

# БЕЗОПАСНЫЙ ИНТЕРНЕТ

Материалы для учащихся **средних классов** к «Уроку безопасного Интернета»



|                                              |    |
|----------------------------------------------|----|
| Зачем это пособие? .....                     | 4  |
| Интернет-зависимость .....                   | 5  |
| Мошенничество в Интернете .....              | 7  |
| Персональные данные .....                    | 11 |
| Общение в Интернете .....                    | 15 |
| Травля в Интернете .....                     | 22 |
| Анонимность в сети .....                     | 25 |
| Твой «Цифровой след» .....                   | 27 |
| Фейки в Интернете .....                      | 30 |
| 10 советов по безопасности в Интернете ..... | 31 |

**Знаешь ли ты, кто такой Билл Гейтс?** Это один из создателей операционной сети Windows, которая, скорее всего, стоит и на твоём компьютере. Можно сказать, что именно этот человек создал для нас те компьютеры, которыми мы пользуемся. Как ты думаешь, сколько времени в день он разрешал своим детям проводить за компьютером?

**Ответ тебя удивит:** 45 минут в будни и 1 час, 45 минут в выходные. При этом он не разрешал детям пользоваться компьютером вечером перед сном, а до 14 лет и вовсе не давал им в руки гаджетов.

**Другой известный человек, Стив Джобс,** основатель Apple и создатель знаменитого «Айфона», запрещал своим детям пользоваться гаджетами по ночам и в выходные дни, а также во время еды.

Почему так? **Да потому что эти люди больше других знают об опасности, которую несет Интернет-зависимость для здоровья и психики пользователей.**

## ПРИЗНАКИ:

- Не ложишься спать, предварительно не посидев в смартфоне.
- Каждый день ешь за компьютером или со смартфоном в руке.
- Почти все выходные проводишь в Интернете, никуда не выходя.
- Злишься или раздражаешься, когда приходится отложить смартфон или оторваться от Интернета.
- Играешь в компьютерные игры два и более раз в неделю.
- Сидишь в социальных сетях или «болталках» в ночное время.
- Не высыпаешься, часто испытываешь головные боли или неприятные ощущения в глазах.

**ОБЩАЙСЯ С ДРУЗЬЯМИ В РЕАЛЬНОЙ  
ЖИЗНИ, А НЕ В ОНЛАЙНЕ!**



## ЕСЛИ ТЫ ХОЧЕШЬ ИЗБЕЖАТЬ ИНТЕРНЕТ-ЗАВИСИМОСТИ, ТО ПРИДЕРЖИВАЙСЯ ПРАВИЛ:

- Сократи время использования гаджетов и компьютера.
- Не бери в руки телефон минимум за час до того, как планируешь лечь спать. Интернет, соцсети или игры могут вызывать яркие эмоции, которые помешают уснуть.
- Не ешь за компьютером и не используй телефон во время еды. Отвлекись от них ненадолго, лучше пообщайся с родственниками или друзьями.
- Старайся на выходных использовать компьютер и гаджеты как можно меньше. В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.

