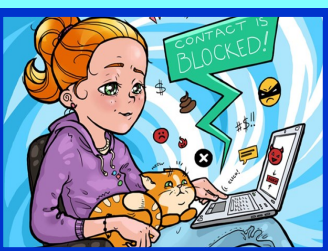


5. Не участвуй в онлайн-перепалках.

Кибертравля — это действительно бич Интернета. Люди вообще жестоки, а подростки порой бывают просто невыносимы. Пытаясь добиться справедливости, ты можешь застрять в бесконечных онлайн-перепалках, которые не принесут тебе ничего, кроме боли и обиды. Не трать время и силы на этих людей, лучше займись чем-нибудь, что тебе действительно нравится. А наткнувшись на по-настоящему сложную ситуацию, если ты чувствуешь, что ситуация выходит из-под контроля, обдумай следующие меры:

- Если тебе кажется, что люди в Интернете ведут себя агрессивно, угрожают или пытаются тебя высмеять, не ввязывайся в бесполезные споры, не опускайся до их уровня. Сообщи о неумных агрессорах администраторам сайта и займись любимым делом.

- Если онлайн-перепалки происходят регулярно и кто-то пытается выйти за грань дозволенного, поговори с родителями. Неважно, кто замешан, даже если это одноклассники или кто-то из школы. Это не трусость и не вранье, так поступил бы



любой взрослый человек. Важно остановить агрессоров до того, как кто-нибудь пострадает.

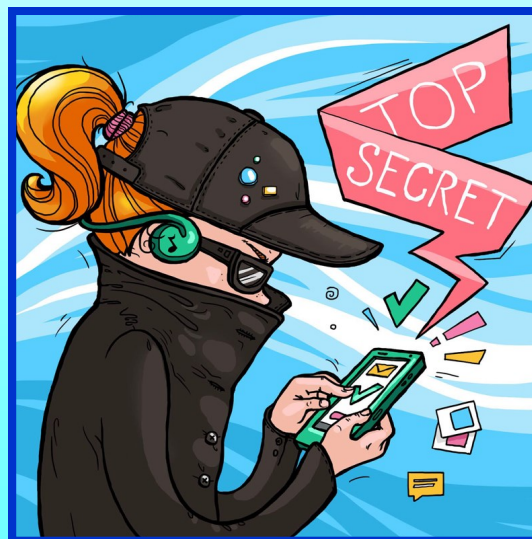
6. В Интернете всё не то, чем кажется

Хваленая интернет-анонимность только поощряет эту пагубную привычку.

Поэтому не стоит верить всем этим суперклевым мальчишкам и девочкам, ведущим сногшибательные странички в соцсетях. Кажется, что они живут идеальной жизнью, но, скорее всего, все совсем не так.

У каждого человека есть свои комплексы, мы все совершаем ошибки, а потом прячем расстройство за милыми улыбками. Часто мы врем даже по пустякам. Так что помни: в Интернете все не так, как кажется.

В Сети нет ангелов, а вот преступники тут действительно водятся и в свое удовольствие пользуются благами хваленной онлайн-анонимности.



Составила Алибаева О.В., методист

<https://www.kaspersky.ru/blog/security-tips-for-kids-3/8362/>



Бюджетное учреждение Ханты-Мансийского автономного округа – Югры «Радужинский реабилитационный центр для детей и подростков с ограниченными возможностями»

Шесть простых советов по кибербезопасности



В школе учат куче вещей, но ничего не рассказывают о том, как вести себя в интернете, чтобы не попасть в неприятности.

У нас есть несколько советов по кибербезопасности.

12+

г. Радужный

1. Не попадись на крючок в Интернете: берегись вирусов.

Как обезопасить ПК от троянов и вирусов?

Многие из них были созданы, чтобы шпионить за пользователями, собирать их пароли и другие важные данные. Устанавливайте антивирусные программы, такие как Касперский (Kaspersky). Убедись, что на твоём компьютере, телефоне или планшете установлена **антивирусная программа**, и следуй её рекомендациям. Она защищает тебя от самых распространённых интернет-атак. Не качай файлы со сторонних ресурсов, лучше загрузи их с сайта разработчика. Если устанавливать программу, скачанную с первого попавшегося ресурса, ты можешь легко загрузить вместе с ними **парочку очень неприятных сюрпризов**.

Если незнакомец прислал тебе программу, не запускай её, не проверив. Вполне вероятно, что даже в маленький файл встроен вирус, способный на самые разные мерзкие действия, такие как похищение паролей, **удаление любых файлов с устройства** или рассылка спама от твоего имени.

Даже если письмо с программой отправил твой друг или член семьи, лучше проверить, не взломали ли его аккаунт, ведь **нередко хакеры притворяются другими людьми**. Так им легче распространять вирусы и вредные программы. Вот почему не стоит сразу кликать по ссылкам или устанавливать файлы, отправленные

2. Используй сложные пароли.

Они являются слабым звеном в защите большинства домашних пользователей. Люди выбирают ненадёжные комбинации символов типа «12345» или «qwerty», хранят их в DOC-файле на жестком файле и отправляют друзьям в онлайн-чатах. Стоит ли говорить тебе, что такая **наивность — не лучший способ вести себя в Интернете?**

3. Храни секреты!

Ты рассказываешь незнакомцам на улице, куда идешь, что ешь на завтрак и по каким адресам живут твои друзья? Наверное, нет. В Интернете нужно следовать этим же правилам. Если ты не задашь верные настройки приватности в социальных сетях, любой сможет узнать все эти факты, просто изучив твою страницу и страницу твоих друзей «ВКонтакте», Instagram или Facebook.

4. Проверь свои подписки и счета.

Киберпреступники знают, как заработать деньги на взломе смартфонов. Самый простой способ быстрого обогащения заключается в незаметном воровстве средств с твоего счета посредством подписки твоего номера на премиальные SMS-услуги или звонков на платные телефоны. А вообще их гораздо больше. Поэтому **мобильный**



- ♦ Установи пароль на свой мобильный, чтобы посторонние не могли рыться в нем в свое удовольствие.
- ♦ Не подключайся к непроверенным Wi-Fi-точкам, особенно к открытым, потому что их легко могут использовать для сбора данных, которые ты отправляешь, в том числе и паролей.
- ♦ Ты можешь контролировать свое устройство удаленно, даже если оно потеряно или украдено. Для этого активируй опции удаленного управления и резервного копирования данных с помощью встроенных возможностей телефона (например, настройки «Найти мой iPhone») или используй специальное приложение.
- ♦ Не забывай, что вирусы поражают и смартфоны тоже. Не качай незнакомые приложения, даже из официальных магазинов. Всегда проверяй список запрашиваемых приложениям разрешений, таких как покупки из приложений, доступ к списку контактов и так далее.

