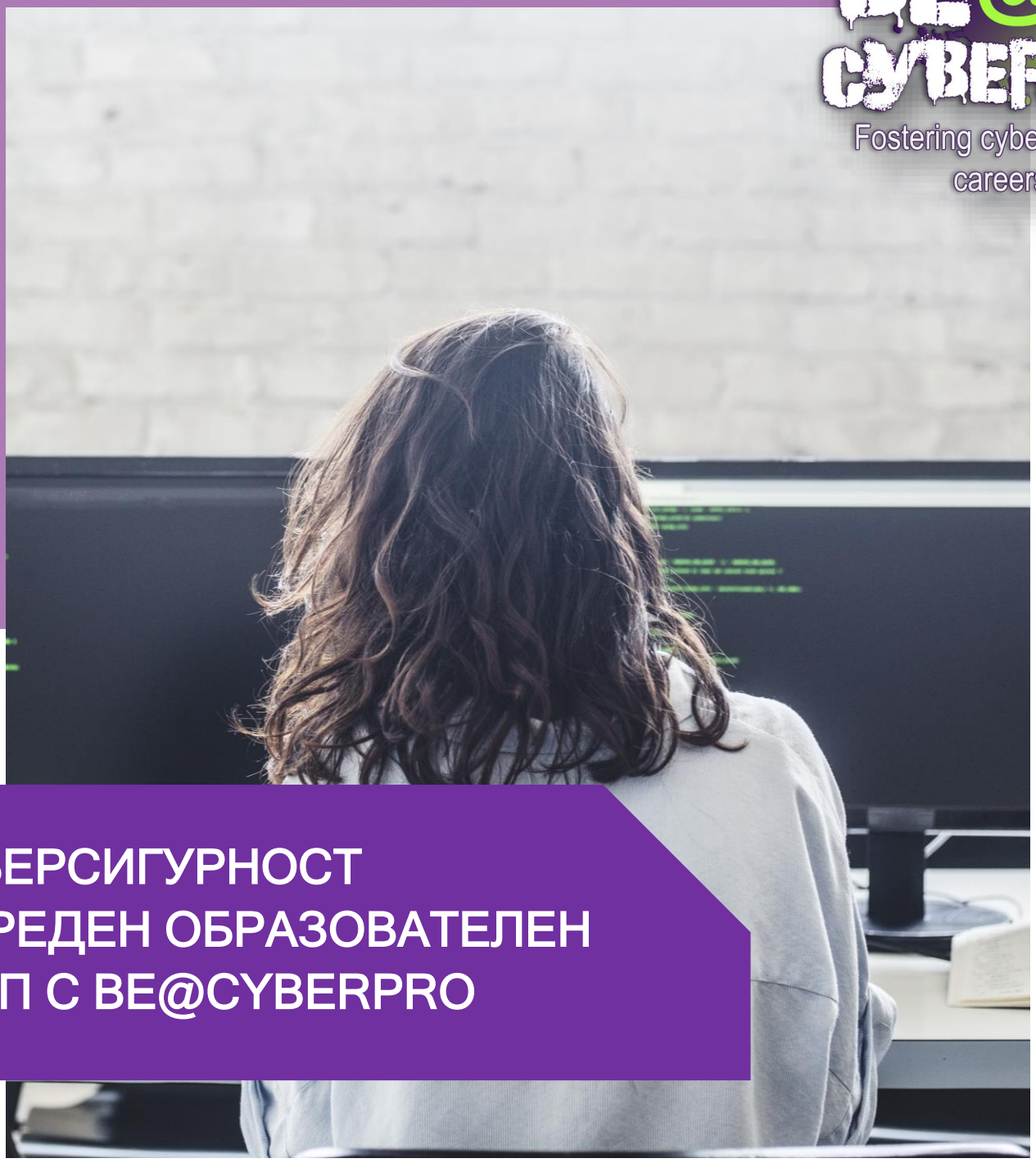
Fostering cybersecurity careers



КИБЕРСИГУРНОСТ В СРЕДЕН ОБРАЗОВАТЕЛЕН ЕТАП С BE@CYBERPRO

ПРАКТИЧЕСКИ НАСОКИ ЗА УЧИТЕЛИ И РОДИТЕЛИ

Този проект с № 2018-1-ES01-KA201-050461 е финансиран с подкрепата на Европейската комисия. Настоящата публикация отразява единствено възгледите на автора и Комисията не носи отговорност за използването на съдържащата се в нея информация.

