Шаблон за обука E-Seniors

|  |  |
| --- | --- |
| **Наслов** | **Тема: Информирање и комуникација преку социјалните медиуми**  **Лекција 3. Закани и предизвици на социјалните медиуми: што треба да правите, а што не?** |
| **Област на обука** | *Ве молиме, одберете една или повеќе од следниве категории:*   |  |  | | --- | --- | | Online безбедност |  | | Културна и медиумска писменост | *X* | | Економски трансакции |  | | Заштита на лични податоци |  | | Дигитален идентитет и online репутација |  | |
| **Клучни зборови (мета-ознаки)** | **Социјални медиуми, комуникација, безбедност** |
| **Овозможено од** | **E-Seniors** |
| **Јазик** | **Англиски** |
| **Резултати / цели / исходи од учењето** | |
| Овој модул има за цел да ги развие знаењата и вештините на корисниците за тоа како да ги користат социјалните медиуми за комуникација и промоција на културата и креативноста. Повозрасните корисници ќе се запознаат со алатките за социјални медиуми, културните ресурси на социјалните медиуми кои ќе им овозможат лесна навигација и откривање културни и комуникациски можности. | |
| **Опис** | |
| Курсот е поделен на 3 нивоа: секој модул е поделен на секции. Насловите на секциите даваат подетална претстава за содржината на модулот.  Структура на модулот:  **Тема: Информирање и комуникација преку социјалните медиуми**  **Модул 3. Закани и предизвици на социјалните медиуми: Што треба да правите, а што не?**  **Секција 3.1:** Закани и предизвици  **Секција 3.2:** 10 добри практики за усвојување за безбедност на социјалните мрежи. | |
| **Содржината поделена во 3 модули** | |
| **Модул 3: Закани и предизвици на социјалните медиуми: Што треба да правите, а што не?**  Има многу закани и предизвици кои се вклучени во пребарувањето на интернет, и на компјутерот и на паметниот телефон. Социјалните мрежи не се исклучок. Постојат неколку ризици поврзани со користењето на социјалните мрежи. Меѓутоа, ако се преземат мерки на претпазливост, не е тешко да се сурфа со минимален ризик.  **Секција 3.1:** Закани и предизвици   * **Фишинг:** фишинг е вид на социјален инженеринг каде напаѓачот испраќа лажна порака дизајнирана да измами човечка жртва. Овие пораки се дизајнирани да ве измамат за да откриете лични информации преправајќи се дека сте од доверлив извор. Пораките може да доаѓаат од луѓе кои тврдат дека се ваши пријатели или позната компанија. Никогаш не споделувајте доверливи информации и никогаш не кликнувајте на веб-страна со сомнителна структура. * **Психолошко хакирање**: психолошко хакирање е процес на добивање доверливи информации од личност преку измама. Измамникот може да започне разговор за работи што ги чита на вашиот профил, како на пр. каде работите итн. Потоа се обидуваат да ве натераат да откриете лични информации, слично на фишинг. * **Малвер:** малициозен софтвер е злонамерен софтвер дизајниран да инфилтрира уреди. Циркулира на социјалните мрежи како линкови со привлечни наслови. Откако ќе се инфилтрира ваквиот софтвер, може да испраќа пораки до контактите, да пристапува до личните информации или да го оштети уредот. Треба да се внимава кога сте во искушение да кликнете на линк од непознат извор. * **Говор на омраза**: говорот на омраза е вообичаен на социјалните мрежи бидејќи неговите автори можат да останат анонимни. Може да се случи да добиете говор на омраза, понекогаш без никаква мрежа, па затоа е важно да се оттргнете од него и да не се двоумите да го пријавите како несакана и злонамерна содржина. * **Сајбер-малтретирање**: е малтретирање што се случува преку дигитални уреди како што се мобилни телефони, компјутери и таблети. Сајбер-малтретирањето може да се случи преку СМС, текстуални пораки и апликации или преку Интернет на социјалните медиуми, форуми или игри каде што луѓето можат да гледаат, учествуваат или споделуваат содржина. Сајбер-малтретирањето вклучува испраќање, објавување или споделување негативна, штетна, лажна или злобна содржина за некој друг. Може да вклучи споделување лични или приватни информации за некој друг што предизвикува срам или понижување. Некој со сајбер-малтретирање ја преминуваат границата на незаконско