Кибербезопасность для педагога — что нужно знать в 2023 году

Добрый день, уважаемые коллеги. Я, Мельник Оксана Михайловна, педагог дополнительного образования Центра дополнительного образования «Поиск». Преподаю теле и медиа журналистику, руководитель творческого объединения образцовая детская телестудия «Фокус. Тема медиа или интернет безопасности мне близка. Впрочем, как и любому другому педагогу.

СДАЙД 1 Согласитесь, эпоха тетрадей для домашней работы, тяжелых учебников и написанных от руки рефератов неумолимо уходит в прошлое. В 21-м веке учеба — это цифровой процесс. Ученики могут делать домашнюю работу, общаться с одноклассниками, проверять свои оценки и проводить исследования онлайн.

Интернет помогает учиться быстрее и предоставляет мгновенный доступ к такому объему информации, который едва ли поместится во всей библиотеке вашего учебного заведения. Вот только онлайн-мир современного образования может быть крайне опасен, причем как для учеников, так и для учителей. Современные школьники 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.

Вам нужно знать, как защитить себя и своих учеников от кибератак. Но давайте обо всем по порядку.

СЛАЙД 2 Что же такое информационная безопасность? Википедия пишет, что это - практика предотвращения несанкционированного доступа,

использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Проще говоря, интернет безопасность - это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные.

СЛАЙД 3 Согласитесь, сегодня Всемирную паутину используют, в основном, не как источник информации, а как способ коммуникации. Многие ученики средних и старших классов практически не пользуются электронной почтой, связываясь с необходимыми им людьми исключительно через социальные сети, оттуда же они получают всю, как полагают, необходимую им информацию. Социальные сети, компьютерные игры для многих стали настоящим «местом обитания», они настолько прочно вошли в жизнь школьников, что о критическом осмыслении размещаемой там информации у многих не идет и речи. Общество, государство обязаны защитить свое молодое поколение от вредоносной информации, и шаги в данном направлении, безусловно, делаются.

СЛАЙД 4 Однако, как показала действительность, шаги эти явно недостаточны. Если взять только крайнее проявление негативного влияния некоторых сайтов и популярных игр – суицид, то статистика, опубликованная в открытом доступе в интернете, показывает, что количество детей и подростков, добровольно ушедших из жизни под влиянием таких печально известных игр, как «Синий кит» и «Тихий дом», в России ежегодно неуклонно возрастает. Опасность составляют «хештеги групп смерти» в социальных проектах, и попытки уменьшить количество этих хештегов к результату не привели, число их участников только возросло.

Одним из тех, кто озабочен вопросами информационной безопасности детей и подростков буквально по долгу службы, является Уполномоченный по правам ребенка в ХМАО-Югре Людмила Низамова. Несколько лет назад специалисты ее аппарата провели экспертизу сайтов школ нашего округа и выяснили, что на многих сайтах присутствуют ссылки, по которым можно перейти на интернет-ресурсы очень сомнительного содержания.

Сегодня никто ни от чего не застрахован, к сожалению. Возможны ситуации, когда ваши ученики окажутся киберпреступниками, однако возможны и другие — в которых они уже будут жертвами.

Да, молодежь быстро осваивает цифровые программы, некоторые даже умеют их взламывать, однако жизненного опыта у них все же маловато. Они могут быть недостаточно проницательны и мудры, чтобы распознать все опасности онлайн-мира, с которыми им доведется столкнуться.

СЛАЙД 5 Мы — педагоги, а потому мы обязаны защитить своих учеников и рассказать им про кибербезопасность, чтобы они могли защититься в Интернете.
Киберугрозы — это реальная опасность, но, к счастью, есть простой способ защитить вас и ваших учеников: образование! Знание — сила, верно? Изучите тему кибербезопасности, новейших приложений и других особенностей современных технологий сами, расскажите об этом своим ученикам, и вы сможете выявлять и устранять проблемы с цифровой безопасностью еще в самом начале. Я обязательно поделюсь ссылками, где можно найти все ответы по интернет безопасности.
СЛАЙД 6 В 2021 году я вместе со своими учениками участвовала во Всероссийском конкурсе-проекте по медиабезопасности. Проект реализуется при поддержке фонда Президентских грантов. Мы победили. Нам предложили стать волонтерами медиабезопасности в нашем округе. И так случилось, что мы стали единственными медиаволонтерами, которые несут знания в массы.
МОЖНО ВИДЕО МЕДИАСТРАЖИ Но мы не сразу стали такими умными всезнгайками в вопросах интернет безопасности. Почти два месяца мы учились, посещали лекции, изучали безопасные сайты, разрабатывали свои кейсы с мастер-классами. А дальше – стали выходить на школьные площадки и в рамкахз уроков безопасности рассказывали детям, что такое медиабезопасность и как не попасть на уловки интернетмошенников.
РОЛИК БЕЗОПАСНОСТЬ ВИДЕО

СЛАЙД 7 Мы в простой и в доступной форме объясняем сложные вопросы. Проводим викторины и показываем видеоролики, которые сами делаем. А еще, для большей наглядности создали медиаконтент в ВК, где размещаем памятки, репортажи, даем ссылки, советы. Каждый желающий может найти нас в социальных сетях, пообщаться, при желании - присоединиться в наши ряды. Мы с ребятами стали участниками муниципального этапа Всероссийской акции «Я – гражданин России», где представили всю сою практическую работу, поделились опытом. И знаете, коглда ребята проводили занятия для школьников, очень много вопросов возникало у педагогов. К сожалению, педагоги, не всегда знают, как правильно себя вести в сети интернет и что нужно знать обязательно.
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. Не буду терять время и приводить примеры…Расскажу про эти угрозы и поделюсь способами, как их можно было бы избежать.
МОЖНО

