**«Цифровой след.**

**Профилактика угроз в Интернете»**

**лекция для родителей**

**Целевая группа:** родители (законные представители) обучающихся 5–11 классов общеобразовательных организаций, студентов 1-2 курсов.

**Цель:** проинформировать родителей о цифровых угрозах, предупредить о возможных последствиях действий школьников в интернет-пространстве.

**Задачи:** показать родителям какие риски имеет цифровая деятельность и от каких угроз важно защитить ребёнка.

**Время проведения**: 7-10 мин.

**Оборудование:** демонстрационный экран, ПК.

**Характеристика проблемы:**

В настоящее время виртуальный мир стал неотъемлемой частью нашей жизни. Онлайн-присутствие играет огромную роль для каждого, поэтому важно уметь управлять своими действиями в цифровой среде и научить этому детей. Ведь все, что мы делаем в интернете, может оставить след на нашей цифровой репутации. Кроме того, онлайн-профиль становится важным аспектом личности, и умение управлять цифровым образом становится необходимостью.

**Слайд 1.**

Цифровая репутация - это образ, который создается о пользователе в сети на основе размещенных им постов, комментариев, фотографий и видеороликов. Дети часто не задумываются об этом.

**Слайд 2.**

При этом каждое действие, совершенное в интернете, оставляет свой цифровой след. Современные технические средства легко позволяют объединить «цифровые следы» одного пользователя в единый портрет.

**Слайд 3.**

Интернет помнит все. На первом месте распространяемой информации – геоданные. На 40 % за год выросло число записей с номерами дома, школы, или места частого пребывания подростков.

**Слайд 4.**

Любые действия в сети остаются там навечно:

- файлы cookie

- поисковые запросы

- история посещения сайтов

- комментарии в соцсетях

-характеристики вашего устройства и пр.

**Слайд 5.**

Наши данные собирают: электронные карты и электронные дневники, камеры в подъездах, компьютеры и смартфоны, планшеты, наушники, смарт-ТВ, умные часы и фитнес-браслеты, интерактивные образовательные порталы.

Сейчас становится нормой, что работодатели при рассмотрении кандидатов на вакансии в компании, сначала изучают профиль кандидата в социальных сетях. Если образ кандидата негативный и потенциально может причинить вред репутации компании, его не пригласят даже на собеседование!

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на реальной жизни ребенка.

**Слайд 6.**

Анализ профилей в социальных сетях несовершеннолетних, проведенный АНО «Центр изучения и сетевого мониторинга молодежной сети» показал, что более 500 профилей несовершеннолетних в Республике Алтай содержат признаки существующего риска проявления девиантного и деструктивного поведения. Таким образом, уже только по одному профилю в социальных сетях ваш ребенок может быть отнесен к категории риска.

**Слайд 7.**

Поэтому важно разъяснять, что в сети накапливается информация о месте жительства, учебе, финансовом положении, особенностях характера, интересах и наклонностях и важно следить за тем:

• как выглядят профиль подростка в интернете;

• какие цифровые следы они оставляют;

• какие ресурсы посещают;

• какие файлы скачивают;

• какие поисковые запросы делают.

Стоит поговорить с ребенком о том, задумывался ли он о том, что:

• Комментарии, размещенные фотографии могут не исчезнуть даже после того, как их удалили.

• Кто-нибудь может сохранить размещенную вами информацию, сделав скриншот или репост.

• Размещенную в сети информацию можно найти и много лет спустя.

• За распространение запрещенных законом материалов в социальных сетях могут привлечь к ответственности, даже уголовной.

**Слайд 8.**

Необходимо знать самим и проинформировать ребенка о том, что на посты, лайки, репосты и комментарии, содержащие раскрытие личной информации, клевету, порнографические элементы, угрозы убийства, призывы к вражде, массовым беспорядкам, нарушению целостности РФ, терроризму, прямое оскорбление личности или власти распространяется Уголовная ответственность.

В соответствии с ч. 3 ст. 20.1 КоАП РФ действия, связанные с распространением в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, квалифицируются как мелкое хулиганство, и в подобных случаях виновному грозит штраф от 30 до 100 тыс. рублей.

**Слайд 9.**

Даже если ребёнок минует киберпреступников, есть риск, что ему навредит нежелательный контент: фейки, насилие, нецензурная лексика, сцены употребления алкоголя и другая запрещёнка, а также прочий «взрослый» контент.

