

ПРИРАЧНИК ЗА ПРЕПОЗНАВАЊЕ И СПРЕЧУВАЊЕ НА САЈБЕР- НАСИЛСТВО И СТЕКНУВАЊЕ НА ВЕШТИНИ ЗА ПРИМЕНА НА МЕРКИ ЗА САЈБЕР БЕЗБЕДНОСТ



Прирачник за препознавање и спречување на сајбер-насилство и стекнување на вештини за примена на мерки за сајбер безбедност

Автор: Гиљман Османи Муслији

Аналитика тинк тенк

Декември 2023 година

СОДРЖИНА

ЦЕЛ НА ПРИРАЧНИКОТ	5
МЕТОДОЛОГИЈА ЗА ИЗРАБОТКА НА ПРИРАЧНИКОТ.....	7
ЗА ПРОЕКТОТ	9
ПРЕГЛЕД НА РЕЛЕВАТНА ЛИТЕРАТУРА	11
ВОВЕД	13
ПОИМ ЗА ВРСНИЧКО НАСИЛСТВО	15
САЈБЕР НАСИЛСТВО	17
ВИДОВИ НА САЈБЕР НАСИЛСТВО.....	18
• Сајбер демнење	18
• Cyberstalking.....	18
• Анонимно и лажно претставување.....	18
• Издавање, измама, имитирање и уценување	19
• Вознемирување	19
• Тролање	19
• Оцрнување	19
• Исклучување	20
• Можни причини за насилство	20
ШТО Е ИНТЕРНЕТ ПРИВАТНОСТ	21
КОМУНИКАЦИЈА НА ИНТЕРНЕТ И ПОСЛЕДИЦИ ОД САЈБЕР НАСИЛСТВО	24
ВЕБ-ПРЕЛИСТУВАЧИ И БЕЗБЕДНОСТ	25
ВИДОВИ НА САЈБЕР НАПАДИ	26
РЕЗУЛТАТИ ОД ИСТРАЖУВАЊЕТО	27
ПРЕПОРАКИ	40
ПРАКТИЧНИ СОВЕТИ ЗА БЕЗБЕДНОСТ	43
ПРАКТИЧНИ ПРЕПОРАКИ И СОВЕТИ ЗА РОДИТЕЛИТЕ.....	44
КОРИСТЕНА ЛИТЕРАТУРА:	46

ЦЕЛ НА ПРИРАЧНИКОТ

5

Во денешното дигитално доба, потребата за сеопфатно образование за сајбер безбедност и ефективни стратегии за спречување на сајбер насилиството никогаш не била поклучна. Целта на овој Прирачник е да ги поттикне младите луѓе и наставниците со знаења и вештини неопходни за безбедна навигација низ дигиталниот свет и светот на интернетот, да ги разберат мерките за сајбер безбедност и да развијат влијателни училишни програми за да се спречи сајбер-насилиството и да се обезбеди безбедна сајбер средина за учениците.

Специфични цели на прирачникот:

Зајакнување преку образование: Преку овој Прирачник ќе им се обезбеди на младите луѓе и наставниците солидна основа на знаење за мерките за сајбер безбедност, онлајн безбедноста и потенцијалните ризици поврзани со сајбер насилиството. Преку активна употреба на Прирачникот ќе се негува култура на дигитална писменост и одговорно онлајн однесување.

Развој на вештини: Преку овој Прирачник ќе се опремаат корисниците (наставниците, стручните служби во училиштата, учениците, родителите и други) со практични вештини за ефективно спроведување на мерките за сајбер безбедност, вклучително и управување со лозинка, навики за безбедно прелистување и разбирање на поставките за приватност на различни платформи. Прирачникот ќе им овозможи на наставниците да ги интегрираат концептите за сајбер безбедност во нивната наставна програма, осигурувајќи дека учениците стекнуваат основни вештини за безбедна навигација низ дигиталниот пејзаж.

Превенција на сајбер малтретирање: Овој Прирачник има за цел да ја подигне свеста за различните форми на сајбер насилиството, неговото влијание врз поединците и пошироката заедница. Преку употребата на Прирачникот ќе се обезбедат ресурси и стратегии за наставниците да креираат и имплементираат училишни програми кои се однесуваат на сајбер насилиство, поттикнувајќи безбедна и инклузивна онлајн средина.

Соработка и поддршка: Примената на Прирачникот ќе ја олеснисоработката помеѓу наставниците, родителите и учениците за да се создаде унифициран пристап кон сајбер безбедноста и превенцијата на сајбер насилиство.

Со постигнување на овие цели, нашиот Прирачник има за цел да придонесе за развој на дигитално еластична генерација која може да ги искористи придобивките од технологијата додека одговорно и етички се движи низ потенцијалните стапици.

Прирачникот е изработен како дел од проектот „Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyberbullying“, имплементиран од Аналитика тинк тенк Скопје, во периодот од септември 2023 година заклучно со февруари 2024 година.

МЕТОДОЛОГИЈА ЗА ИЗРАБОТКА НА ПРИРАЧНИКОТ

7

Овој Прирачник е изработен со користење на повеќе методи методологија насочена кон дијагностицирање на примарни податоци, искуства, перспективи и увиди поврзани со сајбер безбедноста и сајбер насилството. Процесот на изработка на Прирачникот вклучува комбинација од квантитативни и квалитативни методи на истражување за да се обезбеди цврста основа заснована на докази за содржината на прирачникот. Беа користени следните методологии:

1. Прелиминарно истражување: На почеток на изработката на Прирачникот се спроведе опширен преглед на постојните прирачници за сајбер безбедност и спречување на сајбер насилство, едукативни материјали и релевантна литература за да се идентификуваат празнините и областите за подобрување. Анализирани беа секундарни извори на податоци за да се добие увид во тековните трендови, предизвици и најдобри практики во образованието за сајбер безбедност и превенција од сајбер насилство.

2. Методологија на анкета (истражување): За да се соберат опширни сознанија од учениците, беше спроведено структурирано истражување на 507 ученици од пет (5) училишта од урбани и рурални средини. Овој квантитативен пристап овозможи систематско собирање податоци за дигиталните навики на учениците, нивото на свесност и искуствата со сајбер насилството. Резултатите од истражувањето обезбедија квантитативна основа за разбирање на преовладувачките трендови и информирање за содржината на Прирачникот.

3. Фокус групи: За да се навлезе подлабоко во проблематиката на сајбер насилството и сајбер безбедноста, фокус групите беа спроведени одделно и со наставниците и со учениците, за време на спроведените обуки и работилници. Овие квалитативни дискусии им дозволија на учесниците и наставниците да споделат лични искуства, предизвици и перспективи. Квалитативните податоци добиени од фокус групите одиграа клучна улога во обликувањето на содржината на Прирачникот.

4. Анализа на податоци: Собраните податоци од анкетата и квалитативните сознанија од фокус групи беа подложени на анализа. И квантитативните и квалитативните методи на анализа беа употребени за да се идентификуваат моделите, темите кои се повторуваат и клучните наоди. Оваа ригорозна анализа ја постави основата за синтетизирање на информации и извлекување значајни заклучоци кои ја водеа изработката на Прирачникот.

5. Развој на содржина на Прирачникот: Информирана од резултатите од истражувањето и квалитативните согледувања, содржината на Прирачникот беше прецизно изработена за да одговори на специфичните потреби и проблеми идентификувани во процесот на истражување. Интеграцијата на податоците од анкетата и квалитативните перспективи овозможија холистички пристап кон развојот на содржината, осигурувајќи дека Прирачникот одговара на широк опсег на барања на корисниците.

ЗА ПРОЕКТОТ

Овој Приралник е изработен како дел од Проектот “Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyberbullying” и истиот е имплементиран од Аналитика тинк-тенк Скопје, а финансиски поддржан од Амбасадата на Канада за Србија, Северна Македонија и Црна Гора. Проектот е во времетраење од 6 месеци, почнувајќи од септември 2023 заклучно со февруари 2024 година. Проектот вклучува вкупно пет училишта, од кои три средни училишта на територија на Град Скопје и две основни училишта на територија на Општина Карпош.

Главната цел на проектот е да се зголеми употребата на мерките за сајбер безбедност кај учениците и да се создаде мрежа на обучени наставници/едукатори кои ќе ги дисеминираат знаењата и во другите училишни заедници.

- » Во рамките на проектот се предвидени 7 активности, и тоа:
- » А.1. Истражување на знаењето кај младите за сајбер безбедност
- » А.2. Изготвување на анализа со препораки и мерки за подобрување на состојбата со сајбер безбедност;
- » А.3. Дводневна обука за наставници и претставници од граѓански организации и изготвување на предлог програма за училиштата;
- » А.4. Дводневна обука за врнички едукатори;
- » А.6. Работилници со млади и формирање на клубови за врничка едукација;
- » А.7. Дизајнирање и техничко уредување на мобилна апликација.
- » А.8. Финална конференција за споделување на резултатите на проектот и
- » А.9. Кампања на социјални медиуми

Со имплементацијата на истиот очекувано е да се постигнат следниве резултати:

- » P1. Спроведено истражување и идентификувани знаења кај младите за предизвиците на процесот на дигитална трансформација и дигитална безбедност;
- » P2. Дизајниран и публикуван прирачник за сајбербезбедност наменет за наставен кадар, ученици и родители;
- » P3. Зголемена соработка на граѓанските организации и релевантните институции со образовните институции и младите, како и унапредување на нивната улога во создавање на побезбедна средина за младите;
- » P4. Обучени 25 професори за имплементирање на иновативни програми во училиштата од областа на сајбербезбедност на младите;
- » P5. Обучени 25 врснички едукатори и формирани 5 неформални клубови во 5 училишта од целиот регион;
- » P6. Содржина на кампања (инфографици, промотивна прес-конференција);
- » P7. Креирана мобилна апликација со едукативен и информативен карактер;

ПРЕГЛЕД НА РЕЛЕВАТНА ЛИТЕРАТУРА

11

Во ера во која доминираат дигиталните технологии, образовните институции се соочуваат со двоен предизвик за обезбедување на безбедноста на учениците и наставниците во виртуелната област, истовремено искористувајќи ги придобивките од технолошкиот напредок. Овој преглед на литература ги истражува меѓусебно поврзаните теми за сајбер насилство и сајбер безбедноста, со специфичен фокус на учениците и наставниците во образовните услови.