## ПО ДАННЫМ ИССЛЕДОВАНИЙ В РОССИИ:

**80% ШКОЛЬНИКОВ**

не могут обойтись без смартфона

**80% ШКОЛЬНИКОВ**

страдают нарушением зрения

**80% ШКОЛЬНИКОВ**

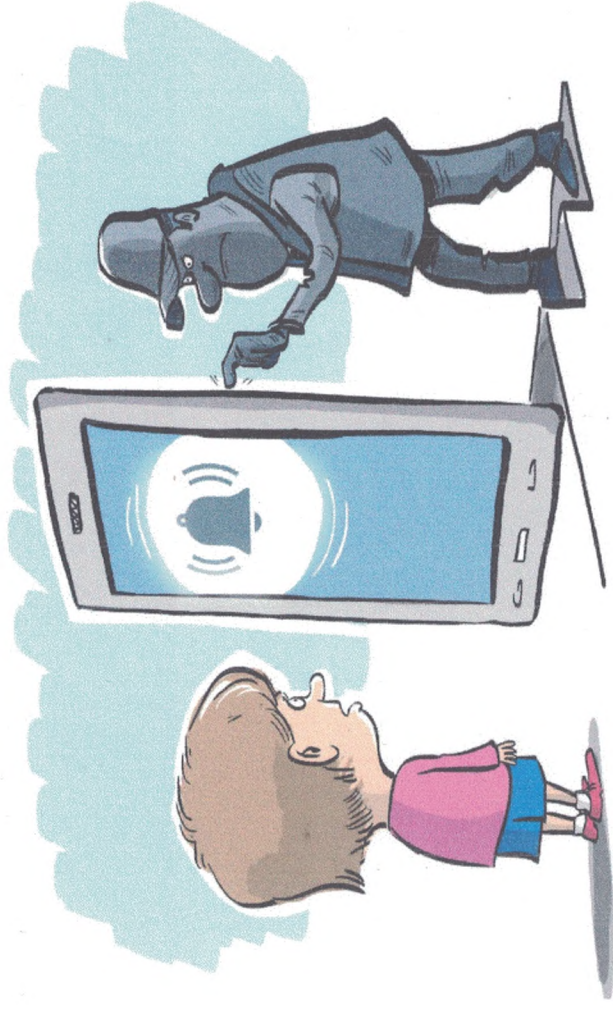
страдают искривлением позвоночника

**3-4% ВЫПУСНИКОВ**

полностью здоровы

## КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

- 1. Взлом аккаунтов в соцсетях и рассылка сообщений от друзей.** Мошенники придумывают разные ситуации и просят срочно перевести деньги.
- 2. Сайты-подделки.** Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-подделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.
- 3. Рассылка писем по электронной почте и в соцсетях с выигрышем.** Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.
- 4. Звонки с поддельных номеров.** Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.
- 5. Шантаж.** Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях.



**Проверяй адрес сайта!**

**Обрати внимание на настоящий адрес сайта! При наведении мыши реальный адрес отображается во всплывающей подсказке**

## ЧЕМ ОПАСНЫ САЙТЫ-ПОДДЕЛКИ?

- Крадут пароли
- Распространяют вредоносное ПО
- Крадут персональные данные
- Навязывают платные услуги
- Крадут деньги



Просят подтвердить логин/пароль

Пугают блокировкой или заражением

Просят прислать  
данные карты и CVV-код

- Закрой страницу, блокировка пропала? Все в порядке!
- Войди в сеть «как обычно» и убедись, что все в порядке!
- Проверь систему своим антивирусом!
- Удаляй письма с неизвестных адресов!
- Игнорируй неизвестные ссылки!
- Используй кнопки «Это спам», «Заблокировать отправителя»

Надежный | <https://vk2.com/>

vk

Поиск

Чтобы просматривать эту страницу, ну



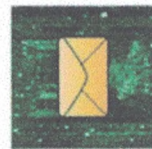
Easy Followers For  
TeamDom

★★★★



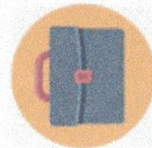
Followers Generator  
TeamDom

★★★★



Spy On Text Messages  
TeamDom

★★★★



Mobile Biz Team 2  
TeamDom

★★★★



Spy On Camera Stream  
TeamDom

★★★★



Unfollow Tracker  
TeamDom

★★★★



Get More Friends  
YUNO

★★★★



Get More Views  
YUNO

★★★★

- **Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию.** При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.
- **Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили.** Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номеру и с какой целью.
- **Проверяй адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.
- **Обращай внимание на наполнение сайта.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.
- **Не переходи по неизвестным ссылкам.**
- **Не открывай файлы из писем или сообщений, которые прислали незнакомые люди.**
- **Если же ты стал жертвой мошенников, то следует сразу же сообщить об этом родителям.**



**ЧТОБЫ НЕ ПОПАСТЬСЯ МОШЕННИКАМ –  
МЫСЛИ САМОСТОЯТЕЛЬНО!**

**Персональные данные** – все данные о человеке, своего рода «паспорт его личности». Их раскрытие в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям.

## ЧТО ОТНОСИТСЯ К ПЕРСОНАЛЬНЫМ ДАННЫМ?



1. **Фамилия, имя, отчество.**
2. **Все твои документы** (паспорт, свидетельство о рождении, аттестат).
3. **Банковские данные** (номер счета, карты, пин-код, CVV-код).
4. **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы).
5. Фотографии и видеозаписи с твоим изображением.
6. Данные о твоих родственниках.
7. Твои логины и пароли.

