

Что делать, если ребенок все же столкнулся с какими-либо рисками

- Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать;
- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете;
- Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей,

проверьте все новые контакты ребенка за последнее время;

- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы);
- Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций



Медиабезопасность в сети интернет

Медиабезопасность – в широком смысле медиабезопасность – это деятельность, направленная на защиту интересов гражданского общества от появления и распространения недостоверной информации в сети интернет, способной негативно повлиять на социальные процессы; в узком смысле медиабезопасность – это деятельность по обеспечению личной безопасности пользователя в сети интернет, которая позволяет ему не только распознавать недостоверную информацию, но и предотвращать распространение вредоносной информации.

ВНИМАНИЕ! ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

- УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА**
- НЕ переходите** по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки
- НЕ сообщайте** свои персональные данные и данные банковской карты
- НЕ верьте** обещаниям внезапных выигрышей
- НЕ используйте** одинаковые пароли для всех аккаунтов
- НЕ указывайте** личную информацию в открытых источниках



Сохрани эту информацию и поделись с другими!

Основные советы по безопасности в социальных сетях:

- Ограничьте список друзей. В списках среди друзей не должно быть случайных и незнакомых людей;
- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату Вашего рождения и другую личную информацию.
- Защищайте свою репутацию - держите ее в чистоте и задавайте себе вопрос: хотели бы Вы, чтобы другие пользователи видели, что Вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить;
- Если Вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегайте размещения фотографий в Интернете, где Вы изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если Вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Основные советы для безопасности мобильного телефона:

- Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда Вам предлагают бесплатный

контент, в нем могут быть скрыты какие-то платные услуги;

- Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоего смартфона;
- Используйте антивирусные программы для мобильных телефонов;
- Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- После того как Вы выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите cookies;
- Периодически проверяйте какие платные услуги активированы на Вашем номере;
- Давайте свой номер мобильного телефона только людям, которых Вы знаете и кому доверяете;
- Bluetooth должен быть выключен, когда Вы им не пользуетесь. Не забывайте иногда проверять это.

ГУО «Вилейский районный социально педагогический центр»

Наш адрес:
Минская область,
аг. Шиловичи
ул. Комсомольская, д. 4
2-17-96;
2-43-54

г. Вилейка
2023 год

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ

01

НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам
- + Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
- + Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

- X Использовать повторения символов
- X Хранить пароли на бумажных носителях
- X Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
- X Сохранять пароль автоматически в браузере
- X Использовать биографическую информацию в пароле


БЕЗОПАСНЫЙ WI-FI

02

- + Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
- + Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
- + Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам
- X Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

03

- + Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов
- X Переходить по непроверенным ссылкам
- X Вводить информацию на сайтах, если соединение не защищено (нет https и )