**Кабардино-Балкарская Республика**

**Прохладненский муниципальный район**

**Муниципальное казенное общеобразовательное учреждение**

**«Средняя общеобразовательная школа им. С. П. Восканова с. Пролетарского»**

**Тема классного часа:**

**Защита персональных данных**

**Подготовила:**

**классный руководитель 7а класса**

**Есипко Елена Владимировна**

**Март 2024 год.**

**Тема классного часа:**  Защита персональных данных

**Цель:**формирование навыков защиты своих персональных данных и информационной безопасности.

**Задачи:**

1.Разъяснить характер опасностей в сети Интернет: проникновение вирусов и вредоносных программ, спама; обман и мошенничество (кардинг, фишинг); агрессивная коммуникация и оскорбления от других пользователей; предоставление личной информации в интернете.

2.Объяснить правила безопасного использования интернета.

3.Дать понятие о персональных данных и их защите.

4.Указать принципы мобильной безопасности.

**Оборудование:** компьютер, проектор, интерактивная доска.

**Ход классного часа**

**I.Оргмомент**

**II.Сообщение темы и цели классного часа.**

**III. Вступительное слово преподавателя**

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

·                     кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;

·                     кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;

·                     с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;

·                     и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

**IV.Просмотр видеоролика о защите персональных данных**

Видеоролик о защите детских персональных данных

(https://drive.google.com/open?id=0B\_h-XyYaD34udmpKcXBSZEVXMlU)

**V. Сообщение новой информации**

**Кибербуллинг или киберзапугивание**

Развитие коммуникационных технологий изменило нашу жизнь. Обычные процессы отношений между людьми с помощью Интернета, приобретают в цифровом мире новые особенности.

Скорость распространения информации в сети Интернет уже через мгновение позволяет делиться своими жизненными новостями, фотографиями и общаться с множеством людей.

Доступ к размещаемой вами информации может быть ограничен только кругом вашего общения или быть доступным неограниченному кругу лиц. Однако оборот личной информации в сети может приводить к проблемам, когда незнакомцы, прохожие или даже друзья используют информацию безответственно и без учёта права на неприкосновенность частной жизни. Так появился кибербуллинг и возможность при помощи технологий проявлять негативные качества, делать это анонимно, не опасаясь ответной реакции.

Основной площадкой кибербуллинга стали социальные сети. В них можно не только оскорблять человека в сообщениях, но и взламывать страницу жертвы или создавать поддельные страницы на имя жертвы, где размещается унизительный контент, распространяются обидные и непристойные сообщения.

Независимо от формы проявления кибербуллинг может причинить значительный вред жертве, а в крайних случаях привести к самым трагическим последствиям.

Как и их коллег – хулиганов в физическом мире, кибер-хулиганов пытаются убедить перестать нарушать права других людей. Разница в том, что кибер-хулиганы в состоянии скрыть свою личность в Интернете, что затрудняет возможность оперативного пресечения такой деятельности.

**Кардинг** - способ мошенничества с использованием банковских карт.

Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя.

**Фишинг**

**Фишинговые сообщения** - это уведомления, отправленные от имени администраторов банковских или других платежных систем. Они призывают пользователей пройти по фальшивой ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету.

**«Нигерийские» письма, невероятная удача и попрошайки!**

**Уведомления о выигрыше:**

В письме сообщается о том, что ты выиграл крупную сумму денег. Цель мошенника - выманить у тебя деньги за получение выигрыша. Обычно он списывает это на налог. Потеряв бдительность, ты можешь перевести крупную сумму на счет мошенников.

**Попрошайничество:**

Мошенники давят на жалость и отправляют письма с просьбой о помощи якобы от благотворительных организаций или нуждающихся людей.

В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные**.**

**«Нигерийские» письма:**

В тексте такого письма обычно содержится информация о том, что у автора письма есть много денег, полученных не совсем законным путём, и поэтому он не может хранить деньги на счету в банках своей страны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя обналичить крупную денежную сумму, в качестве вознаграждения обещая от 10% до 30% от заявленной в письме суммы. Идея мошенничества заключается в том, что пользователь предоставит доступ к своему счету, с которого позже будут списаны все денежные средства.

**Риски, которые влечёт обмен информацией в Интернете**

К сожалению, реальность такова, что люди выдают слишком много информации о себе в Интернете, испытывая при этом ошибочное убеждение, что принадлежащая им информация является конфиденциальной, но как только информация попадает в Сеть, контролировать ее дальнейшее использование уже практически невозможно. Кто, когда и в каких целях может воспользоваться такими данными, прогнозировать невозможно.

