ПРОФИЛАКТИКА
федеральный центр

БЕЗОПАСНОСТЬ ПАРОЛЕЙ: ЧТО НУЖНО ЗНАТЬ

Пароль — это ключ ко всей личной информации вашего ребенка в сети. Если злоумышленник получит доступ к аккаунтам, он сможет украсть личные данные, фотографии, переписки, деньги и даже воспользоваться именем вашего ребенка для мошеннических действий.

- Используйте длинные пароли от 8 символов.
  Пример: «NekotoryySlOzhnyParol123»
- Создавайте уникальные комбинации с буквами разного регистра (заглавные и строчные), цифрами и специальными символами (!@#$%^&*).
  Пример: «7mYpAsSwOrDwItHSpEclaLSymBoL$»
- Не используйте имена, фамилии, даты рождения, номера телефонов или любые легкоугадываемые слова и последовательности («qwerty», «password»).
- Меняйте пароли регулярно (минимум раз в полгода).
- Не записывайте пароли на бумаге или в незашифрованных файлах на компьютере. Используйте специализированные менеджеры паролей.
- Используйте двухфакторную аутентификацию.
- Объясните опасность фишинга. Расскажите детям о рисках перехода по подозрительным ссылкам и ввода персональных данных на незнакомых сайтах.
- Ограничьте доступ к публичным сетям Wi-Fi.



Важно регулярно напоминать эти советы своим детям, ведь безопасность — дело первостепенной важности!

ПРОФИЛАКТИКА
федеральный центр

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ЧТО ЭТО ТАКОЕ И ПОЧЕМУ ВОЗНИКАЕТ?

Интернет-зависимость – это патологическое состояние, характеризующееся неконтролируемым желанием проводить большое количество времени в сети.

Признаки интернет-зависимости:

- потребность постоянно проверять уведомления и обновления социальных сетей,
- раздражительность и агрессия при попытке ограничить доступ к гаджетам,
- снижение интереса к учебе, хобби и общению вне интернета,
- трудности засыпания и бессонница,
- проблемы с концентрацией внимания и памятью.

Причины возникновения интернет-зависимости

- Недостаточная социализация.
- Потребность в самовыражении.
- Отсутствие самоконтроля.
- Эмоциональная неудовлетворенность.
- Низкая самооценка. Для некоторых подростков виртуальное пространство становится



Рекомендации родителям:

- организуйте онлайн-досуг ребенка: развивающие занятия, видеоуроки на проверенных цифровых платформах; фильмы, каналы с видеоконтентом;
- для детей до 14 лет установите соответствующие настройки («семейные», «детские»), минимизирующие встречи с деструктивным контентом;
- способствуйте вовлечению ребенка в реальные группы сверстников (кружки, секции, лагеря и т. д.);
- обратите внимание подростков на опасность общения в Интернете с незнакомцами;
- договоритесь с ребенком о доступном количестве сетевой активности в сутки;
- развивайте цифровую грамотность ребенка;
- расскажите, что в случае встречи в Интернете с неприятным и пугающим контентом, он может поделиться этими фактами с родителями;
- при обнаружении признаков деструктивного поведения ребенка обратитесь за помощью к специалистам (психологи, службы горячей линии).

ПРОФИЛАКТИКА
федеральный центр

КАК ЗАЩИТИТЬ РЕБЁНКА ОТ НЕЖЕЛАТЕЛЬНОГО КОНТЕНТА В ИНТЕРНЕТЕ?

Для защиты детей от вредоносного контента в Интернете можно использовать встроенные функции различных цифровых платформ и устройств.



СЕМЕЙНЫЕ АККАУНТЫ

Многие популярные сервисы предлагают возможность создания семейных аккаунтов, объединяющих взрослых и детей в одну группу пользователей. Это позволяет взрослым контролировать доступ детей к контенту и приложениям.

ДЕТСКИЙ РЕЖИМ

Некоторые устройства и браузеры имеют специальные детские режимы, которые фильтруют результаты поиска, ограничивают доступ к нежелательным сайтам и позволяют выбирать категории просматриваемого контента.

РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Большинство смартфонов и планшетов поддерживают инструменты родительского контроля, которые позволяют ограничивать доступ к определённым приложениям, играм, покупкам и медиаконтенту.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Антивирусные решения с функцией защиты детей не только защищают устройство от вредоносного программного обеспечения и фишинга, но и предоставляют отчёты о действиях ребёнка в интернете.

Важно помнить, что ни одна программа не способна заменить активное участие взрослого в формировании культуры безопасного поведения ребёнка в цифровом пространстве.

ПРОФИЛАКТИКА
федеральный центр

КАК ЗАЩИТИТЬ РЕБЕНКА ОТ ПРОВОКАТОРОВ В ИНТЕРНЕТЕ?

- Обсудите с ребенком активизацию деятельности по вербовке в террористические организации. Расскажите, какую опасность жизни и здоровью людей несут такие организации. Предупредите об уголовной ответственности.
- Сообщите ребенку, что необходимо игнорировать сомнительные предложения и сообщения. Если поступят такие сообщения, необходимо сообщить взрослому. Если сообщения уже поступили, успокойте и поддержите ребенка.
- Вместе изучите настройки социальных сетей и мессенджеров. Поставьте запрет на входящие звонки и сообщения с неизвестных номеров.
- При поступлении информации о призывах к террористической деятельности – сообщите в правоохранительные органы (номер 102).



Помните: лучшая защита вашего ребенка — это ваша осведомленность, поддержка и доверие!