Co-funded by the Erasmus+ Programme of the European Union

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ

За голяма част от европейските граждани, киберсигурността остава непознат термин. Според неотдавнашни данни много европейски граждани все още не са осъзнали важността от познаването на .основните мерки за киберсигурност (Erixon & Lamprecht, 2018; Pupillo, 2018). Приблизително 50 % от професионалистите нямат въведена парола, ПИН или биометрична защита, която да предпазва техните устройства, а 66,6 % съобщават, че съхраняваните от тях данни, не са криптирани (Reischuk, 2019). В този контекст е разбираемо, че през последното десетилетие Европейският съюз (ЕС) започва активна работа за повишаването на общата осведоменост по въпросите на информационната сигурност и подобряването на кибер-защитата на различни нива.

Киберсигурността често се определя като "организация и съвкупност от ресурси, процеси и структури, използвани за защита на киберпространството и системите, свързани с киберпространството, от събития, които се нарушават де юре и де факто с правата на собствеността" (Craigen, Diakun-Thibault, & Purse, 2014). По-конкретно, според International Telecommunications Union (ITU) киберсигурността включва съвкупност от инструменти, политики, концепции за сигурност, мерки за обезпечаване на сигурността, както и насоки, подходи за управление на риска, действия, обучения, добри практики, гаранции и технологии, които могат да се използват за защита на киберсредата и активите на организацията и потребителите на дигиталните продукти (Von Solms & Van Niekerk, 2013).

„Кибератаките стават все по-усъвършенствани, целенасочени, широко разпространени и неоткриваеми“

Според Европейската агенция за киберсигурност (ENISA, 2020 г.) кибератаките стават все по-усъвършенствани, целенасочени, широко разпространени и неоткриваеми. Според ENISA фишингът, кражбата на самоличност и рансъмуерът са се увеличили, особено в контекста на пандемията от COVID-19, която е послужила като среда за насърчаване на атаките срещу домакинства, предприятия, правителства и критични инфраструктури (Kohler, 2020; Sterlini, Massacci, Kadenko, Fiebig, & van Eeten, 2019; Štitilis, Rotomskis, Laurinaitis, Nadvynychnyy, & Khorunzhak, 2020). В резултат на това икономическите загуби, свързани с кибератаки, са огромни за правителствата, агенциите и институциите, предприятията и физическите лица, които са уязвими към зачестилите киберзаплахи (Carrapico & Barrinha, 2018; Lis & Mendel, 2019).

Изчислено е, че киберпрестъпността струва на световната икономика до 575 млрд. долара годишно (Sobers, 2019). В допълнение на това, бързите темпове на развитие на технологии, като интернет на нещата (IoT), с повече от 50 милиарда свързани устройства, увеличава изключително много риска от кибератаки (Lis & Mendel, 2019).

В този контекст е разбираем и ръстът на инвестициите в информационната сигурност. Въпреки това, нуждата на квалифицирани кадри и човешки капитал в сектора на информационната сигурност, все още е водещ проблем. Изчислено е, че до 2021 г. ще има 3,5 милиона незаети позиции в областта на информационната сигурност (Ventures, 2017 г.).

Ето защо и в момента организациите са изправени пред предизвикателството да наемат специалисти в сферата на киберсигурността на пазар на труда, който страда от хроничен недостиг на експерти с подходящи умения и подготовка, за да отговорят на търсенето на пазара (Crumpler & Lewis, 2019). В допълнение на това, ниският дял на квалифицирани жени, работещи в сектора на киберсигурността, задълбочава този проблема. По последни данни делът на жените, наети в този сектор, се оценява на 7 % в Европа (Poster, 2018 г.).

Всичко това вдъхнови създаването на Be@CyberPro - проект, посветен на идеята за преодоляването на проблема с недостига на кадри в сферата, чрез предоставяне на серия безплатни уводни образователни ресурси по киберсигурност за ученици, учители и родители и популяризирането кариерите в областта на киберсигурността.