## КАК ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

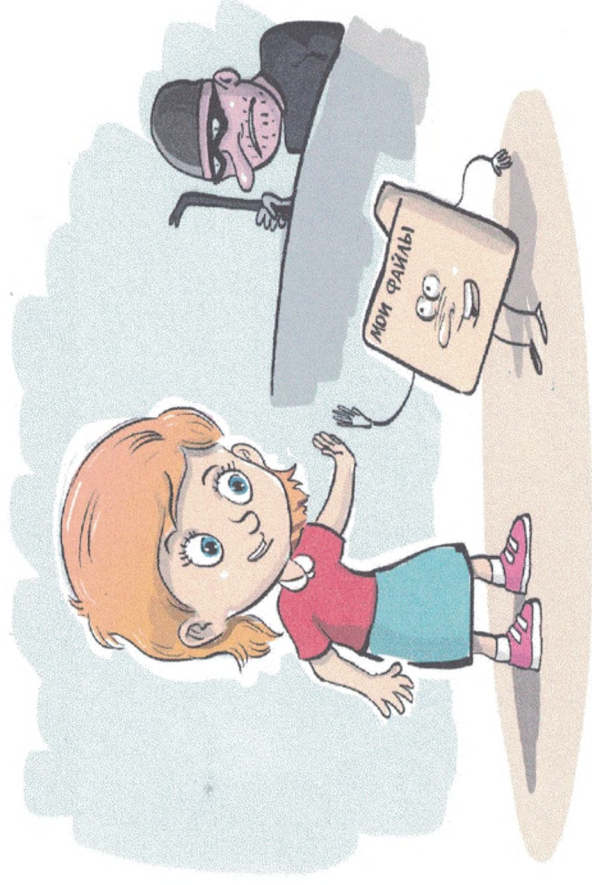
1. **Придумывай и используй разные сложные пароли** для почтовых ящиков, соцсетей и других сайтов. Пароль восстановить проще, чем вернуть украденные деньги.
2. **Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**

3. **Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.

4. **Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.

5. **Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.

6. **Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.



**МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ, НО ВСЕГДА ПОБЕДИМЫ!**

В ИНТЕРНЕТЕ МОЖНО НАЙТИ  
ДАННЫЕ ДАЖЕ С НЕРАБОТАЮЩИХ  
И ОТКЛЮЧЕННЫХ САЙТОВ

РЕГУЛЯРНО ПРОВЕРЯЙ И  
НАСТРАИВАЙ ПРИВАТНОСТЬ

ДАННЫЕ ЧЕЛОВЕКА – НОВАЯ  
ВАЛЮТА, НОВОЕ ЗОЛОТО. ЗА НИМИ  
ОХОТЯТСЯ КРУПНЫЕ КОМПАНИИ И  
ПРЕСТУПНИКИ



## В МОБИЛЬНОМ ТЕЛЕФОНЕ МНОГО ВАЖНОЙ ИНФОРМАЦИИ!



Список контактов

Личные фотографии / видеозаписи

Данные о банковских  
картах и платежах

Привязка к балансу сим-карты

Данные доступа к электронной почте  
и иным аккаунтам в сети

## ПРОВЕРЯЙ, КАКИЕ ПРАВА ПРОСИТ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ!

- Игнорируй звонки и СМС с незнакомых номеров!
- Установи пароль на мобильный телефон!
- Следи за своим мобильным телефоном или планшетом!

### ТЕБЕ СЛЕДУЕТ ОСТЕРЕГАТЬСЯ НЕЗНАКОМЦЕВ В ИНТЕРНЕТЕ, КОТОРЫЕ:

1. Задают много вопросов о семье и личной жизни.
2. Просят об одолжениях в обмен на что-либо.
3. Убедительно просят никому о них не рассказывать и держать дружбу в тайне.
4. Задают вопросы о том, кто еще имеет доступ к твоему телефону, компьютеру или аккаунту.
5. Настаивают на личной встрече.
6. Заставляют тебя чувствовать себя виноватым, шантажируют или даже угрожают.
7. Ведут с тобой такие разговоры, после которых ты ощущаешь печаль, тревогу, грусть, стыд, страх, одиночество, свою ненужность близким, разочарование в жизни или людях, безысходность, злость, ненависть, желание причинить кому-то боль (знай, что все это не твои чувства, а лишь умелая манипуляция твоим сознанием).



**БУДЬ ОСТОРОЖЕН,  
ДОБАВЛЯЯ «ДРУЗЕЙ» ДЛЯ ОБЩЕНИЯ В СЕТИ!**

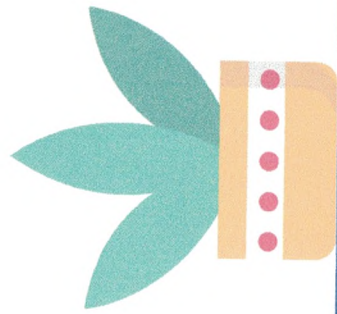
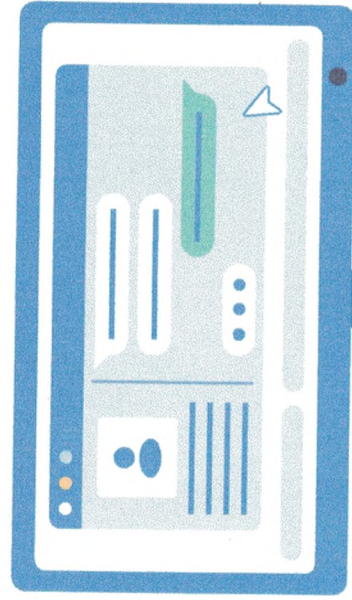
## МОЖНО

Родственники  
Одноклассники  
Друзья и знакомые

## НЕЛЬЗЯ

Интернет-хамы (тролли)  
Преступники  
Незнакомцы  
 Попрошайки  
Излишне любопытные

**ПРЕЖДЕ, ЧЕМ ВСТРЕТИТЬСЯ С «ДРУГОМ» ИЗ ИНТЕРНЕТА,  
ПОСОВЕТУЙСЯ С РОДИТЕЛЯМИ!**



## ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

- 1. Страницы в социальных сетях лучше закрыть от посторонних.** Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои личные данные от попадания в руки преступников. Как правило, информацию о себе, своих увлечениях, хобби, фото с друзьями и многое другое мы публикуем в соцсетях. Очень часто информацию о нас злоумышленники берут в открытом доступе.
- 2. Будь осторожен, когда добавляешь незнакомого человека в друзья, особенно того, кого ты не знаешь в реальной жизни.** Если же новый знакомый задает тебе много вопросов о семье или о том, где ты живешь и учишься, то никогда не рассказывай ему эту информацию. Сразу же сообщай о подозрительном незнакомце своим родителям.
- 3. Будь внимателен, если в переписке тебя призывают к действию и пытаются подловить.** Об этом свидетельствуют такие фразы, как: «А ты сможешь или тебе слабо?» «Все мои знакомые уже это делали, в этом нет ничего такого» и аналогичные. Такие фразы должны тебя насторожить. Рекомендуем сразу блокировать подобные аккаунты.
- 4. Не соглашайся на встречу с людьми из Интернета.** Под профилем твоего ровесника могут сидеть далеко не девочки и мальчики, а самые настоящие преступники. Всегда сообщай своим родителям о своих друзьях из Интернета, а также о том, куда ты направляешься, с кем собираешься встретиться во избежание опасности.
- 5. Если человек, с которым ты общаешься в Интернете заставляет тебя испытывать негативные чувства и эмоции, о которых было написано ранее, поделись об этом с родителями или другими взрослыми людьми, которым ты доверяешь.** Не стесняйся признаться в этом. Такие эмоции может испытывать любой человек, но только взрослых в состоянии помочь избавиться от них и защитить тебя от их воздействия.

## СОВЕТЫ ЭКСПЕРТОВ

Если вы подружились с кем-то онлайн, задайте себе эти вопросы, прежде чем продолжать общение:

? Этот человек попросил меня держать нашу дружбу и переписку в секрете от моих друзей и родителей?

? Кажется ли мне, что я веду себя не так как обычно, общаясь с этим человеком, как будто мной манипулируют?

? Интересовался ли этот человек моими персональными данными или личной информацией о моей семье?

? Возникает ли меня ощущение, что меня к чему-то склоняют или просят сделать что-то, что противоречит моим принципам?

Если на один или более из этих вопросов вы ответили «да», то это опасная и неблагоприятная дружба и общение стоит прекратить.  
Ты заслуживаешь лучшего!

## ВСЕГДА ПОМНИ!

Если кто-то очень назойлив в общении с тобой онлайн, расскажи об этом другу или родным, не отправляй незнакомым людям свои фото! Остерегайся разговоров про личную жизнь с незнакомыми тебе людьми в интернете. Никогда не планируй встречи в жизни с незнакомцами, с которыми ты познакомился через интернет, без присутствия одного из родителей.

КОГДА ЛЮДИ САДЯТСЯ ЗА РУЛЬ И ВЫЕЗЖАЮТ НА ДОРОГУ, ОНИ ОБЯЗАНЫ СЛЕДОВАТЬ ПРАВИЛАМ ДОРОЖНОГО ДВИЖЕНИЯ. СВЕТОФОР ПОМОГАЕТ РЕГУЛИРОВАТЬ ДВИЖЕНИЕ, ПОКАЗЫВАЯ КОГДА БЕЗОПАСНО ЕХАТЬ, А КОГДА НУЖНО ОСТАНОВИТЬСЯ

1. Возьмите три листа бумаги и нарисуйте в каждом круг. Раскрасьте круги, по одному, в зеленый, желтый и красный цвет.

2. Со своей группой прочитайте каждую из представленных историй. Используйте свои круги, чтобы дать оценку ситуации — зеленый цвет, желтый цвет и красный цвет. Положите перед собой выбранный цвет, подходящий ситуации, картинкой вниз.

3. Дождитесь пока закончит группа. Когда все в вашей группе сделали выбор, переверните свои листки и обсудите свои решения. Решите вместе какой из цветов наиболее подходит к ситуации. Это будет ваш общий ответ.

4. После каждой из предложенных ситуаций запишите ваш общий ответ и причину почему вы так решили.

## Стой! Опасность!

Человек, с которым идет общение, ведет себя некорректно и общение немедленно следует прекратить

## Будь осторожен!

Что-то тебе подсказывает, что общение идет не в том направлении, которое для тебя комфортно. Будь внимателен и будь готов прекратить общение, если что-то пойдет не так

## Все хорошо, общение можно продолжать!

Общение с человеком идет непринужденно и не переходит границ дозволенного, но всегда помни, ни с кем не делись персональной информацией!



## ИСТОРИЯ АЛИСЫ

Алисе 14 лет. Вчера Алиса была на празднике у одноклассника Вани, где она познакомилась с родственниками Вани, в том числе его дядей. Зайдя сегодня на свою страницу «ВКонтакте», она обнаруживает заявку в друзья от этого дяди. Она плохо его знает, но вчера они немного поговорили про школу и ее хобби.

**КАКОЙ ЦВЕТ ПОДХОДИТ, ПО ВАШЕМУ МНЕНИЮ, ДЛЯ СИТУАЦИИ, В КОТОРОЙ ОКАЗАЛАСЬ АЛИСА? ОБЪЯСНИТЕ СВОЕ РЕШЕНИЕ.**



## ИСТОРИЯ ВОВЫ

Вове 12 лет, и он обожает играть в онлайн-игры. Когда он только начал играть, он познакомился с другим игроком, который помог ему на начальных уровнях и показал, как работает игра. С этого момента они всегда играют вместе, проходят квесты и участвуют в массовых онлайн-сражениях, где прикрывают друг друга. Как-то, во время игры с другим пользователем при прохождении квеста, у них спросили, сколько им лет, на что друг Вовы ответил: «Какая разница, друг? Никому это не интересно. Сконцентрируйся на миссии»

**КАКОЙ ЦВЕТ ПОДХОДИТ, ПО ВАШЕМУ МНЕНИЮ, ДЛЯ СИТУАЦИИ, В КОТОРОЙ ОКАЗАЛСЯ ВОВА? ОБЪЯСНИТЕ СВОЕ РЕШЕНИЕ**

## ИСТОРИЯ ЛИЗЫ

Лизе 12 лет, и она часто ведет трансляции в новой музыкальной соцсети, куда выкладывает свои ролики под ником Элиза\_12. На прошлой неделе ей поставил лайк парень с ником Миша-Миша-98, после чего он написал ей в «личные сообщения», что она очень талантливая. С этого дня они каждый день переписываются. Лизе нравится общаться с Мишей. С ним легко общаться, а мальчики в Лизинем классе ей не нравятся. Она рассказывает ему о том, что происходит с ней в школе и что ее раздражает дома, но пока не общалась с ним никакой персональной информацией. «Ты очень взрослая для 12 лет», написал ей Миша, - «Мне 20».