Полето на стручна литература од областа на сајбер насилството и сајбер-безбедноста на ученици и наставници има остварено значаен придонес од истакнати истражувачи и организации. Истражувачите како R.A. Sabelle, J. W. Patchin and S. Hinduja, ¹одиграа клучна улога во унапредување на нашето разбирање за сајбернасилство, особено книгите: *Cyberbullying myths and realities*, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*, *Bullying, Cyberbullying, and Suicide*.² Нивните заеднички напори резултираа со бројни влијателни трудови и книги кои навлегуваат во сложеноста на онлајн булингот и стратегиите за превенција. Овие книги обезбедуваат сеопфатно испитување на сајбер насилството, истражувајќи превентивни мерки и стратегии за одговор надвор од традиционалните училишни поставки. Исто така, истражувањето на овие автори навлегува во меѓузависноста на насилството, сајбер насилството и неговите потенцијални врски со самоубиствените идеи.

Истражувачкиот центар Pew Research Center³, добро ценета институција, редовно објавува сеопфатни извештаи за безбедноста на интернет, дигиталната приватност и распространетоста на онлајн вознемирувањето. Извештајот *Teens and Technology*⁴ се фокусира на моделите на употреба на технологија кај тинејџерите, фрлајќи светлина врз нивните онлајн активности и предизвиците со кои се соочуваат. Овој извештај дав вредни сознанија за еволуирачкиот пејзаж на онлајн заканите со кои се соочуваат децата и едукаторите.

1 Computers in Human Behavior 29(6):2703-2711, Journal Review: Cyberbullying myths and realities, November 2013, authors R.A. Sabelle, J. W. Patchin and S. Hinduja.

2 Hinduja, S., & Patchin, J. W. (2018). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Corwin Press. Hinduja, S., & Patchin, J. W. (2015). *Bullying, Cyberbullying, and Suicide*. Archives of Suicide Research.

3 The State of Online Harassment, January 2021, Pew Research Center, available at: <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>

4 "Teens and Technology 2013", Pew Research Center

Во областа на безбедноста на децата на интернет, Извештајот на УНИЦЕФ⁵ се однесува на целокупното влијание на дигиталниот свет врз децата, опфаќајќи ги аспектите на безбедноста, благосостојбата и развојот.

Организации како што се Агенцијата за сајбер безбедност на Европската унија (ENISA) и Националниот центар за сајбер безбедност (NCSC) во Обединетото Кралство имаат клучна улога во полето на сајбер безбедноста. Извештајот на ENISA се фокусира на промовирање на практиките за сајбер хигиена кај децата за да се подобри нивната онлајн безбедност⁶. Извештајот на NCSC⁷ конкретно ја испитува сајбер свеста и практиките на наставниците, нудејќи увид во нивните перспективи и предизвици. Исто така, нуди насоки за обезбедување на сајбер безбедност на децата и младите поединци.

Академските списанија како The Journal of School Violence⁸ често прикажуваат студии поврзани со сајбер насилство и училишното насилство. Овие извори колективно формираат богата извор на знаење, обезбедувајќи им на едукаторите, креаторите на политики и родителите вредни сознанија и алатки за да се справат со предизвиците што ги носи сајбер насилството и да ја зајакнат сајбер безбедноста во образовните услови.

Во македонскиот контекст, Агенцијата за електронски комуникации МКД-ЦИРТ, од спроведените истражувања во 2019 година, изготви брошура со наслов “Сајбер Безбедност во домот, Водич за родители, едукатори и деца”, каде меѓудругото истакнуваат дека корисниците на Интернет во државата се најмногу загрижени за опасностите од кражба на лични податоци, хакирање на профили на социјалните мрежи и измами при купување преку Интернет. Според истото испитување, родителите сметаат дека најважни мерки што треба да се преземат за заштита на децата на Интернет се разговор и едукација на децата, запознаетост на родителите со активностите на децата на Интернет, како и ограничување на времето кое децата го поминуваат на Интернет.⁹

Горенаведените извори и литература пренесуваат важни информации за загрижувачката состојбата за сајбер безбедноста и сајбер насилството.

5 “Children in a Digital World” (2017), UNICEF

6 Сајбер хигиена за деца” (2018): ENISA

7 “Cyber Aware Teacher Survey Report” (2020), NCSC

8 [chrome-extension://efaidnbmnnnnibpcajpcgltclfeindmkaj/https://www.ojp.gov/pdffiles1/ojdp/grants/217918.pdf](https://www.ojp.gov/pdffiles1/ojdp/grants/217918.pdf)

9 <https://mkd-cirt.mk/wp-content/uploads/2021/03/VtoraBroshuraPrint.pdf>

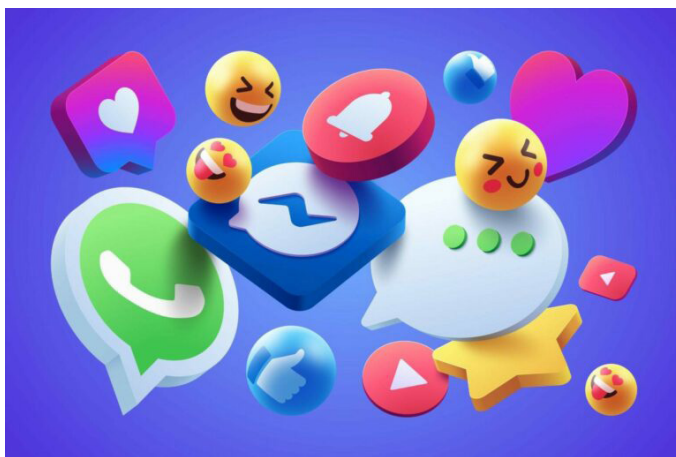
ВОВЕД

13

Живееме во време кога голем дел од нашите животи, лични и професионални, се изложени на дигиталниот свет на Интернет. Ние секојдневните обврски ги вршиме преку интернет, како нашето банкарство, купување, плаќање сметки, социјално планирање, па дури и делови од нашата работа во дигиталниот свет.

Иако придобивките од користењето на интернетот се огромни, мора да бидеме претпазливи во однос на опасностите кои што ги криедигиталниот свет. Најчести опасности се: однесувањето на децата на интернет, несоодветна и недоверлива содржина, остварување на контакт со интернет-насилници и луѓе кои имаат за цел да ги злоупотребат контактите, законски и финансиски опасности, неовластен пристап и злоупотреба на нашите лични податоци др.

Поради ова и преголемата изложеност на децата а и возрасните во дигиталниот свет, а и фактот дека интернетот преку достапноста на повеќе уреди се користи на повеќе места: дома, на училиште, кај другари, потребно е да се развие пристап кој што ќе вклучува повеќе засегнати страни за правилно користење на интернетот, меѓу кои и училишниот кадар, родителите/старателите и учениците, односно младите луѓе. Затоа во продолжение ќе се осврнеме на опасностите кои што ги крие интернетот и неговата употреба, како и на улогата на различните чинители за заштита на младите и учениците од овие опасности.¹⁰



Извор: <https://www.fenews.co.uk/resources/why-social-media-is-effective-for-business/>

Како за учениците така и за наставниците, заканите кои кружат во сајбер просторот се преголемиот број на информации за кои не се знае дали се точни или неточни и истотака не се знае колку е сигурен изворот на самите тие информации. Оттука, потребно е училиштата да обезбедат тим на стручни наставници кои ќе бидат обучени и ќе промовираат методи и начини за превенција и справување во хаотичниот сајбер простор, и заканите на кои се изложени, како што се сајбер насилство и сајбер безбедност.

Исто така, преку соработка со родителите и нивна едукација ќе се промовира безбедно користење на Интернетот.



Извор: https://www.freepik.com/premium-vector/teamwork-collaboration-banner-with-colored-line-icons-team-goal-inspiration-career-typography-infographics-concept-team-work-isolated-vector-illustration_20412457.htm

ПОИМ ЗА ВРСНИЧКО НАСИЛСТВО

15

„20-от век ќе биде запаметен како век обележан со насилство. Тоа нè оптоварува со наследството на масовно уништување, насилство нанесено во размер што не е видно и никогаш не било можно порано во човечката историја. На нашите деца им должиме живот ослободен од насилство и страв. За да се обезбеди ова, ние мора да бидеме неуморни во нашите напори не само да постигнеме мир... туку и да ги решиме корените на насилството. Само тогаш ќе го трансформираме наследството од минатиот век од дробење товар во лекција за претпазливост “ - Нелсон Мандела, Предговор на Светскиот извештај на Светската здравствена организација за насилство и здравје, 2002 година¹¹

Светскиот извештај за насилство и здравје, на Светската Здравствена Организација за насилство и здравје (WRVH) го дефинира насилството како: „Наменета употреба на физичка сила или моќ, загрозува или вистинска, против себе, друго лице, или против група или заедница која или резултира во или има голема веројатност да резултира во повреда, смрт, психолошка штета, лошо развивање или лишување «¹²

Врсничките насилнички однесувања, без разлика дали се виртуелни или лице в лице, имаат негативно влијание не само врз жртвите, врз сведоците, туку и врз самите оние кои го извршиле насилството. Врсничко насилство, односно булинг е форма на агресивно однесување во подолг временски период и се повторува насочено кон исто лице. Со други зборови може да се означи како: намерно, свесно негативно постапување со намера да се повреди една личност или одредена група, со намера да се предизвика заплашеност, понижување или оштетување на репутација. Насилникот секогаш има поголема сила од жртвата, однесување што со ништо не може да се оправда.

Врсничко насилство не е: еднократен инцидент што, ниту пак пријателска расправија, расправија или несогласување, случај или по грешка ненамерно нанесување болка, пријателско закачање или недоразбирање, насилно решавање судир на ставови меѓу пријатели со иста сила.

11 Предговор на Светскиот извештај на Светската здравствена организација за насилство и здравје, 2002 година

12 <https://worldbeyondwar.org/mk/types-of-violence/>

Видови врничко насилство:

- » Вербално/невербално – нарекување со погрдни имиња, исмевање, омаловажување, навреди, дофрлувања, заканувачки погледи, гримаси, исмевање, несакани допири од сексуална природа, следење, уценување;
- » Физичко – удирање, туркање, рушење, крадење и уништување предмети;
- » Социјално – озборување, избегнување, игнорирање, изолирање, ширење лаги и гласини, исклучување;
- » Електронско (сајбернасилство) - испраќање, објавување или споделување негативна, штетна, лажна или зловна содржина за некој друг со користење на електронски уреди

САЈБЕР НАСИЛСТВО

17

Иако придобивките од користењето на интернетот се огромни, мора да бидеме претпазливи во однос на опасностите кои што ги крие дигиталниот свет. Најчести опасности се: однесувањето на децата на интернет, несоодветна и недоверлива содржина, остварување на контакт со интернет-насилници и луѓе кои имаат за цел да ги злоупотребат контактите, законски и финансиски опасности, неовластен пристап и злоупотреба на нашите лични податоци и др.

Како резултат на горенаведените причини и закани, свесни сме дека секој од нас лесно може да стане мета на напади и жртва на насилство во сајбер просторот.

Сајбер насилството се случува преку дигитални уреди како што се мобилни телефони, компјутери и таблети. Сајбер насилството може да се одвива 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. Оваа насилството вклучува испраќање, објавување или споделување негативна, штетна, лажна или зловна содржина за некој друг. Некогаш сајбер насилството ја преминува границата и преминува во незаконско или криминално однесување.

ВИДОВИ НА САЈБЕР НАСИЛСТВО

Сајбер гемнеење

Овој вид на онлајн врсничко насилство е кога жртвата константно се следи преку социјалните мрежи, и ѝ се испраќаат најразлични видови на пораки или реакции на snap/story во форма на закани, навреди или невистини. Потоа, се преземаат одредени фотографии на жртвата, дигитално се менуваат со помош на соодветни апликации и истите се користат за дополнително омаловажување или заканување. Повеќето од децата кои вршат врсничко насилство ја користат оваа форма, бидејќи се чувствуваат недопирливи и мислат дека нема реални последици доколку насилството се врши по дигитален пат. Затоа, од голема важност е децата да се освестат дека штом нешто ќе објават на интернет, невозможно е да се контролира. Дури и работите што се бришат може да постојат во многу електронски копии на друго место и повторно да се појават.

Cyberstalking

Овој вид на сајбер-насилство е кога некој користи технологија за постојано вознемирување, заплашување и заканување некого. Cyberstalkers може да ги следат своите жртви и да се обидат да се сретнат со нив. Многу случаи на сајбер следење вклучуваат возрасни лица (педофили), кои ги пронаоѓаат тинејџерите за да имаат сексуални односи со нив.

Анонимно и лажно претставување

Многу училишта имаат проблеми со вакви „трач“, групи преку социјалните мрежа Instagram, Facebook, TikTok и слично. Обично, еден ученик ќе формира група која ќе ја крсти по името на училиштето во кое учи и потоа ќе привлече стотици ученици како членови кои оставаат анонимни пораки. Овие пораки знаат да бидат исклучително невкусни и да навредуваат и омаловажуваат деца на запрепастувачки суров начин. За да бидат работите уште пореални и погрдни, некои од учениците прават скриншотови, па истите ги споделуваат со жртвата која е предмет на исмејувањето, со што дополнително се разгорува работата.

Честопоати, ученикот/ жртва на ваков булинг користи предрасуда за да претпостави кој би можел да ги пишува лошите работи околу него и честопати и тоа дете ќе започне слична кампања на социјалните мрежи за да се одмазди. На овој начин, и жртвата станува насилник, па така тој негативен круг зазема уште подлабока димензија.

Издавање, измама, имитирање и уценување

Под издавање се подразбира намерно и јавно споделување на чувствителни, приватни или срамни податоци за одредено дете на други деца или во различни групи. Децата често знаат да се доверуваат или испраќаат одредени важни податоци или слики на други деца, па потоа се прави скриншот/ видеа од истите за да се проследуваат на сосема трети лица.

Тука стапува на сила уште една форма на сајбер насилство позната како измама, според која детето насилник се „спријателува“ со жртвата, со цел да извлече одредени работи и информации, кои подоцна ќе бидат искористени за ескалација на врсничкото насилство.

Од друга страна, имитирањето, или frapping е кога едно дете ќе влезе во корисничка сметка на друго дете и ќе започне кампања од постирање и споделување на несоодветни содржини на сите пријатели и следбеници. Може да се срамни изјави, навредувања, или пак некои линкови кои имаат несоодветни содржини.

Како една од најлошите и најзлобните форми на сајбер насилство е онлајн уцена каде, на пример, се користат компромитирачки фотографии од жртвата и од истата се бараат понижувачки услуги; доколку детето не се согласи да го направи тоа што се бара од него, насилникот се заканува дека ќе ги испрати фотографиите на х лица, со цел да го оцрни и понижи пред сите познаници.

Вознемирување

Вознемирувањето вклучува постојано испраќање злонамерни, навредливи или заканувачки пораки до поединец или група на интернет. Ова може да им се направи на жртвите јавно или приватно.

Тролање

Тролањето е намерен чин, кој има за цел предизвикување одговор или реакција, преку употреба на некој вид на запаливи изјави - како што се употреба на навреди или говор на омраза - на онлајн форум. Тролањето често се прави од задоволството што го чувствува тролот, со тоа што ги вознемирува другите.

Оцрнување

Овој вид на сајбер насилство случува кога некој објавува гласини и озборувања за неког на интернет. Сајбер насилниците користат омаловажување со цел да ги уништат односите и репутацијата на жртвата.

Исклучување

Исклучувањето е создавање групи или настани на дигиталните платформи или платформите за комуникација и исклучување некој од истите. Ова може да се случи и со тоа што нема да се означи некој на фотографија или нема да се покани на некој настан, како и да исклучат некој од онлајн разговор.

Постојат многу причини поради кои учениците можат да се вклучат во овие однесувања, вклучувајќи досада, одмазда, гнев како и да предизвикаат реакции од нивните жртви.

Дополнително, самата анонимна природа на интернетот им олеснува на луѓето да малтретираат други на интернет, особено ако и самите се социјални отпадници, на кои им недостига храброст да го направат тоа лице во лице.

Можни причини за насилство

- » Преголемата изложеност на насилство (преку ТВ, видео игри, општиот социо-културен контекст во кој што живееме)
- » Спуштениот е праг на толеранција, и отвореното и прикриеното насилство, како и насилната комуникација кај младите, стануваат начин на живеење и комуницирање.
- » Голем дел од нас не сме ни свесни дека тоа што се случува околу нас е всушност насилство, како и наставниците и стручните служби тешко или воопшто не го препознаваат врсничкото насилство, било тоа да е виртуелно или класично, и не реагираат навремено и соодветно за спречување на истото.

ШТО Е ИНТЕРНЕТ ПРИВАТНОСТ

21

Дали некогаш се прашувате кој и како ги собира нашите лични информации. Какви информации им се потребни, што прават со нашите податоци, со кого ги споделуваат нашите тајни и дали воопшто имаме приватност во виртуелниот свет на кој сме изложени секојдневно?

Нашата приватност е важна за тоа што ни дава простор кој што треба да го развиваме како човечки суштества. Приватноста ни дава слобода на однесување, како да читаме, учиме и изразуваме без да се грижиме за тоа кој може да гледа или слуша, значи да не се чувствуваме осудени за нашите однесувања. Тоа ни дава можност да ја дадеме нашата доверба на другите, така што ќе можеме да купуваме, да се дружиме, да бидеме интимни едни со други и да формираме виртуелни врски што ги одржуваат нашите заедници силни, нашата демократија да функционира и нашите животи да бидат збогатени. Доколку ја немаме таа приватност, не можеме правилно да функционираме како општество или како индивидуи.

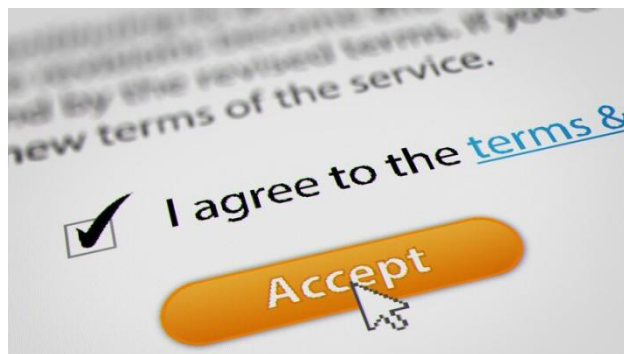
Интернет приватноста го вклучува правото на личните информации во врска со чување, употреба, обезбедување на трети лица и прикажување на лични информации преку интернетот. Приватноста на интернет е подмножество на приватност на податоците. Загриженоста за приватноста е појавена уште од почетоките на мрежно поврзување на компјутерите.¹³

Дигиталната писменост е една од осумте клучни компетенции во задолжителното образование, а стекнувањето вештини за дигитална медиумска писменост може да се смета за составен дел од правото на детето на квалитетно образование, заштита на приватноста и заштита од насилство и злоупотреба. Одговорност на возрасните е да обезбедат соодветна заштита и поддршка за децата да ги уживаат своите права во дигиталниот свет. Безбедно и конструктивно користење на дигиталните уреди и интернетот подразбира поседување соодветни вештини за дигитална писменост: пребарување и критичко оценување информации од интернет, комуникација преку дигитални алатки, создавање дигитална содржина, безбедно однесување на интернет и решавање проблеми во дигиталната средина. Дигиталниот свет е реален, неразделен од искуствата стекнати надвор од него. Дигиталната комуникација е реална, иако се одвива виртуелно.

Сите правила што важат во комуникацијата во секојдневниот живот, важат и за комуникација во виртуелниот свет. Како што не сакаме да ги откриеме нашите лични податоци на сите што ги среќаваме на улица, ло-

13 Vodich_zsajber_bezbednost_PRINT%20(1).pdf

гично би било да не го правиме тоа ни на интернет. Како што не навредуваме или повредуваме луѓе во живо, така тоа не треба го правиме ниту преку дигитални уреди или алатки за комуникација.



Извор: https://www.google.com/url?sa=i&url=https%3A%2F%2Fbetterproposals.io%2Fblog%2Fproposal-terms-and-conditions%2F&psig=AOvVaw0D9C3CMQm6x_92VEJBdLJb&ust=1700920643686000&source=images&cd=vfe&opi=89978449&ved=0CBQQjhqFwoTCODqrKrl3IIDFQAAAAAdAAAAABAE

Правото на приватност и заштита на личните податоци е едно од основните човекови права признаено во најважните меѓународни документи, како што се: Конвенцијата на Обединетите нации за правата на детето (член 16), Универзалната декларација за човекови права (член 12), Европската конвенција за човекови права член 8) и други.

Лични податоци се сите оние податоци што се однесуваат на некое лице, а врз основа на кои може да се идентификува.¹⁴

- » име и презиме на лицето;
- » поштенска адреса;
- » е-адреса;
- » фотографија;
- » IP-адреса;
- » локација на која се наоѓа лицето;
- » податоци од здравствената книшка;
- » податоци собрани во онлајн опкружувањето преку колачиња;
- » податоци што се користат за профилирање на корисникот (економска ситуација, лични интереси, однесување, навики на потрошувачите, движење и така натаму).

Децата и младите се загрижени за тоа кои лични податоци ќе дојдат во сопственост на родителите и пријателите, но не и околу фактот ако истите податоци ги споделат јавно, а честопати не се свесни дека истите може да бидат злоупотребени. Многу е важно да се подигне свеста кај младите околу тоа кои лични податоци не се соодветни за споделување со други луѓе и во дигиталниот простор, во кои ситуации и зошто. Особено многу е битно кога зборуваме за содржината што децата и младите ја споделуваат на интернет, бидејќи во моментот кога објавуваме нешто на интернет, се случува да изгубиме контрола врз содржината што ја објавуваме.

Личните податоци, корисниците ги оставаат на интернет:

- » свесно, на пример, при купување на некои производи, преземање содржини од интернет, објавување фотографии, отворање профили на социјална мрежа;
- » несвесно, на пример, преку колачиња, отпечаток од прст, податоци за локација, IP-адреса на уредот од кој се пристапува на интернет итн.¹⁵

КОМУНИКАЦИЈА НА ИНТЕРНЕТ И ПОСЛЕДИЦИ ОД САЈБЕР НАСИЛСТВО

Истражувањата покажуваат дека умереното користење на дигиталната технологија позитивно придонесува за развојот на децата, додека некористењето и прекумерната употреба имаат негативно влијание. Родителите со своите навики во користењето на дигиталната технологија, многу ја обликуваат нејзината употреба од страна на детето. Редовното следењето и слободата за дискусија за активностите на децата на дигиталните уреди, се многу ефикасни во намалувањето на сајбер насилство, отколку самото ограничување на времето или пристапот до одредени содржини.¹⁶

Забраната за користење интернет не е баш препорачлива мерка, бидејќи на тој начин децата се лишени од бројните можности што ги дава интернетот особено ако се има предвид дека интернетот е моќна информациско-когнитивна алатка и можност за стекнување вештини што се клучни за успешно функционирање во дигиталниот простор.

Препораката за возрасните е нивниот главен фокус да не биде на времето што го поминува детето пред екранот, туку на квалитетот на тоа време, односно на содржината на активностите на користење. Треба да се поддржат младите да не користат интернет исклучиво за забава, туку и за други значајни и корисни активности (стекнување различни вештини, наоѓање корисни информации, училишни задачи и слично).

Виртуелниот свет не е имун на насилство, но сепак „сајбер насилството“ станува форма со која младите сè почесто се соочуваат. За нив многу „полесно“ е да се напише злонамерен коментар, отколку истиот да му се каже некому в лице, или да се кликне на копчето „ми се допаѓа“ на било која насилна објава, наместо да се поддржува лично насилникот додека ја булизира жртвата.

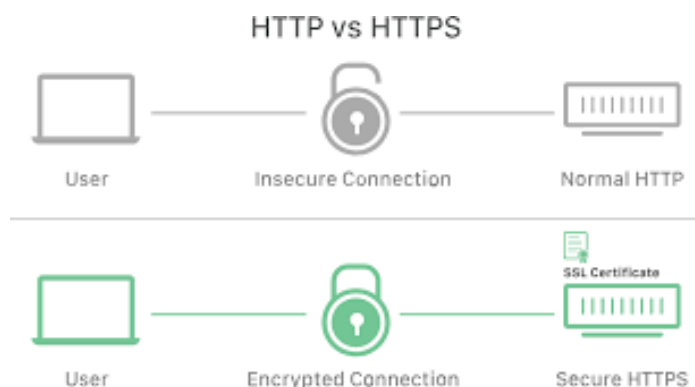
16 (Blum-Ross & Livingstone, 2016)

ВЕБ-ПРЕЛИСТУВАЧИ И БЕЗБЕДНОСТ

Ние во нашето секојдневие со работа на компјутер или некој друг дигитален уред, посетуваме голем број на веб-страници, кои ни нудат безброј услуги потребни за нас и за нашиот личен развој и олеснување во извршување на нашите секојдневни обврски. Користените услуги, како што се читање вести, пребарување на информации, социјални мрежи, слушање музика, симнување на потребни информации и документи, и друго, станаа неизбежен дел на нашиот начин на живеење.

Треба да се има предвид дека секоја веб-страница користи протокол за комуникација и многу е битно да знаеме кои веб-страници користат безбеден протокол и кои веб-страници се безбедни за посета.

HTTP е протокол кој овозможува комуникација помеѓу различни системи. Најчесто се користи за пренос на податоци од веб-сервер на прелистувач со цел да им се овозможи на корисниците да прелистуваат веб-страници. Меѓутоа, со редовниот протокол HTTP е што информациите што течат од сервер до прелистувач не се криптирани, што значи дека може лесно да се украдат, додека пак HTTPS протоколите го поправаат ова со користење на SSL сертификат, кој помага да се создаде безбедна криптирана врска помеѓу серверот и прелистувачот, со што се заштитуваат потенцијалните чувствителни информации од кражба, бидејќи се пренесуваат помеѓу серверот и прелистувачот. HTTPS е особено важен за веб-страниците каде што внесуваме кориснички сметки, лозници и кредитни картички.¹⁷



Извор: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.cloudflare.com%2Flearning%2Fssl%2Fwhy-is-http-not-secure%2F&psig=AOvVaw2Q3ZH8SbLB_T5O7S7ojLVg&ust=1700921098450000&source=images&cd=vfe&opi=89978449&ved=0CBQQjhqFwoTCJDc4oTn3IIDFQAAAAAAdAAAAABAE

¹⁷ Vodich_zaj_sajber_bezbednost_PRINT%20(1).pdf

ВИДОВИ НА САЈБЕР НАПАДИ

Сајбер напад или закана по сајбер безбедност е малициозна активност осмислена од страна на злонамерни луѓе, таканаречени хакери, за крадење или оштетување на вашите податоци или нарушување на системот на еден поединец или цела организација.

Познати се неколку видови на сајбер напади и тоа:

- » Социјален инженеринг
- » Фишинг напади (phishing – риболов)
- » Преземање податоци во поминување (Drive by downloads)
- » Напади Човек-во-средина (MITM напади)
- » Напади со фрлени УСБ уреди
- » Малвер - malware – малициозен софтвер

За да стекнувате вештини за заштита на самите себе и своите системи, првично треба да бидете запознаени и да научите за овие различни видови на сајбер закани и различните начини како да останете безбедни во сајбер просторот.

РЕЗУЛТАТИ ОД ИСТРАЖУВАЊЕТО

27

Ова истражување има за цел анализа и увид на актуелната состојба во идентификувањето, превенцијата од сајбер насилство и сајбер напади, и колку учениците се запознаени со ризиците кои ги крие дигиталниот свет и колку тие ги познаваат и применуваат методите за заштита и приватност на сајбер просторот кој го користат.

Анкетирањето беше спроведено во месец септември 2023 година, на репрезентативен примерок од 507 испитаници, ученици од три средни училишта на Град Скопје и две основни училишта од Општина Карпош (урбани и рурални средини).

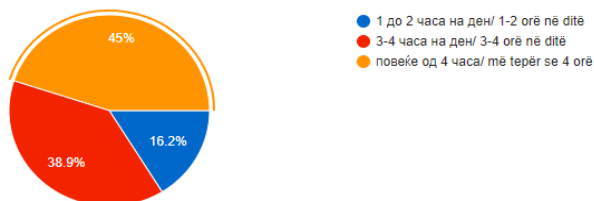
Анкетниот прашалник е основа на нашето истражување, бидејќи нашата почетна точка е постоечката состојба на свеста на учениците и информираноста. Колку тие знаат околу сајбер насилството и како се справуваат со тоа, каква е состојбата во нивното училиште, каква е улогата на постоечките протоколи за справување со насилство, каква е улогата на наставниците и родителите во справувањето со насилството, со кои видови на сајбер напади се запознаени, и кои механизми ги користат за превенција и одбрана од сајбер напади, како ги штитат личните информации и колку се чувствуваат безбедни во сајбер просторот се прашањата на кои добивме одговори користејќи го овој метод.

Инструментот кој беше применет за истражувањето е анкетен онлајн прашалник со 20 прашања, кои се комбинирани од различни типови на прашања, со цел да се добие што е можна појасна слика околу фактичката состојба за сајбер насилство и сајбер безбедност, т.е. на ученикот му се дава можност да одбере еден или повеќе одговори од понудените опции или пак да даде свој личен одговор од неговото искуство.

Колку време поминувате на било која од дигиталните алатки на ден?

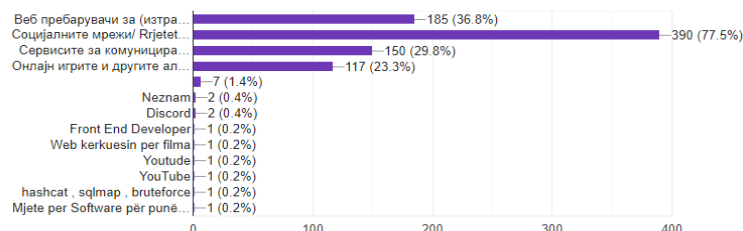
/Sa kohë shpenzoni në cilëndo nga mjetet digjitale në ditë?

507 responses



**Кои од услугите кои ги нуди Сајбер просторот најчесто ги користиш?
Cilin nga shërbimet e ofruara nga Cyber-hapsira e përdorni më shpesh?**

503 responses



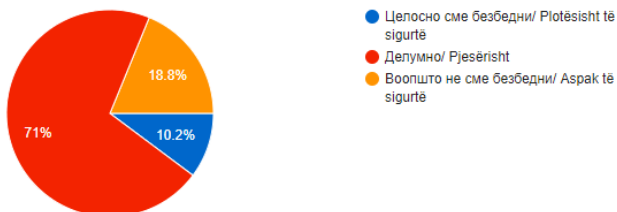
Земајќи ги предвид одговорите на првите две прашања се добива јасна слика за поминатото време на интернет и на што поточно се инвестира тоа време. Од 507 одговори од страна на учениците, приближно 84% од одговориле дека поминуваат повеќе од 3 часа и повеќе од 4 часа на интернет (дигитален свет) и тоа 77.5% од учениците тоа време го поминуваат на социјалните мрежи.

Според овој резултат, несвесно и непродуктивно се губи времето на младите деца и ако се земе предвид дека ретко кој од младите признава дека реално многу голем дел од времето троши на овие „активности“, тогаш може да се каже дека навистина младите преголем дел од времето се всушност под влијание на содржините на социјалните мрежи, со што тоа има големо влијание и на формирањето на нивните ставови, мислења.

Со оглед на тоа што социјалните мрежи се, исто така, еден вид социјализација – ако секој користи одредена социјална мрежа, се појавува стравот дека нешто ќе пропуштат, ако не ја користат одреден период.

**Според тебе колку сме безбедни во Сајбер просторот?/
Sipas teje sa jemi të sigurtë në hapsirën kibernetike?**

500 responses

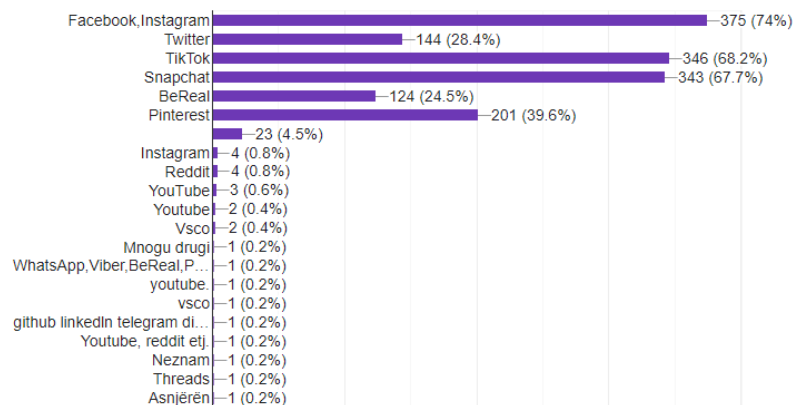


Самиот графикон ја покажува свесноста за тоа колку децата се чувствуваат сигурни во сајбер просторот. 71% од учениците се изјасниле дека делумно се чувствуваат сигурно, што значи дека кај нив постои несигурност и недоволна информираност околу сигурноста во дигиталниот свет. 18.8% од испитаниците се изјаснија дека се чувствуваат целосно безбедни во сајбер просторот, додека пак 10.2% се изјасниле дека воопште не се чувствуваат безбедни.

На кои од долунаведените социјални мрежи имате своја активна сметка (account)?/

Në cilën nga rrjetet sociale të poshtëshënuara keni llogari aktive personale?

507 responses



На прашањето : “ На кои социјални мрежи , децата имаат активна сметка”, учениците имаа за избор повеќе опции како одговор, и според одговорите може да заклучиме дека Facebook и Instagram (74%) ,TikTok (68.2%) и Snapchat (67.7%), се најкористени социјални мрежи од страна на нашите деца.

Голем дел од младите се регистрираат, креираат профили на социјалните мрежи многу млади, на возраст од дванаесет до четиринаесет години. Кога се зборува за позитивниот ефект, како причини се секако олеснувањето на комуникацијата кај одредени деца, полесната достапност до информации, можноста да се истакне креативност, да се споделат идеи со другите, и др.¹⁸

Според тебе што е безбедно да споделуваме во Сајбер просторот?/

Çfarë mendoni se është e sigurt për t'u shpërndarë në hapësirën kibernetike?

507 responses

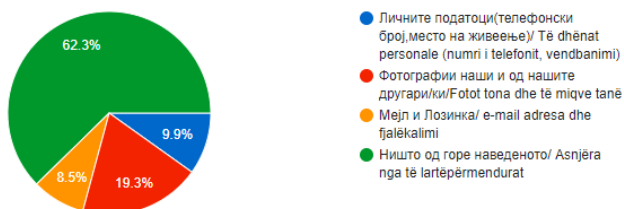


Главната улога за безбедно користење на интернетот ја имаат самите родители и поблиското окружување на децата, но според реалната состојба, како заклучок од одговорите на испитаниците, 38.7% се изјасниле дека повеќето од родителите не се свесни и едуцирани за начинот на кој можат да влијаат врз сајбер сигурноста на своите деца, кои сигурносни мерки можат да ги постават и преку кои алатки. Додека 34.3% изјавиле дека имаат забрана од страна на родителите само на одредени алатки. 15.6% од испитаниците ни самите не знаат дека постои опција со која родителите може да ги контролираат активностите на своите деца на Интернет.

Според тебе што е безбедно да споделуваме во Сајбер просторот?/

Çfarë mendoni se është e sigurt për t'u shpërndarë në hapësirën kibernetike?

507 responses



Резултатите од горенаведеното прашање околу споделувањето, покажуваат дека децата се свесни околу правилата за сајбер сигурност во споделувањето на важни елементи од нашето секојдневие, каде 62,3% од испитаниците се изјасниле дека ни едно од понудените опции не смее да биде споделено на интернет. Останатите испитаници се со различни ставови околу тоа што не смее да се споделува на интернет. Но и покрај таквата свесност, се поставува прашање, зошто сепак сакаме да споделиме статуси, слики или други нешта на социјалните мрежи?

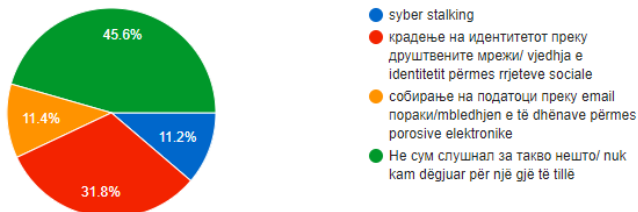
Истражувачите сметаат дека среќата е главен мотиватор за споделувањето на социјалните мрежи. Емоциите што се наталожени и поврзани со среќата се најчести кога станува збор за најуспешните вирални содржини на мрежите. Абигејл Познер од „Гугл“ го опишува споделувањето од среќа како „размена на енергија“. Според неа, кога гледаме или креираме содржина што нè живнува, ја препраќаеме на други за да им дадеме дел од енергијата и живоста. Секој подарок го содржи духот на оној што подарува.¹⁹

19 <https://sovremenitehnologii.mk/socijalni-mrezi/>

Што за тебе претставува „phishing“?

Çka paraqet për ty „phishing“?

507 responses



На прашањето „Што е phishing?“, 45.6% се изјасниле дека не слушнале за таква терминологија, а само 11.4% давале точен одговор. Според ова може да заклучиме дека на децата им треба дополнителна едукација (формална или неформална), која ќе им помогне да научат нешто повеќе околу видовите на сајбер напади, како да ги препознаваат и заштитат од нив.

Играш онлајн игра со својот другар/ка .

На екранот ти се појавува мал прозорец со порака која блинка и на која пишува

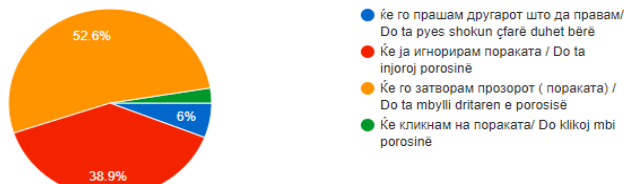
„Клики тука и ќе освоиш многу вредна награда“

Што ќе направиш?

/Ju jeni duke luajtur një lojë online me shokun tuaj.

Një dritare e vogël shfaqet në ekranin tuaj me një mesazh pulsues që thotë "Kliko këtu dhe do të fitosh një çmim shumë të vlefshëm". Çfarë do të bësh?

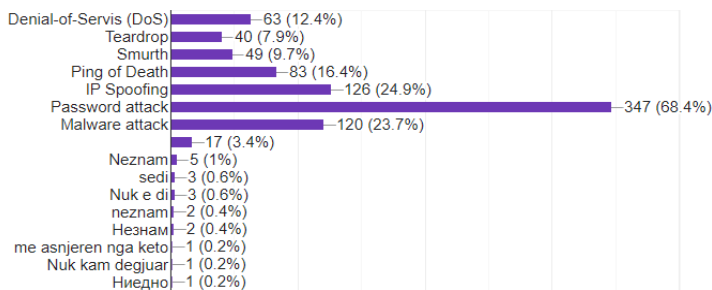
504 responses



Во сличните случаи, кога на екранот неочекувано ни се појавува порака, најдобро е истата да се игнорира. Сите останати постапки ќе доведат до активирање на одреден вирус. Сепак, 52.6% од испитаниците се изјасниле дека најдобро е да се затвори прозорецот, што значи дека автоматски се изложуваат на ризик за кој не се ни свесни. А пак 38.9% од испитаниците се свесни како треба да се постапи во таква ситуација или предизвик.

Кои од долунаведените видови на сајбер напади ви се познати, или сте ги слушнале како терминологиј?
Me cilin nga llojet e mëposhtme të sulmeve kibernetike jeni njohur ose keni dëgjuar për to si terminologji?

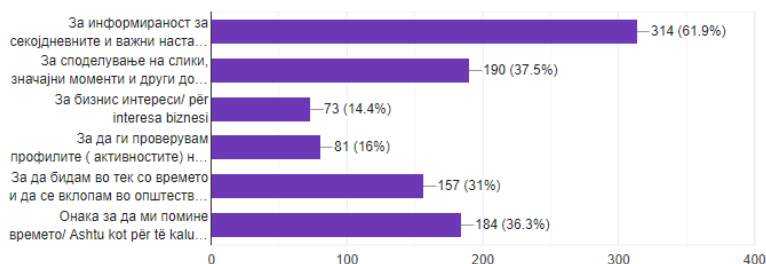
507 responses



Ако се навратиме на резултатите од одговорите на второто прашање, околу тоа што најмногу користат децата од сајбер просторот, наидовме на повеќе одговори дека се социјалните мрежи. Па, затоа децата се најмногу запознаени со passwordattack нападот, бидејќи со самото тоа лично се соочиле. 68.4% од учениците одговориле дека се запознаени со овој вид напад, додека другите видови на напади се помалку познати за испитаниците.

Со каква причина најчесто ги користиш социјалните мрежи?
Për çfarë arsye i përdorni më shpesh rrjetet sociale?

507 responses



Балансот помеѓу животот на социјалните мрежи и реалноста станува сè потежок, бидејќи моќта на инстаграм, фејсбук, твитер, тик ток е голема, зависноста лесно се создава (како и секоја друга зависност), и можноста младите да се „одвојат“ од реалниот живот и да сметаат дека она што го гледаат на социјалните мрежи е всушност тоа кон што треба да се стремат е голема.

Трите најистакнати причини за користење на социјалните мрежи се:

- » за информираност (61.9%),
- » за споделување (37.5%),
- » без причина, само за исполнување на времето (36.3%).

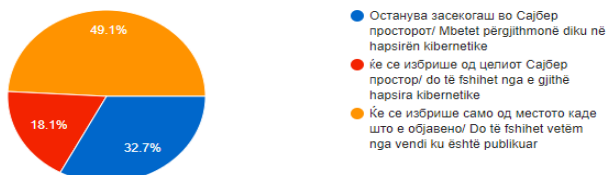
Виртуелниот свет им создава притисок на младите во реалниот свет давајќи им лажна слика за начинот на живот, облекување, социјално однесување, нереални информации и др.

33

Според тебе што ќе се случи кога ќе поставиме нешто на Интернет (пример слика, видео, пост или др) а потоа истото го избришеме ?/

Sipas jush, çfarë do të ndodhë kur ngarkojmë diçka në internet (për shembull, një foto, video, postim, etj.) dhe më pas e fshijmë atë?

507 responses



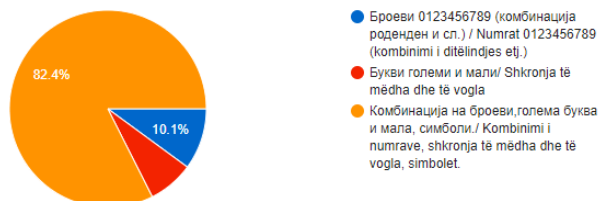
Сите наши активности на Интернет можат да бидат користени, а и веќе се користат за некои цели. Според добиените одговори, 49.1 % од учениците се свесни дека тоа што еднаш ќе се постави на интернет, и да посакаат веднаш да го избришат, нема да успеат, бидејќи останува засекогаш во сајбер просторот. 32.7% од испитаниците веруваат дека тоа што го поставиле на интернет (во сајбер просторот) самото ќе се избрише од местото каде што е објавено, а пак 18.1% од учениците веруваат дека истото целосно ќе биде избришано од сајбер просторот по некое време.

Затоа, треба да бидеме многу внимателни што споделуваме во дигиталниот простор.

Според тебе што треба да содржи една лозинка за да биде безбедна?

/ Çfarë mendoni se duhet të përmbajë një fjalëkalim për të qenë i sigurt?

507 responses



Поставувањето лозинки за користење на разни апликации во дигиталниот простор е многу важна безбедносна мерка. Оттука, според одговорите на учениците, 82.4% од нив се запознаени со важноста на комбинацијата на лозинката и како истата треба да биде составена.

Доколку користите што е можно покомплексни лозинки, особено кога станува збор за социјалните мрежи и е-поштата, на овој начин ги заштитувате вашите податоци, па тие се безбедни. Кога велите „малку посложени лозинки“, мислите на користење долга комбинација од големи и мали букви, бројки и знаци. Според дадените одговори, учениците се запознаени и свесни околу посложеноста на лозинките како мерка за превенција од можен напад.

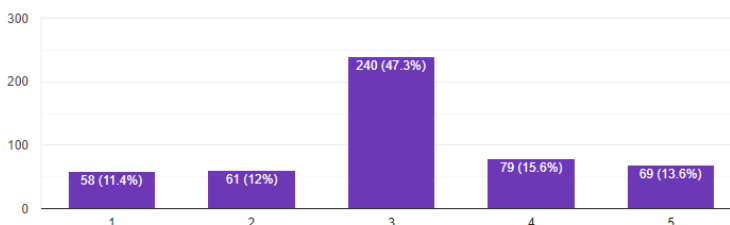
На скала 1 до 5

Како би ја оценил/а свеста во твојата средина во врска со прашањето за сајбер насилство?

Në shkallë nga 1 deri në 5

Si do ta vlerësonit ndërgjegjësimin në mjedisin tuaj për çështjen e dhunës kibernetike?

507 responses



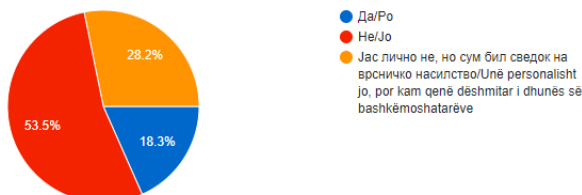
Од одговорите на горенаведеното прашање можеме да видиме дека 70,7% од испитаните ученици сметаат дека свеста во општеството и нивната средина во врска со сајбер насилството е ниска и просечна. Одговорите на учениците укажуваат на фактот дека има итна потреба од подобрувања во насока на подигање на свеста кај сите општествени чинители за важноста и сензитивноста на сајбер насилството и дека треба многу да се работи за да се обезбеди посигурна клима и чувство на безбедност во сајбер просторот.

53.5 % од учениците се изјасниле дека не биле жртва на врсничко насилство. Истовремено, 28.2% од учениците одговориле дека биле сведоци на врсничко насилство, а само 18.3% од нив се изјасниле дека биле жртви на врсничко насилство.

Дали си бил жртва на било кој вид на врсничко насилство?

/ A keni qenë viktimë e cilëso lloj dhunë nga bashkëmoshatarët?

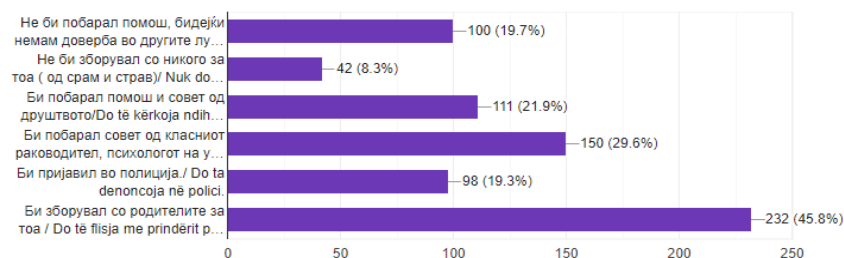
507 responses



Овие резултати од одговорите на учениците отвораат повеќе насоки за размислување за можните причините. Имено, истражувањето на Аналитика тинк тенк од 2022 година, покажа дека дури 62,7% од учениците потврдиле дека насилството е често или постојано присутно во училишната средина²⁰. Истовремено, 37,4%²¹ од учениците одговориле дека електронското насилство е најприсутно во нивните средини, после физичкото и психичкото насилство. Овие резултати упатуваат на тоа дека широката распространетост на насилството можно е да довела до степен до кој голем дел од учениците и не се свесни дека конкретно нивно однесување претставува вид на насилство и оттука истото станува секојдневие и „нормално“, однесување. Односно, постои опасност истото да стане прифатена социјална и општествена норма. Дополнително, големата изложеност на младите на насилство (преку ТВ, видео игри, општиот социо-културен контекст во којшто живеат) дополнително придонесува за „несвесното“, насилно однесување на децата. Тоа значи дека прагот на толеранција е спуштен и отвореното и прикриено насилство, како и насилната комуникација, за жал стануваат начин на живеење и комуницирање помеѓу децата.

**Доколку би бил жртва на сајбер насилство, како би реагирал?/
Nëse do të ishit viktimë e dhunës kibernetike, si do të kishit reaguar?**

507 responses



Загрижува фактот дека 28% од учениците изјавиле дека не би побарале никаква помош доколку бидат жртва на сајбер насилство. Сепак, од друга страна пак, позитивен е фактот дека 72% од учениците се изјасниле дека би побарале помош побарале од стручна служба, класен раководител или од самите родители. Тоа укажува дека сепак отворената комуникација меѓу родителите и децата, или пак наставниците (класниот раководител) и децата е позитивен знак или како клучно решение во справувањето со каков било вид на врсничко насилство. Истовремено, ова ни укажува дека релацијата наставник – деца – родители е навистина значјана и затоа треба да се работи на зајакнување на истата со цел

²⁰ Прирачник за развој на култура на мир и превенција од насилство како основни вредности во образовниот систем во република северна македонија, маја христовска и весна трајковска-стерјов аналитика тинк тенк, јануари 2022. достапно на: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.analyticamk.org/images/2021/12/12/prevencija_nasilstvo_mk.pdf](https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.analyticamk.org/images/2021/12/12/prevencija_nasilstvo_mk.pdf)

²¹ Истражувањето на Аналитика тинк тенк имаше за цел да ги идентификува формите на насилство во училиштата. Притоа, 37,4% од учениците одговориле дека електронското насилство е најприсутно во нивните средини, после физичкото и психичкото насилство. (прирачник за развој на култура на мир и превенција од насилство како основни вредности во образовниот систем во Република Северна Македонија, Маја Христовска и Весна Трајковска-Стерјов Аналитика тинк тенк, јануари 2022)

охрабрување на сите ученици да побараат помош доколку се соочат со секаков вид на насилство.

„Родителите мора да бидат љубопитни, но да не го осудуваат детето. Честопати се случува детето да биде загрижено дека родителот ќе му забрани пристап до уредот, ако искрено зборува за проблемите со кои се соочува, па потребно е да го уверите детето дека нема да му го одземете мобилниот телефон ако се соочува со таков проблем“ – доктор Пол Вегл од Американската Академија за детска и адолесцентска психологија.²²

Дали во вашето училиште се одржуваат едукативни работилници за безбедно користење на Сајбер просторот?

A organizon shkolla juaj puntori edukative për përdorimin e sigurt të hapësirës kibernetike?

507 responses



43,2% од учениците одговориле дека во нивните училишта на се одржуваат едукативни работилници за сајбер безбедност или дека тоа се случува многу ретко. Резултатите од ова прашање се загрижувачки, бидејќи 39.8% од испитаниците одговориле дека не знаат дали се одржуваат работилници за сајбер безбедност. Имајќи предвид дека со напредувањето на технологијата и проширувањето на дигитализацијата, се соочуваме со низа на предизвици и специфични опасности, сепак многу малку се работи на дигиталната едукација, било тоа да е формална или пак неформална.

На оваа прашање учениците имаа можност да ја оценат потребата од неформални врснички клубови, на скала од 1-5 (1 означува најниска оценка а 5 означува највисока оценка). Многу важен факт споделен од учениците е дека 62.2 % од нив сметаат дека е важно постоењето на неформални врснички клубови во нивните училишта преку кои ќе се врши едукација за сајбер безбедност со цел подобрување на училишната клима и справување со насилството. Само 13.8% од испитаниците сметаат дека нема потреба од постоење неформални клубови за врсничка едукација во нивните училишта.

²² <https://www.crnobelo.com/zivot/semestvo/95707-zoshto-decata-zhrtvi-na-sajber-buling-krijat-od-roditelite-deka-se-zlostavuvani-4-znaci-deka-deteto-trpi-maltretiranje>

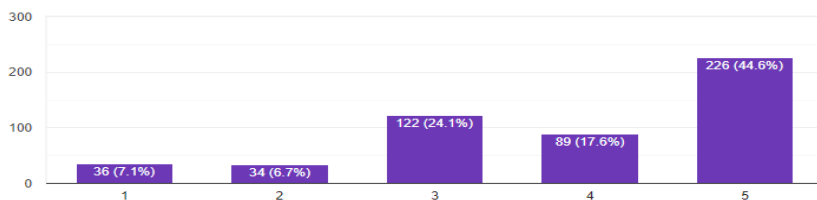
На скала од 1 до 5

Колку сметааш дека е важно постоењето на анти-насилна структура во училиштата како на пример- Неформални врснички клубови */

Në një shkallë nga 1 deri në 5

Sa e rëndësishme mendoni se është të ketë një strukturë kundër dhunës në shkolla si - Klubet joformale të bashkëmoshatarëve *

507 responses



Оттука јасно е дека на учениците треба да им се понуди можност и услови за неформален начин на образование, редовни обуки од областа на неформалното образование и едукација, простор и содржини за нивно ефективно организирање и активирање во насока на унапредување на средината во која живеат и работат.

Преку неформалната едукација, младите ги збогатуваат своите знаења и развиваат вештини кои им помагаат во образовниот процес, како и при остварување на свои граѓански права. Вештините на критичкото размислување, ефективната комуникација и тимската работа кои ги стекнуваат преку неформалната едукација се од клучно значење за нивна партиципација во демократските процеси.

На отвореното прашање – “Која е разликата меѓу http и https? , испитаниците дадоа свои размислувања и одговори. Во прилог наведуваме како цитати само неколку од одговорите:

1. “Sa herë që shkruajmë një adresë interneti ne mund të vërejmë se si para ‘www’ ekziston ose http ose pjesa https. Kjo gjë mund t’jua mos ketë tërhequr vëmendjen tuaj menjëherë, por nganjëherë teksti është HTTP dhe në disa raste është HTTPS, pra cili është dallimi? Nëse shikoni më afër, dalloni se HTTPS ka një ikonë të një dryri pranë tij, që do të thotë hyrja është e kufizuar ose e koduar. / Секогаш кога ќе напишеме интернет адреса, можеме да забележимо како пред „www“ се наоѓа или http или делот https. Можеби ова не ви го привлече вниманието веднаш, но понекогаш текстот е HTTP, а понекогаш е HTTPS, па која е разликата? Ако погледнете подобро, ќе забележите дека HTTPS има икона за катанецдо него, што значи дека пристапот е ограничен или шифриран.”
2. “Нема разлика”
3. “Мислам дека https е побезбедно”
4. “Незнам”

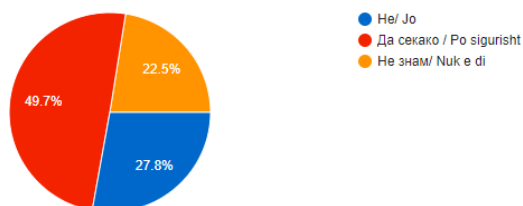
5. "https обезбедува заштита на податоците додека http не"
6. "Незнам, но сакам да знам"
7. "Кога се користи HTTP, сите податоци што се испраќаат се без заштита, а додека пак HTTPS овозможува безбедна, шифрирана комуникација што штити од злоупотреба"
8. "https-znachi deka postoi deka stranica i možeme da ja otvorite a http-ne znam"
9. "Razlicen nacin na sobiranje podatoci"
10. "Навистина не знам што е разликата"
11. "Не знам, но мислам дека https според мене го гледам почесто на веб сајтови, што значи дека мислам тоа е побезбедно од http"

Ако ги разгледаме и анализираме сите одговори на ова отворено прашање на кое учениците даваа свои одговори, можеме да заклучиме дека најголем дел од учениците не ја знааат разликата помеѓу HTTP и HTTPS. И ова секако претставува очекуван резултат. Понатаму, ако ги анализираме одговорите на тие ученици кои одговориле поинаку од "незнам" можеме да видиме дека одговорите се разликуваат во однос на разбирањето и свесноста за разликите помеѓу HTTP и HTTPS. Секако, одреден број на ученици правилно ги идентификуваат разликите додека други изразуваат несигурност или недостаток на знаење. Одговорите што укажуваат на перцепција за HTTPS како побезбедна варијанта се усогласени со заедничкото разбирање на безбедносните карактеристики поврзани со HTTPS. Присуството на одговори од страна на ученици кои изразуваат желба за учење сугерира можност за доедукација на оваа тема. Генерално, анализата на ова отворено прашање укажува на различен опсег на перцепции и нивоа на знаење кај испитаниците.

Дали сметаш дека ти е потребна дополнителна и стручна едукација за Сајбер безбедност?/

A mendon se keni nevojë për arsim shtesë dhe profesional për Sigurinë Kibernetike?

507 responses



Од добиените одговори на прашање за “потребата од доедукација за сајбер безбедност”, може да се заклучи дека, генерално, постои потреба од едуцирање, самите резултати од испитаниците го потврдуваат тоа, каде 49.7% се изјасниле позитивно за потребата од доедукација за сајбер безбедност, 22.5% од испитаниците се изјасниле неутрално околу оваа прашање, додека пак 27.8 % мислат дека нема потреба од ваков вид на доедукација.

Пред сè на самите деца треба да им се пренесе знаење за тоа кој чин се смета за сајбер насилство и сајбер напад, како да го препознаат, како да се справат со тоа и каде да го пријават. Но, истовремено би ја нагласиле и потребата за доедукација на наставниците и стручните служби во училиштата за справување со овој проблем, особено потребата од воведување на нови ефективни мерки и соработка со надлежните институции и родителите и меѓусекторска соработка.

ПРЕПОРАКИ ЗА ПРЕВЕНЦИЈА НА САЈБЕР НАСИЛСТВО И РАЗВОЈ НА САЈБЕР БЕЗБЕДНОСТ ВО ОБРАЗОВНАТА СРЕДИНА

Во денешно време, со развојот на технологијата и дигиталната револуција, користењето на интернетот започнува уште од најрана возраст, во зависност од тоа кој со каква причина ги користи услугите кои ни ги нуди дигиталниот простор.

Според добиените резултати на прашањата од прашалникот, јасно е дека интернет услугите и социјалните мрежи се неизбежен дел од животите и од секојдневниот живот на децата. Дигиталниот простор е реалност која колку и ни да ја олеснува комуникацијата, помага да останеме во контакт со пријателите, семејството, да споделуваме информации, да се забавуваме преку игри и разни други интернет услуги за наши потреби, незнаејќи дека понекогаш може да биде и многу опасна, со можности за предизвикување несакани последици.

Затоа сè повеќе се поставува и прашањето колку е безбеден сајбер просторот, кој покрај позитивните ефекти, како интернет услуги нуди и социјални мрежи кои влијаат на луѓето, посебно на младите кои се најчести корисници на истите и во одредена мерка и “зависници” од социјалните мрежи (самите ученици се изјасниле дека повеќето од нив поминуваат повеќе од 4 часа на интернет и тоа без некоја важна причина).

