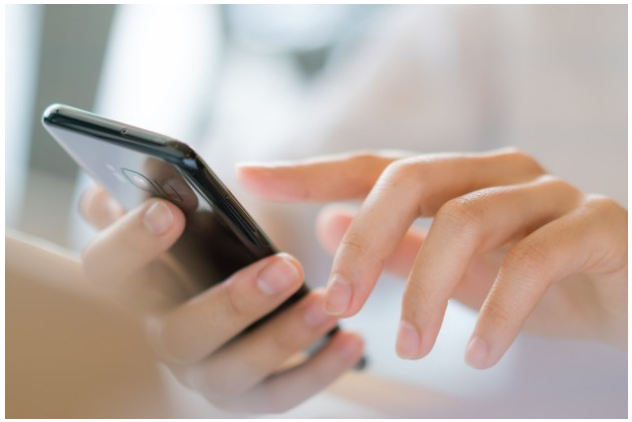
Кибербезопасность или компьютерная безопасность – это совокупность методов и практик защиты взрослого или юного пользователя от атак злоумышленников.

Кибербезопасность является важнейшим критерием и условием использования гаджетов и Интернета. Прежде всего, ребенку необходимо знать, как обхитрить кибермошенника, а для этого существует 7 простых правил:

1. Если компьютер говорит о том, что сайт небезопасен, лучше всего послушать его.
2. В ситуациях определенного рода, лучше умолчать некоторую информацию (например, о том, что ребенок один дома или, что квартира остается без хозяина на несколько недель).
3. За информацией, попадающей в сеть необходимо тщательно следить.
4. Планировать встречи стоит только с реальными друзьями.
5. Каждый аккаунт должен иметь собственный пароль.
6. Пароли должны отличаться сложностью.
7. Все приложения и ПО необходимо своевременно обновлять.

Среди опасностей, поджидающих ребенка на просторах Интернета, стоит уделить особое внимание таким аспектам, как:

- опасные знакомства – интернет-общение с незнакомцем может перерасти в реальную встречу, что является потенциально опасным для ребенка;
- вовлечение в азартные игры – недостаточно сформированная детская психика сильнее подвержена развитию игровой зависимости;
- знакомство с неприемлемым контентом – важная проблема открытого доступа;
- вирусы и вредоносные программы – посещение подозрительных сайтов может стать причиной возникновения на компьютере или телефоне опасного вируса, который может украсть данные или повлиять на работу гаджета.



Детский телефон доверия
8-800-2000-122

Сайт «Детский телефон доверия»
https://telefon-doveria.ru/

Портал «Российский родитель»
http://ruroditel.ru/

КГАУ СЗ «Камчатский центр социальной помощи «СЕМЬЯ»
г. Петропавловск-Камчатский,
ул. Ключевская, д. 28
www.kamsoccentr.ru
e-mail: miloserdie92@mail.ru
Тел. (8-4152) 46-77-96
Режим работы:
Понедельник – Четверг 9.00 – 17.15
Обед с 12.23 – 13.00
Пятница 9.00 – 15.00
Обед с 12.00—12.32
Отделение профилактики безнадзорности несовершеннолетних
г. Петропавловск-Камчатский,
ул. Матросова, д. 37
тел. (8-4152) 46-31-85,
(8-4152) 46-28-02,
(8-4152) 46-33-96

Краевое государственное автономное учреждение социальной защиты
«Камчатский центр социальной помощи семье и детям «СЕМЬЯ»

Как обеспечить кибербезопасность собственному ребенку

Рекомендации родителям

Сложно представить современного ребенка, который способен существовать без гаджета. Несмотря на технологический прогресс, постоянное подключение к сети может представлять особую опасность для ребенка. Рассмотрим эту опасность и определим, что следует знать каждому родителю и его ребенку.

Чему же следует научить ребенка, чтобы повысить его кибербезопасность? Важно своевременно привить следующие навыки:

1. Отказ от разглашения тайн – ни при каких обстоятельствах нельзя раздавать собственные персональные данные.
2. Выявление поддельных сайтов – популярным способом выманивания доступов к личным кабинетам является фишинг (скрытное перенаправление на ложные сайты).
3. Распознавание злоумышленников – необходимо донести вероятную опасность общения с незнакомым в реальной жизни человеком, с людьми с большой разницей в возрасте, а также с теми, кто настоятельно просит скинуть фотографии или какие-либо личные данные.
4. Придумывание сложных паролей и отказ от использования единого для всех сайтов.
5. Различение грани между реальностью и виртуальностью, предполагающей отказ от выполнения в виртуальном мире тех вещей, которые ни за что бы не стали делать в реальном.

Кибербуллинг – относительно новое понятие, означающее травлю с использованием возможностей цифровых технологий. Кибербуллингу подвержены люди всех возрастов, однако, дети находятся в особой группе риска.

Кибербуллинг имеет несколько форм проявления. Наиболее часто встречаемыми на территории России принято считать:

- исключение из общения;
- домогательства с угрозами и преследованием;
- аутинг, предание какого-либо факта гласности;
- кибersталкинг, преследование, перерастающее из виртуального мира в реальный;
- поддельные профили, формируемые на основании известных данных;
- троллинг, предполагающий намеренные провокации и издевательства в сетевом общении.

По поведению ребенка можно определить, что у него имеются какие-либо сложности с общением на просторах Интернета. Ключевыми среди них принято считать:

- отказ или наоборот, чрезмерное использование гаджетов;
- постоянное заметное чувство раздражения и подавленности после взаимодействия с гаджетами;
- резкое снижение успеваемости в школе;
- особая закрытость, настороженность, отказ идти на контакт с близкими.

Чтобы защитить детей от кибербуллинга, важно:

1. Изначально установить правила использования гаджета, предполагающие определенные разрешения и ограничения.
2. Проводите систематические беседы с ребенком, повествующие о том, что Вы всегда открыты для решения вопросов об его отношениях с другими людьми на просторах сети.
3. Будьте готовы к совместному обучению.
4. Ведите постоянные разговоры о возможных психологических проблемах.
5. Отслеживайте изменения в поведении ребенка.
6. Просматривайте и отслеживайте сколько времени ребенок проводит на просторах сети.
7. Умейте спокойно и при этом сочувственно реагировать на проявление переживаний.
8. Находите время для бесед.
9. Не забывайте спрашивать, чего хочется или чего не хватает сыну или дочери.
10. Используйте современные приложения родительского контроля, по типу UniSafe Kids.

Приложение родительского контроля UniSafe Kids – это отличный сервис с расширенными возможностями, позволяющий родителям обеспечить безопасность ребенка не только в сети, но еще и в реальной жизни.

На сегодняшний день, использование приложения UniSafe Kids открывает перед родителями такие возможности, как:

- качественный контроль содержимого устройства ребенка;
- определение опасных приложений/сайтов/сервисов, ограничение доступа к ним;
- установление возрастных ограничений на использование игр и приложений различного типа;
- ограничение временных периодов, в которые допустимо использование гаджетов;
- отслеживание актуального местоположения ребенка;
- возможность получения маршрута следования (в том числе направления реального движения) ребенка;
- чтение сообщений и прослушивание звонков на смартфон;
- отправка уведомлений на устройство ребенка, без возможности его игнорирования.

Управление приложением родительского контроля UniSafe Kids осуществляется через личный кабинет пользователя (родителя). В любой момент можно запросить необходимую информацию о контролируемом устройстве.

А Ваш ребенок достаточно подготовлен к использованию социальных сетей и Интернета? Своевременное знакомство с основами кибербезопасности – залог безопасности любимого ребенка.