*Методическая консультация*

*(23.11.2020г.)*

**«КИБЕРАТАКИ В УСЛОВИЯХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ: КАК ОБЕЗОПАСИТЬ РЕБЁНКА»**

Источник информации: <https://www.yaklass.ru/novosti/akcii-i-novosti-za-2020-god/stati-i-novosti-za-11-2020/kiberataki-v-usloviyah-distancionnogo-obucheniya-kak-obezopasit-rebyonka>

В 2020 году сфера образования рискует подвергнуться кибератаке не меньше, чем финансовые организации. По данным Ростелекома, количество кибератак на образовательные сервисы и онлайн-дневники в этом году выросло в 5,5 раз.   
Рассмотрим, какие угрозы стоят перед современными родителями и школьниками, как можно обезопасить детей и что делать, если ребёнок подвергся кибератаке.

Первое, что важно понять: причина не в самих образовательных платформах, а в нагрузке на них. За последние полгода мы прошли тот путь к цифровизации, для которого в других условиях понадобилось бы 5–6 лет. И, как следствие, появились определённые риски.   
Жертвой кибератаки может стать как сам школьник, так и его родитель.   
Представьте ситуацию: злоумышленники отправляют авторитетному родителю от имени ребёнка срочное сообщение с пометкой «папа, срочно посмотри». В письме содержится вредоносная ссылка. Родитель кликает — получает троян — вся компания идёт крахом.

Также никто, к сожалению, не защищён от риска стать жертвой кибербуллинга — травли в интернете. Так что же с этим делать?

***Есть отличный способ — поговорить***

Пообщайтесь с ребёнком за чаем. Смоделируйте разные ситуации, с которыми он может столкнуться, обсудите, что делать, если вдруг что-то случилось. Например:

* что делать, если тебе пришло странное письмо от какого-то странного друга в интернете? Как ты будешь реагировать?
* Что делать, если тебя куда-то приглашают? Почему нельзя на это вестись?
* Кому ты пойдёшь жаловаться, кому и как ты будешь сообщать? Как ты будешь доказывать?

Проговорите, какие могут быть последствия, объясните, что все переписки нужно сохранять. Если не получится, обращайтесь к специалистам — консультантам по кибербезопасности.  
То же самое относится и к кибербуллингу. К тому, что подобное может случиться, ребёнка нужно подготовить — это лучше, чем потом идти к психологу и делать попытки вернуться к нормальной жизни.   
Основные инструменты для безопасного использования интернета:

* закрытые ссылки;
* родительский контроль.

Однако крайне важно мотивировать ребёнка личным примером и проводить с ним профилактические беседы. Имейте в виду, что разговоры про кибергигиену уместны с 11–12 лет, когда ребёнок уже начинает понимать, как обойти родительский контроль.   
Статистика говорит о том, что только 33 % времени ребёнок проводит на ресурсах, связанных с образовательным контентом. Всё остальное уходит на соцсети, развлечения, покупки.

***Мотивируйте ребёнка собственным примером***

Сейчас многие считают, что современные дети не читают книг. Но в семьях, где принято читать и обсуждать прочитанное, всё обстоит иначе, и там детей постепенно втягивают в чтение — собственным примером. Разговаривайте с ребёнком, интересуйтесь, что он прочитал, что интересного нашёл. Учите его оценивать качество информации. Интернет ведь точно так же служит источником информации, которую мы дальше оцениваем.

***Как нас взламывают***

1. Широковещательно (фишинг, социальная инженерия, зловреды на сайтах, утечки без паролей).
2. Прицельно (брутфорс аккаунтов, заражённые флешки, взлом через наших близких, физический доступ к устройству).
3. По вине нашей беспечности (самостоятельно раскрыли конфиденциальную информацию или не защитили её должным образом).

***Мифы о «цифровых бедняках»***

Люди часто думают, что никому не интересны, что у них нечего красть, что интерес представляют только селебрити. Но мы забываем, что существует ещё и цифровое богатство:

* деньги электронные;
* бонусы. Кроме банковских карт у вас в кошельке наверняка есть бонусные и скидочные карты, карты лояльности и так далее. А теперь представьте ситуацию: вы собрались лететь в отпуск. И у вас были накоплены бонусы «Аэрофлота». Однако их кто-то украл, при этом лететь всё равно надо. Значит, придётся компенсировать потерю этих бонусов лишними расходами, а это уже реальные деньги;
* персональные и медицинские данные;
* репутация и аккаунты в социальных сетях. Фейковый аккаунт могут завести на ваше имя, а это, как следствие, повлияет на репутацию. Интернет не только помнит, но и делает всё доступным;
* переписка. Вырванная из контекста фраза может быть использована против вас и ваших друзей;
* персональные цифровые коллекции (хоть бы даже ссылки или фильмы — это ведь тоже потери) и виртуальные вещи;
* контакты и заметки;
* домены (сайты);
* цифровые ресурсы (Wi-Fi, место в облачном хранилище и т. д.);
* цифровая техника (телефон, компьютер и прочая умная электроника), автомобиль, умный дом.

***Мы повсюду оставляем цифровые следы***

За нами следят приложения в телефоне, мы случайно попадаем на чужие селфи, поисковики запоминают наши маршруты. Цифровые следы бывают двух видов: активные и пассивные.

Активные цифровые следы — это то, что люди делают сами. Это публикации в соцсетях, комментарии, фотографии и т. д. Своей активностью пользователь может управлять, то есть осознанно формировать свой цифровой образ.

Пассивные цифровые следы — это то, что компьютер записывает автоматически (IP-адрес, история посещений сайтов, геолокация и прочее). Если на первое мы можем повлиять, самостоятельно решая, что писать, размещать или загружать, то со вторым гораздо сложнее. Маловероятно, что мы можем быть активным пользователем приложения и постоянно контролировать, какие данные оно записывает. Бояться цифровой тени не стоит — современный человек уже давно оставляет подобный след, это теперь естественная часть нашей жизни. 