Основната целева група на проекта са учениците от средните училища и професионалните гимназии, както и учителите и семействата на тези ученици. Освен това, осигуряването на достъп до повече и по-разнообразна информация за кариерите в областта на киберсигурността, би могло да повлияе положително на повече млади хора при избора на кариера и да мотивира повече млади хора да се запознаят в повече детайли, със сферата на киберсигурността, на което е посветена и настоящата електронна книга.

ЕЛЕКТРОННА ОБРАЗОВАТЕЛНА ПЛАТФОРМА

В рамките на Be@CyberPro, консорциумът разработи уводен онлайн курс по основи на информационната сигурност за ученици, както и отделен курс за преподаватели по предмети, различни от информатика и компютърни науки, за да предоставим и затвърдим фундаментални познания в областта и по отношение на различните професии в сферата.

Курсовете са разработени върху Moodle - модулна учебна среда, която служи като онлайн система (уеб базирана) за преподаване и компютърно интегрирано обучение. Системата не изисква инсталиране на допълнителен софтуер от потребителя. Необходим е само браузър за създаване и преглед на учебното съдържание. Moodle включва възможности за представяне на учебни материали, провеждане на тестове, дискусионни групи (форуми) за общуване и други.

В рамките на курса за учители са включени и **серия дидактически материали за работа с ученици**, както и предложения за учебни планове и упражнения на базата на курсът на Be@CyberPro за ученици:

- Дидактическите материали, подготвени от Be@CyberPro, могат да се използват свободно за работа с ученици.
- Целта на дидактическите материали е да подобри дигиталната компетентност на учениците и най-вече да постави основите за изграждане на отговорно и информирано поведение в съответствие с основните принципи на киберсигурността.

В следващите страници ще бъде оформен примерен график за работа с учениците с виртуалния курс на Be@CyberPro.

Като учители или родители, можете да изберете дали да работите върху цялото съдържание или да изберете отделни модули. Материалите могат да се променят, спрямо специфичните нужди на учениците, и желаните образователни резултати.

Препоръчителният график при адаптация на образователните материали на Be@CyberPro предвижда 8 едночасови сесии и от 1 до 3 сесии за всеки от модулите.

В повечето случаи, груповите образователни занимания могат да бъдат идеалната среда за приложението на тези дидактически материали, особено в случай че не преподавате предмети, конкретно насочени към дигиталните технологии.

ПРАКТИЧЕСКИ НАСОКИ ЗА УЧИТЕЛИ

- Представяйте всяка от темите, чрез диалог с учениците. Задавайте отворени въпроси, които да им позволят да споделят опита и притесненията си един с друг.
- Можете да използвате и някои различни ресурси за въвеждане на темите, като например:
    - Някои актуални събития
    - Откъси от филми
    - Откъси от сериали или книги, насочени към възрастовата група, с която ще работите
    - Реални казуси, които са близки до интересите и нуждите на учениците
    - Бихте могли да поканите експерти и практици от сферата на информационната сигурност, които да започнат диалога с учениците.
- Говорете открито, без да омаловажавате или смекчавате някои рискове, но и без да преувеличавате реалността.
- Насърчавайте критичното мислене на учениците, като противопоставяте информация от различни източници, или провеждате дейности, в които учениците могат да споделят своите идеи и мнения.
- Използвайте разнообразни материали. Освен предложените от нас, можете да намерите още материали в онлайн образователните пространства, като например https://www.betterinternetforkids.eu/. В Европа съществува и така наречената мрежа от центрове за безопасен интернет (SIC). Локалните центрове обикновено включват и центрове за повишаване на осведомеността, телефонна линия, гореща линия и младежки панел.

МОДУЛ 1 - ЗАЩИТА НА УСТРОЙСТВА И ДИГИТАЛНО СЪДЪРЖАНИЕ

ОБРАЗОВАТЕЛНИ ЦЕЛИ

- Запознаване с различни рискове и заплахи в дигиталния свят, като фалшиви новини, рансъмуеър, фишинг, спам, секстинг, нарушаване на авторски права и други.
- Познаване на основни мерки за сигурност и защита.

