Этот материал создан нами, психологами-практиками, многодетными родителями, авторами книги-бестселлера “Детомотиватор”, создателями Академии бережного воспитания ДНК:

- онлайн-школы №1 по обучению родителей и педагогов по версии РБК;
- ПОБЕДИТЕЛЯ премии GetCourse в номинации “Онлайн-школа 2023 года”;
- финалиста премии GetCourse в номинации “Социально значимый проект 2023 года”.

БЕЗОПАСНОСТЬ В СЕТИ: КАК УБЕРЕЧЬ ДЕТЕЙ ОТ ОПАСНОСТЕЙ.

Интернет, мессенджеры, умные колонки и приложения прочно вошли в нашу жизнь. Развлечься, узнать последние новости, погоду, пообщаться с родными и друзьями теперь очень просто - достаточно попросить об этом устройство или нажать пару кнопок.
Но злоумышленники не дремлют.

Никого уже не удивишь Интернет-мошенниками, которые в последнее время стали выбирать себе в жертвы именно детей и подростков. Детей нанимают как “курьеров” для запрещенных веществ, вовлекают в группы смерти, снимают с их участием фильмы для взрослых, втираются в доверие, шантажируют и заставляют совершать иные действия, нужные преступникам. Дети не всегда правильно могут оценить последствия своих действий, многое воспринимают как игру, нечто нереальное.

При этом даже малыши могут пострадать от действий мошенников или “шутников”, которые могут подключаться к умным колонкам и камерам в доме, разговаривать с ребенком, просить совершать определенные действия или пугать его.

Родители при этом находятся в неведении и бывают шокированы, когда(если) все раскрывается. Что делать, чтобы обезопасить детей в сети - об этом ниже.

Что точно делать нельзя:

1 **Запугивать, во всех подробностях описывать известные вам случаи.**
У ребенка будет формироваться базовое недоверие к миру, нервозность и страхи. Все это может вылиться как в неуверенность, так и в повышенную возбудимость и агрессию у разных детей.

2 **Отбирать, запрещать.**
Тотальный запрет ведет к нарушению - дети найдут, как его обойти.

3 **Нарушать границы.**
Читать личные переписки, устанавливать скрытые программы слежки на устройства детей, контролировать каждый шаг. В итоге получите сопротивление, ребенок не будет вам доверять. Тайн и секретов станет в разы больше.

4 **Показывать образовательные фильмы и ролики.**
Этим вы можете подогреть интерес к теме, спровоцировать ее дальнейшее изучение и желание попробовать.

Что делать нужно:

1 Проявлять искренний интерес к ребенку.
Вопросы из серии “Уроки выучил?”, “Поел?” не работают. Нужны открытые вопросы (на которые нельзя ответить “Да” или “Нет”), которые будут провоцировать ребенка на беседу, на обдумывание ситуации.

“Что сегодня было интересного для тебя в школе?”

“Какая твоя самая любимая игра? Почему?”

“Что было сложно сегодня? Как справлялся?”

Открытые вопросы можно начинать со слов:

“Что тебе мешает...”

“Какая помощь тебе нужна...”

“Что бы ты хотел...”

НА ЗАМЕТКУ! Ваш интерес к ребенку должен быть искренним, а это возможно только тогда, когда есть искренний интерес к самому себе.

2 Давать позитивную обратную связь
Мошенники часто заводят дружбу с детьми, дают им массу внимания и позитивной обратной связи, их важность и принадлежность к определенной группе. Если в семье одни претензии, сплошное “должен-должен”, а чтобы взрослые заметили успехи ребенка, нужно кое-что глобальное, то ребенок будет расцветать от любого комплимента незнакомца. Позитивная обратная связь нужна как воздух, каждый день. Это не про “молодец”, это всегда про ребенка и конкретное маленькое достижение.

“Ты так чисто помыл свою тарелку, классно!”

“Ты сегодня даже без напоминания поставил ботинки на место, ты взрослеешь!”

3 **Делиться собственным опытом.**
Рассказывать, с какими мошенниками сталкиваетесь вы в жизни. Как понимаете, что с этим человеком нельзя продолжать контакт. А может вы и сами попадались на их уловки - что упустили, какой опыт извлекли из этой ошибки.

