност, едукација, информации и технологија. Безбедноста на интернет е да се биде свесен за природата на можните закани со кои би можеле да се соочите додека се занимавате со активност преку Интернет, тоа би можеле да бидат безбедносни закани, заштита и управување со вашите лични податоци online и избегнување штетна или нелегална содржина.  **Секција 1.2 Online безбедност во културните содржини**  Дигиталните технологии го револуционизираа секој аспект од нашите животи. Тие имаат влијание врз вредностите на сите културни и креативни индустрии не само во однос на креативниот процес и неговото извршување, туку и во однос на работата на производи или уметнички производи и нивна промоција, дистрибуција, маркетинг и продажба. Некои производствени процеси се исклучиво дигитални и технологијата има огромен потенцијал да ја направи културата достапна за сите, преку демократизација на потрошувачката и вклученоста во културното создавање.  Во исто време, културните институции, како што се музеите, архивите, библиотеките и филмските, телевизиските и музичките радиодифузери ги дигитализираат своите збирки во обид да ги зачуваат и да ги направат пошироко достапни. Понекогаш, дигитализацијата е неопходен чекор, како во случајот со аналогните филмови, кои повеќе не можат да се прикажуваат во нивната оригинална форма, бидејќи кината се опремени исклучиво со дигитална технологија.  Богатство од дигитални културни содржини се достапни на интернет бесплатно, со плаќање или нелегално. Таквата достапност и изобилство на културни содржини и различните начини за нивно користење на интернет носат нови предизвици и можности да се наруши безбедноста и сигурноста на интернет на една личност со различни средства. Затоа, важно е во оваа дигитална ера да бидете информирани и да ги знаете заканите за вашата online безбедност и како да се заштитите додека пристапувате до културни содржини на интернет.    **Единица 2: Најголеми закани за вашата интернет безбедност**  **Секција 2.1 Видови закани за безбедност на интернет**  Заканата за безбедноста на интернет се однесува на секој можен малициозен напад кој има за цел незаконски пристап до податоци, нарушување на дигиталните операции или оштетување на информациите.  Постојат многу online безбедносни закани на Интернет, па затоа решивме да се фокусираме на најопасните и најчестите.  **Малициозен софтвер:**  Малициозен софтвер е злонамерен софтвер како што се шпионски софтвер, откуп, вируси и црви. Малициозниот софтвер се активира кога корисникот ќе кликне на малициозен линк или прилог, што доведува до инсталирање на опасен малициозен софтвер кој штом ќе се активира може:  ● Да го блокира пристапот до клучните мрежни компоненти (откуп);  ● Да инсталира дополнителен штетен софтвер;  ● Тајно да добива информации со пренос на податоци од хард дискот (шпионски софтвер);  ● Ги нарушува поединечните делови, правејќи го системот нефункционален.    **Човек во средината:**  Закана од човек во средината се јавува кога злонамерните поединци се вметнуваат во трансакција меѓу две страни. Откако ќе се најдат во трансакцијата, тие можат да филтрираат и да крадат податоци. Заканата Човек во средина често се реализира кога посетителот користи необезбедена јавна Wi-Fi мрежа. Малициозните поединци се вметнуваат меѓу посетителот и мрежата, а потоа користат малициозен софтвер споменат претходно за да инсталираат софтвер и малициозно да ги користат податоците.  **Фишинг:**  Фишинг нападите користат лажна комуникација, како што е е-пошта, за да го измамат примателот да ја отвори и да ги спроведе инструкциите внатре, како што е давање број на кредитна картичка. Целта е да се украдат чувствителни податоци како кредитна картичка и информации за најавување или да се инсталира малициозен софтвер на уредот на поединец.  **Напади на лозинка:**  Со вистинска лозинка, малициозен поединец има пристап до мноштво информации. Социјалното инженерство е тип на напад со лозинка што се дефинира како „стратегија која во голема мера се потпира на човечката интеракција и честопати вклучува измама на луѓето да ги прекршат стандардните безбедносни практики“.  