ПРОФИЛАКТИКА
федеральный центр

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ РЕБЕНКА В ИНТЕРНЕТЕ?



ОБУЧЕНИЕ ОСНОВАМ ЦИФРОВОЙ ГРАМОТНОСТИ

Рассказывайте детям правила безопасного поведения в интернете, объясняйте последствия необдуманных действий.

ИСПОЛЬЗОВАНИЕ АНТИВИРУСНЫХ ПРОГРАММ И ФИЛЬТРОВ

Установите специальные программы, блокирующие доступ к нежелательным сайтам и защищающие устройства от вирусов.

КОНТРОЛЬ ПРИВАТНОСТИ АККАУНТА

Настройте ограничения видимости профилей и публикаций в социальных сетях, убедитесь, что ребенок правильно настраивает уровень конфиденциальности.

ОГРАНИЧЕНИЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Следите за количеством времени, которое ребенок проводит онлайн, помогайте организовывать режим отдыха и занятий вне интернета.

СОЗДАНИЕ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ

Поддерживайте открытый диалог с ребенком, позволяйте ему делиться своими переживаниями и сомнениями относительно взаимодействия в сети.



ПРОФИЛАКТИКА
федеральный центр

КАК ПРОТИВОСТОЯТЬ ВОВЛЕЧЕНИЮ РЕБЕНКА В ПРОТИВОПРАВНУЮ ДЕЯТЕЛЬНОСТЬ?

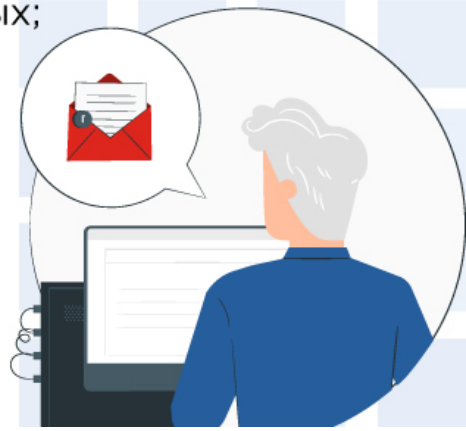
Вовлечение – это склонение, вербовка или иное завлечение ребенка путем уговоров, предложений, обещаний, обмана, угроз или иным способом в совершение преступления или антиобщественных действий.

Это могут быть:

- участие в экстремистских или террористических группировках;
- участие в несанкционированных акциях и митингах;
- сбор информации или выполнение задач в интересах злоумышленников и т. д.

Основные признаки возможного риска

- резкое изменение поведения подростка, изоляция от семьи и друзей, замкнутость;
- частое посещение закрытых групп и чатов, закрытие экрана компьютера или телефона при появлении взрослых;
- появление новых знакомых в социальных сетях, общение с незнакомцами;
- повышенный интерес к радикальным идеям, агрессивная риторика, отрицательное отношение к другим людям и обществу;
- скрытность в финансовых вопросах, появление непонятных источников дохода.



ПРОФИЛАКТИКА
федеральный центр

Что должно насторожить ребенка

- собеседник задает много вопросов о личной жизни;
- просит об одолжении взамен на что-либо;
- задает вопросы о том, кто из родителей, родственников, друзей имеет доступ к телефону или аккаунту;
- просит держать общение в секрете;
- задает вопросы личного и интимного характера;
- заставляет чувствовать себя виноватым или угрожает;
- настаивает на личной встрече;
- лестно говорит о внешнем виде.

Виды опасных сообщений

- призывы к совершению противоправных действий, самоубийству, причинению себе телесных повреждений;
- инструкции по изготовлению взрывных устройств и оружия;
- распространение экстремистских идей (материалов) и пропаганды;
- угрозы, шантаж;
- подозрительные тематические подборки



ПРОФИЛАКТИКА
федеральный центр

ЧТО ВАЖНО СДЕЛАТЬ РОДИТЕЛЯМ?



- Поддерживайте открытый диалог с ребенком.
- Установите правила пользования интернетом совместно с ребенком, обсудив последствия нарушения правил.
- Регулярно проверяйте историю посещений, устройства и приложения, которыми пользуется ребенок.
- Изучите основные методы вербовки, используемые злоумышленниками.
- Предупредите ребенка о рисках публикации личной информации, фотографий, местоположения. Обучите правилам защиты персональных данных, использованию надежных паролей.
- Подавайте личный пример. Соблюдайте принципы безопасной цифровой гигиены.

ПРОФИЛАКТИКА
федеральный центр

КАКИЕ РИСКИ ЕСТЬ В ИНТЕРНЕТЕ?

- **Фишинговые атаки.** Фишеры маскируются под официальные ресурсы и службы, пытаясь обмануть пользователей и украсть личные данные, пароли и финансовую информацию.
- **Кража персональных данных.** Утечка персональной информации может привести к финансовым потерям, шантажу или другим негативным последствиям.
- **Интернет-мошенничество.** Детей привлекают яркие рекламные объявления и заманчивые предложения, такие как бесплатные подарки, скидки или участие в розыгрышах. Однако зачастую подобные акции оказываются приманкой для хищения денег или компрометации аккаунтов.
- **Буллинг и травля в сети.** Онлайн-травля способна нанести серьезный психологический ущерб ребенку, приводя к депрессии, замкнутости и даже самоубийству.
- **Нецелесообразное использование Интернета.** Подростки нередко теряют контроль над временем, проводимым онлайн, что негативно сказывается на учебе, здоровье и социальной активности.