4 **Давать право на ошибку.**
Иногда преступники начинают шантажировать детей тем, что уже сделано - фото, переписка, выполненные задания. Дети боятся наказания, расстроить родителей/не оправдать их надежды, поэтому молчат и продолжают общение. Право на ошибку - это про безопасность. Да, я могу ошибиться, но это не конец света, меня любят и поддержат.
Вы можете не ругать ребенка за ошибки, а просто закатывать глаза, видя разбитую чашку, сокрушаться над порванными штанами или каждый раз искать виноватых в любой мелочи - ваш ребенок поймет, что ошибаться нельзя.

5 **Помогать ребенку проживать его эмоции и оказывать поддержку, когда это необходимо.**
Может ли ребенок злиться, хлопая дверьми? Спорить с вами, отстаивая свое мнение? Или рыдать у вас на плече? Есть ли та самая ценная поддержка, когда нет страха высказаться, страха быть непонятым и непринятым?

Если пока ваш ответ “нет”, то в этом направлении также следует начинать работать. На курсе “Эмоджинариум” мы подробно знакомимся со своими эмоциями, учимся замечать их проявления у себя и близких, а также практикуем их здоровую разрядку.

Рекомендации, которые позволят ограничить доступ злоумышленников к устройству.

Внимание! Без соблюдения пунктов, описанных выше, эти рекомендации не сработают! По мере взросления ребенка вы все меньше можете контролировать его нахождение в сети. Поэтому без доверия, контакта и ощущения безопасности в семье, ребенок оказывается беззащитен перед угрозами.

Если у вас подросток, все действия производит он сам, либо вы с его согласия.

1 Специальные детские аккаунты в приложениях.

Так вы обезопасите детей от нежелательного контента. Актуально для младших школьников.

Некоторые браузеры и антивирусы предлагают функцию “цензура контента”.

2 Установка спам-фильтра от мобильного оператора.

Сейчас у каждого оператора есть такая возможность - количество нежелательных звонков снижается в разы. Полезно как детям, так и взрослым.

3 Заблокировать звонки от тех, кто не внесён в список контактов.

В мессенджерах и телефоне. Можно заблокировать неизвестные и скрытые номера, добавление в каналы и группы.

4 Менять пароли.

Периодически во всех аккаунтах и в домашней сети нужно менять пароли, в том числе обязательно менять заводские пароли на новых устройствах (камерах, колонках, телефонах и пр). Где это возможно, должна быть настроена двухфакторная аутентификация.

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ

1. Помнить, что любая информация, опубликованная в Интернете, остается в Интернете. Даже из личных переписок. Не стоит делиться тем, что вы не готовы рассказать всему миру - ни фото, ни в сообщениях.
2. Не делиться публично данными о своей геолокации, телефоне, адресе и ближайших планах на передвижение.
3. Не отправлять личные данные - паспорт, банковские карты и пароли в сообщениях.
4. Можно не отвечать на сообщения и комментарии, которые не нравятся или оскорбляют. А их автора блокировать.
5. Если кто-то систематически травит, оскорбляет в сети, в личной переписке - стоит сделать скриншоты и записи сообщений. Травля виртуальная, а ответственность - реальная, вплоть до уголовной.

Как определить злоумышленника

В Интернете можно создать любой аккаунт, представиться кем хочешь. Этим часто пользуются различные преступники.

Признаки, которые должны насторожить при общении:

- Собеседник задает вопросы о семье, пытается узнать адрес, график, финансовое положение.
- Хочет что-то подарить, предлагает встретиться в безлюдном месте, в темное время суток.
- Пытается убедить, что окружающие не ценят вас, предлагает помочь.
- Собеседник просит прислать фотографии интимного характера.
- После общения портится настроение.
- Собеседник пытается манипулировать, выставляет условия общения и давит, требуя быстрее принять решение.
- Предлагает быстро заработать, или наоборот просит финансовой помощи

Если есть любой из этих признаков, стоит прекратить общение, сделать скриншоты переписок и обратиться за помощью.