Други видови на напади со лозинка вклучуваат пристап до базата на податоци за лозинки или целосен пристап.    **Единица 3: Идентификување информации што недостасуваат, дезинформации, лажни информации и лажни вести во културен контекст**  Сега, повеќе од кога било културната содржина е широко достапна, таа е отворена и за online закани, ширење информации што недостасуваат, лажни информации, дезинформации и лажни вести и може да го оштетат искуството на една личност додека ужива и се информира за културни активнисти или настани.  **Секција 3.1 Што значат лажни вести, лажни информации и дезинформации?**  **Лажни вести** се намерно креирани, сензационални, емотивни, погрешни или целосно измислени информации.  Постојат два вида лажни вести:  1. Приказни кои не се вистинити. Ова се целосно измислени приказни креирани да ги натераат луѓето да веруваат во нешто лажно, да купат одреден производ или да посетат одредена веб-страница.  2. Приказни кои имаат одредена вистина, но не се 100 проценти точни. Повторно, ова може да биде намерно, да ги убеди читателите во одредено гледиште или може да биде резултат на ненамерна грешка.    Терминот **дезинформација** се однесува на информации кои се лажни или неточни и често се широко распространети со други, без оглед на намерата да се измами.  Додека дезинформациите се лажни информации што се создаваат и се шират без оглед на намерата да се наштети или измами, **лажните информации** се вид на дезинформации што се создаваат за намерна измама. И двете форми може да се распространуваат насекаде, без разлика дали споделувачот знае дека информацијата е погрешна.  Платформите за социјални медиуми овозможуваат речиси секој да ги објави своите мисли или да споделува приказни со светот. Проблемот е што повеќето луѓе не го проверуваат изворот на материјалот што го гледаат на интернет пред да го споделат, што може да доведе до брзо ширење на лажни вести. Во исто време, станува потешко да се идентификува оригиналниот извор на вестите, што може да го отежни проценувањето на нивната точност.  **Секција 3.2 Како да препознаете лажни вести, дезинформации, лажни информации и информации што недостасуваат во културен контекст?**  За да можете да забележите лажни вести, дезинформации, лажни информации и информации што недостасуваат, поставете си ги следните прашања и направете го следново:  **● Кој го напишал тоа?** Проверете го името на авторот. Дали името е достапно или недостасува? Повеќето автори кои вложуваат време во добро истражeна статија, најверојатно ќе го имаат нивното име прикачено на неа.  **● Кои се нивните квалификации?** Ако името на авторот е наведено, дознајте која е личноста и кои се нејзините компетенции.  ● **Проверете го делот „За нас“.** На врвот или на дното на веб-локацијата, треба да има дел наречен „За нас“. Овој дел ја прикажува целта на веб-страницата.  ● **Дали статијата ве информира за сите страни во однос на темата?** Новинските написи треба да ви даваат факти од различни гледишта.  ● **Дали содржината се совпаѓа со насловот на статијата?** Насловот треба да ви даде идеја за што е целата статија, но може да се користи и за да ве убеди да верувате во нешто пред да ја прочитате статијата.  ● **Кога е објавена оваа статија?** Постарите написи може да не содржат ажурирани факти и може да имаат прекинати линкови.  ● **Дали написот бил пренаменет или ажуриран?** Пренамената или ажурираната содржина има тенденција да има одрекување од одговорност на почетокот или крајот на статијата.  ● **Колку е важен датумот?** Датумот ви дава индикација за тоа кога е објавенa статијата.  ● **Дали оваа веб-адреса (URL) изгледа точно?** Внесувањето на погрешна веб-адреса ќе ве упати на веб-страница што не сте имале намера да ја посетите. Тоа може да ве доведе до страница со претходно споменатите закани за безбедност на интернет.  ● **Дали ова го најдов на социјалните мрежи? Платформите за социјални медиуми не се организации за вести. Ова се платформи за луѓето да креираат и/или споделуваат содржина.**  ● **Дали го најдов ова на блог/веб-страница? Блоговите** содржат содржина напишана неформално и управувана од поединец или мала група.    **Единица 4: Заштитете се од online безбедносни закани**  **Секција 4.1 Заштитете се додека сте на интернет**  Еве неколку работи што може да ги направите за да се заштитите додека сте на интернет:  **1. Не користете необезбедени WiFi мрежи**  Најдобро е да избегнувате било која WiFi мрежа што не бара лозинка и наместо тоа, само користете го вашиот сопствен интернет.  **2. Користете моќен антивирус**  Антивирус е вашата најдобра опција да го заштитите вашиот уред од вируси со малициозен софтвер кои претходно ги презентиравме. Не дозволувајте името да ве збуни - Антивирусот се бори против вирусите, но најмногу цели на малициозен софтвер (вирусот е вид на малициозен софтвер). Погрижете се да го ажурирате и често да скенирате - особено откако ќе преземете нови датотеки. Всушност, најдобро е да не ги отворите без претходно да ги скенирате.  **3. Секогаш користете VPN онлајн**  VPN (Виртуелна приватна мрежа) е онлајн услуга што можете да ја користите за да ја скриете вашата вистинска IP адреса и да ја шифрирате вашата online комуникација. Тоа е еден од најдобрите начини да ја подобрите вашата online безбедност и да ги скриете вашите дигитални траги. Сè додека се користат соодветните методи за шифрирање, никој нема да може да го следи вашиот online сообраќај за да види што правите на Интернет.  **4. Избегнувајте обиди за фишинг**  Ако примите е-пошта или пораки за кои се тврди дека се од некој ваш близок, од вашата банка или од полицијата кои бараат од вас да преземете прикачени прилози, да пристапите до кратки линкови или да споделите чувствителни информации, игнорирајте ги. Наместо тоа, стапете во контакт со наводниот испраќач за да ја дознаете вистината. Обидете се да пребарувате делови од пораката што сте ја примиле. Ако се работи за фишинг измама, најверојатно ќе добиете резултати од други луѓе кои зборуваат за примање на истата порака.  **5. Не го оставајте вклучен Bluetooth-от**  Иако Bluetooth има свои намени, да се држи вклучен во секое време е прилично небезбедно. Во 2017 година беше откриен нов метод за хакирање со Bluetooth кој влијаеше на милиони уреди дозволувајќи им на хакерите да користат Човек во Средина, закана за да ги добијат информациите за вашиот уред. Сè на сè, подобро е да бидете на безбедна страна и да го исклучите Bluetooth кога не го користите за да ја зачувате вашата online безбедност.  **6. Исклучете ги услугите за локација на вашите мобилни уреди**  Услугите за локација можат да бидат навистина корисни, но можат да бидат и многу ризични, поради фактот дека некои апликации може да ја шират вашата локација. Ако тоа се случи, тоа не значи дека ќе бидете во непосредна опасност. Сепак, вашата online безбедност ќе биде загрозена.  **7. Користете блокатори на скрипти на вашите пребарувачи**  Блокаторите на скрипти се екстензии на пребарувачот што можете да ги користите за да се осигурате дека веб-локациите до кои пристапувате нема да извршуваат неовластени скрипти и приклучоци во заднина што може да ја загрозат вашата безбедност на Интернет. Не заборавајте - некои скрипти може да бидат толку опасни што можат да го заземат вашиот пребарувач, додека други можат да прикажуваат пренасочувања или реклами за фишинг, па дури и копање за криптовалути со користење на вашиот процесор.  **8. Одржувајте го вашиот оперативен систем ажуриран**  Неинсталирањето на најновите ажурирања на вашиот оперативен систем може сериозно да и наштети на вашата online безбедност. Бидејќи малициозните посредници можат да ги користат потенцијалните пропусти во своја полза – пропусти што можеби би биле поправени со најновото ажурирање.  **9. Размислете за користење на шифрирани апликации и е-пошта**  Ако сакате навистина да бидете сигурни дека вашата online комуникација е безбедна, можете да се обидете да користите различните апликации за пораки. Таа карактеристика навистина e моќна за шифрирање.  Што се однесува до е-пошта, тоа е исто, пребарувајте на интернет за различни апликации и каква безбедност тие нудат.  **10. Користете силни лозинки**  Да имате моќни лозинки за вашите профили е исклучително важно, но да се дојде до навистина добра е полесно да се каже отколку да се направи.  Ако ви треба помош, еве неколку добри идеи што можат да ви помогнат:  1. Користете празни места доколку е дозволено.  2. Користете само долги лозинки. Идеално, не се задржувајте само на еден збор.  3. Не користете зборови од речник како лозинка.  4. Користете големи и мали букви и по случаен избор измешајте ги.  5. Користете симболи (како $, %, или \*) во вашата лозинка.  6. Вклучете броеви во вашата лозинка.  7. Обидете се да ја направите вашата лозинка целосна реченица.  8. Превртете некои зборови што ги користите во лозинката (наместо „стол“ користете „лотс“).  9. Исто така, обидете се да не ја користите истата лозинка за сите ваши профили. Подобро е да користите различни лозинки, или барем варијации на вашата лозинка.    **4.2 Совети за online безбедност во културен контекст**  Благодарение на интернетот, постојат неколку начини за потрошувачите да добијат билети за културни настани. Негативната страна е што има и многу замки што потрошувачите треба да ги избегнат. Со кликнување на погрешен линк или доверување на погрешна веб-локација може да дојде до лажен билет и изгубени средства.  Еве неколку совети за тоа како да бидете безбедни онлајн, со конкретен пример за купување билети преку Интернет за културен настан:  • **Купувајте директно од местото секогаш кога е можно.** Многу официјални агенти за продажба на билети сега нудат и секундарни продажни опции. Не кликајте од е-пошта или online реклами; вообичаен трик за измама со билети е креирање веб-адреса што е слична на добро позната компанија.  **• Размислете за вашиот извор.** Знајте ја разликата помеѓу професионален продавач на билети (легитимен и акредитиран препродавач), скалпер на билети (нерегулиран и нелиценциран продавач на билети) и измамник кој продава билети за измама.  **• Дознајте ја политиката за рефундирање.** Треба да купувате билети само од препродавач на билети кој дава јасни детали за условите на трансакцијата. Продавачите треба да му ја откријат на купувачот, пред купувањето, локацијата на седиштата претставени со билетите, усно или со покажување на табелата за седење; и, ако билетите не се достапни за непосредено подигањеод купувачот, да информираат кога билетите ќе се испорачаат или ќе бидат достапни за подигање.  **• Користете начини на плаќање што доаѓаат со заштита**. Секогаш користете кредитна картичка, за да имате повраток на средства доколку билетите не се како што било ветено. Дебитни картички, плаќање преку банки или готовински трансакции се ризични; ако билетите се лажни, најверојатно нема да можете да ги вратите парите.    **• Внимавајте на рекламите.** Кога пребарувате на интернет за online билети, често ќе се појавуваат реклами за евтини билети. Користете добро расудување; некои од овие реклами ќе бидат измами со билети, особено ако цените се ниски.  **• Ако не сте сигурни, проверете ги вашите билети.** Посетете ја арената каде што ќе се одржи настанот. Презентирајте го вашиот билет до службата за корисници и тие можат да потврдат дали вашиот билет е легитимен и да ви покажат како да препознаете дали билетот е лажен.  **3. ЗАКЛУЧОК**  Безбедноста на интернет во поширок културен контекст е многу интересна тема бидејќи културните содржини се широко достапни и се предмет на online закани.  