или криминално однесување. * **Online ageism (дискриминација врз основа на возраст) :** online ageism се однесува на стереотипите (како размислуваме), предрасудите (како се чувствуваме) и дискриминацијата (како постапуваме) кон другите или кон себе врз основа на возраста. Online ageism дискриминацијата влијае на сите. Децата на возраст од 4 години стануваат свесни за старосните стереотипи на нивната култура. Од таа возраст па наваму тие ги интернализираат и ги користат овие стереотипи за да ги водат своите чувства и однесување кон луѓето од различни возрасти. Тие, исто така, се потпираат на старосните стереотипи на културата за да се согледаат и разберат себеси, што може да резултира со самонасочен стажизам на која било возраст. Агеизмот се вкрстува и ги влошува другите форми на неповолност, вклучително и оние поврзани со полот, расата и попреченоста.   **- На што да внимавате за да избегнете измами на Фејсбук:**  o Луѓе кои не ги познавате лично од вас бараат пари или ваши банкарски податоци.  o Непроверени страници кои тврдат дека претставуваат голема организација или јавна личност.  o Луѓе кои бараат од вас да го продолжите разговорот надвор од Facebook, во помалку јавна или помалку безбедна поставка, како што е посебна адреса за е-пошта.  o Луѓе кои бараат од вас да им ги испратите вашите банкарски податоци за да добијат награда.  o Секој што тврди дека е ваш пријател или роднина во неволја.  o Луѓе кои лажат за тоа каде живеат.  o Објави или публикации кои содржат правописни и граматички грешки.  o Луѓе или сметки кои ве пренасочуваат на страница за да добиете награда.  **Секција 3.2: 10 добри практики што треба да се усвојат за безбедност на социјалните мрежи:**  1- **Заштитете го пристапот до вашите сметки:** користете силни лозинки кои се различни од еден до друг профил. Апликациите за управување со лозинки може да ви помогнат лесно да ги зачувате вашите лозинки. На пример https://keepassxc.org/  2- **Проверете ги вашите поставки за приватност**: Стандардно, поставките за приватност често се отворени (на лични информации како што се име, телефонски број, е-пошта). Овие податоци можат да бидат достапни за сите претплатници на социјалната мрежа. Можно е да се ограничи оваа видливост со прилагодување на конфигурацијата на профилот за да се задржи контролата врз она што го гледаат другите корисници.  3- **Контролирајте ги вашите објави:** вашите објави може да излезат од контрола и да бидат повторно објавени или толкувани повеќе отколку што сте замислиле. Не објавувајте лични или чувствителни информации.  4- **Внимавајте со кого разговарате**, вашите пријатели можеби споделуваат злонамерна содржина без да го знаат тоа или можеби самите биле хакирани. Никогаш не испраќајте пари без да го потврдите идентитетот на лицето, не испраќајте приватни видеа, не се сомневајте во натпревари, неочекувани добивки или „големи зделки“ што може да сокријат измами.  5- **Контролирајте апликации од трети страни:** некои апликации нудат интеракција со една од вашите сметки на социјалната мрежа. Тие бараат дозволи кои треба внимателно да се испитаат, бидејќи некои од нив може потоа да имаат пристап до вашите податоци. Внимавајте да не инсталирате апликации за кои се сомневате дека се злонамерни.  6- **Избегнувајте јавни компјутери и мрежи:** Користењето компјутер со отворен пристап или јавен Wi-Fi е ризично бидејќи тие можат да бидат компромитирани или под контрола на сајбер-криминалци. Избегнувајте да внесувате чувствителни информации или да ги користите доколку е можно.  7- **Редовно проверувајте ги најавувањата на вашиот профил:** повеќето социјални мрежи ви дозволуваат да гледате активни конекции или сесии на сметката. Редовно проверувајте ги овие информации за да бидете сигурни дека друг уред не е поврзан со еден од вашите профили. Ако е, исклучете го и сменете ја лозинката.  8- **Внимавајте на лажни вести**: некои објавени информации може да бидат лажни, намерно или не. Пред да разгледате или пренесете каква било информација, проверете ја нејзината автентичност.  9- **Проверете ги вашите идентификации со вашите сметки:** некои веб-локации нудат да ве регистрираат со вашата сметка на социјалната мрежа. Ова ја избегнува потребата од креирање лозинка, на пример, но може да обезбеди лични податоци на страницата или да дозволи сајбер криминалец кој ја хакирал вашата социјална мрежа да пристапи до вашата сметка и на таа страница.  10- **Избришете ја вашата сметка ако повеќе не ја користите:** за да ги избегнете сите ризици опишани погоре, за да се осигурате дека вашата сметка не се користи без ваше знаење, избришете ја вашата сметка кога повеќе нема да ви треба. | |
