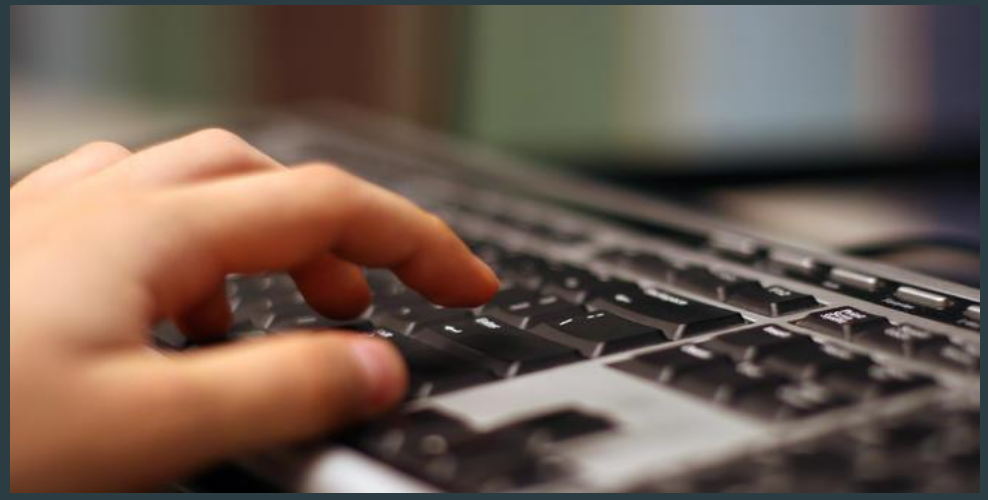
Опасностите, които дебнат в интернет

Интернет – прозорец към света

- С настъпването на сегашното извънредно положение, интернет отвори още по-широко вратата към един свят на безкрайни възможности. В сравнение с общуването в реалната среда, виртуалното пространство е място, където любознателността и творчеството имат много по-голяма възможност за изява, където хората могат да се представят, за това, което искат да бъдат.



Как прекарват времето си децата в интернет?

- Гледат видео клипове, посещават социални мрежи, играят онлайн игри и слушат музика, а в настоящия момент цялото им обучение се осъществява чрез интернет. Децата търсят и намират информация.

Опасностите

- Мрежата крие своите опасности и капани. Различни изследвания показват, че сред най-честите рискове са контакт с неподходящи хора, риск от онлайн тормоз, излагане на неподходящо съдържание, фалшиви профили, споделяне на твърде лична информация, приложения и измами, „вливане“ във виртуалния свят за сметка на реалния.

Опасностите в социалните мрежи

- Огромна част от учениците имат профили в социалните мрежи като facebook, twitter, instagram и други, ползват snapchat, както и сайтове за разговори и запознанства. Именно от социалните мрежи и сайтовете за запознанства идват и най-големите опасности. Когато разговаряме с непознатия отсреща, ние в действителност не знаем дали наистина човекът е това, за което се представя. Дали името му е истинско, дали е на същата възраст, дори дали е от същия пол.

Опасният непознат

„Дебнещите“- Децата са склонни да споделят прекалено много информация в своя виртуален свят. Споделят истинските си имена, датата и мястото на раждане, училището, в което учат, своите приятели, семейството, дори снимки на своя дом. Това са добри предпоставки да улесним максимално човек, поставил си за цел да ни навреди или да се възползва от нас по някакъв начин.

Опасният непознат

Обикновено целта на тези хора е да се сдобият с лична информация, която после да използват срещу нас с цел измами и изнудване, или пък събират снимки с неподходящо съдържание на деца, с цел задоволяване на своите тъмни нагони. Изпращането на една такава снимка води до изнудване и искане на още снимки с още по-неподходящо съдържание, видео клипове и реални срещи. Те лесно откриват деца, които са манипулируеми, които се доверяват, деца, изолирани от другите. Представят се за техни връстници, сближават се, споделят „тайните си“ и когато спечелят достатъчно доверието на едно дете показват истинската си цел.

Цел

Обикновено в началото искат невинни снимки, като изпращат и „свои такива“ (разбира се фалшиви), в един момент искат все по-неприлични снимки. Когато получат снимка, с която да могат да изнудват детето, те се възползват и започват да искат нови и нови. Децата се поддават на изнудването и изпълняват желанията на човека отсреща. А тези хора са невероятни манипулатори и могат да накарат детето да вярва, колко много могат да навредят на него и семейството му, ако то не изпълнява техните желания.

Какво да правя?!

Дори да сгрешиш и да изпратиш снимка на такъв човек, никога не се поддавай на изнудването му, той няма за цел да те издаде на родителите и приятелите ти, няма да спечели нищо от това, неговата единствена цел е да се сдобие с още повече твои предизвикателни снимки. Ако такъв човек потърси контакт с теб, не се замисляй за секунда, веднага кажи на родителите си или на друг възрастен.

