

Министерство науки и образования РД
Государственное бюджетное профессиональное образовательное
учреждение РД
«Колледж экономики и права»

Отчет

Лекция беседа: «Единый урок по безопасности в сети Интернет»

21.10.2021г.



Составил: куратор гр. 493ЧС- 2

Шингарова Амина Мамедовна,

Специальность 20.02.02.

«Защита в чрезвычайных ситуациях»

Дербент 2021

Лекция беседа: «Единый урок по безопасности в сети Интернет»

Цель: формирование информационно-коммуникативной компетенции.

Задачи:

Образовательная:

- ознакомиться с понятием «Интернет», «Вирус»,
- изучить приемы безопасности при работе в сети Интернет;

Развивающая:

- развитие интереса к предмету, информационной культуры;
- формирование приёмов логического мышления;
- развитие способность анализировать и обобщать, делать выводы;

Воспитательная:

- воспитание аккуратности, точности, самостоятельности, привитие навыков групповой работы, сотрудничества;

Здоровьесберегающая:

- соблюдение санитарных норм при работе с компьютером,
- соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;

Ключевые слова: безопасность, компьютерный вирус, методы защиты, сети, мобильный телефон, социальные сети, кибербуллинг, игры.

Форма проведения: урок с применением ИКТ.

Оборудование: мультимедийный проектор, компьютер, карточки с заданиями.

Ход урока:

Организационный момент

- Здравствуйте, ребята! Сегодня наш урок посвящён безопасности. Безопасность нужна всегда и везде. Мы соблюдаем правила безопасности на улице, в колледже, в транспорте и т.д., но важно соблюдать несложные правила при работе с компьютером, а именно в сети Интернет. Вот об этом сегодня и поговорим!

Вводная беседа

- С каждым годом молодежи в интернете становится больше, а учащиеся - одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

Опрос: Какие компьютерные угрозы Вы встречали в своём личном опыте или знаете о них? (ответы учащихся)



Итак, давайте разбираться далее.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ (раздача карточек-памяток)

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливай цифровые заплатки, которые автоматически устанавливаются с целью доработки программы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Работа с памятками (кто из ребят применял данные методы в своей практике)

Сети Wi-Fi

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». Да, бесплатный интернет- доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-Fi: (раздача карточек-памяток)



- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- Используй и обновляй антивирусные программы. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Физпауза

- Выполняем движения по моей команде со словом «безопасно», если я говорю «вирус» - движение выполнять не нужно! Итак, руки вверх – безопасно, руки на плечи – безопасно, руки вниз – вирус и т.д.

- Продолжаем нашу беседу:

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.



Опрос: в каких социальных сетях вы зарегистрированы? Чем они вас привлекают? Что полезного вы находите в них?

Основные советы по безопасности в социальных сетях: (раздача карточек-памяток)

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твоё местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов — анонимные и не анонимные. Разница в том, что анонимные — это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Основные советы по безопасной работе с электронными деньгами: (раздача карточек-памяток)

- Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
- Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
- Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, \$tR0ng!;
- Не вводил свои личные данные на сайтах, которым не доверяешь.

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом: (раздача карточек-памяток)

- Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
- Управляй своей киберрепутацией;
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за

анонимным аккаунтом;

- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
- Соблюдай свой виртуальную честь смолоду;
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
- Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения всеи.

Мобильный телефон

Основные советы для безопасности мобильного телефона: (раздача карточек-памяток)

- Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоего смартфона;
- Используй антивирусные программы для мобильных телефонов;
- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- После того как ты выйдешь с сайта, где вводил личную информацию, зайдя в настройки браузера и удали cookies;
- Периодически проверяй какие платные услуги активированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься.
Не забывай иногда проверять это.

Online игры

Основные советы по безопасности твоего игрового аккаунта: (раздача карточек-памяток)

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
- Не указывай личную информацию в профайле игры;
- Уважай других участников по игре;
- Не устанавливай неофициальные патчи и моды;
- Используй сложные и разные пароли;

- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Цифровая репутация

(опросить ребят об их осведомлённости в этом вопросе, нужно ли беречь свою репутацию, зачем это нужно, как это сделать?)

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации: (раздача карточек-памяток)

- Подумай, прежде чем что-то опубликовать и передавать у себя в блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Рефлексия

- Какие вы знаете компьютерные угрозы?
- Что такое цифровая репутация и как её сберечь?
- Как пользоваться электронными деньгами и стоит ли это делать вообще?
- Как вы себя теперь будете вести в социальных сетях?
- Стоит ли вступать в бой-противостояние с кибер-хулиганами?

Итог урока

- Сегодня мы попытались разобраться в тех угрозах, которые несёт нам Интернет, а также выявили основные правила безопасности, которые соблюдать в будущем вам будет совсем несложно. Памятки помогут вам в этом. Желаю насыщенной, интересной, а главное, безопасной деятельности в сети Интернет.



Использованные интернет-ресурсы:

1. <http://сетевичок.рф/dlya-shkol>
2. <http://www.ligainternet.ru/>
3. <http://www.e-parta.>

Спасибо за внимание!

