ПАМЯТКА ПЕДАГОГАМ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.

2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.

3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.

4. Проявляйте интерес к "виртуальной" жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.

5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставайте на посещении проверенных сайтов.

6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.

7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.

8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.

9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.

10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.

11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью.

12. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

Риски учителя

Ваши ученики куда лучше разбираются в современных технологиях, чем вы можете себе представить. Многим взрослым приходится время от времени заглядывать в справочные материалы, чтобы разобраться в тонкостях работ программ и приложений, а вот молодежь со всем этим на «ты». Они интуитивно понимают, как работают приложения, мобильные устройства и онлайн-платформы, причем настолько хорошо, будто бы проработали с ними всю жизнь.

Это значит, что, имея соответствующую мотивацию, ваши ученики вполне могут подобрать пароль к вашим учетным записям. Например, какая-нибудь ученица недовольна своей оценкой: если она взломает ваши учетную запись, то сможет с легкостью исправить свои отметки. А если какой-нибудь ученик захочет вас разыграть, то ничто не помешает ему заменить все изображения в вашей презентации, над которой вы так долго работали в PowerPoint.

Возможны ситуации, когда ваши ученики окажутся киберпреступниками, однако возможны и другие — в которых они уже будут жертвами.

Вы — учитель, а потому вы обязаны защитить своих учеников и рассказать им про кибербезопасность, чтобы они могли защититься в Интернете.

Ученики как источник опасности для учителя

Пусть даже совершенно случайно и без злого умысла, но ваши ученики и их цифровые привычки могут здорово подставить как их самих, так и одноклассников, вас и даже всю вашу школу.

Защищайте свои записи.

1. Используйте «школьный» адрес электронной почты для регистрации на образовательных порталах. Так вы отделите свой личный адрес электронной почты от учетных записей, к которым могут получить доступ ваши ученики.
2. Придумывайте сложные пароли. В паролях должны использоваться строчные и заглавные буквы, цифры и символы. Тогда угадать пароль будет сложнее.
3. Меняйте пароли раз в три месяца.
4. Для разных аккаунтов используйте разные пароли. Например, пароль от личного кабинета на школьном портале не должен совпадать с паролем от личной страницы в социальной сети. Если кто-то подберет один ваш пароль, то не сможет взломать и все остальные ваши учетные записи.
5. Воспользуйтесь системами двухфакторной аутентификации, если возможно. Здесь вам потребуется не только ввести пароль, но и указать специальный код, который будет отправлен вам на электронную почту или телефон. Это лучший способ защитить важные учетные данные (например, личную почту или банковский личный кабинет). Многие сервисы поддерживают двухфакторную аутентификацию, но если вы не знаете, как ее включить, то обратитесь в техподдержку соответствующего сервиса.

Мобильная защита.

Вы активно пользуетесь смартфонами: для общения с друзьями, проверки почты, просмотра социальных сетей. С помощью смартфона имеется возможность проверять домашние работы и отчеты учеников и ставить им оценки. Смартфоны очень удобны и полезны, но также крайне уязвимы ко взлому учениками.

Ваш смартфон, возможно, дорогой, но хранящиеся на нем данные еще более ценные. Фотографии, аккаунты в социальных сетях и банках, личная переписка и прочая конфиденциальная информация — вот что хранится в смартфоне.

4 способа защиты конфиденциальных данных, хранящихся на смартфоне, от потенциальных хакеров:

1. Регулярно обновляйте ваши устройства. Хакеры специально ищут уязвимости в компьютерах системах, причем им удается находить их почти так же быстро, как специалистам по другую сторону баррикады — устранять их. Нет на 100% безопасной компьютерной системы, однако регулярное обновление ПО смартфона было, есть и остается самой надежной мерой его защиты. Советуем включить автоматическое обновление ОС и приложений.
2. Используйте биометрические пароли. Это одни из самых надежных способов авторизации для мобильных устройств. Защитить свой смартфон можно, настроив вход или разблокировку экрану по отпечатку пальца, если такая возможность есть.
3. Отключайте Wi-Fi и Bluetooth почаще. Рекомендуем отключать эти сети, пока вы не пользуетесь смартфоном. Таким образом ваше устройство станет менее заметным.
4. Загляните в настройки шифрования. Заводские настройки смартфона и базовые настройки приложений могут быть недостаточно мощными. Если ваше устройство не зашифровано по умолчанию, активируйте эту опцию. Также настройте права доступа различных приложений к вашим данным.