СЛАЙД 8 Итак…Интернет в классе
Как я уже сказала, ваши ученики гораздо лучше вас разбираются в современных технологиях. Возможно, они отлично знают все особенности

популярных онлайн-программ и цифровых устройств, что дает им колоссальное преимущество перед вами — например, если они захотят взломать ваши учетные записи.
Вашим первым порывом может быть введение полного запрета на цифровые устройства в классе. Впрочем, едва ли это сработает. Ученые заявляют, что в 2018 году у «95% подростков был доступ к смартфону, причем 45% из них заявляли, что они «онлайн практически постоянно».
Иными словами, едва ли вы сможете на самом деле сделать класс территорией, свободной от смартфонов, планшетов и ноутбуков. Побороться, конечно, можно, но удовольствия от этого никто не получит. Уж лучше сделать так, чтобы пребывание в Интернете стало для ваших учеников более продуктивным занятием. Например, пусть они готовятся к урокам с помощью Сети.
Слайд 9 Кто работает за вашими учетными записями?
У вас наверняка есть множество учетных записей в различных сервисах. Личная электронная почта, учетные записи в социальных сетях, а также различные школьные платформы. А теперь представьте, что у ваших учеников есть доступ к данным, хранящимся там. Они смогут прочитать вашу личную переписку, изменить свои домашние задания и оценки, посмотреть отчеты других учеников, опубликовать что-нибудь недостоверное на странице вашей школы в социальной сети от вашего имени и организовать вам еще множество других поводов поволноваться.
Едва ли ученикам будет очень сложно взломать ваши учетные записи. Ухудшает ситуацию и тот факт, что во многих школах в принципе нет ничего, что напоминало бы систему киберзащиты, призванную ограничить доступ к вашим учетным записям.
Чтобы защитить свои личные данные от юных хакеров, необходимо на пятерку знать основные принципы защиты учетной записи.
Далее я расскажу, как защитить свои личные аккаунты. Эти советы применимы и к учительским онлайн-порталам, и к личным учетным записям, и к электронной почте, и к страницам в социальных сетях. Вот что я советую:
Слайд 10 • 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.
- Придумывайте сложные пароли. В паролях должны использоваться строчные и заглавные буквы, цифры и символы. Тогда угадать пароль будет сложнее.
- Почаще меняйте пароли. Эксперты советуют менять пароли раз в полгода, но для учителя это слишком длинный период. Мы советуем менять пароли раз в три месяца.
- 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.

- Проверьте, достаточно ли сложный у вас пароль, с помощь специальных сервисов (например, нашего). Эти сервисы показывают, насколько просто или сложно взломать пароль.
- Используйте менеджер паролей для их создания или хранения на устройстве или в браузере. Менеджер паролей использует специальную базу данных для создания и хранения надежных паролей, и вам уже не придется из запоминать.
- Используйте биометрические пароли (например, вход по отпечатку пальца), если есть такая возможность. Это исключительно безопасное решение — только вы сможете авторизоваться.
- Воспользуйтесь системами продвинутой или 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.

Так вы сможете защитить свои учетные записи от учеников и других потенциальных хакеров.

Возможно, вы активно пользуетесь смартфонами: для общения с друзьями, проверки почты, просмотра социальных сетей. Может, с помощью смартфона вы даже проверяете домашние работы и отчеты учеников и ставите им оценки.

Смартфоны очень удобны и полезны, но также крайне уязвимы ко взлому. 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.

Если не принять соответствующие меры предосторожности, то любой злоумышленник сможет получить ко всему этому доступ. Есть 4 способа защиты конфиденциальных данных, хранящихся на смартфоне, от потенциальных хакеров:

Слайд 11 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. И снова: 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. Есть нет, то хотя бы пароль используйте.

3. Отключайте Wi-Fi и Bluetooth почаще. Да, если вы используете смартфон, то оставьте эти сети включенными. Но если вы, скажем, легли спать или ушли в офлайн, то включенный Wi-Fi и Bluetooth могут заинтересовать хакеров. 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 от потенциальных хакеров, с которыми вы можете столкнуться где угодно, если у вас при себе есть смартфон или планшет.

Защищайте личную онлайн-репутацию.

Многие учителя, слушая о безопасности, готовы полностью удалить все, что выложили в Интернет о себе, однако это не обязательно. В конце концов, доступ в Интернет вам тоже нужен — чтобы общаться с друзьями, самовыражаться, выкладывать фото и так далее.

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

Слайд 12 Интернет-ресурсы для педагогических работников:

http://www.fid.su/projects/deti-v-internete
сайт Фонда Развития Интернет

http://www.ligainternet.ru/
Лига безопасного Интернета.

http://ppt4web.ru/informatika/bezopasnyjj-internet.html

презентации о безопасном Интернете.

http://www.microsoft.com/ru-ru/security/default.aspx
сайт Центра безопасности Майкрософт.

http://www.nachalka.com/node/950
Видео «Развлечение и безопасность в Интернете»

http://i-deti.org/
портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы

http://сетевичок.рф/
сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности

http://www.igra-internet.ru/
онлайн интернет-игра

«Изучи Интернет – управляй им»
http://www.safe-internet.ru/ сайт Ростелеком «Безопасноть детей в Интернете, библиотека с
материалами, памятками, рекомендациями по возрастам
Информация о мероприятиях, проектах и программах, направленных на повышение
информационной грамотности педагогических работников
http://www.ligainternet.ru/news/
мероприятия Лиги безопасного интернета. Лига безопасного
интернета — крупнейшая и наиболее авторитетная в России организация, созданная для
противодействия распространению опасного контента во всемирной сети.