• *В Интернете нет кнопки «Удалить», чтобы удалить информацию, размещённую в Интернете. Вы можете пожалеть о создании, например, комментария в виде замечания по отношению к любому человеку, потом, удалив его в течение часа, крайне удивиться, что этот комментарий уже прочитан десятками или сотнями людей и столько же людей перенаправили его по разным адресам.*

**VI. Решение практических задач**

**Задача  1:**

Именинник после празднования дня рождения выложил в сеть отрицательный комментарий по поводу подарка одного из своих гостей, после чего он подвергся резкой критике со стороны других пользователей, которые в диалоге раскрывали место проведения праздника и свое отношение к нему, на именинника было оказано огромное давление, что привело его к необходимости принести публичные извинения.

**•  Ответ***Возможно, вы осторожный и аккуратный человек, и, прежде чем, выложить фотографию или информацию в сеть воспользовались настройками приватности. Соответственно, к информации, которую размещаете Вы, имеет доступ ограниченный круг лиц, определённый Вами. Однако следует всегда знать и понимать, что вы не будете иметь никакого контроля в случае, когда ваши друзья скопировали информацию и распространили ее в дальнейшем, при этом, не спросив вашего мнения или разрешения.*

**Задача 2:**

Два пассажира в метро поссорились из-за одного свободного места. Спор был заснят на видео другим пассажиром посредством использования смартфона, видео было размещено им в Интернете и разошлось по сети. Интернет-пользователи раскрыли имена и номера телефонов главных героев. В результате в Интернете, после раскрытия личности героев, пассажиры столкнулись с огромным давлением, кроме того резкой критикой поведения двух пассажиров теперь завалено большинство Интернет-форумов.

**•  Ответ**  *То, что вы говорите или то чем вы делитесь в Интернете может повлечь за собой критику. Информация, которой вы поделились с другими может стать мишенью для кибер-хулиганов. Они выставят вас на всеобщее обозрение, подвергнут вас «суду» за ваши он-лайн слова или действия и вынесут вам свой «вердикт».*

**Задача 3:**

Пациент оказался недоволен услугами врача, к которому обратился за помощью и разместил видео, где грубо назвал врача непрофессионалом и заявил, что клиника не соответствует заявленному уровню. Свой гнев он выразил неприятными словами. К его удивлению, пользователи сети нашли его поступок необоснованным и он сам стал объектом нападения. Его фото, домашний и рабочий адреса были опубликованы в Интернете. Была создана даже группа в социальной сети, призывающая его извиниться.

**•  Ответ** *Кибербуллинг также может произойти, когда злоумышленник создает ложную учетную запись жертвы и использует ее для отправления оскорбительных, агрессивных или неуместных сообщений на почту друзей и семьи, а также на их аккаунты в социальных сетях, включая друзей, таким образом, создавая впечатление, что сообщения были отправлены жертвой.*

**Задача  4:**

Девочка поделилась со своей подругой паролем от своего аккаунта в социальной сети. Подруга периодически использовала этот пароль для входа в аккаунт и просматривала личные сообщения и однажды, в своему разочарованию увидела в личных сообщениях отрицательный комментарий по отношению к себе. Тогда девушка под видом своей подруги послала неприятные сообщения многим из ее друзей.

**•  Ответ** *Кибер-хулиганы могут специально создавать поводы заставляя сердиться свою жертву до такой степени, что они рано или поздно отвечают разгневанным или оскорбительным замечанием. После такой реакции кибер-хулиган может уведомить администратора ресурса о недопустимом содержимом и нарушении правил пользования услугами сети, после чего ваш аккаунт может быть заблокирован.*

**Задача  5:**

Подруги сильно поссорились. Обе выплёскивали свой гнев друг на друга на Интернет-форуме. У обеих были свои сторонники, которые довели их оскорбительные комментарии до сведения администраторов ресурса, что привело к блокировке аккаунтов обеих девушек.

•**Ответ***Вы можете быть уверенными, что находитесь в безопасности от кибер-издевательств, если вы никогда не раскрывали ваших личных данных в Интернете. Тем не менее, поскольку Интернет настолько проник в нашу обычную жизнь, любое лицо, Интернет-пользователь или нет, является уязвимым к безответственному онлайн – поведению.*

В законодательстве отсутствует конкретное положение, предусматривающее ответственность за кибер-издевательства, это вызвано тем, что такая деятельность довольно широка и охватывает собой значительный перечень уже имеющихся составов преступлений и правонарушений, это в первую очередь нарушение права на неприкосновенность частной жизни, выражающееся в незаконном сборе или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну. Также в соответствии с Конституцией Российской Федерации достоинство личности охраняется государством и ничто не может быть основанием для его умаления, никто не должен подвергаться унижающему человеческое достоинство обращению или наказанию. Основным законом, определяющим порядок оборота персональных данных, является Федеральный закон «О персональных данных» № 152-ФЗ, который содержит ряд принципов, помнить и знать которые необходимо. Например, сбор личных данных для преступных целей недопустим, потому что сама цель незаконна. Даже если данные предоставлены субъектом самостоятельно, это не даёт права третьим лицам использовать такие данные по своему усмотрению.