С помощью этих мер вы защитите свой смартфон как от учеников, так и от потенциальных хакеров, с которыми вы можете столкнуться где угодно, если у вас при себе есть смартфон или планшет.

Личная конфиденциальность и безукоризненная онлайн-репутация

Вы — учитель, а потому вам следует строго контролировать все, что могут найти о вас в Сети ваши ученики. Если они узнают о том, что вы недавно пережили разрыв отношений, или увидят ваши фото с какого-нибудь концентра, или прочитают какое-нибудь ваше неоднозначное высказывание, то могут перестать чувствовать себя комфортно в одном классе с вами или даже усомнятся в вашем авторитете. А вы сами прекрасно понимаете, насколько важно оставаться для учеников авторитетом.

Чтобы защитить свою личную информацию от учеников (и всех остальных, кому вы не доверяете), вам необходимо грамотно скрыть свое онлайн-присутствие.

1. Поищите информацию о себе в поисковиках. Все, что вы можете найти через Google и прочие системы, ваши ученики тоже найдут. Этот метод позволит найти все, что есть о вас и про вас в Сети. Далее вы сможете найти источник и удалить

оттуда данные, чтобы ваши ученики или кто-нибудь другой уже не получил к ним доступ.

2. Измените настройки конфиденциальности. Многие аккаунты по умолчанию недостаточно приватны. Если вы хотите защитить свои личные данные от учеников, то сделайте все записи, твиты и другой контент в социальных сетях приватным, видимым только вам или вашим подписчикам. Так вашим ученикам будет гораздо сложнее что-то про вас найти.
3. Удалите или отключите учетные записи, которыми вы не пользуетесь. Если у вас есть старая учетная запись в какой-нибудь социальной сети, которой вы давно не пользуетесь, то удалите или отключите ее. Так ее никто не взломает и не будет что-то писать от вашего имени. Если вы хотели бы оставить старые учетки, то переведите их в приватный режим.
4. Обязательно меняйте настройки безопасности всех устройств имеющих возможность выхода в Сеть.

Интернет в классе

Школьная локальная сеть, скорее всего, и станет основным способом выхода в Интернет для вас и ваших учеников. С ее помощью можно заблокировать доступ к нежелательным сайтам и улучшить киберзащиту школы.

Опять же, ученики могут обойти сетевые ограничения самыми разными способами и получить доступ к заблокированным сайтам. К услугам учеников есть VPN-сети, прокси-сервисы и портативные браузеры. Все эти инструменты позволяют обходить блокировки и загружать нежелательный онлайн-контент во время учебы — прямо в вашем классе! Это может быть опасно как для них самих, так и для учебного процесса.

Для обеспечения ограничения доступа детей к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред здоровью и развитию детей, содержащейся в сети «Интернет» создана Единая сети передачи данных (далее – ЕСПД). Среди сервисов ЕСПД наиболее важным является контент-фильтрация по технологии «белых списков», которая представляет собой список разрешенных адресов, в которые включаются сайты из каталогов образовательных ресурсов, сайтов образовательных учреждений и образовательных порталов, а также любые другие, соответствующие нормам безопасности. Все ресурсы, которые не попали в «белый список», автоматически блокируются. Так как эта фильтрация осуществляется не на компьютере или школьном сетевом оборудовании, а на оборудовании провайдера, доступ к запрещенной информации блокируется еще до загрузки в школьную сеть, обойти такую защиту невозможно.

Внедрение ЕСПД позволило создать универсальный механизм блокирования доступа к информации, наносящей вред здоровью и развитию детей, содержащейся в сети «Интернет».

Угроза кибербуллинга (интернет-травли)

Кибербуллинг заключается в использовании технологии для преследования, унижения, запугивания или высмеивания другого человека. Кибербуллинг может оказать разрушительное влияние на развитие детей и подростков, причем даже в долгосрочной перспективе.

