Зачем нужна цифровая гигиена?

Интернет — это круто: ты можешь учиться, общаться, играть и находить друзей. Но в сети есть и опасности: мошенники, вирусы и люди, которые могут навредить. Цифровая гигиена — это правила, которые помогут тебе оставаться в безопасности, как мытье рук защищает от микробов.

Какие опасности есть в интернете?

- **Мошенники**: Могут притворяться твоими друзьями или просить твои данные (пароли, адрес, номер телефона).
- **Кибербуллинг**: Оскорбления или угрозы в соцсетях.
- **Вирусы и вредные программы**: Могут украсть твои данные или сломать телефон/компьютер.
- **Опасный контент**: Сайты или группы, которые подталкивают к опасным и противоправным поступкам.

Правила безопасного поведения в интернете

1. **Не делись личной информацией**
   Никогда не отправляй незнакомцам свой адрес, номер телефона, данные паспорта или фото. Даже если кто-то представился "сотрудником банка" или "другом друга".
   Пример: Тебе пишут: "Я из службы поддержки игры, дай пароль, чтобы вернуть аккаунт". Это мошенник!
2. **Создавай надежные пароли**
   Хороший пароль — это минимум 8 символов, с буквами, цифрами и знаками.
   Не используй один пароль для всех сайтов.
   Совет: Придумай фразу, которую легко запомнить, например:
   "Я люблю пиццу!" → "YalubluPizzu2025!".
3. **Проверяй ссылки и файлы**
   Не открывай ссылки и не скачивай файлы от незнакомцев. Они могут содержать вирусы.
   Пример: Тебе прислали ссылку с текстом "Смотри, как круто!".
   Не кликай, пока не убедишься, что это безопасно.
4. **Будь осторожен в соцсетях**
   Не добавляй в друзья всех подряд. Настраивай приватность: пусть твои посты видят только друзья. Не выкладывай, где ты сейчас, или личные фото.
   Пример: Фото с геолокацией "Дома один!" может привлечь мошенников.
5. **Защищай свои устройства**
   Установи антивирус и обновляй приложения. Не давай телефон незнакомцам, даже если они просят "позвонить".
   Совет: Включи двухфакторную аутентификацию (например, код из SMS) для важных аккаунтов.
6. **Не верь всему, что видишь**
   Мошенники могут создавать фейковые сайты или сообщения, похожие на настоящие. Проверяй, официальный ли это сайт (например, адрес должен быть "vk.com", а не "vk-login.ru").
   Пример: Сообщение "Ты выиграл телефон!" — скорее всего, обман.
7. **Обращай внимание на кибербуллинг**
   Если кто-то пишет тебе гадости или угрожает, не отвечай. Сделай скриншот, заблокируй этого человека и расскажи взрослым.
   Совет: Никогда не участвуй в травле других — это может навредить и тебе.

Что делать, если что-то пошло не так?

- **Тебя обманули или украли аккаунт**: Немедленно смени пароли и сообщи родителям или учителю. Если украли деньги или данные, обратись в полицию.
- **Ты видишь опасный контент**: Не участвуй и не распространяй. Расскажи взрослым.
- **Ты стал жертвой травли**: Не молчи! Поговори с родителями, учителем или позвони на горячую линию доверия: **8 (800) 2000-122** (бесплатно).

Помни!

Интернет — это твой помощник, а не враг. Соблюдай правила цифровой гигиены, и ты будешь в безопасности. Если сомневаешься, спроси у родителей или учителей — они помогут!

Основано на рекомендациях МВД России и образовательных порталов по кибербезопасности.

Почему цифровая гигиена важна?

Интернет — это часть жизни вашего ребенка: он учится, общается и развлекается онлайн. Но в сети есть риски: мошенники, кибербуллинг, вирусы и опасный контент. Цифровая гигиена помогает защитить ребенка, сохранить его данные и здоровье. Вы можете научить его безопасному поведению, как учите переходить дорогу.

Какие угрозы есть в интернете?

- **Мошенники**: Могут обманом выманивать пароли, деньги или личные данные, представляясь друзьями или сотрудниками компаний.
- **Кибербуллинг**: Оскорбления, угрозы или травля в соцсетях.
- **Вредоносные программы**: Вирусы, которые крадут данные или ломают устройства.
- **Неподходящий контент**: Сайты или группы, подталкивающие к опасным действиям (например, экстремальным челленджам).

Как защитить ребенка в интернете?

1. **Говорите с ребенком об интернете**
   Объясните, почему нельзя делиться личной информацией (адрес, телефон, фото) с незнакомцами. Расскажите, как распознать мошенников.
   Пример: Сообщение "Вы выиграли приз, перейдите по ссылке!" — это обман.
   Попросите ребенка показывать вам такие сообщения.
2. **Настройте устройства**
   Установите антивирус и включите родительский контроль на компьютере, телефоне и в приложениях (например, в YouTube или Google). Ограничьте доступ к сайтам с неподходящим контентом.
   Совет: Используйте пароли вроде "Solnce2025!" (не менее 8 символов, с буквами, цифрами и знаками) и не повторяйте их на разных сайтах.
3. **Проверяйте соцсети**
   Помогите ребенку настроить приватность: пусть его профиль видят только друзья.
   Регулярно смотрите, с кем он общается, и объясните, почему нельзя добавлять незнакомцев.
   Пример: Если кто-то предлагает встретиться в реальной жизни, ребенок должен сначала рассказать вам.
4. **Учите проверять информацию**
   Покажите, как отличать настоящие сайты от фейковых (например, "vk.com" — это официально, а "vk-login.ru" — нет). Научите не открывать подозрительные ссылки и не скачивать файлы от незнакомцев.
   Совет: Попросите ребенка спрашивать вас, если он сомневается в сообщении или сайте.
5. **Следите за экранным временем**
   Ограничьте время в интернете, чтобы ребенок не стал зависимым. Договоритесь о правилах: например, не больше 2 часов в день на соцсети.
   Пример: Установите приложение для контроля экранного времени или договоритесь выключать Wi-Fi после 21:00.
6. **Будьте примером**
   Соблюдайте цифровую гигиену сами: не делитесь личной информацией, используйте надежные пароли, проверяйте ссылки. Дети учатся, глядя на вас.
   Совет: Покажите ребенку, как вы проверяете сообщения или сайты перед тем, как на них кликать.
7. **Обсуждайте кибербуллинг**