КОМПЕТЕНТНОСТИ, БАЗИРАНИ НА DIGCOMP

4.1. Защита на дигитално съдържание и устройства
Знания:

- K1. Рискове и заплахи в дигиталната среда
- K2. Методи за защита на дигиталните устройства, като използване на антивирусни програми, антиспам филтри, пароли, актуализиране на софтуер.
- K3. Лична информация. Нива на защита в зависимост от естеството на данните.

Умения:

- S13. Умение за прилагане на различни методи за защита на устройства и дигитално съдържание и умение за споделяне на тази информация.
- S14. Умение за разпознаване на широк набор от рискове и заплахи в дигиталния свят, като фалшиви новини, рансъмуеър, фишинг, спам, секстинг, нарушаване на авторски права и други.
- S15. Умение за прилагане на мерки за сигурност и защита.
- S16. Умение за използване на различни методи за обезпечаване на поверителността.

Съдържание[1]:

1.1. Защита на дигиталните устройства

1.2. Рискове и заплахи в дигиталната среда

1.3. Защита на дигиталното съдържание

[1] Примерно съдържание е налично на уебсайта на проекта: https://www.beacyberpro.eu/

1.4. Отговорно ползване на технологията

СЕСИЯ 1

- Първоначален разговор: "Предимствата и рисковете, за които вече знаем, когато използваме смартфон".
- Обсъждане на специфичната терминология от урока, като фишинг, спам, секстинг, нарушаване на авторски права и други.
- Идентифициране на проблемни ситуации в група. Обсъждане на проблемите и техните евентуални решения.

СЕСИЯ 2
Сексторшън[2]

- Гледане и обсъждане на откъси от филма *Skam,* разглеждащ случай на сексторшън.
- Търсене на новини за случаи на сексуално изнудване.
- Попълнете дърво на решенията[3] на база на ситуация, свързана със сексуално изнудване: " Ако непознат човек се опитва да флиртува с вас в социалните мрежи..."

СЕСИЯ 3
Фалшиви новини

- Първоначален разговор: Какво знаем за фалшивите новини? Споделяме някои от тях, които познаваме или подготвяме някои актуалните примери.
- Насоки за разпознаване на фалшиви новини.
- Упражнение в група: На учениците се предоставят няколко новини. Те трябва да определят дали са фалшиви или не, като съпоставят информацията от различни източници.

[2] Тази тема може да не се счита за подходяща за учебните програми в България. Моля, консултирайте се с училищното настоятелство или със специалист по сексуално образование, преди да я разгледате

[3] *"Дървовидна диаграма, която се използва за вземане на решения в бизнеса или компютърното програмиране и в която разклоненията представляват избори със съответните рискове, разходи, резултати или вероятности" (Merriam-Webster)*

МОДУЛ 2 - ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И НЕПРИКОСНОВЕНОСТТА

ОБРАЗОВАТЕЛНИ ЦЕЛИ

- Прилагане на стратегии за предотвратяване на физически и психологически рискове, произтичащи от използването на цифрови технологии
- Разграничаване на нежелани въздействия върху околната среда, произтичащи от използването на цифрови технологии-
- Насочване на връстници и ученици към използването на технологични ресурси, полезни за социално включване.

КОМПЕТЕНТНОСТИ, БАЗИРАНИ НА DIGCOMP

4.1 Управление на дигитални идентичности

Умения:

- S1. Критично използване на различни цифрови идентичности и контекстуалното им ползване.
- S2. Управление на дигитални идентичности, документи и данни, създадени от мен.
- S3. Прилагане на различни методи за защита на дигиталната идентичност.

4.2. Защита на личните данни и неприкосновеността на личния живот в цифрова среда

Знания:

- K1. Рискове, произтичащи от неправилна защита на лични данни или информация.
- K2. Прости инструменти и методи за защита на личните данни и информация.
- K3. Основни аспекти и факти на политиките за защита на личните данни.
- K4 Инструменти и стратегии за защита на лични данни и съдържание (средно ниво).
- K5 Технологични ресурси за защита на данните.

