Методическая разработка конспект занятия «Организация места за компьютером. Безопасность в Интернете. Угрозы, правила личной безопасности» в рамках сетевого взаимодействия

Цель: освоение учащимися основных правил безопасного поведения при столкновении с различными видами интернет-угроз.

Задачи:

- познакомить с понятием «кибербезопасность»;
- рассмотреть различные угрозы в сети Интернет;
- изучить основные правила безопасного поведения при работе в Интернете;
- рассмотреть способы отличия в Интернете учащимся негативной, вредной и опасной информации, а также уметь проверять информацию на достоверность.

Ожидаемые результаты:

- ученик научится использовать в повседневной практической деятельности (в том числе – размещать данные) информационные ресурсы интернет-сервисов и виртуальных пространств коллективного взаимодействия, соблюдая авторские права и руководствуясь правилами сетевого этикета;
- ученик получит возможность научиться критически оценивать информацию, полученную из сети Интернет.

Развивать универсальные учебные действия:

Личностные: формирование культурного пользователя Интернета. Готовность обучающихся к конструктивному участию в принятии решений, затрагивающих их права и интересы.

Метапредметные: осуществлять деловую коммуникацию как со сверстниками, так и со взрослыми. Координировать и выполнять работу в условиях реального, виртуального и комбинированного взаимодействия.

Предметные: овладение основами безопасного поведения в сети Интернет. Применять правила безопасного поведения для защиты личности.

План урока

I. Организационный период

II. Подготовка учащихся к усвоению нового материала

III. Теоретическая часть. Изучение нового материала

IV. Практическая часть. Первичное закрепление знаний

V. Рефлексия

Ход урока

I. Организационный период

Ученики готовятся уроку, приветствие, проверка присутствующих.

II. Подготовка учащихся к усвоению нового материала

Учащимся на экране включаем видеоролик https://www.youtube.com/watch?v=9OVdJydDMbg. После просмотра задаем вопрос «Как вы думаете, какой теме будет посвящен наш урок? Что они увидели в этом видеоролике?»

Учащиеся приводят примеры, высказывают свое мнение.

III. Теоретическая часть. Изучение нового материала

- Да, как вы уже сказали, наш урок посвящен безопасности в Интернете. На сегодняшний день появился новый термин «Кибербезопасность», это не просто защита данных, а формирование культуры поведения в сетевом пространстве. Сегодня на уроке Вы познакомитесь с понятием «Кибербезопасность», какие бывают информационные угрозы в сети Интернет, как они проявляются, что является источником информационных угроз, какие бывают способы защиты личной безопасности в сети и уметь проверять информацию на достоверность.

- И так, что вы понимаете под словом «Кибербезопасность»?

Ответы учащихся.

Кибербезопасность – это умение оценить достоверность информации, умение сохранить свои личные и персональные данные, умение защитить свои и не нарушить чужие авторские права.

В настоящее время мы являемся активными пользователями Интернета, в том числе и дети, начиная с раннего возраста используют Интернет, они предоставляют доступ к свои личным данным, а цифровые устройства за каждым из них непрерывно наблюдают. Передвижения, разговоры, приобретения, круг общения, фотографии, запросы – всё это, при желании, отслеживается, то есть осуществляется глобальный сбор информации о любом пользователе Интернета.

- Как вы думаете, для чего ведется сбор информации о пользователе?

Учащиеся приводят примеры, высказывают свое мнение.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы в Интернете, а может, о каких-то угрозах вы слушали от своих родителей, по телевидению?

Учащиеся приводят примеры.

Молодцы! Перед вами на экране представлен список самых распространенных угроз в сети Интернет.

Рассмотрим каждую угрозу более подробно:

(На каждом слайде приведены примеры)

– **Фишинг** (от англ. – «рыбалка») - это несанкционированный доступ к паролям и логинам. Мошенничества, связанные с поддельными или несуществующими Интернет-магазинами, с фишинговыми сайтами, которые полностью копируют официальные сайты банков, социальных сетей и т.д.

– **Фарминг –** это тип мошенничества похожий на фишинг, характерным отличием которого является скрытая переадресация ничего не подозревающих пользователей на поддельные сайты для последующей установки вредоносного ПО или похищения таких конфиденциальных данных, как пароли, учетные или банковские данные.

