План-конспект занятия
Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Тема занятия: Медиаурок «Защита персональных данных в сети Интернет»
Целевая аудитория: школьники в возрасте от 9 до 18 лет.
Цель занятия: ознакомление учащихся с понятием "персональные данные", формирование теоретических знаний и практических навыков безопасного поведения в сети Интернет.
Задачи занятия:
образовательные: формирование устойчивых знаний по теме «персональные данные».
развивающие: развитие коммуникационной компетенции, навыков индивидуальной практической деятельности.
воспитательные: формирование ответственного отношения к персональным данным и личной информации.
Тип занятия: изучение нового материала, обобщение и систематизация знаний.
Форма деятельности: фронтальная.
Методы обучения: словесно-визуальный (ознакомления с новым материалом в форме просмотра медиаурока).
Оборудование: проектор, проекционный экран, персональный компьютер (иное оборудование, позволяющее демонстрировать аудио-видеофайлы).

Ход урока:
1. Организационный этап: приветствие, готовность к уроку.
2. Постановка темы и целей урока. Введение.
- «Персональные данные» - что такое персональные данные и какие они бывают;
- опасности в сети Интернет при использовании личной информации.

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить как конкретную личность.
Таких идентифицирующих данных огромное множество, к ним относятся:
фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.
Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.
Получается, что персональные данные - это не просто ваши фамилия или имя, персональные данные - это набор данных, их совокупность, которые позволяют идентифицировать вас.

В целом можно сказать, что персональные данные - это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

3. Трансляция видеоролика «ВГТРК» (11 минут).

4 . После просмотра ролика обсуждение с учащимися основных тезисов и смысловых направлений видеосюжета (10 минут):

- ошибки при размещении информации в сети Интернет;
- как избежать разглашения своих персональных данных: допустимый объем информации при размещении в сети.

5. Просмотр видеоурока: кибербуллинг (5 минут) Обсуждение.

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.

Существует много каналов, по которым наши персональные данные попадают в интернет. Что - то выкладываем мы сами, что то пишут о нас наши друзья и знакомые, определенную информацию собирают приложения и онлайн-ресурсы. Все наши «цифровые следы» хранятся в наших компьютерах и смартфонах. Если вы хотите сохранить определенный уровень конфиденциальности и хорошую репутацию в сети, эти «следы» необходимо контролировать. Важно знать, что они хранятся и на серверах разработчиков приложений и онлайн - ресурсов и удалить их

оттуда практически невозможно. Поэтому всегда надо крайне внимательно относиться к той информации, которую вы выкладываете в сеть, а также к тому, что вы делаете в интернете, какие ресурсы посещаете, какие файлы скачиваете, какие поисковые запросы делаете.

Персональные данные, размещенные в сети Интернет самим субъектом персональных данных, становятся общедоступными, и доступ к ним получает неограниченный круг лиц. Причем в пользовательских соглашениях многих социальных сетей изначально поставлено условие согласия пользователей на общедоступность и согласие на право пользования ими третьими лицами. Поэтому, регистрируясь в социальных сетях, необходимо внимательно читать условия регистрации и правила пользования сайтом.

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.

6. Просмотр видеоурока: как защитить свои персональные данные (7 минут).

Обсуждение: как защитить гаджеты от вредоносных программ.

1. Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.
3. Используйте проверенные сайты. Прежде чем вводить свои данные убедитесь, что вы находитесь именно на том ресурсе, на который хотели попасть, а не поддельный (фишинговый) странице, созданной мошенниками. Всегда обращайте внимание на адресную строку браузера. Адрес поддельной страницы может отличаться всего на одну букву, которую легко не заметить.
4. Систематически проверяйте свои домашние компьютеры на наличие вирусов.
5. Делайте резервную копию важных данных.
6. Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

7. При использовании мобильных устройств отключайте функции, которые не нужны в данный момент времени (например: геолокация, Wi-Fi).
8. При установке приложений на мобильные устройства внимательно читайте условия пользовательского соглашения.
9. Не стоит переходить на ресурсы по ссылкам, которые вы получили по электронной почте или в личной переписке и которые требуют ввода персональных данных - многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а лучше используйте для поиска нужных ресурсов надежные поисковые системы, например Яндекс.
10. Прежде чем вводить персональные данные в Интернете, убедитесь, что ресурс использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры Https://

7. Заключение:

- подведение итогов: что усвоено, что нового узнали;
- вопросы учащихся по теме урока.