Умения:

- S13. Прилагане на различни методи и инструменти за защита на данните

- S14. Ограничаване на информацията и споделяните данни, контролиране на публичното излагане на данни и информация
- S15. Познаване на различията в политиките за поверителност на използваните

Съдържание:

2.1. Значение на защитата на личните данни и информация

2.2. Инструменти и методи за защита на личните данни и информация онлайн

2.3. Инструменти и методи за защита на личните данни и информация офлайн

2.4. Политики за поверителност и дигитален феърплей

СЕСИЯ 1

- Първоначален диалог: Знаем ли кои лични данни не могат да бъдат споделяни без разрешение? Как можем да защитим личните си данни?
- Обсъждане на казуси в група.
  - Някой е снимал видео как се спъвате и падате на улицата, и иска да го качи в TikTok.
  - Ваш приятел поства във Facebook албум със снимки от лятото, в който има и Ваша снимка по бански.
  - Непознат ви следва в Instagram и коментира снимките ви. Твърди, че ви познава, но вие не знаете кой е той.
- Заедно преглеждаме политиката за поверителност на някоя от социалните мрежи, които ползваме и я обсъждаме.

МОДУЛ 3 - ЗДРАВЕ И ОПАЗВАНЕ НА ОКОЛНАТА СРЕДА

ОБРАЗОВАТЕЛНИ ЦЕЛИ

- Уважаване на авторските права, лицензите и ограниченията за използване на ресурси
- Методи за защита на чувствителни данни

КОМПЕТЕНТНОСТИ, БАЗИРАНИ НА DIGCOMP

3.1. Етично и здравословно използване на цифровите технологии
Знания

- Познаване на ефектите от продължителна употреба на дигитални технологии
- Познава пристрастяващите аспекти на технологиите
- Разбиране на въздействието на компютрите и електронните устройства върху околната среда и рециклиране на дигитални устройства.
- Определяне на безопасни ползване на дигитални технологии.

Умения:

- S11. Умения за прилагане на различни стратегии за предотвратяване на физически и психологически рискове, произтичащи от използването на цифрови технологии
- S12. Разграничаване на различни нежелани въздействия върху околната среда, произтичащи от използването на цифрови технологии
- S13. Умения за напътстване на други при използването на технологични ресурси

3.2. Защита на околната среда
Умения:

- S14.Познаване на различни методи за защита на околната среда от въздействието на цифровите технологии и тяхното използване.

Съдържание:

3.1. Положителни и отрицателни ефекти от използването на дигитални технологии.

3.2. Опазване на физическото здраве по време на използването на технологии.

3.3. Грижа за душевното здраве при използване на технологии и приложения

3.4. Дигитални технологии за социално включване

3.5. Защита на околната среда

СЕСИЯ 1

- Първоначален разговор: Технология и здраве: Влияе ли използването на технологични устройства върху физическото и психическото здраве? Установени са предишни знания и са дадени съвети.
- Учителят възлага на групите да извършат определена дейност (да обобщят, да напишат есе, да направят списък и т.н.) със съвети за превенция на рискове за физическото и физическото здраве при използване на технологиите.
- Съвети за рециклиране.

МОДУЛ 4 - ПРОФЕСИОНАЛНИ ПРОФИЛИ

ОБРАЗОВАТЕЛНИ ЦЕЛИ

- Култивиране на положително отношение към дигиталните технологии, и познаване на възможните рискове и ограничения.
- Запознаване с някои стратегии за превенция, идентифициране и реагиране при опасно използване на цифрови устройства и публикуване на цифрово съдържание от учениците.
- Разработване на стратегии за защита на личните данни и дигиталната идентичност онлайн.
- Запознаване със стратегии за превенция, идентифициране и реагиране на поведението, което оказва негативно влияние върху здравето и благосъстоянието, при употреба на дигитални технологии.

Съдържание

4.1. Професионални профили

СЕСИЯ 1

- Първоначален разговор: „Познавате ли някой, който работи в сферата на киберсигурността?“
- Представяне на електронната книга на Be@CyberPro за ученици.
- Разговор върху представената книга: „Какво ви изненада?“
- Индивидуално занимание "Ако работех в областта на киберсигурността, бих искал да правя..." и какво бихте попитали някой, който работи в областта на киберсигурността?