Фишинговые сайты внешне ничем не отличаются от официального, однако, на самом деле является фишинговым. Ничего не подозревающий

человек переходит на фальшивую страницу и вводит свои данные (к примеру, логин и пароль для авторизации). В результате таких действий, владельцы фишингового сайта получают доступ к аккаунту жертвы. Фишинговый сайт можно отличить от официального по названию адреса сайта. Например, сайт Вконтакте, посмотрите внимательно на фотографию. Как вы думаете, официальный сайт это или нет?

Учащиеся отвечают «Нет».

- Как вы об этом догадались?

В адресе сайта есть лишняя буква vkontaktte, есть лишняя буква t.

- Правильно, в адресе сайта присутствует лишняя буква? Представим другой случай, вам необходимо скачать браузер Chrome. С какого сайта вы его будете скачивать?

Ответы учащихся (например, с любого или с официального сайта).

- Как вы узнаете официальный это сайт или нет?

Ответы учащихся.

- Надо обращать внимание на адресную строку. Сайты с протоколом https, как правило, являются более защищенными, чем сайты с более распространенным протоколом http. Это поэтому, что незаконным сайтам нет дела до получения сертификата.

- Если вы попадетесь на крючок фишинговых мошенников, что необходимо сделать в первую очередь?

Ответы учащихся.

- Да, срочно менять пароль в учетной записи официального сайта.

– **Смс-мошенничество -** это предложение отправить сообщение на короткий номер, согласие на рассылку приводит к уменьшению средств на телефонном счету без уведомления хозяина.

- Приходили вам такие сообщения? Как вы поступали в этом случае?

Ответы учащихся.

Здесь тоже существуют простые правила:

•оценить реальность информации. Например, подумать, где мог бы находиться якобы попавший в беду родственник. Позвонить ему лично на мобильный телефон;

•обратить внимание на номер отправителя. Мошенники часто используют похожие номера возможного реального отправителя;

•если получатель решил перезвонить, то на счету к списанию должна быть доступна минимальная сумма;

•если вы получили смс с короткого и неизвестного номера о снятии денег с вашей банковской карты и вас просят в ответ отправить код. Не надо никому ничего отправлять. Прежде всего, надо убедиться в этом, позвонив на горячую линию банка по бесплатному номеру.

– **Кибербуллинг –** это подростковый психологический виртуальный террор и давление на жертву, жертвой становятся из-за вредоносных ссылок и непроверенных приложений. Кибербуллинг связан с унижениями и оскорблениями, угрозами в социальных сетях.

Здесь важно знать, что кибербуллинг, как и прямое психологическое насилие являются уголовно наказуемыми, даже несмотря на анонимность. Поэтому будьте аккуратны в социальных сетях, никого не унижайте, не оскорбляйте, не распространяйте личные данные человека. За это могут привлечь к уголовной ответственности.

Поэтому первоочередным для защиты от подобных атак являются:

•сбор фактов, угроз, преследований, шантажа, которые нужно сохранить, распечатать для доказательства, для обращения в полицию;

•использовать функцию блокировки, в любом мессенджере и в социальных сетях она присутствует;

•никогда не стоит следовать требованиям агрессора, вступать в переговоры или пытаться откупиться;

•не пытаться с угрозами бороться в одиночку, необходимо оповестить родителей.

«Кражи личности» - это кража аккаунта в социальной сети, онлайн игре, системе обмена информацией и действия от имени данной личности.

Обычно мошенники взламывают аккаунт в социальных сетях и пишут от вашего лица вашим друзьям, родственникам сообщение с просьбой одолжить денег до завтра и т.д.

Правила защиты точно такие же, как и при смс-мошенничестве.

Безвыигрышные онлайн-лотереи, для участия в которых нужно заплатить небольшую сумму, как правило, через отправку платной смс. В Интернете появились такие опросы, где якобы можно выиграть деньги.

Очень часто встречается в Интернете такая реклама «Пройди опрос и получи деньги». Вопросы самые простые и в разных опросниках одинаковые. Пройдя этот опрос, чтобы получить выигрыш, необходимо внести якобы «закрепительный платеж», сумма небольшая, поэтому многие люди переводят, а взамен ничего не получают.

Встреча с нежелательным контентом

Нежелательный контент — это все, что в идеальном мире не должен видеть ребёнок до своего совершеннолетия: порносайты, паблики про оружие, наркотики, самоубийства, алкоголь и так далее. Именно нежелательный контент, согласно данным «Лаборатории Касперского», — самая частая угроза, с которой сталкиваются дети в интернете. При этом почти половина опрошенных подростков признают, что скрывают от взрослых подробности онлайн-жизни: часто это как раз увиденные сайты, фильмы и сериалы, не подходящие им по возрасту.