Дигиталните технологии го револуционизираа секој аспект од нашите животи. Тие имаат влијание врз вредностите на сите културни и креативни индустрии не само во однос на креативниот процес и неговото извршување, туку и во однос на работата на производи или уметнички производи и нивна промоција, дистрибуција, маркетинг и продажба. Како што продолжува дигиталната промена, се повеќе уметници, филмски работници , продуценти, музичари и така натаму дигитално ги дистрибуираат своите производи.  До крајот на овој модул ќе стекнете знаење во однос на препознавање на лажни вести и информации што недостасуваат, како и online безбедност во културен контекст. Со користење на советите и понудените примери како упатство додека сте online, можете да ја зајакнете вашата безбедност на интернет. Со безбедносните закани како малициозен софтвер, измами, фишинг, хакирање и ширење на дезинформации и лажни вести кои стануваат сè почести во денешно време, безбедноста на интернет стана поважна од кога било.  Безбедност на интернет? Заклучок / Клучни точки  Безбедноста на интернет ги претставува правилата што ги следите, активностите што ги преземате и процесите што се случуваат за да се осигурате дека сте безбедни на интернет. Бидејќи безбедносните закани (малициозен софтвер, измами, фишинг, хакирање итн.) стануваат сè почести во денешно време, безбедноста на интернет стана поважна од кога било.  Вообичаено, најдобриот начин да се уверите дека сте безбедни на интернет е да користите силна антивирусна програма, сигурен VPN, моќни лозинки и блокирачи на скрипти (меѓу другото).  Лажните вести се однесуваат на намерни невистини или приказни кои содржат одредена вистина, но кои не се целосно точни, случајно или креирани.  Некои луѓе исто така тврдат дека вистинити приказни се „лажни вести“, само затоа што не се согласуваат со нив. Ова може да доведе до опасно игнорирање на важни совети.  Лажните вести можат да имаат негативно влијание врз социјалните и културните аспекти на општеството, па затоа е клучно да знаете како да ги одделите вистинските од лажните вести, како и да препознаете лажни информации или дезинформации, како и да препознаете кога недостасуваат информации. Можете да го направите ова следејќи ги овие шест чекори:  1. Развијте критички начин на размислување.  2. Проверете го изворот.  3. Погледнете кој друг ја презентира приказната.  4. Испитајте ги доказите.  5. Не земајте во предвид слики според изгледот.  6. Проверете дали „звучи правилно“. | |
| **Содржина** | |
| ● Културните содржини се широко достапни на интернет и отворени за online закани, ширење на лажни информации, дезинформации, информации што недостасуваат и лажни вести кои можат да го нарушат искуството на една личност додека ужива и се информира за културни активности или настани.  ● Безбедноста на Интернет се состои од низа безбедносни тактики за заштита на активностите и трансакциите што се вршат преку интернет.  ● Заканата за безбедноста на интернет се однесува на секој можен малициозен напад кој има за цел незаконски пристап до податоци, нарушување на дигиталните операции или оштетување на информациите.  ● Сигурност на интернет значи да се биде свесен за природата на можните закани со кои може да се соочите додека се занимавате со активност на интернет, тоа би можеле да бидат безбедносни активности, заштита и управување со вашите лични податоци на интернет и избегнување штетна или нелегална содржина. Безбедноста на интернет ги заштитува луѓето кои вршат активности online преку свесност, едукација, информации и технологија.  ● Постојат многу безбедносни закани на интернет, овој модул е ​​фокусиран на најопасните и најчестите, како што се: Малициозен софтвер; Човек во средина; Фишинг; Напади на лозинка, итн.  ● Корисниците на Интернет треба да знаат како да препознаат лажни вести, лажните информации, дезинформациите и соодветно да се заштитат себеси, како и да препознаат кога недостасуваат информации. | |
| **5 поими од речник** | |
