6 главных правил детской безопасности в интернете

Когда мы слышим истории о том, как школьница переписывалась с незнакомцем, а он оказался педофилом, хочется закрыть детей дома и отключить Wi-Fi. Но задача родителей — не спрятать ребенка от жизни, а научить противостоять опасностям. Рассказываем с «Лабораторией Касперского» о том, как безопасно использовать возможности

1. Не запрещайте ребенку заводить страницу в соцсетях

Это вредно и бессмысленно: он просто сделает это втайне от вас. Как показало исследование «Лаборатории Касперского», у 40% детей в младшей школе и у 97% старшеклассников есть страница в соцсетях.

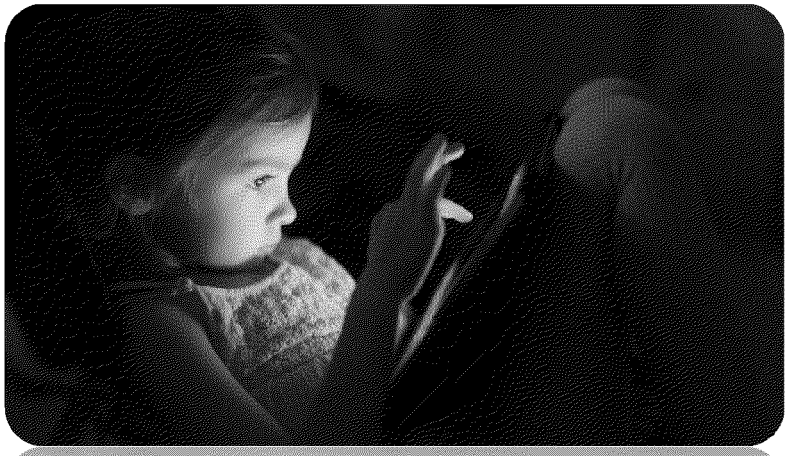
Лучше сами помогите ребенку создать аккаунт, став его проводником и наставником в виртуальном мире.

2. Покажите ребенку, как пользоваться настройками приватности

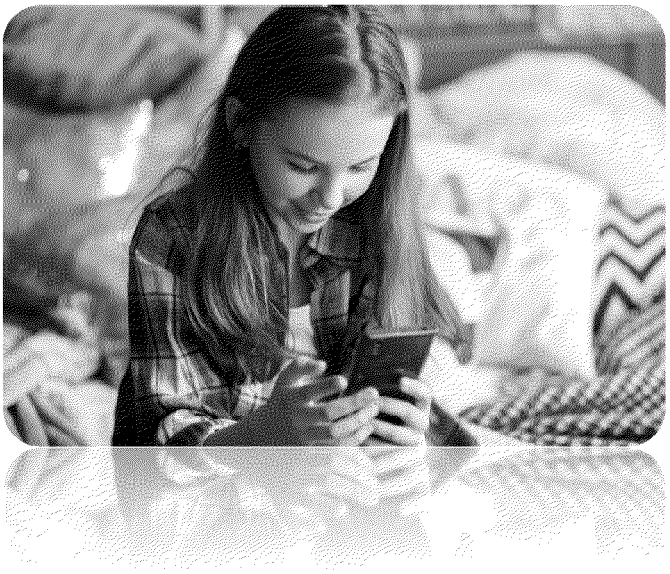
Расскажите, какой информацией лучше вовсе не делиться в интернете. Адрес, телефон, личные фото, сканы документов — все это, попав в руки злоумышленников, может быть использовано против него.

Расскажите, что не стоит ставить в постах реальные геотеги и рассказывать о своих планах.

Покажите, как распознать спам и как грамотно на него реагировать. Скажите ребенку, что вы всегда рядом и готовы помочь, если у него появятся вопросы.



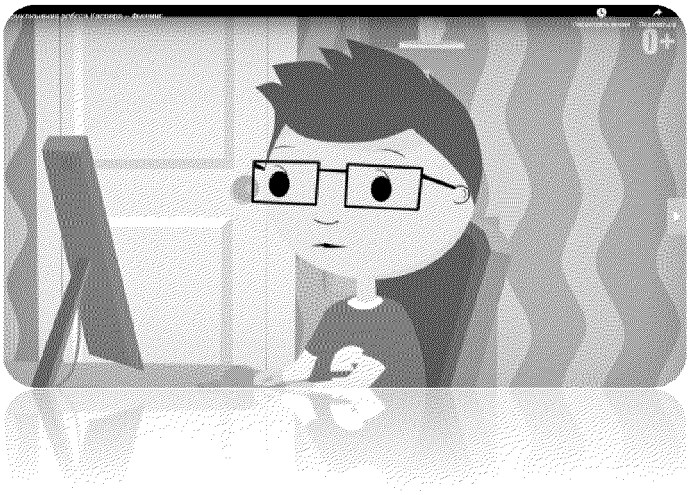
3. Объясните ребенку, что в интернете не нужно делать ничего, чего бы он не стал делать в реальной жизни



Поэтому — «нет» оскорблениям, травле, излишней навязчивости, неграмотной речи, нарочито эпатажному поведению.

Прежде чем опубликовать что-то, стоит потратить три секунды и подумать, не будет ли кому-то неприятно или обидно это читать.

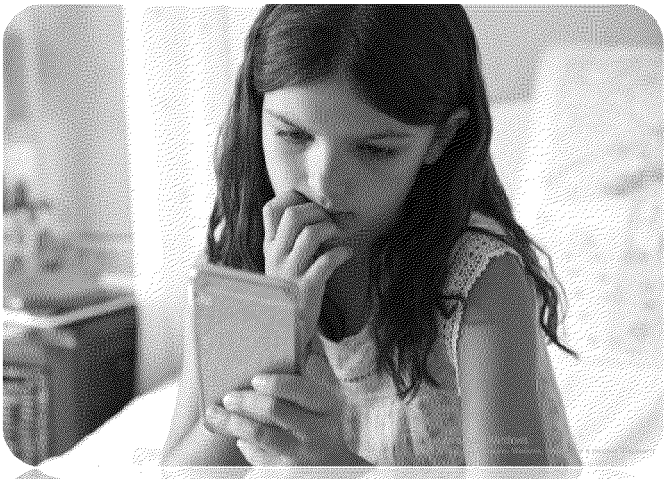
4. Помогите ребенку придумать сложный пароль



Для каждого аккаунта – свой. Он должен состоять из микса букв, цифр и символов и не должен включать личные данные (например, дату рождения).
Расскажите, что далеко не всем сайтам можно доверять свой логин и пароль. Об опасности «фальшивых» сайтов (они называются фишинговыми) есть отличный мультфильм. Посмотрите его вместе с ребенком!

5. Подключите двухфакторную аутентификацию

Это подтверждение входа в аккаунт через код, который приходит на телефон.



Объясните, что эти коды нельзя передавать никому и ни при каких обстоятельствах. Даже если человек представляется сотрудником техподдержки соцсети (настоящая техподдержка никогда не запросит такие данные). Даже если об этом пишет «друг», у которого якобы возникла проблема с собственным телефоном (его могли взломать или создать фейковый аккаунт с именем и фото).

6. Периодически просматривайте список «друзей» ребенка

И паблики, на которые он подписан. Согласно исследованию «Лаборатории Касперского», 70% школьников получают приглашения дружбы от незнакомых людей (при этом 18% — от незнакомых взрослых).

Объясните ребенку, что никогда нельзя знать наверняка, кем на самом деле является незнакомый человек, который представляется его ровесником и предлагает общаться. Расскажите, какие существуют опасности.