СЕСИЯ 2

- Посещение на експерт от сферата на информационната сигурност.
- Въпроси и отговори към гостите.
- Презентации по групи: „Най-важното от последните уроци“

ПРАКТИЧЕСКИ НАСОКИ ЗА РОДИТЕЛИ

Целта на това ръководство е да помогне на родителите да говорят с децата си за основните принципи на киберсигурността и да възпитат отговорно и информирано поведение онлайн.

- Поддържайте открит диалог с децата си. Задавайте отворени въпроси, които да им позволят да споделят преживяванията и притесненията си. Това не винаги ще бъде лесно, а и децата ви не винаги ще бъдат отзивчиви. Намерете време, за да оставите разговорът да тече.
- Можете да използвате някои други ресурси, за да започнете разговора, като например
  - Актуални събития
  - Филмови откъси
  - Откъси от телевизионни предавания или сериали, подходящи за възрастовата група на Вашето дете.
- Не е нужно да правите всичко сами. Ако смятате, че детето ви може да има проблем, поговорете с преподаватели в училището, в което учи детето ви, за да можете да действате координирано.
- Говорете открито, без да омаловажавате или смекчавате някои рискове, но и без да преувеличавате реалността.
- Насърчавайте критичното мислене на детето си, като противопоставяте информация от различни източници, или провеждате дейности, в които детето Ви може да сподели своите идеи и мнение.
- Важно е да приспособите тона на диалога спрямо нивото на самостоятелност и зрялост на детето Ви.

В следващите няколко страници ще намерите съвети как да работите по различни проблеми на киберсигурността с детето си у дома.

ЗАЩИТА НА ДИГИТАЛНО СЪДЪРЖАНИЕ И СВЪРЗАНИ УСТРОЙСТВА

ЦЕЛИ

- Създаване на положителни нагласи спрямо цифровите технологии.
- Запознаване с някои възможни рискове и ограничения.
- Умение за разпознаване на някои рискове и заплахи в дигиталната среда, като: фалшиви новини, секстинг, шантаж и др. и как да се предпазим от тях.
- Запознаване с някои мерки за защита и тяхното приложение.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

ДОВЕРИЕ

- Внимавайте как реагирате, ако децата ви кажат, че имат проблем. Това не е момент за обвинения, а за съвместна работа за решаване на проблеми и взаимопомощ.

НАПЪТСТВИЕ

- Напътствайте децата си по отношение на подходящото използване на технологиите.
- Бъдете пример за подражание
- Споделяйте онлайн занимания. Не става въпрос да нахлувате в онлайн пространството на децата си и да "харесвате" всичко, което те публикуват, но бихте могли да прекарвате време заедно в търсене на информация онлайн, необходима на децата Ви за учебно занятие.

НАДЗОР

- Бъдете наясно с онлайн присъствието на Вашите деца, приложенията, които използват най-често и социалните мрежи, в които имат профили.
- Можете да използвате ресурси за родителски контрол, за да ограничите достъпа до опасни сайтове. (Qustodio, Secure Kids или Parental Click са някои примери).
- Следете за съдържание, което насърчава рисково или негативно поведение

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И НЕПРИКОСНОВЕНОСТТА

ЦЕЛИ

- Прилагане на различни стратегии за предотвратяване на физическите и психологическите рискове, произтичащи от неправилната употреба на дигитални технологии и устройства.
- Разграничаване на различни нежелани ефекти върху околната среда, произтичащи от използването на цифрови технологии.
- Напътствие при употребата на технологични ресурси.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

ДОВЕРИЕ

- Работете за създаването на атмосфера на доверие, за да можете да говорите свободно за присъствието на детето Ви в мрежата, за информацията, която получава, и за информацията, която споделя.

ПОДКРЕПА

- Помогнете на децата си да създадат силни пароли.
- Прегледайте заедно опциите за настройките за сигурност на устройствата и на услугите в мрежата, които детето Ви ползва
- Бъдете пример за подражание

НАДЗОР

- Кодексът за поведение на PEGI класифицира приложенията по препоръчителна възраст, за която са предназначени. Прегледайте приложенията, до които децата Ви имат достъп, за да избегнете използването на неподходящи такива.

ЗДРАВЕ И ОПАЗВАНЕ НА ОКОЛНАТА СРЕДА

ЦЕЛИ

- Разработване на стратегии за превенция, идентифициране и реагиране на поведението на децата, което оказва негативно влияние върху здравето и благосъстоянието им, като се използват цифрови технологии.

КАКВО МОЖЕТЕ ДА НАПРАВИТЕ?

ДОВЕРИЕ

- Разговаряйте открито за вредните последици от неподходящото използване на технологиите върху здравето, благосъстоянието или околната среда
- Прекомерната употреба може да повлияе на съня, социалните отношения или ученето. Говорете за това с децата си и определете какво означава „прекомерна употреба“ във Вашия дом
- Доверявайте се на децата си. Вашата роля не е да бъдете техен надзорник, а родител, който да ги напътства, съветва и да им помага да разрешават проблемите си.

ПОДКРЕПА

- Бъдете пример за подражание
- Ако детето ви има проблем и в него са замесени други непълнолетни, свържете се с техните родители или настойници, за да изясните ситуацията и да я разрешите по координиран начин.

НАДЗОР

- Наблюдавайте поведението на децата си и се уверете, че се спазват основните препоръки за подходящо използване на технологиите, без да нарушавате личното им пространство.
- Установете ясни граници, за да предотвратите възможността те да станат жертви или да упражнят насилие чрез технологии.

КОМПЮТЪРНА ИГРА

В рамките на Be@CyberPro, консорциумът разработи многоезична игра, която се използва за изучаване на различни професии и предизвикателства в областта на киберсигурността. Играта е интерактивна, достъпна през браузър, и не изисква допълнителна инсталация на софтуер, за да могат ученици от различни контексти и с различно оборудване да могат да играят.

CLICK HERE TO PLAY THE GAME:

Играта, е разработена така, че за да бъде изиграна, между 40 минути и 1 час - продължителността на един редовен училищен час.

В рамките на играта, учениците влизат в ролята на герой в измислена среда. Главният герой е момиче, което учи в гимназия, и която трябва да се изправи пред серия предизвикателства, свързани с киберсигурността, за да помогне на своите приятели и съученици.

Как се играе играта:

- Следвайте връзката, за да играете играта.
- Ще се появи стартовото меню на играта със следните опции за бутони: Нова игра, Продължи и Опции.

За да започнете, щракнете върху „Нова игра“ с мишката или тракпада.
Когато екранът се зареди, щракнете навсякъде с мишката/тракпада, за да започнете да разговаряте с героите.

- Използвайте стрелките на клавиатурата или кликнете върху даден участък на екрана, за да накарате героя да се движи.
- За да заговорите някой от героите в играта, трябва да се приближите до него.

- Щракнете където и да е върху екрана, за да продължите разговорите.
- Щракнете върху изскачащите бутони с помощта на мишката или натиснете клавиша за въвеждане, за да изберете своя отговор.
- За да преминете в различни стаи, трябва да се приближите към врате.
- Натиснете ESC по всяко време, за да видите менюто с опции.

Ето няколко предложения за използване на играта в класната стая.

- Преди да покажете играта на своите ученици, изиграйте я и вие, за да се запознаете с управлението, историята, както и учебното съдържание, свързано с играта.
- Помислете за начини да включите и родителите на своите ученици.
- Отделете време за последователна игра в клас. За да сте сигурни, че учениците ви ще имат достатъчно "време за игра".
- Преди да започнете, обяснете ясно очакваното поведение по време на използването на играта и последиците от неспазването на тези очаквания.
- Въведете накратко темата и обяснете на учениците целите и сюжета на играта, преди да започнете да я играете.
- Оставете учениците да изиграят първото ниво и ги помолете да спрат играта, когато приключат.
- След като всички са завършили първото ниво, обсъдете с тях какво са научили до момента. Някои предложени точки за обсъждане са:
    - Какво са научили учениците от това ниво.
    - Какво мислят за това, което са научили до момента.
    - Дали някой е имал подобен опит
    - Дали някой е имал трудности при разбирането на материала
    - Дали учениците са мотивирани да продължат с играта?
- Помолете учениците да продължат да играят играта, като следват същата структура (ниво на игра, след това точки за обсъждане)
- Използвайте данните, събрани от дискусиите и обратната връзка, за да създадете уроци, използвайки своите изводи. Например, фокусирайте се върху често срещано проблемно място.