Расскажите, что делать, если кто-то пишет гадости: не отвечать, сделать скриншот, заблокировать и сообщить вам. Поддерживайте ребенка, чтобы он не боялся делиться проблемами.
Пример: Если одноклассники создали чат для травли, помогите ребенку выйти из него и обратитесь к учителю.

Опасные способы заработка: как защитить ребенка?

Мошенники и преступники часто вербуют подростков через соцсети, мессенджеры или игровые чаты, предлагая "лёгкие деньги". Такие схемы незаконны и опасны, могут привести к уголовной ответственности и испортить будущее ребенка. Вот что нужно знать:

1. **Дропинг (дропы)**
   Что это? Подростков просят предоставить свои банковские карты или открыть новые счета для перевода денег. Мошенники используют эти счета, чтобы обналичивать украденные средства.
   Риски: Ребенок может стать соучастником преступления (ст. 159 УК РФ — мошенничество, до 7 лет лишения свободы). Карты блокируются, а на ребенка могут оформить кредиты. По данным Сбербанка, около 60% дропов — молодёжь до 24 лет.*Пример*: Ребенку пишут: "Дай карту для перевода, получишь 5000 рублей". После перевода он теряет доступ к карте и оказывается под следствием.

2. **Курьеры для запрещённых веществ (кладмены)**
   Что это? Подростков нанимают раскладывать "закладки" с наркотиками по тайникам или доставлять их покупателям. Вербовка идёт через соцсети под видом "работы курьером".
   Риски: Это уголовное преступление (ст. 228 УК РФ, от 4 до 20 лет лишения свободы). Даже несовершеннолетние привлекаются к ответственности. По данным МВД, школьники и студенты — основная группа кладменов.*Пример*: Объявление "Курьер, 10 000 рублей за день, просто развози посылки". Ребенок забирает свёрток, не зная, что там наркотики, и попадается полиции.

3. **Курьеры для мошеннических средств**
   Что это? Детей просят забирать наличные у жертв мошенников (например, пожилых людей) и передавать их организаторам. Мошенники представляются "работодателями".
   Риски: Соучастие в мошенничестве (ст. 159 УК РФ, до 7 лет). Ребенок может быть задержан как пособник.
   Пример: Ребенку говорят: "Забери деньги у бабушки, это оплата за товар". На самом деле это обман, а ребенок — курьер мошенников.

Как распознать и защитить?

- *Признаки*: Ребенок внезапно получает большие суммы, прячет переписку, уходит из дома без объяснений или покупает дорогие вещи без видимого дохода.
- *Что делать*:
  - Расскажите ребенку, что предложения "лёгких денег" в интернете — это обман. Объясните, что даже разовое участие в таких схемах ведёт к уголовной ответственности.
  - Проверяйте банковские карты ребенка: установите лимиты на переводы и снятие наличных (с 29 марта 2025 года банки не открывают счета подросткам 14–18 лет без согласия родителей).
  - Наблюдайте за его поведением: если ребенок стал скрытным или нервным, поговорите спокойно, чтобы он поделился проблемами.
  - Научите говорить "нет" подозрительным предложениям в соцсетях, мессенджерах или играх.

- *Совет*: Если ребенок уже получил деньги или карту, не возвращайте переводы самостоятельно — обратитесь в банк или полицию.

Что делать, если ребенок столкнулся с проблемой?

- **Мошенничество или кража данных**: Смените пароли, заблокируйте аккаунты и обратитесь в полицию (телефон 102). Если украли деньги, свяжитесь с банком.
- **Кибербуллинг**: Сохраните доказательства (скриншоты), обратитесь в школу или к психологу. При угрозах сообщите в полицию.
- **Вовлечение в преступные схемы**: Немедленно обратитесь в полицию (102) или к адвокату. Не пытайтесь "решить" ситуацию самостоятельно, чтобы не усугубить последствия. Сохраните переписку с "работодателями" как доказательство.
- **Опасный контент**: Заблокируйте доступ к сайту или группе. Расскажите ребенку, почему это опасно, и сообщите в Роскомнадзор через сайт rkn.gov.ru.
- **Эмоциональные проблемы**: Если ребенок стал замкнутым или тревожным из-за интернета, поговорите с ним или обратитесь к психологу. Позвоните на горячую линию доверия: **8 (800) 2000-122** (бесплатно).

Помните!

Вы — главный помощник ребенка в интернете. Будьте в курсе его онлайн-жизни, но не запрещайте всё подряд: это может вызвать протест. Учите, поддерживайте и доверяйте друг другу.

Основано на рекомендациях МВД России и образовательных порталах по кибербезопасности.