| **Содржина во точки** | |
| ● Најчестите закани и предизвици за користење на социјалните медиуми е да се одбраните од фишинг, малициозен софтвер, говор на омраза итн.  ● Можете да ги избегнете заканите и ризиците од социјалните мрежи следејќи ги препораките и советите наведени во овој модул за обука. | |
| **5 поими од речник** | |
| **Безбедност на социјалните медиуми:** безбедноста на социјалните медиуми се однесува на сите мерки што корисникот треба да ги преземе за да избегне ризици, измами и напади на неговата лична сметка.  **Говор на омраза:** говорот на омраза се изговорени зборови кои се навредливи, навредливи и/или заканувачки за поединец или група врз основа на одреден атрибут на тоа лице или лица кои се цел.  **Психолошко хакирање**: психолошко хакирање е процес на добивање доверливи информации од личност преку измама.  **Сајбер-малтретирање:** е малтретирање што се случува преку дигитални уреди како што се мобилни телефони, компјутери и таблети  **Online ageism:** се однесува на стереотипите (како размислуваме), предрасудите (како се чувствуваме) и дискриминацијата (како постапуваме) кон другите или кон себе врз основа на возраста. Online ageism дискриминацијата влијае на сите. | |
| **Библиографија и дополнителни референци** | |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)  [**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) | |
| **Пет прашања со повеќе избори за самопроценка** | 1) Безбедно е да се користат јавни компјутери  а. Вистина  б. Неточно  **Точно: Б**  2) Што е злонамерен софтвер?  а. Злонамерен софтвер е софтвер дизајниран да инфилтрира уреди.  б. Измама со идентитет.  в. Говор на омраза.  **Точно: А**  3) Што е говор на омраза?  A. Говорот на омраза се изговорени зборови кои се навредливи, навредливи и/или заканувачки за поединец или група врз основа на одреден атрибут на тоа лице или лица кои се цел.  Б. Говорот на омраза е процес на добивање доверливи информации од личност преку измама.  В. Говорот на омраза е злонамерна информација дизајнирана да навлезе во уреди и да нападне луѓе.  **Точно: А**  4) Безбедност на социјалните медиуми:  A. Се однесува на сите мерки што ги користат компаниите за да ја одбранат online измамата.  Б. Се однесува на сите мерки што корисникот треба да ги преземе за да избегне ризици, измами и напади на неговата лична сметка.  В. Упатете ги алатките на социјалните медиуми дизајнирани за корисниците.  **Точно: Б**  5) Што да направите ако наидете на online говор на омраза?  A. Обидете се да ги избегнете напаѓачите.  B. Обидете се да ги пријавите напаѓачите.  В. Сите горенаведени се точни.  **Точно: В** |
| **Поврзан материјал** | **Како да ги препознаете и ги избегнете најчестите измами на социјалните медиуми:** [**https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/**](https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/)  **Како да избегнете измами на социјалните медиуми:** [**https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html**](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)  **Сајбер-малтретирање и говор на омраза:**[**https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf**](https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf) |
| **Поврзана PPT** |  |
| **Референтни линкови** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **YouTube видеа (ако има)** | **Што претставуваат социјалните медиуми? На едноставен англиски:**  [**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)  **Неверојатен читател на мисли го открива својот “талент”:**  [**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |