Прирачник за развој на култура на сајбер безбедност во образовниот систем на Северна Македонија

FOUNDATION ФОНДАЦИЈА
OPEN ОТВОРЕНО
SOCIETY ОПШТЕСТВО
MACEDONIA МАКЕДОНИЈА

Прирачник за развој на култура на сајбер безбедност во образовниот систем на Северна Македонија

Автор: Ана Дионисиева

Аналитика тинк тенк

Декември 2023 година

CONTENTS

ЦЕЛ НА ПРИРАЧНИКОТ

Прирачникот е наменет за широка група на чинители во Северна Македонија кои работат на полето на сајбер безбедност на учениците, превенција на сајбер насилство на учениците, дигитализација и образовни политики, за да се информираат за повеќедимензионалните аспекти на сајбер безбедноста. Целта на овој прирачник е да ги обезбеди наставниците и младите луѓе во училиштата во Северна Македонија со средства и ресурси за подобрување на своите капацитети во областа на сајбер безбедност и противоставување на сајбер насилство. Преку различни модули и активности, Прирачникот има за цел да ги зголеми знаењата и вештините на учесниците за безбедно користење на интернет и други дигитални технологии. Воедно, тој се стреми кон развивање на ефективни училишни програми за превенција на сајбер-насилство и создавање на безбедно училишно околина.

Со брзиот развој на информатичката технологија и социјалните мрежи, информациите стануваат подостапни, се олеснува комуникацијата, а луѓето споделуваат многу фотографии и видеа, кои во иднина може да бидат злоупотребени. Според податоците на Државниот завод за статистика во Северна Македонија[1], заклучно со 2022 година, 86,6% од домаќинствата имале пристап до интернет дома. Според спецификацијата на населението по возрасни категории, младите на возраст од 15 до 24 години користат интернет 100%, и 100% од нив го користат интернетот неколку пати во текот на денот. Најчести интернет активности на младите се учество во социјални мрежи (креирање корниснички профил, испраќање пораки или други прилози на Фејсбук, Твитер итн.) со 93.1% и користење на инстант-пораки, т.е. размена на пораки, на пример, преку Skype, Messenger, WhatsApp, Viber секој ден или речиси секој ден со 95,5%. Ова е значително поголем интензитетна користење на интернет во споредба со другите возрасни групи. Високиот процент на млади корисници на интернет сами по себе носи ризик од постоење на потенцијални жртви на дигитални закани. Социјалните медиуми се глобална мрежа преку која се разменуваат голем број лични информации за интеракција со членовите на заедницата. Од една страна, ова го олеснува комуницирањето на

1 ИНФОРМАТИЧКО ОПШТЕСТВО - INFORMATION SOCIETY СООПШТЕНИЕ - NEWS RELEASE Користење на информатичко-комуникациски технологии во домаќинствата и кај поединците, 2022, Државен Завод за Статистика, достапно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf

денешното модерно време каде информациите стануваат слободно достапни, но истовремено создава голем простор во кој се одвива електронска размена на податоци - сајбер просторот. Во овој простор, електронските податоци можат да бидат злоупотребени.

Социјалните медиуми воведоа нови облици на однесување, со зголемена динамика на споделување лични информации, како што се фотографии, видеа, локации и други. Овие активности доведуваат до зголемен ризик и закана за корисниците на социјалните мрежи. Преку социјалните медиуми, текстуални пораки, апликации или интернет, луѓето можат да бидат изложени на сајбер-булинг во форма на споделување на негативни, штетни, лажни и злобни содржини контент. Сепак, важно е да се постави прашањето дали имаме соодветен образовен систем што активно го поддржува безбедното користење на интернет, особено во контекстот на креирање лични содржини, употреба на социјални медиуми и медиумска писменост кај младите корисници.

Оттука, Прирачникот служи како кориснички, лесен за читање водич за клучните аспекти на сајбер безбедност кај младите и превенција на сајбер булинг во учиштата со препораки за за идни мерки и политики. Има за цел да ја стави сајбер безбедноста на младите на агендата бидејќи тоа е едно од клучните прашања со кое во моментов се соочуваат младите од Северна Македонија, и чија важност дополнително ќе се зголемува

Прирачникот беше изработен како дел од проектот «Развој на култура на сајбер безбедност во образовниот систем на Северна Македонија - Зајакнување на капацитетот на младите луѓе и наставниците за примена на мерки за сајбер безбедност и развој на ефективни училишни програми за спречување на сајбер-насилство», реализиран од Аналитика во периодот од август 2023 година заклучно со февруари 2024 година.

МЕТОДОЛОГИЈА

Прирачникот вклучува примена на метод на истражување, метод на фокус група од спроведена обука и метод на синтеза на информации. Првично, истражувањето и анализата се базира на идентификација на ученици и наставен кадар, со фокус на нивното разбирање и примена на мерките за сајбер безбедност.

Во истражувањето, беа вклучени истражувачки методи како анкетирање, со анкетен прашалник од 25 прашања, кои беа дизајнирани од страна на аналитички експерти (информатичар и професор во училиште). Истражувањето беше спроведено во три средни училишта во Скопје, со учество на 313 испитаници. Примарните податоците добиени од истражувањето се однесуваат на постоечката состојба во училиштата и служат како основа за формулирање на препораки и заклучоци.

Прашалникот разгледува различни аспекти на дигитализација, користење на социјални медиуми, сајбер безбедност како и личните искуства на младите ученици со сајбер булинг и справување со истото. Учениците исто така беа прашани да ги оценат вклученоста на училиштата, наставниот кадар и родителите во справувањето со сајбер насилството и мерките кои се превземаат од страна на училиштата за зголемување на сајбер бездноста на учениците. Вредноста на знаењето и учеството на учениците е клучно за да се оцени моменталната состојба во училиштата во однос на сајбер безбедноста и да се дада препораки за дејствување во иднина. Резултатите од истражувањето не се репрезентативни, туку нудат длабинско разбирање на искуствата на учениците во врска со сајбер безбедноста и сајбер булингот.

Секундарните податоци во овој прирачник се извештаи и друга литература за сајбер безбедност во Северна Македонија. Прирачникот се служи и со статистички податоци, анализи на политики и медиумски извори.

ЗА ПРОЕКТОТ

Проектот,,Зајакнување на капацитетот на младите луѓе и наставниците за примена на мерките за сајбер безбедност и развој на ефективни училишни програми за спречување на сајбер-насилство›› е финансиран од Фондацијата ,,Отворено општество» Македонија. Општата цел на проектот е запознавање на младите со придобивките од дигиталната трансформација и зголемување на употребата на мерките за сајбер безбедност кај младите со што ќе се зголеми нивното безбедно присуство на Интернет и ќе се намалат негативните ефекти.

Прирачникот е дел од од проектот. Специфични цели на проектот се: идентификување на учениците и наставниот кадар од дигиталната трансформација на општеството со фокус на образовните програми и степенот на примена на мерките за сајбер безбедност од страна на младите, подобрување на соработката и трансферот на знаење помеѓу граѓански организации ,образовните институции и институциите надлежни за креирање на политики од областа на сајбер безбедност и институциите надлежни за санкционирање на сајбер криминалот,зголемување на улогата на локалните граѓански организации во обезбедување на помош поддршка на образовните институции и младите за подобро користење на потенцијалот на информатичко-комуникациските технологии.

Целта на ова истражување и оттука Прирачник е да се прикаже колкав е капацитетот на младите во справувањето со различни видови на сајбер напади, контруктивното користење на интернетот и комуникациските технологии , како и да даде препораки за пронаоѓање на механизми кои би придонеле за зајакнување на вештините кај ученицитеи наставниците за безбедно користење на интернот преку нивна едукација.Заклучоците и препораките од ова истражување ќе треба да влијаат на релевантните инситуции за понатамошно спроведување на активностите и мерките. Проектот е имплементиран во три средни училишта на град Скопје со цел да се применат активности кои ќе ги зајакнат вештините кај младите преку содржини за сајбер безбедност.

ПРЕГЛЕД НА ЛИТЕРАТУРА

Со ширењето на дигиталната трансформација, академската и стручната литература во областа на сајбер безбедност и насилство кај младите се развива како значаен извор на знаење. Специфичната природа на интернетот и дигиталните платформи предизвикуваат многу предизвици и шанси, а истражувачката литература игра клучна улога во раскривање на овие аспекти.

Истражувањата од светски експерти, како што е работата на Livingstone и Görzig (2017)[2], се фокусираат на различните аспекти на сајбер безбедност и насилство меѓу младите. Студиите на случај од Норвешка, Финска, и Холандија прикажуваат дека интернетот често се користи за сајбер насилство, а литературата предлага препораки за подобрување на безбедноста на младите во дигиталното опкружување.

Во Европа, истражувањата како тоа на Kowalski et al. (2014)[3]се обидуваат да го идентификуваат обемот и карактерот на сајбер насилството кај младите. Тие го анализираат влијанието на социјалните мрежи, форумите и онлајн игрите врз младите и нудат мерки за развивање на стратегии за превенција.

Во македонскиот контекст, наодите од извештајот[4]"Baseline assessment for awareness raising and capacity buildin" меѓудругото истакнуваат дека свеста на учениците за сајбер-безбедносни закани треба дополнително да се зајакне, имајќи предвид дека 40% од студентите сметаат дека се ранливи додека се на интернет, од кои повеќе од 13% самите имале некакво лошо лично искуство. Ова пренесува важни информации за состојбата на сајбер безбедноста во училишта во Македонија.

2 Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective January 2012, DOI: 10.1332/policypress/9781847428837.003.0012, Publisher: Policy PressISBN: 1847428827

3 Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth Robin M Kowalski 1, Gary W Giumetti 2, Amber N Schroeder 3, Micah R Lattanner 4, Affiliations expand PMID: 24512111 DOI: 10.1037/a0035618

4 RESEARCH REPORT Baseline assessment for awareness raising and capacity building, CRPM

ВОВЕД

Развојот на дигиталната технологија и неограниченот пристап кон Интернетот ја зголемија загрижеността за сајбер безбедноста на младите во Сајбер просторот. Уште од мала возраст учениците се изложени на сајбер напади. Младите претставуваат многу ранлива категорија бидејќи континуирано го користат сајбер просторот со ограничени вештини за рабирање на сајбер заканите и воедно превземање на заштитни мерки.

Сајбер насилството,онлајн измамите и сајбер нападите значително се зголемени поради недостаток на свест кај младите и потребен механизам за заштита од овие негативни влијанија.Нивото на свесност кај корисниците е сеуште умерено.Како значителна мерка која може да се превзме е едукацијата на младите во училиштата.Попрецизно, младите треба да се едуцираат како да го користат безбедно интернетот и како да се заштитат.

Голем број на информации и дезинформаци кои кружат во сајбер просторот се потентицијални сајбер закани за учениците.Училиштата потребно е да обезбедат наставницикои ќе бидат обучени и ќе промовираат критички притап кон сајбер безбедноста.Исто така, преку соработка со родителите и нивна едукација ќе се промовира безбедно користење на Интернетот.

Еден од поголемите предизвици со кои се соочуваат училиштата е недосаток на експерти,финансии и ресурси со цел да се спроведе сајбер безбедноста во образованието. Брзината на технолошките промени бара поголеми технолошки вештини кај наставниците со цел да се подобри едукацијата кај младите.

Вклучувањето на теми од сајбер безбедност во годишните програми ќе има значителна улога во подигањето на свеста кај младите со цел да се намалат сајбер инцидентите и нападите.Зада се биде безбеден на интернет потребно е соодветно поставување на училишни активности во врска со онлајн можностите и ризиците,штетите и заканите на Интернет преку едукација за правилно користење на дигиталните технологии и едукација за безбедност на Интернет.

ВИДОВИ НА САЈБЕР НАПАДИ

Користењето на компјутери, таблети, интернет и други технологии станаа дел од секојдневието. Секојдневно младите користат различни сервиси за комуникацијакако што се Facebook,Snapchat,Viber и др. Голем дел од нив не се свесни за ризиците кои постојат по нивната сајбер безбедност.

Речиси 70% од децата и адолесентите ширум светот биле изложени на сајбер ризици во 2023 година. Сајбер ризиците варираат во зависност од возраста, исто така голем дел од учениците се изложени на ризична содржина ,контакт и малтретирање со прекумерното користење на технологија.[5]

Сајбер нападот е дефиниран како непријателска активност со цел да се украдат,изложат оневозможат,уништат податоци препу неовластен пристап на компјутерскиот систем или дигиталниот уред.Сајбер нападите најчесто се насочени кон индивидуалци комапнии и институции користејќи интернет, мобилни и компјутерски технологии.

Најчесто се користат платформи како што се социјалните мрежи,веб страниците, електронските пошти за да се извршат сајбер нападите. Хакерите исто така користат вештачка интелигенција за да прикријат малициозен код кој е програмиран да се изврши подоцна и да се создадат програми за малициозен софтвер што можат соодветно да се приспособат за време на напад. Младите претставуваат ранлива категорија изложена на различни видови на напади.

Сајбер нападите може да се искористат и да се извршат на повеке начини. Целта е да се добие неограничен пристап до одредени информации на корисникот.

Најчести сајбер напади врз младите се :

- Cyber grooming
- Phishing
- Cyber bullying
- Social Engineering
- Online Gaming
- Ransomware

5 Almost 70% of children & adolescents have been exposed to cyber risks:Security magazine,достапно на www.securitymagazine.com/articles/100099-almost-70-of-children-and-adolescents-have-been-exposed-to-cyber-risks

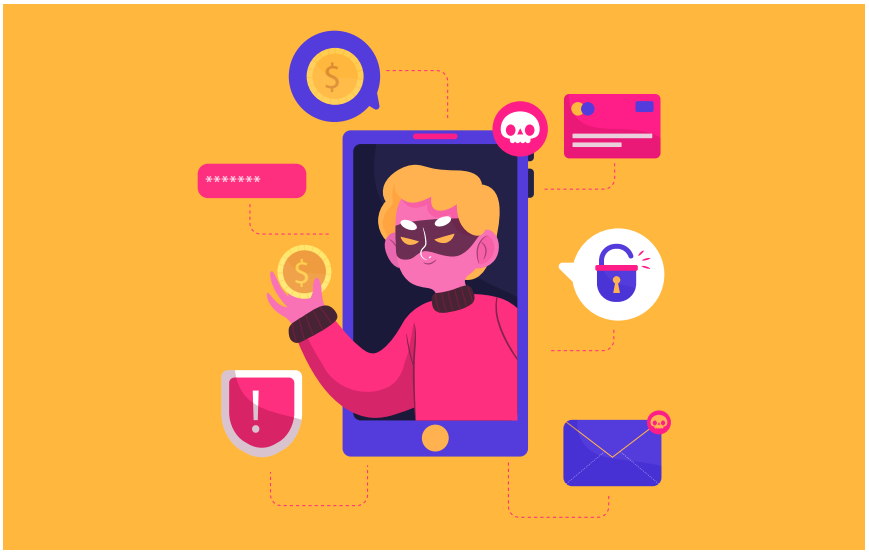
Cyber grooming

Cyber grooming е една од најрастечките закани со кои се соочуваат децата и адолесцентите.Во овој процес cyber groomer се обидува да стекне доверба кај младите за да воспостави емотивна врска преку социјалните мрежи со цел да се врши сексуално вознемирување или експлотација.Главните цели на cyber grooming се:добивање на лични податоци (честопати експлицитни слики ,видеа и разговори) со цел да се упати закана и уцена кон индивидуата.[6]

Преку креирање на лажен акаунт,cyber groomerot се претставува како дете кој комуницира преку социјалните мрежи,емаил,чат соби и инстант пораки.

Најголема таргет група за cyber groomerot се адолесцентите бидејќи во тој период голем дел од нив се соочуваат со физички промени. Љубопитноста на младите ја зголемува нивната онлајн активност и ги прави ранливи за cyber grooming. Самиот процес на cyber grooming може да влијае негативно врз жртвата и да остане долгорочно.Покрај тоа што ученикот се чуствува навредено и изневерено, жртвата се чувствува дека заслужено е злоупотребен што доведува до ниска самодоверба и самообвинување.

Од клучно значење е подигање на свеста како и законски мерки за спречување на ваков вид на напад. Овој вид на напад е влез за понатамошна експлотација на децата.



https://www. freepik.com/free-vector/hacker-activity-illustrated-concept_8088561.htm#page=9&query=cyber%20grooming&position=21&from_view=search&track=ais&uuid=5fd5f6ee-7839-45ca-b515-b068d8bf963c

6 What is cyber grooming?:HackerNoon,достапно на: www.hackernoon.com/what-is-cyber-grooming

Phishing

Повеќето сајбер напади почнуваат со фишинг (phishing – риболов) е-пошта. Фишинг е вид на социјален инженеринг во кој сајбер криминалците ќе ја измамат жртвата да им даде чувствителни информации или да инсталира малициозен софтвер. [7]

Фишингот е заоснован на малициозен софтвер кој претставува стандарден начин за незаконско стекнување на чуствителни податоци. Кај младите многу контакти со фишингот се остварени преку социјалните мрежи и паметните телефони.

И покрај тоа што техничките мерки за безбедност стануваат сè подобри, фишингот останува еден од најевтините и најлесните начини сајбер криминалците да добијат пристап до чувствителни и лични информации.Ако корисниците кликнат на линк, нивната безбедност може да биде загрозена и да станат жртви на кражба на идентитет. Со еден клик корисниците исто така можат да ги компромитираат своите лични информации, најави како што се кориснички имиња и лозинки и финансиски информации како што се броеви на кредитни картички.

Напаѓачите често го постигнуваат ова со малициозна е-пошта која делува како да е од извор од доверба, но понекогаш користат и други методи.Постојат неколку причини поради кои “риболовците”сакаат нелегитимен пристап до сметката на младите на Фејсбук или друга мрежа а тоа се:[8]

- Ширење малициозен софтвер
- Отварање на небезбедни хиперврски
- Спам
- Собирање на информаци и податоци од најблиските

Phishing scams – publishing is vulnerable too. What you need to know - Science & research news | Frontiers (frontiersin.org)

7 What Is Phishing? A Brief Guide to Recognizing and Combating Phishing Attacks, www.comptia.org/content/articles/what-is-phishing

8 Phishing Attacks Targeting Young Adults: December 15, 2017 by Daniel Brecht, достапно на: www.resources. infosecinstitute.com/topics/phishing/phishing-attacks-targeting-young-adults/

Cyber bullying

Сајбер булингот е една од најчестите сајбер закани со кои се соочуваат младите.Сајбер малтретирањето се случува на интернет онлајн или преку користење на мобилни телефони. Овој вид на сајбер напад вклучува заканувачки или навредливи зборови испратени или објавени на Интернет до или за некоја личност. Сајбер булингот се јавува преку различни форми:[9]

- Објавување или испраќање на засрамувачи закани преку текстуални пораки
- Поттикнување на континуирано малтретирање
- Испраќање или објавување на негативни,лоши или засрамувачки фотографии (кои или се вистински или се фотошопирани)
- Крадење на корисничко име и лозинка или мобилен телефон , за подоцна да се имитира поединецот со цел да се наруши неговиот углед
- Снимање на телефонски разговори тајно, а потоа нивно онлајн објавување
- Последиците од сајбер булингот кај младите се колективни.Тие може да влијаат на нивното ментално,физичко и психичко здравје со секојдневно манифестирање.

Cyberbullying Information for Parents | How You Can Help | Kids Helpline

9 Cyberbullying behind fronteers:Deviant Behaviors and Intercultural Factors in Digital Communications:Gulia Mura www.academia.edu/1298055/Cyberbullying_behind_fronteers_deviant_behaviours_and_intecultural_factors_in_digital_communication

Социјален инженеринг

За младите голем број на онлајн сервиси се интересни несвесно користејќи ги стануваат ранливи на онлајн ризиците.Желбата да се стекнат нови пријатели,споделувањето лични информации со другите ги прави лесна мета за онлајн напади од социјален инженеринг.

Социјалниот инженеринг се користи да се доведат во заблуда или манипулираат метите, со цел добивање на информации или пристап до нивните компјутери. Сајбер криминалците го користат пристапот преку социјалните мрежи да ги скријат своите прави идентитети и мотиви и се претставуваат како лица од доверба. Тоа се врши со мамење на корисникот да кликне малициозен линк или преку добивање на физички пристап до компјутерот со измама.[10]

Младите не се секогаш свесни за ризиците со симнување или преземање на датотеки од непознати извори. Колку повеќе информации споделуваме толку е поголема шансата да бидеме жртва на социјален инженеринг.

https://cheapsslsecurity.com/blog/social-engineering-attacks-and-prevention-methods/

10 Прирачник за сајбер закани: идентификација и борба против ризиците за корисниците во јавниот и приватниот сектор и граѓаните:Александар Братиќ,Октомври 2022,Geneva Centre, For Security Sector Governance достапно на : www.dcaf.ch/sites/default/files/publications/documents/GuidebookCyberThreats_MK_web_Jan2023.pdf

Online gaming

Онлајн играњето преставува забава за младите. Еден од начините за поврзување и интеракција со другите. Многу играат игри без разлика дали се на конзоли за игри, компјутери или мобилни уреди. Гејминг заедницата станува се поголема и со тоа и се зголемуваат онлајн измамите, сајбер булингот и споделувањето на несоодветна содржина.[11]

Онлајн игрите преставуваат безбедносен ризик за децата и младите. Некои од ризиците се:

- Изложеност на несоодветна содржина која може да пропуштена од софтверот за родителска контрола и филтрирање на податоците
- Изложеност на проблематична содржина како што е насилство,сексуална содржина или несоодветно однесување од страна на други играчи
- Сајбер малтретирање и вознемирување преку онлајн игри или пораки во чет соби кои можат да бидат анонимни и таргетирани
- Намамување преку Интернет.Познато е дека поединци се злонамерни и честопати користат популарни игри со повеќе играчи за поврзување со деца/млади со цел да се започне разговор или видео преку играта

Со опсегот на игри кои се достапни онлајн и можноста да се игра со други играчи глобално може да е интересно но исто така и ризично. Затоа потребно е младите да знаат како да се заштитат во одредени ситуации.

https: //www. internetsafetystatistics.com/risks-online-gaming/

11 Cyber security issues in online games: RESEARCH ARTICLE | APRIL 18 2017: IP Conf. Proc. 1955, 040015 (2018) Chen Zhao

Ransomware

Ransomware е вид на злонамерен код кој ги шифрира податоците на компјутерот на жртвата и бара паричен откуп за да го дешифрира. Популарноста на овој вид на малициозни програми се зголеми од крајот на 2013 година поради појавата на криптовалути со кои се го олесни плаќањето на откупот, односно го отежна следењето на напаѓачите. Ransomware работи со шифрирање на податоците на жртвата. Жртвата ќе може да ги дешифрира податоците само доколку добие пристап до користениот клуч за шифрирање, кој е во сопственост на напаѓачот. Откако ќе го плати откупот, напаѓачот треба да и го достави на жртвата клучот, што често не е така, па под знак прашалник е дали воопшто има смисла да се плати откупот. Ransomware најчесто се шири преку тројанските коњи кои по инсталацијата вршат шифрирање и печатење на пораки во заклучени податоци и инструкции до корисниците за да го плати откупот.

Некои од врстите на ransomware го блокираат компјутерот со појавување на уценувачка порака. Другиот начин е шифрирање на датотеки. Во замена за дешифрирање на податоците се бара плаќање на пари.

https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021

РЕЗУЛТАТИ ОД ИСТРАЖУВАЊЕТО

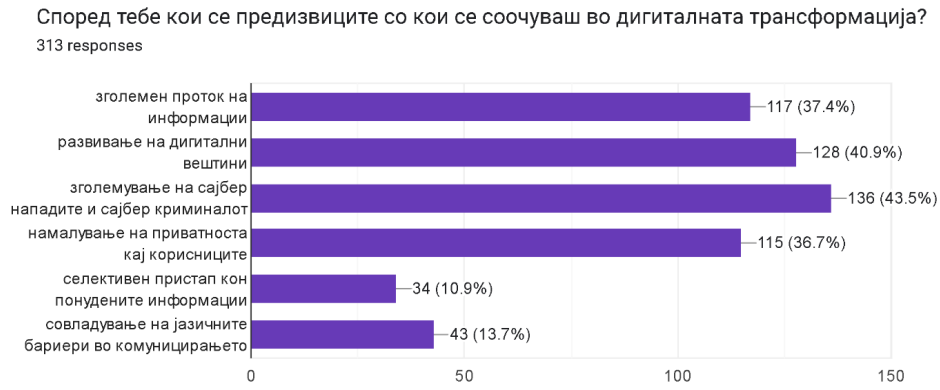
Податоците од истражувањето се однесуваат на постоечката состојба во училиштата и нивната улога во едуцирањето на младите за Безбедно користење на Интернетот.Ова истражување прави анализа за дигиталната трансформација, примената на методите и механизмите за сајбер безбедност кај младите преку идентификација на различните видови на сајбер напади, начини за заштита од сајбер нападите,информираноста на младите за опасностите во сајбер нападите

Со истражувањето беа опфатени вкупно 313 испитаници од средните училишта СУГС Гимназија„Никола Карев”,СУГС„Георги Димитиров”и СУГС„Шаип Јусуф”. Инструментот кој беше применет за истражувањето е анкетен прашалник со 25 прашања дизајнирани од аналитички експерт.

Анкетирањето беше спроведено во период од месец Август 2023 година,на репрезентативен примерок од 313 испитаници,ученици на средни училишта во град Скопје

Анкетирањето е појдовната точка за моменталната примена на механизми и методи за спроведување на сајбер безбедност кај младите во средните училишта како ја доживуваат дигиталната трансформација,-дали може да откријат сајбер напад,како се справуваат со сајбер напади и колку се информирани за опасностите кои постојат во сајбер просторот,се прашањата на кои беше потребно да добиеме одговор.

На прашањето Што преставува дигитализација? - 42,5% од младите се изјасниле дека за нив дигитализација претставува употреба на дигиталните технологи во сите процеси од општеството, 37,7% ја доживуваат дигитализацијата како претварање на информациите од физички формат во дигитален формат, додека 11,5% ги сметаат Интернет објавите како дигитализација. Дигиталните технологи обезбедија голем број на можности за вклучување на популацијата во сите сфери на дигитализација на општеството. Оттука, можеме да заклучиме дека младите ја разбираат дигитализацијата бидејќи голем дел од нив се вклучени во нејзините процеси во обликување на дигиталната ера.



Анализата од истражувањето покажа дека 136 од испитаниците сметаат дека најголем предизвик за нив во дигиталната трансформација се зачестените Сајбер напади .Веднаш зад нив е можноста за развивање на дигиталните вештини кај младите , зголемениот проток на информаци и намалување на приватноста. Новите технологии придонесуваат за континуирано појавување на нови ранливости, а со тоа и нови закани по приватноста, доверливите материјали и достапноста на сервисите. Од она што можеме да видиме е дека најголемиот предизвик за нив се сајбер нападите. Очигледно е дека потребна е поголема безбедност и наоѓање на начини за справување со предизвиците.

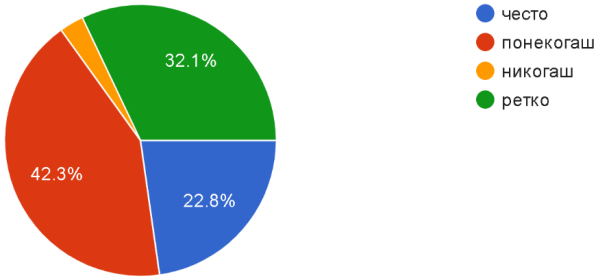
Од повеќето понудени можности кои ги нуди дигиталната трансформација, 181 испитаници го одбрале брзиот пристап до информациите, 146 новите начини на учење, 115 се одлучиле за користење на различни технологии, додека само 68 испитаници ја одбрале можноста за размена на искуства во онлајн заедницита. Интернетот е јавен глобален простор кој го користат милјарди луѓе со широк спектар на информации и оттука може да ја согледаме и поголемата бројка на испитаници кој ја согледуваат дигитализацијата за креирање, споделување и пронаоѓање на информации. Дигитализацијата ги отстранува сите географски бариери, поттикнувајќи глобално учење. Новите методи на учење преку онлајн платформи, онлајн работилници се можности кои ги користат младите со цел да стекнат некои нови дигитални вештини.

54% од вкупниот број на испитаници делумно знаат каква е дигитализацијата во образованиот процес, додека 33,9% не знаат за дигитализацијата во образовниот процес.

Еден од најголемите предизвици со кои се соочува денешното образование е неговата дигитализација. Дигитализација не го вклучува само користењето на компјутерите и Интернетот туку и пронаоѓање на вистинските информации нивно филтрирање и обработување. Од овој наод можеме да забележиме дека голем е процентот на учениците кои не знаат каква е дигитализацијата во образовниот процес, со тоа можеме да кажеме дека секој од учениците има различна технолошка способност од која зависи неговата имплементација во дигиталниот процес.

Колку често во редовната настава ги користите дигиталните алатки?

312 responses



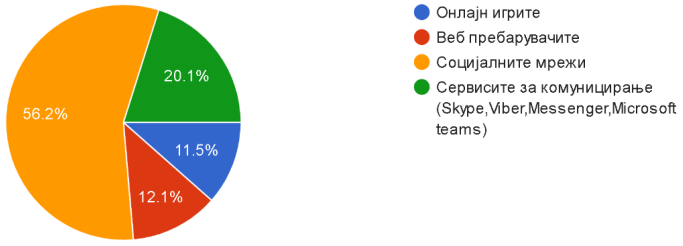
На прашањето: Колку често во редовната настава користите дигитални алатки? - 42,3 % од учениците се изјасниле дека понекогаш ги користат дигиталните алатки,32,1 % ретко ги користат дигиталните алатки .

Од ова можеме да заклучиме дека потребно на учениците да им се овозможи пристап кон дигиталното учење, со што се очекува зголемено знаење и вештини како од областа на предметите кои што ги изучуваат така и од областа на информатичките технологии и сајбер безбедноста при користењето на алатките. Дигиталните содржини треба да бидат мултимедијални, односно да содржат текст, анимација, звук и презентација. Дигиталната наставна содржина треба да биде достапна во училиштата за време на наставата и да биде присутна надвор од наставата во домовите на учениците.

Овој наод може да демонстрира дека поретко се користат дигиталните алатки за време на наставата. Еден од факторите може да е и малиот број на дигитални уреди со кои училиштето располага или недоволно застапеност на е-содржини во наставните програми.

Кои од услугите кои ги нуди Сајбер просторот најчесто ги користиш?

313 responses



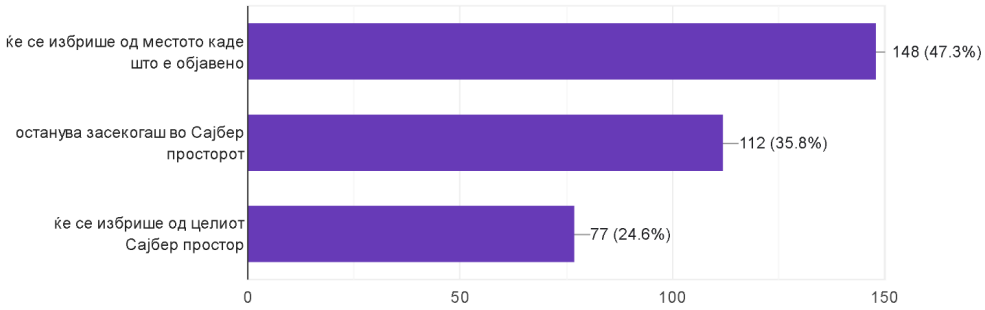
На прашањето Кои од услугите кои ги нуди Сајберот просторот најчесто ги користиш? - 56,2% се изјасниле дека ги користат социјалните мрежи. Голем дел од младата популација се корисници на социјалните мрежи Tic Tok, Instagram, SnapChat и Facebook. Јасно е дека сами по себе се подложни на закани во сајбер просторот. Овој наод прикажува дека социјалните мрежи имаат лесен и отворен пристап за корисниците. Во голем дел на овие платформи се споделуваат приватни и доверливи информации. Младите често пати ги сметаат социјалните мрежи за забавни кои им даваат можност да комуникцираат разменат слики видеа и новости. Резултатите покажуваат дека речиси голем дел од младите до информациите доаѓаат преку социјалните мрежи и интернет порталите. Социјалниот живот на младите е префрлен на социјалните мрежи и се одвива онлајн.

Исто така, можеме да кажеме дека младите не се свесни за ризиците кои ги имаат социјалните мрежи како што: сајбер булинг, споделување на приватни податоци, изложување на несоодветна содржина.

На прашањето Што е безбедно да се споделува на Интернет? - 54% одговориле дека споделувањето лични податоци, локација, фотографија од другари/ки, лозинки, не е безбедно,но исто така 23,3 % од испитаниците сметаат дека споделувањето на лозинки фотографии од пријателите на Интернет е безбедно. Голем број на младите објавуваат фотографии од себе и нивните пријатели на социјалните мрежи. Тие сеизложуваат на потенцијален ризик од сајбер напад. Загрижувачки е фактот дека 23,3% од младите се изјаснуваат дека може без никаков ризик да ги споделуваат своите лозинки.

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

313 responses



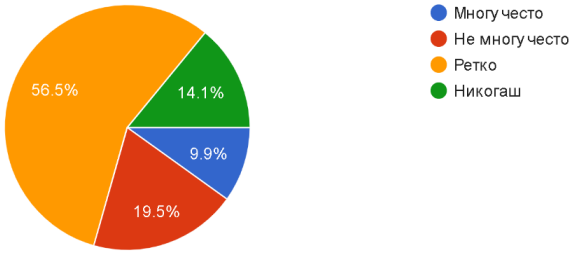
Според тебе што преставува Spam?

313 responses

Резултатите на ова прашање покажуваат дека 39,6 % од испитаниците имаат вистинско сознание за дејствијата на спам пораките. Спам-мејловите стануваат опасни само во зависност од тоа како ракувате со нив. Користењето на смарт телефони е секојдневие за младите затоа потребно е да знаат што се случува доколку отворат спам мејл. Една од опасностите е содржината која е содржат самите спам-мејлови која се користи за заплашување. Исто така, и малициозниот софтвер кој може да предизвика штета на уредите. Затоа, потребно е да се знае дека секоја спам порака може да ја означат,потоа да ја избришат и да се подесат одредени механизми за заштита на мобилните уреди.

Колку често во училиште дискутирате за опасностите кои ги има во Сајбер просторот

313 responses

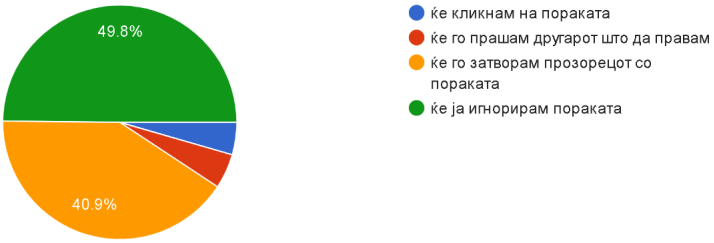


Одговорите на прашањето: Колку често дискутирате за опасностите кои ги има во Сајбер просторот? покажуваат дека 56,5 % ретко се дискутира во училиштата на темата Сајбер безбедност, 19,5% не многу често а само мал процент 9,9% често разговараат за опасностите во Сајбер просторот. Постои голема потреба во училиштата да се спроведува обука за свесност за безбедноста како и за зајакнување на заштитата на податоците на различни уреди. На учениците, наставниците им треба пристап до алатките за учење неопходни за разбирање, откривање и избегнување на сајбер заканите со кои може да се сретнат секојдневно. Изминатите годинисе покажа дека образованието доживеа рекордни сајбер напади со тоа стана најранлива категорија изложена на ризик од малициозен софтвер.

Како постапуваш кога некој непознат ти праќа порака и покана за пријателство , а ти се претставува дека е пријател на твој другар?

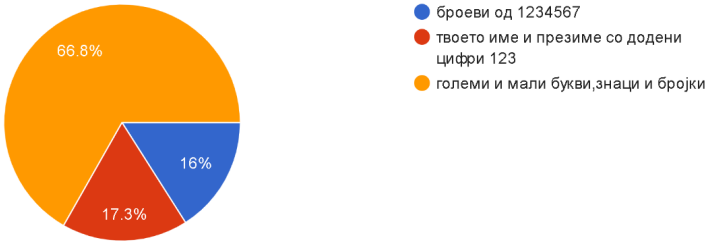
313 responses

Играш онлајн игра со својот другар/ка . На екранот ти се појавува мал прозорец со порака на која пишува „Кликни тука и ќе освоиш милион долари" Што ќе направиш?
313 responses



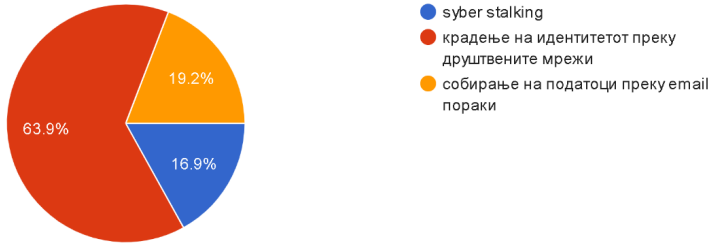
Еден од честите сајбер напади се собирањето на податоци преку мали pop up прозорчиња кои ги мамат корисниците со парична награда. 49,8% од испитаниците ја игнорираат порака додека 40,9% го затвораат прозорецот кој се појавува. Игнорирањето на пораката не е најбезбедниот начин да се заштитиме. Најбезбедно е целосно да се затвори преку прелистувачот, наместо само да го притискате копчето за затворање на рекламата. Намалување на појавата на ваквите прозорчиња можно е да се избрише преку пребарувачката историја.

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



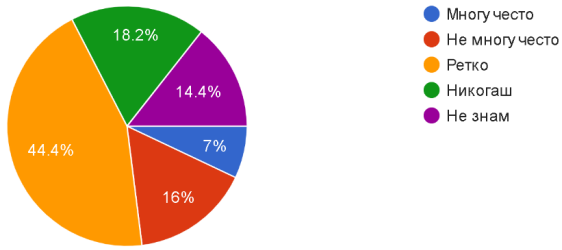
Ерата на Интернетот постави пред луѓето многу ризици од кои сеуште не сме подготвени да се заштитиме. 16% од учениците на прашањето што е за нив безбедна лозинка одговориле дека броевите од 1234567 за нив претставуваат безбедна лозинка. Општо е правилото, да се избегне ваков избор. Со ваквиот начин на креирање на лозинка стануваме лесна мета за хакерите. Така, 17,3 % се изјасниле дека при креирање на лозинката ги наведуваат името и презимето и броевите од 123. Потребно е да ги избегнуваме ваквите зборови,треба да додадеме интерпукциски знаци ,броеви кои може да се замена за буквите. Едно од правилата е да не се користи иста лозинка за различни сметки. Почестото менување на лозинки ја зголемува заштита од сајбер напади.

Според тебе што претставува „phishing"?
313 responses

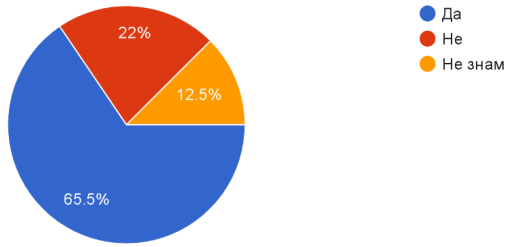


63,9% од учениците се изразиле дека phisingot е крадење на идентитетот преку друштвените мрежи. Главната цел на phising е собирање на податоци за корисникот преку емаил пораки. Од тука можеме само да видиме дека 19,2% делумно го познаваат значењето и функцијата na phisingot како еден од најзачестените Malware напади. Потребно е напредно развивање на дигиталните вештини кај младите за можат да го препознаат phishingot .

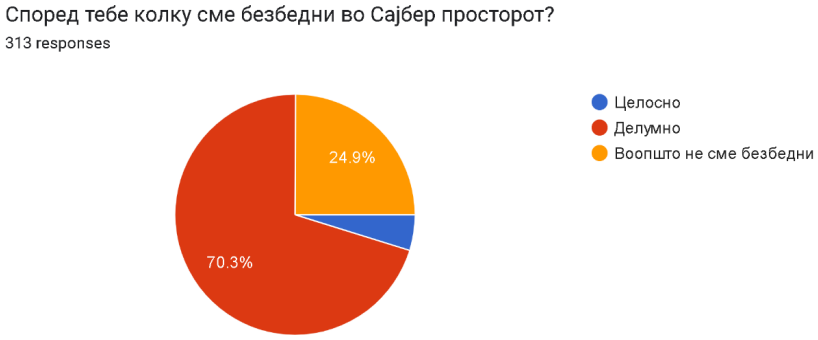
Дали во вашето училиште се одржуваат едукативни работилници за безбедно користење на Сајбер просторот?
313 responses



Дали сметаш дека ти е потребна доедукација за Сајбер безбедност
313 responses



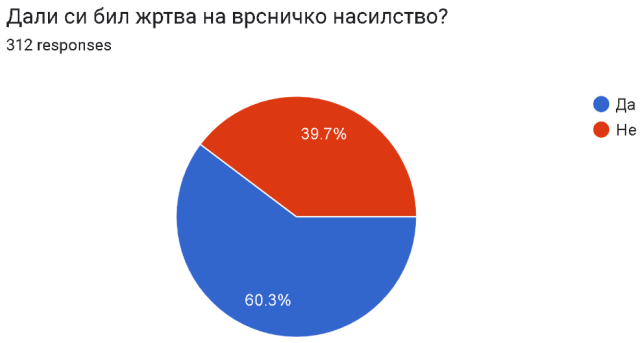
Согласно со прашањето дали во училиштето се одржуваат едукативни работилници за безбедно користење на сајбер просторот 44,4 % се изјасниле дека ретко се одржуваат работилници на тема сајбер безбедност додека 18,2% од учениците се изјасниле дека никогаш не присуствувале на работилница за сајбер безбедност во нивното училиште. Во корелација со второто прашање на кое голем дел од учениците се изјаснуваат дека имаат потреба од доедукација за Сајбер безбедност бидејќи сметаат дека немаат доволно знање за заштита од хакерски напади и пробивање на личните податоци. Најпопуларни апликации кај младите кои ги користат се Facebook, SnapChat, Instagram за контактирање со своите пријатели но исто така за информирање преку различни вести. Еден од проблемите кој се појавува е автентичноста на инфомраците.Колку младите се дигитално писмени и едуцирани за да се заштитат од лажни вести. Од големо значење е имплементацијата на Сајбер безбедност во училиштата.



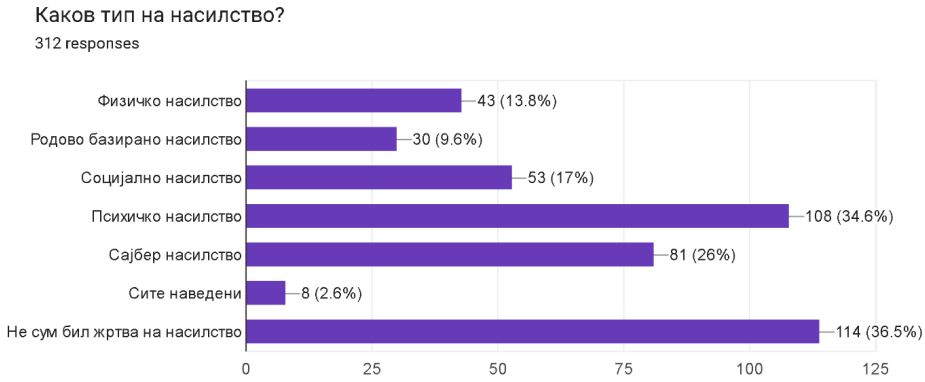
Интернетот е најголем и неисцрпен извор на информации во историјата на човечката цивилизација, што придонесе кон целосна дигитализација на секојдневното функционирање на човекот.[12] Невозможно е да се одреди големината на интернетот во било кој момент, бидејќи тој постојано се зголемувасо тоа и се зголемуваат сајбер нападите Податоците добиени од истражувањето укажуваат дека 70,3% од анкетираните сметаат дека интернетот е делумно безбеден, додека 24,9% од испитаниците сметаат дека Сајбер просторот е целосно небезбеден за нивните податоци, фотографии и приватноста. Со овој наод се покажува дека ученици сепак сметаат дека делумно се запознаени со сајбер безбедност како термин но не и со техниките, методите и механизмите за заштита од хакерски напади.

Исто така, и голем дел од испитаниците воопшто не се чуствуваат безбедни на Интернет бидејки се свесни за опасностите што се шират, знаат дека нивните податоци, слики може лесно да се најдат на различни веб сајтови.

12 Alatka za bezbednost i zashtita na decata.pdf (ugd.edu.mk)

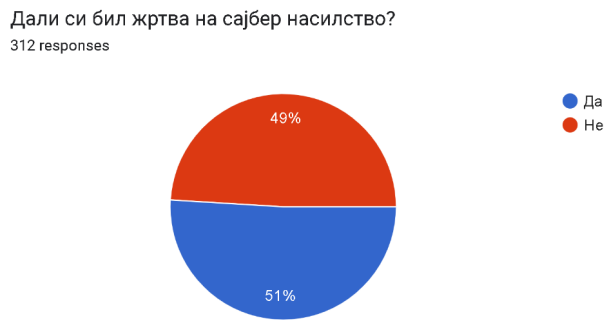


Еден од најголемите предизвици со кои се соочуваат училиштата е врсничкото насилство. Од 60% кои одговориле дека биле жртва на врсничкото насилство можеме да кажеме дека во училиштата каде и најчесто се случува овој вид на насилство меѓу учениците е во голем пораст. Насилството помеѓу врсниците е континуриано кое може да биде директно или индиректно со цел да се докаже доминација и моќ во друштвото. Индиректното насилство може да се појави во форма на сајбер насилство преку ширење на дезинформации, слики од скриени профили кои ќе му наштетат на поедниецот. Насилството помеѓу врсниците може исто така да биде физичко ,психичко насилство,социјално родово базирано насилство.



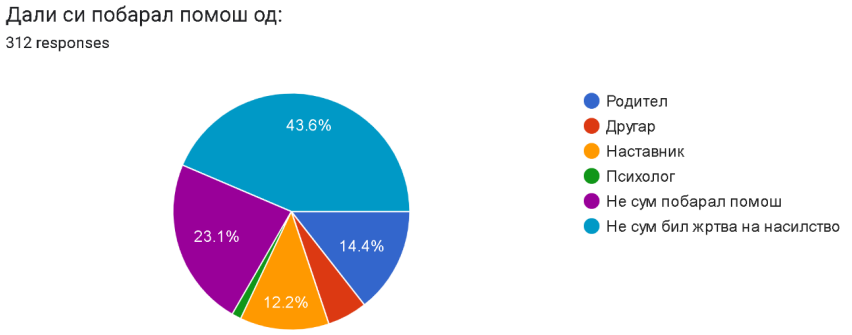
Овој наод покажува дека доминантен вид на насилство кое постои помеѓу учениците е психичкото насилство бидејќи скоро 34% од испитаници одговориле дека овој тип на насилство е доминантен во училиштето во кое се образуваат. Веднаш зад него се наоѓаат електронското насилство и социјалното насилство кои се на второто, односно третото место. Загрижува тоа што во училиштата веќе неколку години се спроведуваат програми креирани и поддржани од министерствата и институциите креатори на образовни политики кои имаат за цел да придонесат во справувањето со физичкото и психичкото насилство, а сепак и во 21 век овие форми на насилство остануваат да бидат доминантни.

Очигледно дека електронското насилство е вид на насилство кое зема се поголем замаф и сè повеќе ги засега учениците и наставниците. Од друга страна, постои недоволна информираност и умешност за справување со него кај учениците но и кај наставниот кадар. Цениме дека е потребна едукација за позитивна употреба на технологијата, која ќе создава безбедни и ефективни практики, а е клучна во превенција од злоупотреба на технологијата.



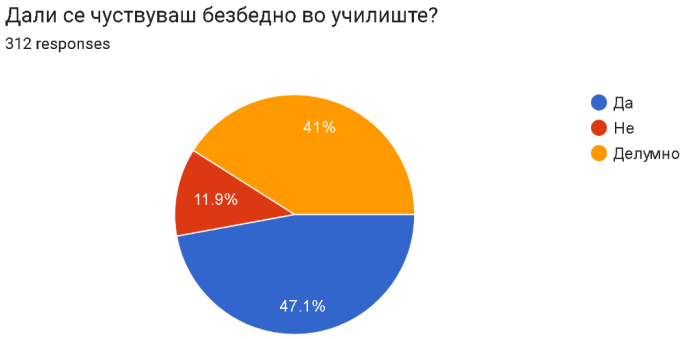
Од овие два наоди можеме да кажеме дека голем е процентот на ученици кој биле жртви на сајбер насилство но исто така е загружувачки 39,1% кои биле повеќе од два пати жртви на сајбер булинг. Какви промени манифестираат децата кои биле жртви на насилство, дали наставниот кадар, стручните служби и родителите би можеле да ги детектираат овие појави на насилство, што превземале возрасните за да се справат со насилството и да обезбедат помош и поддршка на учениците, се прашања на кои треба да се работи во најблиска иднина, со цел сите фактори да можат да се вклучат и да ја променат актуелната состојба со насилството во средните училишта

Од одговорите на ова прашање 28,5 % кои биле жртви на сајбер насилство не го пријавиле што укажува дека сепак постои страв кај жртвите да пријават. Младите луѓе не бараат помош за сајбер-малтретирање од многу од истите причини поради кои не посегнуваат по поддршка по малтретирањето во реалниот свет. Од одоговороите дадени на ова прашање можеме да ги издвоиме следноите причини: Тие се чувствуваат засрамени. Тие не сакаат да ги гледаат како кодоши и да изгубат уште поголем социјален статус. Се плашат од одмазда. Чувствуваат дека е нивна одговорност да се справат со тоа. Оттука, потребно е поттикнување и охрабување да се пријави сајбер насилникот бидејќи сајбер булингот не застанува во училиштата продолжува надвор од нив.



Одговорите на ова прашање даваат една многу важна информација а тоа е дека 43,6% од учениците ќе побараат помош и поддршка од родители за решавањето на сајбер насилството кое го доживуваат, додека 23,1% не побарале помош што е загрижувачки. Друга причина поради која младите не сакаат да побараат помош од возрасните за нивните искуства поврзани со сајбер-малтретирањето може да биде тоа што младите имаат тенденција да мислат дека сајбер-малтретирањето не е сериозен проблем и затоа не им потребна помош.

Една од можните причини, зошто младите не им кажуваат на наставниците за сајбер-малтретирањето може да биде затоа што тие не сметаат декаво нивното училиште има ресурси за справување со сајбер-малтретирањето. Овие резултати сугерираат дека можеби е потребна дополнителна обука за наставниците за да ги идентификуваат ефективните начини за справување со сајбер-малтретирањето во училишната средина.



Овој наод покажува дека 41 % од испитаниците делумно се чувствуваат безбедно во училиштето, 11, 9 % не се чувствуваат безбедно а 47,1 % се безбедни за време на нивниот престој во училиште. Училиштата се образовни институции во кои децата поминуваат голем дел од своето време и ги градат сите свои вредности. Исклучително е важно учениците да се чувствуваат безбедно, сигурно и среќно во училиште. Многу е важно училиштето, наставничкиот кадар и стручните служби да имаат јасна политика на нулта толеранција на насилство и јасна перцепција што тоа значи, не само на хартија, туку како го живееме и имплементираме во начинот на организација на животот во училиштето. Исто така, важно е да се создаде училишна средина во која секој ќе се чувствува безбедно, сигурно и ќе има чувство на припадност. Припадноста е особено важна за младите. Училиштата треба да бидат места каде интегритетот и човечноста на секое дете и наставник бескомпромисно ќе се почитуваат и каде за ова ќе постојат мерки, обука и следење.

ПРЕПОРАКИ ЗА ПОДОБРУВАЊЕ НА САЈБЕР БЕЗБЕДНОСТА ВО УЧИЛИШТАТА

Проблемот со сајбер заканите е алармантен во образованието поради обемот на податоци со кои се менаџира,недостаток на ресурси, едукација на наставниците, стручниот кадар како и намалена свест на учениците за Сајбер безбедност. Големиот обем на напади утврди дека училиштата треба да ги зголемат мерките за заштита на податоците од сајбер напади.

Од исклучителна важност е соработката со институциите како што се Министерство за образование и Министерството за внатрешни работи од секторот за Сајбер криминал, бидејќи само така може да се дојде до најодржливо решение кое би ги спречило и минимизира сајбер нападите.

Сајбер безбедноста мора да биде составен дел од годишната програма на секоја образовна институција. На учениците и наставниците им треба пристап до алатките за учење неопходни за разбирање, откривање и избегнување на сајбер заканите со кои може да се сретнат секојдневно.

Истражувањето ни покажа дека голем број ученици биле жртви на сајбер напад, но исто така ни докажува дека учиниците немаат доволно дигитални вештини и механизми за Сајбер безбедност. Во спроведената анкета резултатите покажаа дека во училиштата ретко се спроведуваат едукативни работилници на тема Сајбер безбедност. Оттука произлегува и потребата да се зголеми свеста кај учениците за пронаѓање на Сајбер механизми кои ќе ги заштитат од ризиците на Интернетот.

Со цел да се подобри состојбата со училиштата потребно е вклучување на сите засегнати страни во процесот, како: наставниците, учениците, стручната служба и институтциите.

Потребно е:

- Информирање на наставниците, учениците и стручниот кадар за најновите безбедносни ризици со цел навремено да реагираат
- Пронаоѓање на одржливи решенија за антивирусен и антималициозен софтвер со цел да се заштити компјутерскиот систем во училиштата и да се блокира секаков вид на малициозен софтвер
- Редовно ажурирање на софтверот и негово одржување за да се елиминираат сите пропусти за ризик од откупни софтвери
- Информирање на наставниците и учениците за фишинг нападите и нивно препознавање
- Воведување на содржини во наставните програми од темитеСајбер безбедност
- Обуки наменети за учениците и наставници посветени на Сајбер безбедноста значењето на сајбер заканите и нивна превенција
- Организирање на работилници во кои ќе учествуваат ученици, наставници и родители за запознавање со правилата за користење на Сајбер просторот.
- Формирање на училишни тимови за сајбер безбедност составена од обучени наставници ученици и стручна служба.
- Училишните тимови да изготват и имплементираат програма за обука за развивање на механизмите за спречување на Сајбер напад
- Развивање на сајбер култура во училиштата со цел да се спречат потенцијалните напади
- Едукација на учениците и родителите со можните правни мерки за делување против сајбер насилство и воедно запознавање на учениците и родителите со конкретните членови од Кривичниот закоником по кои им се дава можност да делуваат
- Постапување по кривичниот законик член 251-Оштетување и неовластено навлегување во компјутерскиот систем,член 151-а Правење и внесување на компјутерски вирус и член 151-б Компјутерска измама.

КОРИСНИ СОВЕТИ ЗА САЈБЕР БЕЗБЕДНОСТ

Сајбер Безбедност

Сајбер безбедноста е има цел да не заштити од какви било малициозни дигитални сајбер-напади. Сајбер безбедноста може да се имплементира во училиштата како и во сите институцииипротив сајбер-напади кои се предизвикани преку јавно достапна интернет конекција, е-пошта за фишинг, сомнителни врски, документи или апликации што може да се преземат.

Интернетот стана секојдневние во нашиот живот. Во образованието, интернетот е исклучително важен и исто така постојано расте. Веднаш по пандемијата децата се потпираа само на интернет за да учат.. Интернетот неизбежно стана од огромно значење. Сите ние ја чувствуваме потребата за интернет во сите сфери на животот. Во областа на образованието, интернетот е исклучително важен и исто така постојано расте.

Во нашиот образовен систем, зависноста од интернет е огромна, што го прави неопходно да се има сајбер безбедност од фишинг напади ,malware, сајбер булингот и др напади.

Причините поради кои се случуваат вакви напади се :

- Недостаток на технички вештини и знаење
- Ниска свест кај младите за сајбер безбедноста
- Зголемено користење на Интернет

Заштита од cyber grooming

Со растот на платформите за социјални мрежи, онлајн игрите и апликациите за инстант пораки, децата можат да разговараат со секого – пријатели или непознати – од целиот свет. Ова може да им користи на многумина со тоа што ќе ги направи да се чувствуваат помалку изолирани, но за некои може да ги остави ранливи на cyber grooming.[13]

Online groomingo е кога луѓето користат лажни информации и профили за да се спријателат со луѓе на интернет, обично за сексуални цели.Овој вид на напад најчесто се случува преку социјалните мрежи. Многу е поголема веројатноста децата да веруваат во информациите што луѓето им споделуваат информации без да се сомневаат во нивната легитимност. Grommerot на интернет може да одвои време за да дознае за својата жртва, да ги разгледа нивните онлајн профили, да ги открие нивните допаѓања и недопаѓања од тие профили со цел да дознаат информации за својата жртва.

Постојат механизми за заштита од овој вид на напад еден од нив е едукацијата на младите за Сајбер безбедноста .

Совети за превенција од ваков вид на напад:

- Да не се инсталира софтвер ,игри и апликации од непознат извор
- Да не се прифаќа пријателство од непозната личност бидејќи голема е веројатност
- Cyber grommerot да креирал лажен профил со цел да разговара со своите жртви
- Подесување на поставки за приватност на социјалните мрежи (објави видливи само за пријателите)
- Да се избегне разговор со луѓе кои поставуваат прашања за вашите сексуални искуства.
- Да се избегне вклучување на веб камера при разговор со непознати
- Не одете да запознаете личност која сте ја запознале сами преку Интернет. Секогаш земајте пријател или постар човек со вас.
- Да не се споделуваат фотографии со непознати

13 Online grooming: what it is and how to protect your child | Internet Matters

Заштита од фишинг напади

Еден од начините да се заштитиме од овие напади е да знаеме како да ги детектираме.Постојат неколку начини на детекција на вакви видови напади .Емаил-фишингот има специфични карактеристики преку кои може да се препознае меѓу кои се:

- Прилози или линкови
- Правописни грешки Лоша граматика
- Непотребна итност за веднаш да ја потврдите вашата адреса за е-пошта или други лични информации

https://www.internetsecurity.tips/the-dangers-of-phishing-scams-prevention-and-protection-tips/

Мерки за заштита од емаил -фишингот се:

Никогаш да не се отвараат алармантни пораки. Познатите компании нема да бараат информации за лична идентификација или детали за сметката, преку е-пошта. Ова ги вклучува вашата банка, секоја компанија со која соработувате.

Ако некогаш добиете е-пошта со барање за какви било информации за сметката, веднаш избришете ја и потоа повикајте ја компанијата за да потврдите дека вашата сметка е во ред. Не отворајте прилози во овие сомнителни или чудни е-пораки - особено Word, Excel, PowerPoint или PDF прилози. Избегнувајте постојано да кликате на хиперлинкови во е-поштата, бидејќи тие може да се интсалираат со малициозен софтвер.

Бидете внимателни кога примате пораки од трети лица; никогаш не кликнете на URL-адреси во оригиналната порака. Наместо тоа, посетете ја страницата директно со внесување на точната URL адреса за да го потврдите барањето.

Одржувајте го софтверот и оперативниот систем. Најчесто Windows оперативните систем се мета на фишинг и други малициозни напади, затоа бидете сигурни дека сте безбедни и ажурирани.

Заштита од сајбер булинг

Иако не постои целосен начин да се спречи децата да бидат дел од сајбер булингот има работи што можете да ги направиме заедно за да ја намалиме веројатноста дека ќе биде цел. Ова вклучува спроведување на безбедносни механизми, како и тековни разговори за сајбер-малтретирањето. Исто така, важно е едукација за младите за тоа како безбедно и одговорно да ги користат социјалните мрежи и што треба да прават ако се малтретирани преку Интернет.

Некои од механизмите за заштита од сајбер булинг се:

Заштита на сметките и уредите Кога станува збор за спречување на сајбер малтретирање, важно е да се користи лозинки за сè. Лозинките се еден од најефикасните начини за заштита на сметките и уредите. Треба да им се нагласи на децата деканикогаш не треба да ги споделуваат своите лозинки со никого, вклучително и со својот најдобар пријател

Користењена алатките и поставките за приватност Без разлика што праватдецата на интернет, потребно е да ги запознаеме со алатките за безбедност на сите социјални мрежи. Речиси секоја платформа за социјални медиуми, вклучително и Instagram, Twitter, SnapChat и TikTok имаат поставки за приватност.

Управување со споделување налокација Некои паметни телефони им дозволуваат на корисниците да ја споделат својата локација со пријателите. Ова значи дека ако ја споделат својата локација со луѓе, овие луѓе секогаш ќе знаат каде се.Исто така некои фотографи имаат географски ознаки кои ја одредуваат локацијата на поединецоте. Од голема важност е да се знае дека ваквите фотографии не треба да се споделуваат онлајн.

Одјавете се кога користите јавни уреди

Едно од најважните правила е да одјавување од јавни компјутери или лаптопи на училиште или во библиотеката,од било која смсетка. Ова вклучува одјавување од е-пошта, сметки на социјалните медиуми, нивната училишна сметка.Затворање на јазичето не е доволно. Ако некој се качи на компјутерот веднаш откако ќе заврши, можеби сепак ќе може да влезе во вашата сметка. И откако ќе имаат пристап, тие можат да ја преземат контролата врз таа сметка со промена на лозинките. Откако ќе го изгубите пристапот до сметката, може да биде тешко и одзема многу време да се врати контролата. Одбијте да одговорите на сајбер насилниците.

Заштита од социјален инжинеринг

Најдобар начин да се спречат нападите од социјалниот инженеринг е да знаете како да ги забележите. Откако веќе сте фатени во мрежата на социјален инженер, може да биде тешко да се раздвоите. Не треба да бидете технолошки експерт за да практикувате добра превенција од социјален инженеринг

Променете ги поставките за е-пошта за спам

Еден од најлесните начини да се заштитите од нападите на социјалниот инженеринг е да ги прилагодите вашите поставки за е-пошта. Можете да ги зајакнете вашите филтри за спам и да спречите е-пошта за измама од социјално инженерство да се лизгаат во вашето сандаче. Можете исто така да додадете адреси на е-пошта на луѓе и организации за кои знаете дека се легитимни директно на вашите списоци со дигитални контакти - секој што во иднина ќе тврди дека е нив, но користи друга адреса, најверојатно е социјален инженер.

Истражете го изворот

Ако примите е-пошта, СМС или телефонски повик од непознат извор, внесете ги во пребарувачот и видете што ќе се појави. Ако е дел од познат напад од социјален инженеринг, испраќачот можеби бил означен претходно. Дури и ако испраќачот изгледа легитимен, проверете во секој случај, бидејќи адресата на е-пошта или телефонскиот број може да испаднат дека се само малку поинакви од вистинскиот извор - и може да се поврзани со небезбедна веб-локација .Ако веб-пребарувањето не е успешно друг начин да спречите напад е директно да контактирате со организацијата која тврди дека ве контактирала.

Ажурирајте го вашиот антивирус/антималвер софтвер

Проверете дали се вклучени автоматски ажурирања Периодично проверувајте дали се применети ажурирањата и скенирајте го вашиот систем за можни инфекции

Заштита од Онлајн ѓејминг

Онлајн играњето е забавно, но за да се зголеми безбедноста, од витално значење е да се практикува сајбер безбедност. Еве неколку механизми за заштит што треба да ги следите:

Користете силни лозинки.

Еден од наједноставните начини да се заштитите е да користите силна лозинка. Следењето на бројни лозинки може да биде тешко - па користењето на менаџер за лозинки може да помогне

Поставете повеќефакторска автентикација

Ако играта винуди автентикација со два или повеќе фактори, овозможете ја. Ова додава уште еден чекор во процесот на најавување, како што е испраќање код на вашиот телефонски број или адреса на е-пошта. Автентикацијата со два или повеќе фактори обезбедува дополнителна безбедност на вашата сметка на играта - некои игри нудат дури и награди во играта на играчите кои го овозможуваат тоа.

Заштитете ги вашите лични податоци

Не вклучувајте информации за идентификација во вашите кориснички имиња за игри - како што се вашето име, датум на раѓање или локација - и избегнувајте споделување лични податоци на форумите за игри. Кога ги користите слушалките за игри, внимавајте кои лични информации ги кажувате на глас.

Преземајте само одавтентицирани извори

Чувајте го вашиот компјутер и себеси безбедни со избегнување на преземања од нелегални извори. Без разлика дали се работи за игриили шифри за измами, преземањето од неофицијални или пиратски извори ризикува да внесе вируси или малициозен софтвер за игри на вашиот компјутер

Одржувајте го софтверот ажуриран

Погрижете се да ги ажурирате вашите уреди и софтвер. Ажурираниот софтвер ќе се погрижи да имате корист од најновите безбедносни закрпи за решавање на сајбер пропустите.

Инсталирајте и користете VPN кога играте игри

Ако играте игри на десктоп компјутер, криењето на вашата локација е важно за да се заштити вашиот идентитет. Кога користите виртуелна приватна мрежа или VPN, вашиот компјутер може да изгледа дека е некаде на друго место во светот, што ги спречува напаѓачите да ја најдат вашата локација

Заштита од ransomware

Ransomware е еден вид на malware кој може да го инфицира компјутерот и да превземе податоци од поединецот кој ќе ги чува се додека не се плати “откупот. Овој вид на напади се опасни за училиштата. Доколку превземат податоци голем е ризикот да ги објават јавно. Постојат повеќе начини за заштита од ransomware инфекција.

Backup на податоците

Поставување на податоците на надворешен диск и онлајн облак со цел да се намали ризикот.

Во случај на напад на откупнина, корисникот може да го избрише компјутерот и повторно да ги инсталира резервните датотеки.

Ажурирајте ги сите системи и софтвер

Секогаш чувајте го вашиот оперативен систем, веб-прелистувач, антивирус и кој било друг софтвер што го користите ажуриран на најновата достапна верзија. Злонамерниот софтвер, вирусите и откупниот софтвер постојано се развиваат со нови варијанти кои можат да ги заобиколат вашите стари безбедносни карактеристики, па затоа ќе сакате да бидете сигурни дека сè е закрпено и ажурирано[14]

Инсталирајте антивирусен софтвер и огнени Firewall

Сеопфатниот антивирусен и анти-малициозен софтвер се најчестите начини за одбрана од откупни софтвери. Тие можат да скенираат, откриваат и реагираат на сајбер заканите. Сепак, ќе треба да го конфигурирате и вашиот заштитен sид бидејќи антивирусниот софтвер работи само на внатрешно ниво и може да го открие нападот само штом веќе е во системот. Заштитните sидови често се првата линија на одбрана против какви било дојдовни, надворешни напади. Може да заштити и од софтверски и од хардверски напади.

14 How to Protect Yourself from Ransomware (kaspersky.com)

КОРИСТЕНА ЛИТЕРАТУРА И ЛИНКОВИ

1. ИНФОРМАТИЧКО ОПШТЕСТВО - INFORMATION SOCIETY СООПШТЕНИЕ - NEWS RELEASE Користење на информатичко-комуникациски технологии во домаќинствата и кај поединците, 2022, Државен Завод за Статистика, достапно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf
2. Проф. д-р Гордана Лажетиќ, Д.-Н. П.-р. (2020). Алатка за безбедност и заштита на децата од насилство во дигиталниот свет. Скопје.
3. Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth, Robin M Kowalski 1, Gary W Giumetti 2, Amber N Schroeder 3, Micah R Lattanner 4, Affiliations expand, PMID: 24512111 DOI: 10.1037/a0035618
4. Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective, January 2012, DOI: 10.1332/policypress/9781847428837.003.0012, Publisher: Policy PressISBN: 1847428827
5. RESEARCH REPORT Baseline assessment for awareness raising and capacity building, CRPM
6. Protect your child from online grooming. (2023).
7. Ransomware protection: How to keep your data safe in 2023. (2023).
8. Free Vector | Free vector hacker activity illustrated concept (freepik.com)
9. Cyberbullying Information for Parents | How You Can Help | Kids Helpline
10. The Risks of Online Gaming and How to Prevent Cybercrime (internetsafetystatistics.com)
11. Ransomware attacks nearly doubled in 2021 | Security Magazine

Автори: Овој Прирачник е изготвен од Ана Дионисиева, истражувач од Аналитика тинк тенк.

Овој Прирачник е изработен во рамки на проектот „Развој на култура на сајбер безбедност во образовниот систем на Северна Македонија - Зајакнување на капацитетот на младите луѓе и наставниците за примена на мерки за сајбер безбедност и Развојот на ефективни училишни програми за спречување на сајбер-насилството", што го спроведува Аналитика - Скопје, со финансиска поддршка на Фондацијата Отворено општество – 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 Фондацијата Отворен оопштество – Македонија.