Как сделать интернет безопасным для ребенка?

Каждый родитель беспокоится о безопасности своего ребенка. Но стоит помнить, что защищать своё чадо нужно не только в реальной жизни, но и в ИНТЕРНЕТЕ!

У большинства людей путешествие по всемирной паутине начинается с поисковика, но ни один из них не гарантирует предоставление вашему ребенку только безопасной информации. Что делать в такой ситуации?

1. Установить Безопасный режим

Для этого необходимо создать отдельную учетную запись на сайте выбранной вами поисковой системы.

2. Использовать детские поисковики

Такие как Гогуль или Спутник.дети. Популярность этих ресурсов, несмотря на их безопасность и ориентированность именно на детскую аудиторию, сегодня крайне низкая.

Оба этих способа имеют один недостаток - ребенок не всегда сможет найти актуальную и важную информацию по своему запросу, поэтому не стоит категорично запрещать ему пользоваться обычными поисковыми системами. В этой ситуации важен постоянный контроль со стороны родителей. Например, множество антивирусов сегодня имеют функцию родительского контроля, позволяющую наблюдать за тем, что ребенок делает в Сети.

В целях предотвращения проблем, перед тем, как допустить ребенка к Сети, родителям необходимо провести предварительную беседу с юным пользователем о том, что он может повстречать на просторах интернета. Помните, что в защиту Вашего ребенка в первую очередь входит Ваше личное общение с ним на тему кибербезопасности.

Для того, чтобы оградить ребенка от противоправного контента (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы) Вам следует сформировать ряд легко выполнимых правил:

Договоритесь, чтобы ребенок сообщал Вам о нахождении нежелательной информации.

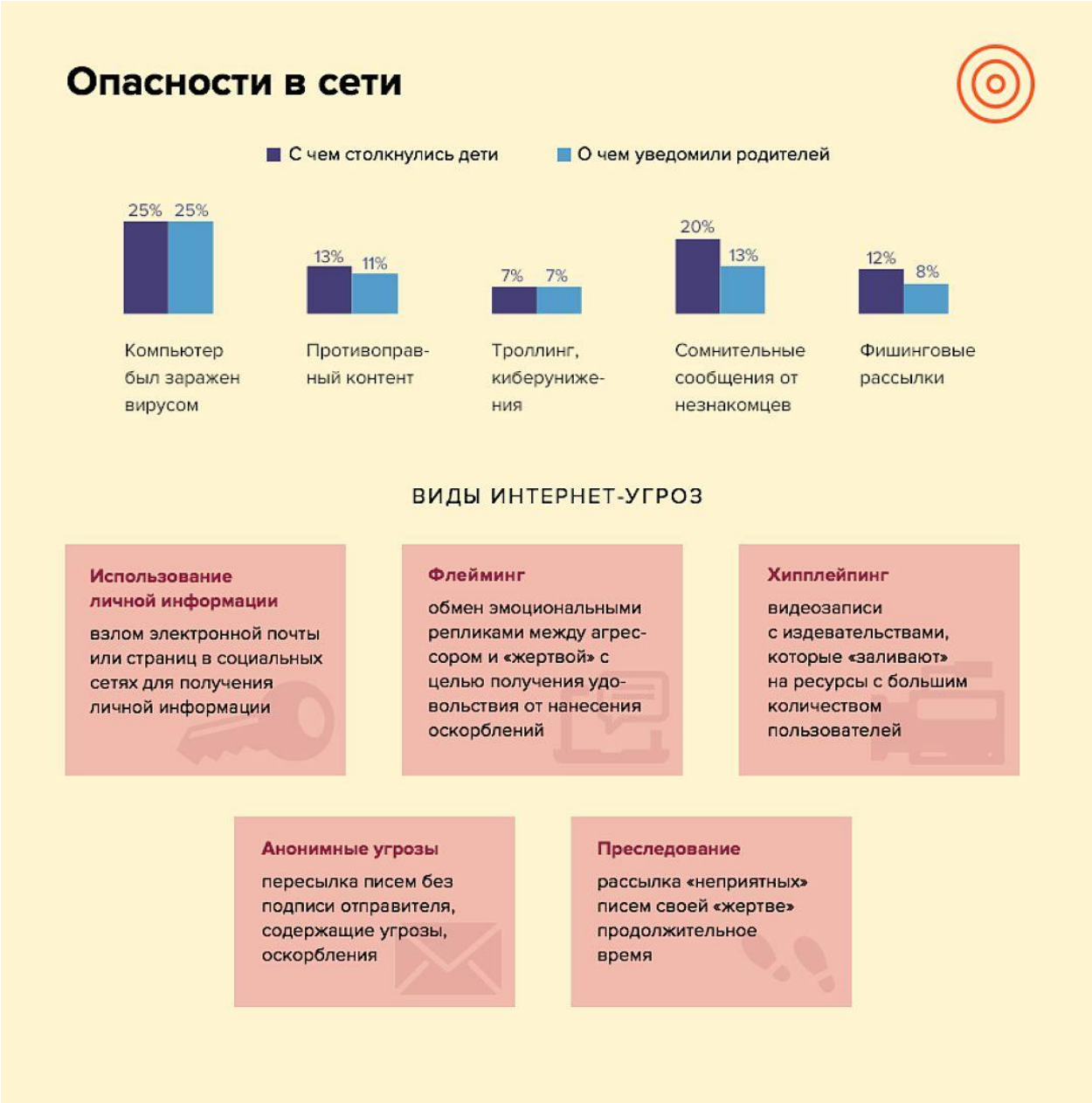
Расскажите, что не вся информация в интернете достоверная и приучите его советоваться с Вами по любому непонятному вопросу.