Гаджето

„Изоставеното гадже“ – често срещано в интернет е, под влияние на чувствата гаджета да си изпращат еротични снимки, но се случва при раздяла единият да разпространи снимките и да ги качи в мрежата с цел да се подиграе на другия. Обикновено това правят момчетата. Трябва да знаеш, че нещо веднъж качено в мрежата си остава там завинаги, не може да бъде напълно изтрито. Последствията от това могат да бъдат достатъчно сериозни. Така, че колкото и да харесваш гаджето си, по никакъв повод не се снимай и не изпращай снимки, чрез които после може да бъдеш уязвим.

Покана за среща

„Среща с непознат“ – идеята на повечето сайтове за запознанства и разговорите в интернет е да се стигне до среща. Много хора са склонни да отидат на такава среща. Преди да отидеш обаче, помисли дали това наистина е човекът, за който се представя. Искай възможно повече доказателства, че това е той (тя), настоявай да включи камерата си за да го видиш. В днешно време няма човек без камера. Ако все пак решиш да отидеш на такава среща , избери място, на което има много хора, помоли някой твой приятел да те придружи, сподели с приятели къде и с кой отиваш. **СЪВЕТ: НЕ ХОДИ НА СРЕЩА С НЕПОЗНАТИ!!!**

“Fishing”

Фишингът е опит за измама, умишлена заблуда, с цел споделяне на данни за достъп до банкови сметки, онлайн разплащателни процесори, акаунти на доставчици на лицензирани услуги или софтуер, акаунти в онлайн магазини, лични профили, акаунти в социални медии и всякаква друга чувствителна информация.Ако опитът за измама успее и потребителят предостави доброволно исканата информация за достъп, престъпниците влизат в съответния акаунт и последиците от моментното невнимание, небрежност или непредпазливост на жертвата се установяват след време като откраднатата самоличност, източени пари от банкова сметка, изпращане на спам от пощенски акаунти или от профили в социални мрежи и всякакви подобни негативни сценарии.

Класически пример за “Fishing”

Получавате покана да гласувате в някакъв онлайн конкурс, обикновено социално значим. Когато отворите дадения ви адрес, ви изпраща на фейсбук страницата. При по-внимателно наблюдаване, ще видите , че адресът въобще не е “facebook.com”, а нещо съвсем различно. В случай, обаче че не забележите тази разлика, а напишете потребителското си име и паролата, то вие вече сте жертва (Fish). Още по-неприятното е, че когато въведете потребителското си име и паролата наистина ще ви прехвърли на вашият фейсбук профил, и вие може никога да не разберете, че сте жертва на измама. Подобна метод се използва почти във всички измами с кражба на лични данни. Фишинг измами стават и по имейл адрес, на същия принцип.

Как да се предпазим от фишинг атака

- Винаги следете внимателно интернет адреса, на който ви препраща
- Поздрав в писмото - ако имейла претендира да е изпратен от компания, в която имате реален профил, много вероятно е поздравът да съдържа вашето име или фамилия. Липса на поздрав или формален поздрав, липса на име на служител, длъжност, адрес на компанията и *unsubscribe* линк в подписа на съобщението трябва да алармира вашето внимание
- Правописни и граматически грешки, грешно използване на термини от вашата индустрия

Как да се предпазим от фишинг атака

- Чувство за спешност - трябва да задейства ярко червен фишинг флаг
- Пренасочващи линкове - ако писмото е от Google, линковете в него не трябва да водят към страница на Yahoo :)
- Звучи твърде добре, за да е истина - каква е реалната вероятност супер богат нигерийски принц да се обърне към вас за помощ?

Правила за безопасно интернет поведение !!!

Правила за безопасно интернет поведение !!!

Давай възможно най-малко лична информация за себе си – имена, снимки, адреси, училище, местоположение, не качвай видео клипове, на които си ти. Заключвай профила си, нека само познати и приятели виждат нещата, които споделяш.

Избягвай контактите с непознати - не приемай покани от непознати, отказвай чатовете, блокирай тези, които ти досаждат

Ако някой те заплашва или тормози онлайн не оставяй нещата така – сигнализирай на възрастни – родители, учители

Избягвай да качваш снимки в интернет – свои или на твои познати, особено без тяхно разрешение

Правила за безопасно интернет поведение !!!

Изключвай локацията на телефона си – по-добре е непознатите да не знаят къде си сега, къде ще пътуваш.

Изключвай камерата си –Не пускай камерата на непознати, при възможност е добре да сложиш лепенка върху нея. Има достатъчно програми, които могат да те запишат, когато се показваш на камера

Не посещавай сайтове за възрастни

И НАКРАЯ ЗАПОМНИ!!!

БЪДИ ВНИМАТЕЛЕН, СЪРФИРАЙ БЕЗОПАСНО!!!

Къде да подам сигнал?!

https://www.cybercrime.bg/bg/contacts -Официален сайт за борба с компютърните престъпления

https://116111.bg/ -Национална телефонна линия за деца

Полезни страници

- www.cybercrime.bg
- https://www.safenet.bg/
- http://www.az-deteto.bg/safe/
- http://safe.abcbg.com/
- https://www.gdbop.bg/bg/cyber
- https://www.youtube.com/watch?v=y-k4q6V7ERc

Изготвил:
Бистра Тодорова – педагогически съветник