Ако не се контролираат, ефектите од сајбер насилството и самата зависност од користење на социјалните мрежи, може да доведат до екстремн стрес и депресија, а учениците кои се жртви може да се склони кон негативни неконтролирани однесувања, како резултат на нивните искуства. Но, за да може да се развива личноста во тек со новите дигитални експресији, сепак е потребно да го познава и начинот на кој треба да се заштити и сигурноста во дигиталниот простор, бидејќи за истото постои недостиг на информации, не само кај децата, туку и кај родителите и училиштата, како што покажуваат и самите резултати од нашето истражување.

За таа цел издвојуваме неколку препораки кои ќе го олеснат секојдневното истражување и употреба на Интернетот:

„Младите се тие кои подобро го знаат сајбер просторот, го чувствуваат како нивен, и затоа врсничката едукација и солидарност се клучни за справување со онлајн насилството”- ова е еден од главните заклучоци од дискусијата на тема: „Сајбер насилство – безбедност и самоцензура”²³

- » Ако се има предвид горенаведениот заклучок, многу е важно и потребно да се развие свеста кај децата и младите дека во виртуелниот свет постојат правила, обврски, барања, граници, дека одговорноста и претпазливоста се исто толку важни колку и во реалниот свет. Нашите деца седат до нас дома или се на училиште, но сепак се изложени на ризици во виртуелниот свет полн со непознаници и предизвици како никогаш досега. Децата и младите се технички повешти и поупатени од нас, но имаат потреба од искуството на возрасните за да бидат заштитени и одговорни во виртуелниот свет, да имаат различни бенефити од дигиталната ера и да можат соодветно да се соочат со голем број на предизвици кои им престојат. Затоа е потребна едукација на учениците и секако доедукација на возрасните за свеста околу ризиците во сајбер просторот.
- » Бидејќи децата што доживеале сајбер насилство полесно се обраќаат за помош на своите врсници, неопходно е да се спроведе врсничка едукација на училиште, да се организираат тимови од едукатори врсници или онлајн советување за млади луѓе кои биле жртви на сајбер насилство.
- » Училиштето исто така треба да обезбеди стратегии, техники и начини за пријавување на било каков вид на насилство, и тоа: поставување на сандачиња во просториите на училиштето каде што децата сведоци ќе можат анонимно да пријават случаи на насилство, поставување на линк на интернет страна каде што децата ќе имаат пристап да пријават насилство, и др.
- » Ученици треба да бидат правилно информирани и едуцирани да не бидат учесници или пасивни набљудувачи во актот на врсничкото насилство (сведоци на сајбер напад). Неопходно е учениците да се поттикнат во вакви ситуации да се обратат за помош и поддршка до возрасните, блиските луѓе од доверба, стручните соработници и наставниците во училиштето.
- » Еден од начините за превенција или справување со сајбер насилство или сајбер напад е и воспоставување на посилна врска меѓу родителите/старателите и училиштето, преку почести ефикасни активности и работа со учениците, со што ќе се постигне благовремена мобилизација која ќе влијае превентивно, односно организирање на неформални работилници или пак некој вид на кампањи кои ќе имаат за цел информираност на родителите за предизвиците и ризите на сајбер просторот.

²³ „Сајбер насилство – безбедност и самоцензура”, која се одржа во социјалниот клуб Комитет, во организација на Хелсиншкиот комитет за човекови права

- » Исто така во училишните простории пожелно е да бидат истакнати испечатени постери со некои „стандардни“ мерки за заштита и безбедност во сајбер просторот.
- » Реализирање на дополнителни обуки за стекнување на вештини кои им се потребни на наставниците и стручните служби за да можат да применуваат различни пристапи со кои би ја унапредиле климата и комуникацијата во паралелките за време на часовите.

ПРАКТИЧНИ СОВЕТИ ЗА БЕЗБЕДНОСТ ВО ДИГИТАЛНИОТ ПРОСТОР

43

- » Треба да бидете многу внимателни со своите лични информации и дигитален идентитет;
- » Креирајте и користете посложени лозинки (комбинација на Голема буква, мала буква, бројка и знакови;
- » Двапати размислете и проверете ги линковите пред да кликнете;
- » Грижете се за тоа да користете безбедни WI-FI мрежи;
- » Користете VPN;
- » Не заборавате да користете сајтови кои почнуваат со <https://>;
- » Исклучете го вашиот Блутут (Bluetooth), ако немате потреба од истиот;
- » Користете антивирус и антимаљвер софтвер и истите ажурирајте ги почесто;
- » Направете (резервни копии) на вашите податоци (Backup);
- » Внимавајте каква содржина споделувате - избегнувајте објавување лични и доверливи информации, како што се: адреса на е-пошта, телефонски број, адреса на живеење, броеви на картички, пинови, лозинки, и слично.
- » Избегнувајте пополнување на формулари со барање на вашите лични податоци, бидејќи тие често се поддржани од злонамерни корисници кои можат да ги злоупотребат вашите информации.
- » Користете ја опцијата за ограничување на прикажувањето на содржината што ја гледате или објавувате, истата да биде видлива само на доверливи пријатели на социјалните мрежи.

ПРАКТИЧНИ ПРЕПОРАКИ И СОВЕТИ ЗА РОДИТЕЛИТЕ ЗА БЕЗБЕДНОСТ ВО САЈБЕР ПРОСТОР

Како треба да се однесувате со Вашето дете да ги ограничите ризиците во сајбер просторот и да бидете во тек со каква било злоупотреба или сајбер напад, имаме наведено неколку корисни препораки и совети за вас родители.

- » Разговарајте заедно со децата и објаснете ги Вашите правила и очекувања доколку му обезбедите на вашето дете дигитален уред.
- » Договорете се за тоа што е прифатливо да се објавува и испраќа и за истото детето да се консултира со вас како родител.
- » За постарите деца, пожелно е да користите примери од реалниот живот од вестите што ги илустрираат ризиците, опасностите и правните прашања.
- » Ако сакате Вашето дете да Ви верува и да ги сподели работите со Вас, било тоа да се непријатни или не, па дури и надвор од Вашите етички принципи, треба да бидете подготвени да го сослушате и да го поддржите, без да го осудувате.
- » Погрижете се Вашите деца да не прифаќаат непознати корисници како „пријатели“.
- » Проверувајте почесто како Вашето дете комуницира со технологијата: дали го прави тоа на начин така што се менува неговото однесување кога ќе влезете во собата? Дали го исклучува компјутерот и сл.
- » Одржувајте ги највисоките поставки за приватност на сите уреди и платформи.
- » Редовно проверувајте ги тие поставки бидејќи понекогаш сами се ресетираат кога платформите вршат ажурирања или ги менуваат условите за користење.
- » Научете ги Вашите деца сериозно да размислат пред да објават или споделат било што на интернет.

- » Погрижете се Вашето дете да знае дека секогаш може да дојде и да разговара со Вас за сè што се случува, дека вие како родител нема да го осудите.
- » Пријавете кривично дело во полиција или Јавно обвинителство.
- » Кривично дело може да се пријави во најблиската полициска станица, преку телефонот 192 или до Одделението за компјутерски криминал при Министерството за внатрешни работи, на е-пошта на cybercrime@moi.gov.mk или на страната „Црвено Копче“.

КОРИСТЕНА ЛИТЕРАТУРА:

1. Computers in Human Behavior 29(6):2703-2711, Journal Review: Cyberbullying myths and realities, November 2013, authors R.A. Sabelle, J. W. Patchin and S. Hinduja
2. Hinduja, S., & Patchin, J. W. (2018). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Corwin Press. Hinduja, S., & Patchin, J. W. (2015). Bullying, Cyberbullying, and Suicide. Archives of Suicide Research
3. The State of Online Harassment, January 2021, Pew Research Center, available at: <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>
4. "Teens and Technology 2013", ,Pew Research Center
5. "Children in a Digital World" (2017), UNICEF
6. Статистички извешетaj, 2022, достапно на: https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf <https://mladietv.mk/wp-content/uploads/2022/10/Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf>
7. Сајбер хигиена за деца“ (2018): ENISA
8. “Cyber Aware Teacher Survey Report” (2020), NCSC
9. <https://www.ojp.gov/pdffiles1/ojdp/grants/217918.pdf>
10. <https://mkd-cirt.mk/wp-content/uploads/2021/03/VtoraBroshuraPrint.pdf>
11. Прирачник за справување со кибер насилство, Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf
12. <https://akademik.mk/sajber-nasilstvoto-e-prodolzhenie-na-nasilstvo-to-vo-fizichkiot-prostor/>
13. <https://medium.edu.mk/aktiviraj-se/socijalni-mrezi-mladite-zarobeni-vo-lazniot-svet-na-influenserite/>
14. <https://goce.mk/zhivotot-na-sociz%D1%98alnite-mrezhi-i-zhivotot-izgubeni-vo-prevodot/>
15. file:///C:/Users/Elsa/Downloads/Vodich_za_sajber_bezbednost_PRINT%20(1).pdf
16. https://www.dcaf.ch/sites/default/files/publications/documents/Guide-bookCyberThreats_MK_web_Jan2023.pdf
17. <https://alobushavko.mk/mk/parents/110-soveti-za-digitalno-roditelstvo>
18. <https://worldbeyondwar.org/mk/types-of-violence/>

Автори: Овој Прирачник е изготвен од Гиљман Османи Муслији,
истражувач од Аналитика тинк тенк.

Овој Прирачник е изработен во рамки на проектот „ Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyberbullying”, што го спроведува Аналитика Скопје, со финансиска поддршка на Амбасадата на Канада за Србија, Црна Гора и Северна Македонија. Содржината на овој Прирачник е единствена одговорност на Аналитика Скопје и на ниту еден начин не може да се смета дека ги одразува ставовите на Амбасадата на Канада за Србија, Северна Македонија и Црна Гора