Расспрашивайте ребенка о том, какие сайты он посещал и какую информацию видел.

Включите программы родительского контроля, чтобы оградить ребенка от нежелательного контента.

Не будет лишним напоминание правил безопасности в Сети.

Помните, что чрезмерный контроль может усилить желание выйти за рамки дозволенного, поэтому доверительное и открытое общение с детьми зачастую гораздо эффективнее.



Одной из самых распространенных угроз, связанных с общением в Сети, являетсякибербулинг. Это форма запугивания, насилия и травли детей с помощью телефонов и интернета. Кибербулинг опасен не меньше, чем издевательства в привычном понимании, ведь “жертва” кибербулинга находится в большом психологическом напряжении, и не каждый ребенок сможет его вынести самостоятельно.

Кибербулинг включает в себя:

Анонимные угрозы – пересылка писем без подписи отправителя, содержащие угрозы, оскорбления, часто с использованием ненормативной лексики;

Преследование – рассылка “неприятных” писем своей “жертве” продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами ее жизни;

Использование личной информации – взлом электронной почты или страниц в социальных сетях для получения личной информации для шантажа или издевательств;

Флейминг – обмен эмоциональными репликами между агрессором (иногда их может быть несколько) и “жертвой” с целью получения удовольствия от нанесения оскорблений;

Хипплейпинг – видеозаписи с издевательствами, которые “заливают” на ресурсы, где их сможет увидеть большое количество пользователей. Такие ролики, естественно, “заливаются” без согласия “потенциальной жертвы”.

Для того, чтобы понять, попал ли Ваш ребенок под тяжелую руку кибер-хулиганов, следует обращать внимание на следующее:

Изменилось ли настроение ребенка в худшую сторону?