Непреднамеренная трата денег

Очень часто мошенники обманывают детей и крадут деньги через бесплатные приложения, тесты в соцсетях, почтовые рассылки. Жертвам предлагают перейти по ссылке, ввести номер телефона или банковской карты взрослых, отправить смс или одолжить деньги вдруг попавшему в беду другу. Результат как правило один — списание денег в неизвестном направлении. Вывод средств может происходить и вполне легально.

Кибергруминг

Во время кибергруминга взрослый устанавливает эмоциональную связь с подростком в соцсетях с целью дальнейшей сексуальной эксплуатации.

Преступники создают профиль, заполняют его выдуманной информацией и чужими фотографиями. Чтобы втереться в доверие, они общаются на интересные для ребенка темы, делают ему комплименты. Как показало одно исследование, опытный преступник может уговорить ребенка на личную встречу за полтора часа.

По данным «Лаборатории Касперского», больше половины детей в возрасте 7-18 лет получали в сети приглашение «дружить» от незнакомых людей, в 34% случаев это были взрослые. Более того, к каждому девятому ребёнку в возрасте 11-14 лет незнакомцы уже пытались «втереться в доверие». А каждый третий школьник даже встречался с людьми, с которыми познакомился в соцсетях.

Как вы видите, угроз много и вы должны уметь находить наличие угрозы в Интернете и обезопасить себя и свои данные. Для этого необходимо соблюдать основные правила защиты личной безопасности.

- ни в коем случае не переходить по подозрительным ссылкам;
- скачивать приложения и программное обеспечение только с официального сайта;
- не поддаваться унижениям, оскорблениям в сети Интернет;
- не переводить деньги в подозрительные компании;
- игнорировать подозрительные смс-сообщения.

Не меньший шквал сетевых опасностей обрушивается и на детей, которые в силу возраста, отсутствия знаний или опыта не всегда могут им противостоять. Поэтому, наша задача — стать кибергероем для ребенка и защитить его от онлайн-угроз.

Кибербуллинг

Кибербуллинг, или онлайн-травля — это сообщения с угрозами, оскорбления, сплетни, призывы бойкотировать конкретного человека. С последствиями интернет-буллинга детям приходится справляться в реальном мире. По данным «Лаборатории Касперского», 33% детей слышали или сталкивались с онлайн-травлей. А между тем кибербуллинг приводит к

снижению самооценки и успеваемости в школе, замкнутости, бессоннице и даже депрессии.

Просмотр видеоролика «Ты не один»

https://resh.edu.ru/page/cyberproject-4

Травля (буллинг) – одно из самых опасных явлений в коллективе. С ней может столкнуться любой, и очень важно заранее иметь определенный «иммунитет» к агрессии. Особенно это важно в интернет-среде. С одной стороны, она кажется более безопасной, ведь мы не сталкиваемся с обидчиком лицом к лицу. С другой стороны, травля в сети может быть очень изобретательной и неожиданной.

Особенность кибербуллинга в том, что он возникает в пространстве, которое по определению небезопасно. Проявления травли в такой среде обычно заметны. Но в сети ребенок в значительной степени предоставлен сам себе. Поэтому так важно, чтобы он осознавал угрозы и думал о безопасности.

Дети часто стараются молчать, если сталкиваются с преследованием в интернете. Так же им трудно заранее распознать ситуации травли в сети, отличить их от обычного общения или безобидного интереса.

Не стоит забывать, что дети могут быть не только жертвами кибербуллинга, но и быть теми, кто занимается травлей в интернете. Мы должны сначала понять, почему дети это делают. Вот краткий обзор восьми основных причин, по которым дети используют интернет для издевательств.

Причина: Месть

Когда детей подвергают издевательствам, они часто ищут мести, потому что не справляются с ситуацией более здоровыми способами. Мотивация заключается в возмездии за боль, которую они испытали. Они чувствуют себя оправданными в своих действиях, потому что их тоже преследуют и мучают. Запугивая других, они также могут испытывать чувство облегчения. Эти дети часто подвергают кибербуллингу своего обидчика. В других случаях они нацеливаются на кого-то, кого они считают слабым или более уязвимым, чем они.