Използването на обучение, базирано на игра, което включва цели, правила, предизвикателства и взаимодействия, може да помогне за ангажиране на учениците и повишаване на резултатите от обучението. Обучението, основано на игри, може също така да спомогне за:

- Изграждането на емоционална връзка с ученето и предмета.
- Предоставянето на възможност за обратна връзка и практика.
- Подпомагането на индивидуална форма на обучение.

Като част от образователната употреба на информационните и комуникационните технологии игриге могат да се използват като инструменти за учене, мотиватори и генератори на любопитство и в резултат на това игрите в класната стая са широко приети като ефективно средство за оптимизиране на ученето и представянето на учениците в ежедневната образователна практика. Положителната връзка между ангажираността на учениците, докато използват игри, е потвърдена от различни независими проучвания през последните години (Cojocariua, Boghiana, 2014; Papadakis, 2018).

РЕФЕРЕНЦИИ

- Ahuja, M. K. (2002). Women in the information technology profession: A literature review, synthesis and research agenda. European Journal of Information Systems, 11(1), 20-34.
- Armstrong, D. J., Riemenschneider, C. K., Allen, M. W., & Reid, M. F. (2007). Advancement, voluntary turnover and women in IT: A cognitive study of work-family conflict. Information & Management, 44(2), 142-153.
- Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. IT professional, 12(1), 24-31.
- Cojocariu, V. M., & Boghian, I. (2014). Teaching the relevance of game-based learning to preschool and primary teachers. Procedia-Social and Behavioral Sciences, 142, 640-646.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
- Crumpler, W., & Lewis, J. A. (2019). Cybersecurity Workforce Gap. Center for Strategic and International Studies (CSIS).
- ENISA (The European Union Agency for Cybersecurity) (2020). ENISA Threat Landscape 2020: Cyber Attacks
- Becoming More Sophisticated, Targeted, Widespread and Undetected. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.
- Erixon, F., & Lamprecht, P. (2018). The next steps for the digital single market: From where do we start. ECIPE Policy Brief, 2, 2018.
- Heaton, C. A. N., & McWhinney, G. (1999). Women in management: the case of MBA graduates. Women in Management Review.
- Kohler, K. (2020). Estonia's National Cybersecurity & Cyberdefense Posture.
- Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economics and Business Review, 5(2).
- Papadakis, S. (2018). Evaluating pre-service teachers' acceptance of mobile devices with regards to their age and gender: a case study in Greece. International Journal of Mobile Learning and Organisation, 12(4), 336-352.
- Parasuraman, S., Purohit, Y. S., Godshalk, V. M., & Beutell, N. J. (1996). Work and family variables, entrepreneurial career success, and psychological well-being. Journal of vocational behavior, 48(3), 275-300.
- Poster, W. R. (2018). Cybersecurity needs women.
- Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. CEPS Policy Insight, (2018/06).
- Reischuk, R. (2019). Let's Encrypt: Cybersecurity disruptieren.
- Sobers, R. (2019). must-know cybersecurity statistics for 2019. Varonis.
- Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. IEEE Security & Privacy, 18(1), 46-54.
- Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National Cyber Security Strategies: Management, Unification and Assessment.

- Trauth, E. M., Quesenberry, J. L., & Morgan, A. J. (2004, April). Understanding the under representation of women in IT: Toward a theory of individual differences. In Proceedings of the 2004 SIGMIS conference on Computer personnel research: Careers, culture, and ethics in a networked environment (pp. 114-119).
- Ventures, 2017
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Този проект с № 2018-1-ES01-KA201-050461 е финансиран с подкрепата на Европейската комисия. Настоящата публикация отразява единствено възгледите на автора и Комисията не носи отговорност за използването на съдържащата се в нея информация.

Co-funded by the
Erasmus+ Progra
of the European