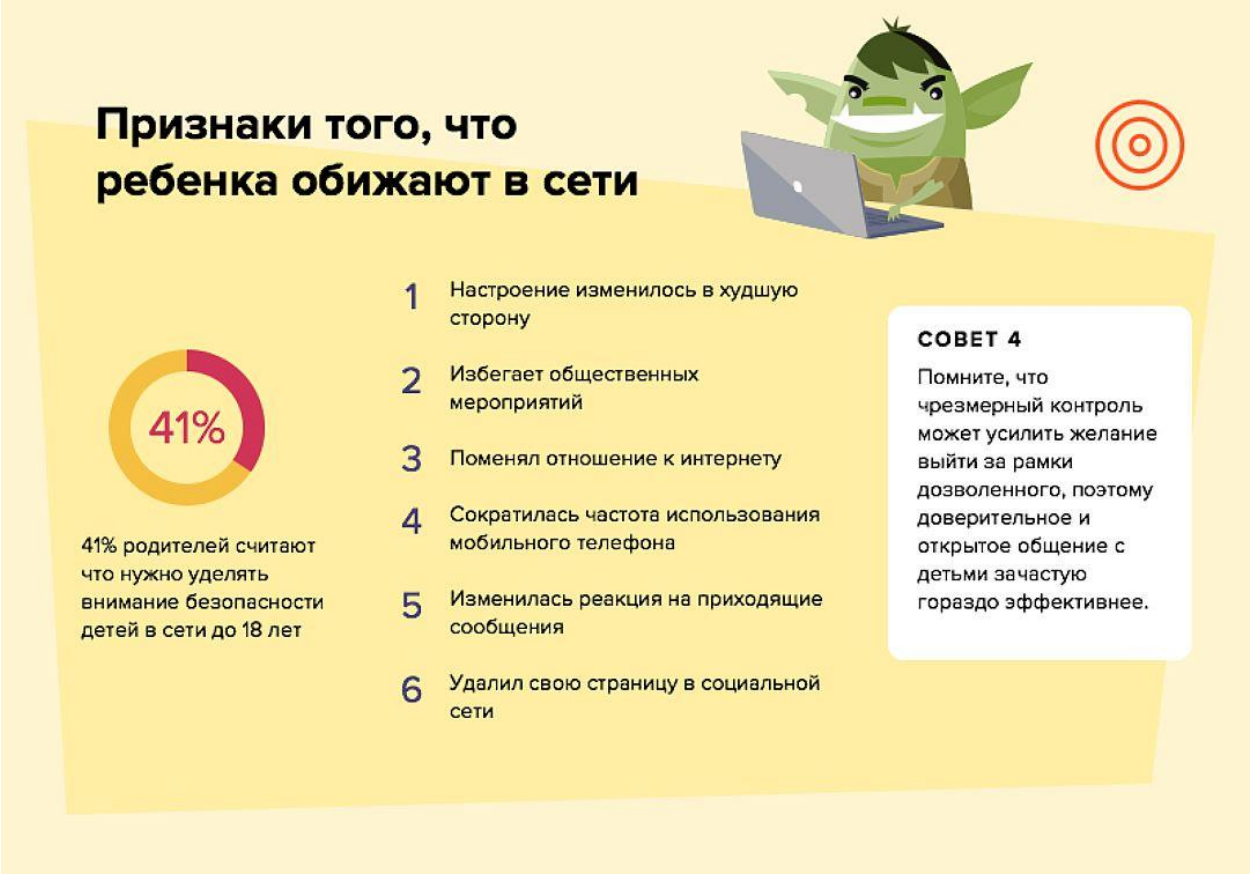
Избегает ли он общественных мероприятий?

Поменял ли он отношение к интернету?

Сократилась ли частота использования мобильного телефона?

Какова реакция на приходящие сообщения?

Не удалял ли он свою страницу в социальной сети?



Вот несколько правил, которым стоит следовать, чтобы сохранить безопасность своего смартфона и смартфона Вашего ребенка:

Установите пароль, чтобы личная информация не попала к посторонним лицам.

Не стоит подключаться к непроверенным wi-fi точкам, особенно открытым, так как их легко могут использовать для сбора отправляемых данных, в том числе и паролей.

С помощью специального приложения Вы можете контролировать устройство удаленно, даже если оно украдено.

Не стоит скачивать неизвестные приложения: пользуйтесь только официальными магазинами AppStore, GooglePlay и Windows Market, проверяйте запрашиваемые приложением разрешения.

Не обязательно создавать отдельный аккаунт для Вашего ребенка в магазине приложений. Разные производители дают возможность подключить одного и более членов семьи к одной банковской карте – так Вы сможете контролировать, что собирается купить Ваше чадо.

Основные правила

1. Говорите с ребенком об интернете
2. Пользуйтесь интернетом и смартфоном вместе с ребенком
3. Рассказывайте больше о сайтах и сервисах в интернете
4. Научите бережно относиться к паролям
5. Научите использовать настройки конфиденциальности
6. Обращайте внимания на возрастные ограничения сайтов
7. Расскажите о том, что за слова, сказанные в интернете, ребенок несет ответственность
8. Привлекайте к обсуждению этой темы других взрослых, компетентных в этом вопросе
9. Используйте антивирус и регулярно обновляйте его
10. Научите ребенка не открывать вложения и не принимать файлы от неизвестных людей в электронной почте