Причина: Они верят, что жертва этого заслуживает

Запугивание часто вращается вокруг социального статуса человека в школе. Например, девочка может стать объектом кибербуллинга от анонимной группы девушек, которые надеются вывести ее на ступеньку или две ниже в социальной лестнице школы. Или, наоборот, средняя девочка могла бы травить девушку, которая отлично учится, потому что ревнует к ее успеху. Какими бы ни были причины, дети иногда считают, что их поведение оправданно. Следовательно, они обычно не чувствуют угрызений совести или вины за кибербуллинг.

Причина: Просто скучно

Дети, которые скучают и ищут развлечений, иногда прибегают к кибербуллингу, чтобы добавить в их жизнь какое-то волнение и драму. Часто им не хватает внимания и надзора со стороны взрослых. В результате интернет становится их единственным источником развлечений и способом привлечения внимания. Вместо того, чтобы найти другие возможности провести свое время, они развлекаются, создавая цифровую драму.

Причина: Давление сверстников

Иногда дети пытаются таким образом вписаться в группу. Они больше заботятся о том, чтобы устроиться в коллективе, чем беспокоятся о последствиях.

Причина: Они думают, что все это делают

Когда подростки считают, что много людей запугивают онлайн, они, скорее всего, будут делать то же самое. В их сознании это не кажется значительной проблемой, потому что их группа сверстников поступает точно так.

Причина: Увеличивают свою значимость за счет других

Кибербуллинг может быть проявлением социального статуса. Дети, которые популярны, часто высмеивают детей, которые менее популярны. Точно так же дети, которые привлекательны, могут выделить других, которых они считают непривлекательными. Они используют интернет для реляционной агрессии. Дети, которые пытаются подняться по социальной

лестнице в коллективе или школе, прибегают к кибербуллингу, чтобы привлечь внимание. Какова бы ни была мотивация, общая цель состоит в том, чтобы увеличить свою значимость, уменьшив силу кого-то другого.

Причина: Они верят, что их не поймают

Анонимность интернета дает детям ложное чувство безопасности. Они считают, что их не поймают. Более того, дети, которые используют интернет для буллинга не обязательно видят реакцию жертвы, что позволяет очень легко говорить и делать это.

Причина: Они считают, что это не страшно

Большинство детей, которые издеваются в интернете считают, что это неважно. Поскольку они не видят боли, которую причиняют, то не чувствуют раскаяния в своих действиях. Было проведено исследование при котором, большое количество детей сообщили, что использование онлайн-издевательств заставляет их чувствовать себя забавными, популярными и крутыми.

Чтобы дети не занимались кибербуллингом, говорите им о последствиях издевательства над другими в интернете. Помимо этого, убедитесь, что они знают, как запугивание заставляет других чувствовать себя. Предоставляя им возможность делать правильный выбор, вы уменьшите вероятность того, что они будут участвовать в этом разрушительном поведении.

Буллинг в интернете существует во множестве форм.

Бойкот

Эта форма кибербуллинга проявляется в том, что жертву исключают из всех кругов общения в интернете. Группы, чаты, паблики – любая площадка, где происходит общение. При этом изгнание может быть (и часто бывает) молчаливым: человеку об этом даже не сообщают. Изгнание может быть и неявным – в этом случае сообщения жертвы просто игнорируются. Исключенного не допускают к играм, встречам и другим активностям.

Если обстановка в классе или коллективе располагает к травле, поводом для исключения может стать любая мелочь: ребенок «странно»

общается (не знает сленга, пишет неграмотно – или, наоборот, слишком грамотно), состоит «не в тех» группах, слушает «не ту» музыку. Исключать могут и за то, что у ребенка (в отличие от остальных) нет смартфона или он не пользуется социальными сетями.

Домогательство

Один из самых опасных видов травли в интернете. При нем ребенку постоянно присылают личные сообщения: угрожают, оскорбляют, высмеивают, ведут с ним психологические игры – например, задают вопросы и подлавливают на «неправильных» или «глупых» ответах. Одноклассники могут делать это в качестве «наказания», ради веселья или просто потому, что ученик им не нравится.

Эта форма кибербуллинга особенно опасна тем, что у нее обычно нет внешних свидетелей. Если ребенок, столкнувшийся с домогательствами, не сообщает о них, ситуация может продолжаться долго, а агрессор имеет над ней полный контроль. Когда сообщения приходят постоянно, у ребенка нет времени сделать передышку. Такой прессинг может напугать ребенка и сделать неуверенным в себе.