**КАКОЙ ЦВЕТ ПОДХОДИТ, ПО ВАШЕМУ МНЕНИЮ,  
ДЛЯ СИТУАЦИИ, В КОТОРОЙ ОКАЗАЛАСЬ АЛИСА?  
ОБЪЯСНИТЕ СВОЕ РЕШЕНИЕ.**

Лиза продолжает общение с Мишей, они переписываются уже больше недели. Ей приятно общение, ведь он старше нее. Так как Лизе не нравятся никто из школы, ей нравится общаться с Мишей онлайн. Как ей кажется, у нее неплохо получается. Пару раз он уже намекал ей на непонятные темы, что Лизе показалось странным. Сегодня он написал ей, «можно я тебе отправлю фоточку?». До того, как Лиза успела ответить, он добавил, «Пусть это будет только между нами, ок? Ты мне нравишься, Лиза. Надеюсь, я тебе тоже понравлюсь»

**КАКОЙ ЦВЕТ ПОДХОДИТ, ПО ВАШЕМУ МНЕНИЮ,  
ДЛЯ СИТУАЦИИ, В КОТОРОЙ ОКАЗАЛАСЬ ЛИЗА?  
ОБЪЯСНИТЕ СВОЕ РЕШЕНИЕ**



**Травля в Интернете является большой проблемой для всех пользователей.** Травлю в сети еще называют кибербуллингом. Она включает в себя издевательства, оскорбления, унижения, преследование человека.

## КАК ВЫГЛЯДИТ ТРАВЛЯ В ИНТЕРНЕТЕ?

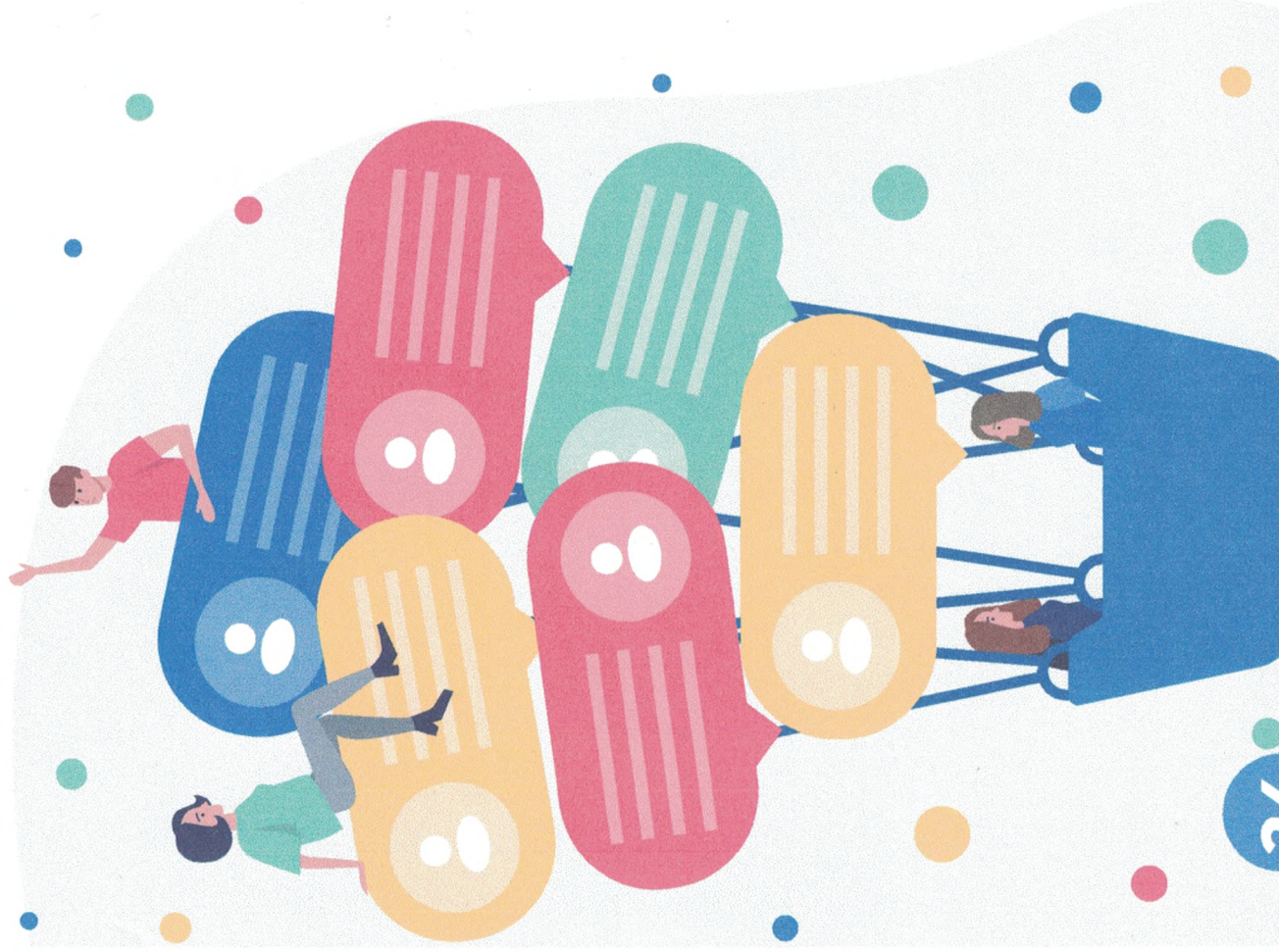
1. Оскорбительные и угрожающие сообщения, изображения или видео.
2. Передразнивание, бойкоты или унижительные комментарии в сети, в которых упоминается личность человека.
3. Распространение неприятных слухов и обсуждение человека за его спиной.
4. Создание поддельных аккаунтов от имени конкретного человека с целью обмануть или унижить его.
5. Специально смонтированные фото или видео с изображением человека.