**Специальные персональные данные ( см. презентация- дополнение)**

**К специальным персональным** данным относятся*:*

*расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.*

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам. Например, человек может сказать: я демократ или я христианин. По таким данным можно сформировать представление о человеке.

Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

**Биометрические персональные данные**

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся:

*отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.*

**Набор цифр как персональные данные**

Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить как конкретного человека, установить нашу личность.

*Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.*

Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию. Шифрование может производиться банковской организацией, например, номер банковской карты тоже индивидуальный, он не повторяется и принадлежит исключительно держателю банковской карты.

**Большие данные**

Каждое наше действие, совершаемое в сети Интернет, оставляет определенный цифровой след.

Такие следы оставляет информация, которую вы добровольно размещаете в сети Интернет, например, фотографии в социальных сетях, высказывания на форумах, «лайки» новостей и многое другое.

Кроме того, цифровые следы оставляет та информация, о наличии которой вы можете и не подозревать, например, информация о посещенных сайтах, о совершенных покупках, о вашем географическом месторасположении и пр.

Если обработать всю эту информацию, то получится очень точный портрет («профайл»), который можно использовать для принятия решений в отношении конкретного человека. Например, направить ему адресную рекламу в соответствии с предпочтениями, «лайками» или отказать в поступлении на работу и пр.

Сегодня информационные технологии позволяют обрабатывать и анализировать огромные объемы данных для выявления новой информации, представляющей ценность для принятия различных решений.

Представьте себе данные о следах всех пользователей сети Интернет России или другой страны, которые они оставили за последние 10 лет.

Этот колоссальный объем информации, подлежащий обработке и анализу, получил название BigData или Большие данные.

При этом Большие данные получают не только благодаря Вашим цифровым следам, их добывают из иных источников, например, с помощью датчиков погоды или геолокационных систем.

**VII. Подведение итогов классного часа**

**Составление памятки**

1**)     Ограничить объем информации о себе, находящейся в Интернете;**

**2)     Не отправлять кому-либо свои данные, не убедившись, что адресат – действительно тот, за кого себя выдает;**

**3)     Если в сети Интернет кто-то просит предоставлять ваши персональные данные, посоветоваться с родителями;**

**4)     Использовать только сложные пароли, разные для разных учетных записей;**

**5)     Заводить себе два адреса электронной почты: частный и публичный.**

**VIII. Рефлексия деятельности на классном часе.**

**Памятка по персональным данным.**

1) Ограничить объем информации о себе, находящейся в Интернете;

2) Не отправлять кому-либо свои данные, не убедившись, что адресат – действительно тот, за кого себя выдает;

3) Если в сети Интернет кто-то просит предоставлять ваши персональные данные, посоветоваться с родителями;

4) Использовать только сложные пароли, разные для разных учетных записей;

5) Заводить себе два адреса электронной почты: частный и публичный.

Появились вопросы, обращайся на портал ***персональныеданные.дети***

---------------------------------------------------------------------------------------------------

**Памятка по персональным данным.**

1) Ограничить объем информации о себе, находящейся в Интернете;

2) Не отправлять кому-либо свои данные, не убедившись, что адресат – действительно тот, за кого себя выдает;

3) Если в сети Интернет кто-то просит предоставлять ваши персональные данные, посоветоваться с родителями;

4) Использовать только сложные пароли, разные для разных учетных записей;

5) Заводить себе два адреса электронной почты: частный и публичный.

Появились вопросы, обращайся на портал ***персональныеданные.дети***

----------------------------------------------------------------------------------------------------

**Памятка по персональным данным.**

1) Ограничить объем информации о себе, находящейся в Интернете;

2) Не отправлять кому-либо свои данные, не убедившись, что адресат – действительно тот, за кого себя выдает;

3) Если в сети Интернет кто-то просит предоставлять ваши персональные данные, посоветоваться с родителями;

4) Использовать только сложные пароли, разные для разных учетных записей;

5) Заводить себе два адреса электронной почты: частный и публичный.

Появились вопросы, обращайся на портал ***персональныеданные.дети***