Главный принцип защиты: при первых признаках агрессии (требования, угрозы, шантаж) заканчивать разговор. Не реагировать на попытки буллера возобновить его. Если домогательства повторяются, нужно заблокировать агрессора и сообщить об этом факте взрослым.

Троллинг

Это слово знакомо всем. И это один из самых распространенных вариантов буллинга в интернете. Троллингом называют общение в провокационном стиле, часто с использованием оскорблений или ненормативной лексики. Троллинг очень похож на издевательства в реальной жини. Но у интернет-тролля есть преимущества: он может выступать анонимно, писать с фейковых аккаунтов, атаковать в любой удобный ему момент.

Разъясните детям, что основная цель тролля – унизить, разозлить жертву и заставить ее выйти из себя и перейти на оскорбления. Троллю

всегда нужна «пища» в виде явных обид, ответных выпадов, угроз. Тот, кто не поддерживает общение с троллем, игнорирует его сообщения и комментарии, рано или поздно перестанет быть ему интересен. Поэтому лучшая тактика в этом случае – игнорирование. Но если троллинг перерастает в угрозы – стоит обязательно обратиться к взрослым.

Аутинг

Публикацию личной информации человека без его согласия называют Аутингом. Причем к травле относится именно целенаправленная публикация такой информации с целью его унизить или шантажировать. Сюда же относятся и угрозы распространить личную информацию, передать ее учителям, полиции, использовать для создания клеветнических публикаций.

Главный способ предотвратить аутинг – выкладывать минимум личной информации в общедоступное поле. Не публиковать в соцсетях номер телефона, не вывешивать адрес, не открывать свой аккаунт для незнакомых людей, не давать читать свои личные переписки третьим лицам. И, как и в случае с другими видами буллинга, нужна четкая позиция: угрозы аутингом – это травля. О ней нужно обязательно сообщать –взрослым, психологу, на анонимный телефон помощи.

Диссинг

Распространение информации, которая может опорочить человека-это диссинг В оффлайне диссинг обычно существует в форме сплетен и слухов. При травле в соцсетях к нему добавляется создание «фотожаб», оскорбительных мемов, сфабрикованных текстов сообщений, скриншотов с недостоверной информацией.

Чтобы запугать жертву, буллеры часто преувеличивают «компрометирующий» характер информации – например, пугают жертву, что за нахождение в определенных группах или выражение определенных взглядов ее исключат, «посадят», у ее родственников будут проблемы. Жертве могут внушать и без всяких доказательств, что знают о ней нечто «нехорошее».

Борьба с диссингом похожа на борьбу с троллингом. Агрессору важна реакция, важно понимать, что он контролирует жертву и может принудить ее плясать под свою дудку. Если и отвечать на «диссы», то спокойно, с юмором, Но лучше всего не показывать, что тебя в принципе задели нападки.

Фрейпинг

Получение доступа к аккаунту, и измена его данные (в том числе пароль и коды доступа, что делает невозможным его вернуть) и публикации с нежелательным контентом от имени владельца – называется Фрейпинг. Обычно цель буллера в том, чтобы выставить жертву в смешном, глупом виде. Но чем старше, тем опаснее могут быть эти действия – вплоть до написания агрессивных комментариев и сообщений от лица владельца, аутинга и размещения запрещенного контента.

Фрейпинг – один из самых болезненных приемов кибербуллинга, он наносит ребенку огромное унижение. Необходимо познакомить ребенка с навыками цифровой безопасности (создание надежного пароля, использование двухфакторной идентификации, осторожность при посещении сайтов, которые требуют коды и пароли). Объясните, что резкое, необычное изменение данных аккаунта друга или одноклассника может говорить о перехвате аккаунта.

Если ребенок все же стал жертвой фрейпинга, ему нужно обратиться к руководству сети. Как правило, доступ к аккаунту через какое-то время можно вернуть. Чем скорее это будет сделано, тем меньше шансов, что обидчик причинит ребенку большой вред. Объясните, что угон аккаунта – неприятно, но не смертельно. Такое случается, и другие отнесутся к этому с пониманием и быстро забудут о случившемся.

Кетфишинг

Этот способ похож на фрейпинг и тоже связан с манипуляциями с аккаунтом. Только на этот раз агрессор не угоняет его, а создает новый, полностью идентичный оригинальному профилю жертвы. Там могут быть все доступные фотографии, тот же текст – или слегка измененный. С

помощью «фейка» агрессор может троллить других, устраивать провокации или пытаться выставить владельца оригинального профиля на посмешище.

