КИБЕРБУЛЛИНГ ИЛИ ВИРТУАЛЬНОЕ ИЗДЕВАТЕЛЬСТВО

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

Виды кибербуллинга

Троллинг – провокативные сообщения или комментарии, которые должны вызвать эмоциональный ответ.

Хейтинг – более агрессивные, чем троллинг, нападки личностного характера, безосновательная критика.

Киберсталкинг (киберпреследование): жертва получает повторяющиеся сообщения с различными угрозами. Это также сбор личных данных жертвы, чтобы потом использовать их во вред.

Секстинг – рассылка личных фото- и видеоматериалов жертвы с целью подорвать репутацию, навредить.

Игнор, исключение: жертву исключают из групп, форумов, сообществ в сети.

Взлом или создание фейковых аккаунтов для того, чтобы публиковать недостоверную информацию о жертве.

Методы борьбы с кибербуллингом

Никогда не отвечать на киберагрессию.

Травля всегда направлена именно на вытягивание эмоций — при их отсутствии агрессору становится неинтересно продолжать. Если жертва включается в диалог, ее комментарий сразу же используется для дальнейшего раздувания конфликта.

Зафиксировать факт буллинга.

Сделать скриншот или фото. Это поможет доказать администрации учреждения или правоохранительным органам, что педагог не выдумал травлю.

Помнить, что жертва не виновата.

Во время травли педагог может испытывать стыд или вину и думать, что он что-то сделал не так, чем-то спровоцировал травлю. Как правило, это не так и зачинщик «набрасывается» на педагога только из-за его профессионального статуса — «Ты здесь главный? Ну, сейчас получишь».

Сообщить о травле. Если травля продолжается, нужно заблокировать агрессора в соцсетях или мессенджерах. Затем отправить письма администрации интернет-ресурса или сервиса с требованием оперативно заблокировать контент и его распространителей. Например, нажать кнопку «Пожаловаться» на конкретной публикации или сообщении. Все крупные площадки сегодня понимают масштабы кибербуллинга, поэтому разбираются в ситуации в течение суток.

Дальше следует оперативно сообщить администрации учреждения о происходящем — она сможет задействовать доступные ей механизмы и методики для решения проблемы. Кроме того, необходимо оповестить родителей несовершеннолетних фигурантов травли, если агрессия исходит от детей. Если сообщения содержат в себе угрозы, клевету, порочат честь и достоинство, стоит обращаться в правоохранительные органы

Обратиться за помощью. Для поддержки своего эмоционального состояния педагогу, столкнувшемуся с травлей, можно также получить консультацию психолога.

Как предотвратить травлю в интернете

Выстраивать личные границы. Оговорите с родителями правила общения: как личного, так и виртуального. Договоритесь о том, общаетесь на «ты» или на «вы», обсудите недопустимость мата и другой сниженной лексики. Кроме того, заранее расскажите о том, как вы проводите уроки и оцениваете успехи учеников — это сформирует правильные ожидания у родителей и, возможно, предотвратит часть конфликтов.

Соблюдать правила осторожного поведения в интернете. Если есть возможность, закрывайте личную страницу от родителей и детей, оставляйте доступ только к профессиональной странице, на которой вы делитесь информацией об обучении.

Оценивайте риски каждой публикации в соцсетях. Наиболее опасными становятся посты с указанными геоданными, а также фотографии на фоне дорогостоящих вещей: машин, бытовой техники, дорогого ремонта, аксессуаров. Люди публикуют их ради внимания, но это тоже может стать поводом для травли. Нужно помнить, что педагоги становятся публичными персонами, и фотографии с бокалом вина могут также вызвать недовольство со стороны родителей.

Вместе с этим важно понимать, где именно стоит что-либо публиковать, а где — нет.

Формировать здоровые отношения с администрацией учреждения. Доверительные отношения помогут педагогу обратиться за помощью и советом. Администрация со своей стороны должна организовать площадку взаимодействия между родителями и педагогом. Руководителям образовательных организаций нужно знать основы конфликтологии и выстраивания отношений при кибербуллинге. И регулярно с педагогами рассматривать разные кейсы, как выходить из подобных ситуаций.

ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
“ЦЕНТР ТВОРЧЕСТВА “ЭВЕРЕСТ”
Г.МОГИЛЕВА”

ИНФОРМАЦИОННАЯ ПАМЯТКА

ЦИФРОВАЯ БЕЗОПАСНОСТЬ ДЛЯ ПЕДАГОГОВ

СОЦИАЛЬНЫЕ СЕТИ

Для коммуникации в сети интернет педагог должен грамотно выстроить собственное сетевое пространство: правильно презентовать себя в сети интернет, выстраивать и поддерживать отношения с учащимися, создавать и развивать сообщества. Это подразумевает высокую ответственность при использовании социальных сетей. Поведение педагога в социальных сетях может проявляться в виде:

- **Отказа от общения в социальной сети с учениками.** При таком поведении педагога в социальных сетях уменьшается эффективность воспитания учащихся, однако оно способствует обучению детей уважению личного пространства учителя и демонстрирует возможность использования социальных сетей, не выставляя личную жизнь напоказ.
- **Включения учеников в «друзья», общение с ними в социальных сетях.** Данный инструмент воспитания является наиболее эффективным, т. к. непосредственно затрагивает безопасность детей в сети интернет и вопросы учительской репутации и авторитета. Соответствие образа педагога в реальной и виртуальной жизни способствует повышению доверия среди учеников.

Главными направлениями, которым необходимо уделить особое внимание педагогам, активным в сети, являются:

- культура поведения и речи;
- размещаемая информация, в том числе фото- и видеоконтент;
- степень открытости информации о себе и своих друзьях;
- контроль включения в группы посторонних пользователей;
- самоконтроль вступления в группы с сомнительным и/или порочащим имя содержанием;
- педагогическая работа.

Наблюдая за активностью педагога в социальной сети и просматривая размещенные им материалы, ученики воспринимают эту информации как допустимую и приемлемую.

Репутация педагога в сети интернет напрямую зависит от:

- самопрезентации пользователя,
- его поведения в виртуальном пространстве,
- уровня культуры общения и размещаемого контента.

Во избежание потери педагогом репутации и для поддержания своего авторитета среди учеников и их родителей, следует соблюдать некоторые правила:

- не размещать в своем аккаунте фото и видео сомнительного содержания;
- не использовать ненормативную лексику и нецензурную брань;
- не оскорблять/подшучивать («троллить») других пользователей.

Для обеспечения безопасности учеников в сети педагогу рекомендуется придерживаться следующих правил:

- личный профиль должен быть открыт только для друзей;
- ученики в списке друзей скрыть ото всех;

группа класса приватная – вступить в нее можно только по приглашению администрации.

Социально ответственный учитель может целенаправленно проводить с детьми педагогическую работу в сети.

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".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая 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 РАБОТЫ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI:

1. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера

2. Используйте и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство

3. При использовании Wi-Fi отключите функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе

4. Не используйте публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту

5. Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://"

6. В мобильном телефоне отключите функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ?

1. Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию. При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.
2. Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили. Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номеру и с какой целью.
3. Проверяй адрес сайта. Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.
4. Обращай внимание на наполнение сайта. Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку. 5. Не переходи по незнакомым ссылкам.
6. Не открывай файлы из писем или сообщений, которые прислали незнакомые люди.

КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

1. Взлом аккаунтов в соцсетях и рассылка сообщений от друзей. Мошенники придумывают разные ситуации и просят срочно перевести деньги.
2. Сайты-подделки. Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-поделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.
3. Рассылка писем по электронной почте и в соцсетях с выигрышем. Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.
4. Звонки с поддельных номеров. Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.
5. Шантаж. Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях. Современные технические средства позволяют мошенникам подделать любой номер телефона, любой сайт, взломать почту или личную страницу. Будьте бдительны и перепроверяйте информацию.