По данным исследований центра «Безопасность 2.0» одной из основных причин кибербуллинга в отношении детей в прошлом году стал контент, который выкладывают родители. Им пользуются агрессивные одноклассники, начинающие травлю в интернете. По данным центра, за год только таких ситуаций стало на треть больше или 23% от общего числа выявленных сетевых конфликтов. Зафиксировано около 8 тыс. случаев, когда количество активных или пассивных участников травли превысило 100 человек.

Например, фото в неловкой ситуации или видео с семейного праздника могут быть использованы одноклассниками для издевательств.

**Слайд 10.**

Травлю в интернете могут организовывать и незнакомые люди. На первых этапах это может быть не чистая травля, а флейминг — спор ради спора и нагнетание негатива.

На слайде представлены различные виды кибербуллинга.

**Слайд 11.**

Причиной возникновения травли эксперты центра также назвали чрезмерную открытость несовершеннолетних. Кроме того, угрозу представляют кража личных данных, деструктивные сообщества и мошеннические манипуляции вокруг политических тем, а также недостоверная информация, полученная от нейросетей.

С развитием нейросетей стало сложнее отличить достоверную информацию и легче ввести пользователей в заблуждение, что также может быть использовано как инструмент для манипуляций, подчеркнули эксперты.

Эксперты выделяют новый тренд, связанный с использованием преступными и запрещенными организациями различных онлайн-игр, сообществ в соцсетях. Через них с помощью манипуляций детей склоняют совершать реальные преступления.

**Слайд 12.**

**Как родителям защитить ребёнка в интернете:**

Согласно опросу Альянса по защите детей в цифровой среде, родительскому контролю больше доверяют учителя, а вот родители и подростки единогласны в методе понятных объясняющих ликбезов по цифровой безопасности

Родительский контроль — это полезно, но не всегда выход. Подобные функции предлагают расширения для браузера на домашнем компьютере, антивирусы для любой техники, встроенные или скачиваемые приложения на смартфон и планшет и прочие. Такое ПО может ограничить доступ к опасным ресурсам, не дать скачать вирус, ограничить доступ к приложениям и играм по времени и длительности.

Однако подобные ограничения — это примерно, как шлагбаум в чистом поле: для ребёнка, а тем более подростка обход препятствий может превратиться в увлекательное испытание собственной ловкости и находчивости. Так что полагаться только на ограничения нет смысла. Предлагаем системное решение, которое защитит не от разовой угрозы, а в целом научит ребёнка избегать угроз.

**Слайд 13.**

Говорить о безопасности в интернете полезно с детьми как можно раньше. Важно объяснять причины волнений и запретов, приводить примеры и случаи из жизни. Например, вместо «Нельзя никому давать ПИН-код и CVV банковской карты» понятнее и убедительнее прозвучит: «Нельзя, потому что с карты могут списать все деньги. Помнишь, когда у бабушки списали 15 тысяч с карты и она очень переживала? Всё потому, что она по наивности продиктовала коды злоумышленникам».

Стоит также объяснить, что за аватаркой очень милого в общении ребёнка может скрываться опасный взрослый и что любые аккаунты могут взломать мошенники и писать со страниц друзей. И конечно, что никто никогда просто так не предлагает деньги и подарки. Это ловушка.

Помогите установить настройки приватности: сделать публикации доступными только для друзей, спрятать общедоступный номер телефона и другие чувствительные данные. А ещё полезно подписаться на ребёнка и проверять, не публикует ли он что-то слишком личное.

**Слайд 14.**

**Боремся с кибербуллингом:**

Стоит подключиться, если ребёнок столкнётся с травлей в Сети. В этом случае важно заблокировать обидчиков, ограничить доступ к странице и отключить комментарии к постам. Не стоит отвечать им: агрессоры добиваются именно ответной реакции. Если угрозы принимают серьёзный характер, собираем доказательства (скриншоты и ссылки) и обращаемся в полицию.

Если ребенок уже попал в такую ситуацию, когда его высмеивают за опубликованные фото или видео, ему важно объяснить, что с ним всё в порядке, а люди могут смеяться над чем угодно. Кроме того, важно обратиться за помощью к детскому или семейному психологу, чтобы совместно поработать над ситуацией.

**Слайд 15.**

**Расскажите ребенку о маркерах цифровой угрозы:**

- вопросы о месте жительства, домашнем адресе;

- попытки выяснить номер телефона, Ф. И. О. и другие данные;

- просьбы одолжить и перевести деньги;

- просьбы перейти по ссылке, где нужно ввести номер телефона, почту, а особенно любые пароли и код от карточки (своей, родителей);

- предложения скачать файлы неизвестного происхождения.

**Слайд 16.**

**Объясните детям, что цифровая репутация – это их лицо в сети, поэтому важно сделать все возможное, чтобы она была безупречной.**