В отличие фрейпинга, этот вид буллинга в интернете не требует сложных манипуляций – для этого достаточно иметь минимум доступной информации. Сложность борьбы с кетфишингом в том, что его не всегда можно вовремя отследить. Агрессор за подложным профилем может никак не контактировать с владельцем оригинала, а «окучивать» его знакомых или оставлять следы в группах, в которых он состоит.

Главный метод борьбы с кетфишингом в соцсетях – написание запроса к администрации сайта с просьбой удалить «фейковый» профиль. Если все же агрессор успел «наследить», можно разместить на своем профиле (в статусе, в ленте) сообщение такого содержания: «ВНИМАНИЕ! От моего лица действует фейковый профиль. Если он пишет вам, оскорбляет или провоцирует вас, знайте: это не я».

Что бы не стать жертвой:

Не выкладывайте в сеть лишнюю информацию или медиафайлы, которые могут компрометировать Вас или Ваших знакомых. Также не стоит отправлять такую информацию людям, которые не вызывают доверия.

Не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться желание мести.

Игнорируйте сообщения, в которых Вас оскорбляют, унижают или угрожают. Также стоит уведомить о таких сообщениях администрацию сайта или сервиса.

Не угрожайте хулигану «найти и наказать». Это лишь спровоцирует его на продолжение социального давления и усугубит ситуацию.

Удалите злоумышленника из социальных сетей, заблокируйте доступ к Вашей странице, добавьте в черный список.

Не присоединяйтесь, если Ваши друзья дразнят, кого- то в сети. Попросите их остановиться, предупредите о вредных последствиях кибермоббинга.

Чаще меняйте пароли в социальных сетях, так как злоумышленники могут писать от Вашего имени.

Как уберечь ребенка от киберугроз

Научить ребенка основам кибербезопасности быстро вряд ли получится. Это процесс комплексный, требующий сил, терпения и времени. Приступать к обучению лучше всего с момента, когда ребенок получает первый гаджет.

Обсуждать онлайн-жизнь

Компания AVG провела онлайн-опрос взрослых и опекунов из России об уровне независимости детей в Интернете и обнаружила, что только 32% опрошенных регулярно обсуждают с детьми, что они делают и чем делятся в сети. Ещё 45% россиян иногда обсуждают с детьми их онлайн-активности. Из тех, кто не обсуждает безопасность в интернете, 14% заявили, что просто не хотят; 6% сказали, что не будут чувствовать себя комфортно; и 4% хотели бы, но их дети противятся этому.

Онлайн-пространство будет более безопасным, если взрослые и дети будут обсуждать подходящее поведение в онлайне, возможные риски, а также что делать, если какая-то ситуации или какой-либо человек в интернете заставляет чувствовать ребенка некомфортно. Открытые и честные разговоры являются одним из лучших способов защиты от киберзлоумышленников, ненадлежащего контента и интернет-травли.

Научить сетевому этикету

Современные дети, в отличие от нас, не знают времен «до интернета». Для них это неотъемлемая часть жизни. По данным «Лаборатории Касперского», более 70% детей общаются с друзьями в онлайне. И если в младших классах страничка в социальных сетях есть у 43% детей, то к старшей школе этот показатель возрастает до 95%. Запреты тут не сработают. Поэтому вместо того, чтобы наглухо оградить детей от интернета, лучше подумать, что предложить взамен.

Как и в реальной жизни, основой общения в онлайне должен стать сетевой этикет. Интернет помнит все. Поэтому важно научить ребенка общаться в нем так, чтобы не было стыдно ни за одно оставленное слово или отправленный файл. Научите его уважать приватность других людей, не разжигать конфликты, делиться проверенной информацией и помнить, что приоритет в общении всегда отдается реальному собеседнику.

Рассказать про основы безопасной жизнедеятельности в сети

Главное правило — не все, что кажется реальным в интернете, реально на самом деле. Научите ребенка сохранять приватность: не оставлять в соцсетях личную информацию вроде домашнего адреса или адреса школы, имен взрослых и номеров телефонов. Не ставить геометки в местах, где он часто бывает. Не встречаться с незнакомыми людьми из сети без вашего ведома. Даже если знаком с человеком давно, не делиться с ним логинами, паролями и прочей конфиденциальной информацией.