| **1) Безбедност на интернет**  Безбедноста на Интернет се состои од низа безбедносни тактики за заштита на активностите и трансакциите што се вршат преку Интернет.  **2) Сигурност на интернет**  Сигурност на интернет значи да се биде свесен за природата на можните закани со кои може да се соочите додека се занимавате со активност на интернет, тоа би можеле да бидат безбедносни активности, заштита и управување со вашите лични податоци на интернет и избегнување штетна или нелегална содржина. Безбедноста на интернет ги заштитува луѓето кои вршат активности online преку свесност, едукација, информации и технологија.  **3) Културен контекст**  Културниот контекст е поврзан со општеството во кое поединците се израснати и со тоа како културата влијае на однесувањето. Вклучува вредности кои се учат и ставови кои се споделуваат меѓу групи луѓе. Вклучува верувања, значења, обичаи, идеи, јазик, норми.  Се однесува на симболичното значење, уметничката димензија и културните вредности од кои потекнуваат или изразуваат културни идентитети.  **4) Лажни вести**  Лажни вести, честопати од сензационална природа, создадени за да бидат широко споделени или дистрибуирани со цел да се генерираат приходи, или да се промовира или дискредитира јавна личност, политичко движење, компанија итн.  **5) Недостaток на информација**  Претставува нецелосна или неточна информација која има за цел да го одвлече вниманието од точни информации, да предизвика конфузија или да го промени контекстот на реченицата, дејството, активноста итн. | |
| **Библиографија и дополнителни референци** | |
| * <https://www.mindtools.com/pages/article/fake-news.htm> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media> * <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf> * <https://www.nature.com/articles/s41586-021-03344-2> * <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf> * <https://academicguides.waldenu.edu/library/fakenews/examples> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690570> * <https://en.wikipedia.org/wiki/Fake_news> * <https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news> * <https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users> * <https://researchguides.austincc.edu/c.php?g=612891&p=4258046> | |
| **Пет прашања со повеќе избори за самопроценка** | 1) Е-пошта во вашето сандаче бара да се најавите со лозинка поради некои безбедносни причини. Што би направиле?  А. Ништо, ќе ја игнорирам пораката.  Б. Ќе направам како што се бара, тоа е безбедносна причина.  В. Ќе контактирам со ИТ експерт за да добијам повеќе информации.  **Точен одговор: А**  2) Вие сте на веб-страна која продава бесплатни билети за културен настан во ваша близина. Тие се бесплатни и бараат само некои од вашите лични податоци. Што би направиле?  А. Ќе ги купам билетите и ќе ги внесам моите лични податоци.  Б. Ќе ја проверам веб-страната за да видам дали е вистинска или не, потоа ќе ја пријавам страницата.  В. Ќе ја споделам страницата за да можат и другите да ги добијат билетите.  **Точен одговор: Б**  3) Посетивте виртуелна турнеја на добро позната културна локација. Забележавте дека недостасуваат информации на една од страниците. Што би направиле?  А. Сам ќе го пополнам празното место.  B. Ќе го известам виртуелниот туристички водич за оваа можна грешка.  В. Нема да направам ништо.  **Точен одговор: Б**  4) Креирате профил на веб-страна и треба да креирате лозинка. Која лозинка е најбезбедна?  А. Вашето име.  Б. Случајна линија од броеви и букви што можете да ги напишете на парче хартија за да ги запомните.  В. Вашиот број за социјално осигурување.  **Точен одговор: Б**  5) Дали ги чувате вашите лични податоци безбедни кога користите социјални мрежи?  А. Да.  Б. Не.  В. Не сум сигурен.  **Точен одговор: Изборен, сите одговори се точни.** |
| **Поврзан материјал** | How to identify missing information and fake news online in a culture relevant context\_PPT\_CDI  Како да се идентификуваат информациите што недостасуваат и лажните вести на интернет во културен контекст\_PPT\_ИРЗ |
| **Поврзана PPT** |  |
| **Референтни линкови** |  |
| **YouTube видеа (ако има)** | <https://youtu.be/vPAW5j_L4-c>  <https://www.youtube.com/watch?v=0yL-k5nB65o> |