Как понять, стал ли ученик жертвой онлайн-травли

1. Ребенок/подросток кажется более одиноким или изолированным от окружающих. Столкнувшиеся с онлайн-травлей дети зачастую отстраняются от друзей и начинают думать, что никому не могут довериться.
2. Неожиданные или внезапные проблемы с друзьями. Порой кибербуллингом начинают заниматься сами друзья ребенка/подростка. Разумеется, что в такой ситуации проводить время вместе с ними ваш ученик/ученица уже не захочет.
3. Неожиданные изменения эмоционального фона. Сюда можно отнести чувства опустошенности, тревоги, грусти и злости.
4. Ребенок/подросток необычно часто расстраивается, в том числе по неожиданным поводам. Вывести из равновесия ученика, ставшего жертвой онлайн-травли, может что угодно. Также это может связано с действиями других учеников, напоминающих жертве о том, что происходит или произошло в Сети.
5. Ухудшение успеваемости. Ставшие жертвами онлайн-травли ученики испытывают сложности с концентрацией на учебе (как следствие страха, тревоги и стресса), из-за чего их оценки начинают ухудшаться.
6. Ученики начинают отвлекаться на занятиях или не обращать внимания на учителя. Жертвы кибербуллинга погружены в себя — в свои страх и волнение, а потому уделяют гораздо меньше внимания и сил работе на уроке.
7. Частые пропуски занятий. Если кто-то из ваших учеников столкнется с онлайн-травлей со стороны одноклассников, то может начать прогуливать уроки, чтобы избежать контакта с ними.
8. Потеря интереса к внеклассным занятиям. Дети и подростки, ставшие жертвой кибербуллинга, могут заявить о желании бросить все свои кружки и секции, лишь бы держаться подальше от своих преследователей. Также они могут начать проявлять меньше интереса к внеклассной деятельности из-за стыда, скромности или страха вновь столкнуться с травлей.
9. Ученики начинают страдать от все усиливающихся проблем с самооценкой. Дети и подростки, ставшие жертвой онлайн-травли, чувствуют себя все менее и менее уверенно, так как могут начать верить во все негативное, что про них говорят.
10. Ухудшение физического самочувствия. Эмоциональный и ментальный стресс, вызванный кибербуллингом, может также стать причиной ухудшения физического самочувствия.

Также необходимо научить учеников, что надо делать в том случае, если они станут жертвами кибер-травли, а именно:

1. Обратиться ко взрослому, которому они доверяют. Учителя, родители, взрослые друзья семьи (и так далее) — вот кого мы имеем в виду. Когда взрослый разберется в ситуации, он или она сможет проанализировать ее и помочь ученику найти решение проблемы: например, провести встречу жертвы, хулигана и их родителей.
2. Сохранить свидетельства и доказательства факта травли. Скриншоты, голосовые сообщения, другие материалы — все это очень пригодится, если дело дойдет до суда. Опять же, с такими свидетельствами разговор с родителями киберхулигана может получиться очень предметным.

3. Не отвечать. Как говорится, «не кормите троллей»! Увидев реакцию на свои действия, киберхулиган может войти в раж. Опять же, любые негативные реакции могут быть расценены как встречная онлайн-травля.
4. Сообщите о факте онлайн-травли администраторам платформы или сервиса.

Обучение как способ решения проблемы

Один из лучших способов профилактики кибербуллинга заключается в том, чтобы рассказать ученикам про это явление. Вы можете научить избегать кибербуллинга, объяснить, когда надо сообщать взрослым о тех или иных онлайн-действиях, а также о причинах, по которым нельзя поддерживать подобную активность.

Скажите ученикам, что они всегда могут обратиться за помощью к вам, своим родителям или опекунам, если столкнутся в Интернете с чем-то тревожным или опасным. Необходимо дать ученикам понять, что они могут доверять вам и своим родителям/опекунам. Объясните, что помогать им — это ваша работа, и если они чувствуют себя в опасности, работая в Сети, то пусть обсудят это с вами.

Вы — учитель, а это значит, что у вас есть уникальная возможность повлиять на будущее поколение и научить своих учеников правильно реагировать на соответствующие проблемы.