Расскажите, что даже если его страница закрыта и доступна только для друзей, пароль могут украсть. Научите ребенка не кликать на подозрительные баннеры и не переходить по подозрительным ссылкам.

Научить говорить «нет»

Очень важно научить ребенка не бояться отказывать. Как рассказывает Григорий Сергеев, один из основателей, и председатель поисково-спасательного отряда «Лиза Алерт», «в нашей работе мы довольно часто сталкиваемся с пропажей детей после того, как они пообщались в соцсетях и пошли куда-то вместе с незнакомыми взрослыми. Поэтому очень важно научить ребёнка говорить «нет» любому незнакомцу, который не является его родственником или хорошим другом семьи».

В случае с соцсетями ситуация может выглядеть не так однозначно, ведь ребёнку кажется, что он знает того человека, с которым собирается встречаться, — они же уже общались и успели подружиться. Эксперт рекомендует наблюдать за жизнью детей в соцсетях: иметь доступ к странице, быть в курсе, кого они добавили в друзья и какой контент публикуют.

Погрузиться в онлайн-мир ребенка

Если ребенок постоянно сидит в телефоне, не спешите его «пилить». Лучше искренне поинтересуйтесь, что он делает в интернете, какие сайты посещает, какие видео смотрит. С разрешения ребенка понаблюдайте, что и как о делает. Задавайте вопросы. Поощряйте навыки критического мышления и оценки правдоподобности.

Иногда дети боятся или не считают нужным делиться со взрослыми подробностями своей интернет-жизни. И часто взрослый бывает последним, к кому они пойдут за советом в случае проблемы. Чтобы этого не произошло, отношения с ребенком нужно выстраивать, когда гаджеты только входят в их жизнь. И, конечно, вместе проводить время без гаджетов. Доверяя вам, детям будет проще обсуждать с вами свою жизнь в интернете.

Просмотр видеоролика https://resh.edu.ru/page/cyberproject-1 - фильм «На игре»

Наслаждайтесь онлайн-пространством вместе — обменивайтесь веселыми и интересными видео, играйте в онлайн-игры, выбирайте красивые фото, чтобы поделиться с друзьями. Таким образом, дети будут чувствовать, что взрослые понимают их увлечения, смеются над теми же шутками и к ним можно обратиться в случае проблемы.

Стать для ребенка примером

Прежде чем учить ребенка кибербезопасности, взрослому не помешает самому овладеть этой наукой.

Контролировать ситуацию

Есть множество инструментов контроля за детьми в интернете. Браузеры блокируют опасные или нежелательные сайты. Мобильные, планшеты и игровые приставки часто оснащены собственными средствами родительского контроля. Кроме того, все больше производителей разрабатывают гаджеты специально для детей: функции защиты присутствуют в них по умолчанию. Тем не менее, прилагаем список популярных решений.

Использование данных приложений позволит быть в курсе, где находится ребенок, сколько времени он проводит в интернете, какие сайты посещает, что пишет в соцсетях. Так же есть игры, которые помогут детям познакомиться с кибербезопасностью.

IV. Практическая часть. Первичное закрепление знаний.

Чтобы закрепить наши знания, поиграем с вами в онлайн-игры:

https://learningapps.org/9922731

https://learningapps.org/10003308

https://learningapps.org/9921801

V. Рефлексия

Вопросы ученикам:

1. Была ли для вас услышанная на уроке информация полезной?
2. Была ли для вас услышанная на уроке информация новой?
3. Будете ли вы применять полученные знания в своем личном опыте?

Литература

1. Бороненко Т.А., Кайсина А.В., Федотова В.С.. Международный электронный научный журнал. «Развитие цифровой грамотности школьников в условиях создания цифровой образовательной среды», 2019 г.
2. ГольчевскийЮ.В., НекрасовА.Н.«К вопросу о кибербезопасностиинтернет-пользователей»
3. Король В.В., Пашкова В.А., Даньшина Н.А., Самойленко О.Б. Ученые записки Орловского государственного университета. №2 (83), 2019 г. «Современные аспекты обучения безопасности в сетевом пространстве».
4. Ратинер Т.Г. «Информационно-психологическая безопасность школьников при работе в интернете // Современное образование», 2014 г.
5. https://nbpublish.com/library_read_article.php?id=10923
6. https://ok.ru/video/363025207737
7. https://www.avast.ru/c-phishing