## ЧТО ДЕЛАТЬ, ЕСЛИ ТЫ СТОЛКНУЛСЯ С ТРАВЛЕЙ В ИНТЕРНЕТЕ?

1. **Поговори с родителями или учителями об этой ситуации.** Они не оставят тебя одного в неприятном состоянии и помогут наилучшим способом разрешить любую ситуацию. Расскажи им, что ты воспринимаешь эту ситуацию серьезно и объясни какие чувства ты испытываешь.
2. **Постарайся сохранять спокойствие и не отвечать обидчику.** Как правило, его цель – вывести тебя на эмоции. Помни, что твой обидчик распускает о тебе слухи, оскорбляет тебя не потому, что на самом деле считает тебя таким, а потому, что у него самого серьезные проблемы (возможно даже с психикой).
3. **Вместе с родителями собери доказательства:** сделай скриншоты переписки, скопируй ссылки на аккаунты обидчика, тебе это может пригодиться в случае обращения в полицию.
4. **Заблокируй обидчика и внеси его в черный список,** чтобы у него больше не было возможности оскорбить тебя или задеть ложными и неприятными высказываниями.
5. **Никогда не оставайся сторонним наблюдателем, если травле подвергнулся кто-то другой.** Собери в группе (в чате), в которой вы общаетесь команду единомышленников, обговори с ними стратегию действий против обидчика. Вам необходимо выступить единым фронтом против любых оскорбляющих действий и требовать прекращения недопустимого поведения. Как правило, обидчики не осмеливаются идти против большой группы людей, действующих заодно, у них не хватает на это смелости. Если действия обидчика не прекратятся и в этом случае, следует всей команде единомышленников демонстративно выйти из группы (чата), это окажет психологическое воздействие на остальных участников, а также будет поддержкой для жертвы травли. Попробуй выйти на личное общение с жертвой травли и поддержать ее. Если жертвой травли стал твой знакомый, расскажи об этом учителю или его родителю. Тем самым ты можешь помочь человеку, который самостоятельно не видит выхода из сложившейся ситуации и страдает.

**ПРОВОДИ БОЛЬШЕ ВРЕМЕНИ В РЕАЛЬНОЙ ЖИЗНИ!**



Будь вежлив и дружелюбен

Откажись от общения с неприятным человеком, включи его в «черный список», удали из «друзей»

Если тебя обижают в интернете — посоветуйся с родителями или учителями!

**НЕЛЬЗЯ**

Редактировать чужие фотографии

Выкладывать сцены насилия и унижения

Грубить и оскорблять в письмах и комментариях

Использовать чужие материалы без разрешения

## АНОНИМНОСТЬ В ИНТЕРНЕТЕ — МИФ

IT-специалист легко определяет автора специальными методами

### ЗАДУМАЙСЯ

с кем ты общаешься в сети

кто скрывается за ником и почему

### ВКОНТАКТЕ ЗАРЕГИСТРИРОВАНО

Владимир Путин — 5 387 чел.

Ботаник — 190 чел.

Колобок — 1 187 чел.

Барби — 2 016 чел.

Бетмен — 909 чел.

Королева красоты — 11 чел.

### АДМИНИСТРАЦИЯ РЕСУРСА ПРОВЕРЯЕТ И ПОДТВЕРЖДАЕТ

аккаунты знаменитостей

официальные группы и сообщества

Многим людям до сих пор кажется, что Интернет – безопасное и абсолютно анонимное место, где каждый может писать и делать все, что ему вздумается. Но это не так. Поэтому тебе следует помнить две важных истины:

1. Всё, что однажды попало в Интернет, остаётся там навсегда.
2. В Интернете можно найти кого-угодно, даже если пользователь попытался скрыть о себе всю информацию.

Многие пытаются скрыть свою личность в Интернете. Например, простые пользователи делают это, чтобы друзья или близкие не узнали о каких-то их увлечениях. Но гораздо чаще это делают хулиганы или преступники, которым важно, чтобы их действия остались в тайне. Они боятся проблем с законом и пользуются различными способами: создают фейковые профили в соцсетях, используют специальные программы-анонимайзеры.

Следует помнить, что каждое твое действие в Интернете содержит информацию о том устройстве, с которого ты это делал – например, о телефоне или компьютере. А твой Интернет-провайдер видит все, что ты делаешь в Интернете, несмотря на любую программу. Следовательно, эта информация может быть доступна кому угодно: от сотрудника полиции до преступника.



**АНОНИМНОСТЬ В СЕТИ – МИФ!**

Наши телефоны включены круглосуточно. И все это время они собирают о нас информацию. Больше всех - приложения соцсетей и мессенджеров. Фото, видео, история переписок, хобби и увлечения, даже места, в которых ты бываешь - все это приложения собирают и хранят. **А все, что однажды попало в Интернет, остается там навсегда и удалить это невозможно.**

## ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ ВСЯ ЭТА ИНФОРМАЦИЯ?

- 1. Соцсети, поисковые сайты, Интернет-магазины и прочие крупные Интернет-ресурсы собирают данные для того, чтобы потом показывать своим пользователям рекламу.** Чем точнее реклама попадает в интересы и увлечения каждого конкретного пользователя, тем она качественнее и дороже.
- 2. За этими данными охотятся злоумышленники.** Они могут использовать их для того, чтобы как можно больше узнать о жертве, выяснить, где человек работает, в каком банке у него открыт счет, как его зовут и так далее.
- 3. Соцсети собирают информацию буквально о каждой твоей активности.** Под какими постами ты ставишь лайки, сколько времени ты читаешь новосты, какие заголовки тебе нравятся больше, с какими людьми ты дружишь и общаешься, какую музыку ты слушаешь, какие видео тебе нравятся. У соцсетей есть информация даже о том, что ты пишешь и какие фото отправляешь друзьям.



**Вся эта информация называется цифровым следом, который каждый из нас оставляет в сети.** В Интернете, как и в реальной жизни, нужно быть очень внимательным со своими словами и действиями. Особенно осторожно следует относиться к публикуемому и пересылаемому личным фотографиям. Ни в коем случае никому не отправляй фотографии интимного характера! Из Интернета, как мы помним, ничего не удаляется. Всегда помни: чем меньше мы используем гаджеты - тем лучше!

**ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!**

## Помни!

Все, что попало в интернет, остается там навсегда



фотографии



личные  
контакты



семья  
и родители



дом  
и покупки



школа  
и отпуск



комментарии

Фотографии, которые ты выложил вчера, смогут увидеть послезавтра и позже

одноклассники

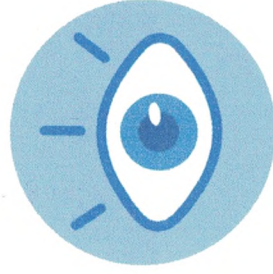
родители

соседи

учителя

преподаватели ВУЗА

твои дети



Действуй сегодня так, чтобы завтра не было стыдно!

В Интернете есть много интересного, веселого и познавательного контента. Но необходимо подвергать сомнению все, что мы читаем и смотрим в Интернете. **Фейк – целенаправленно распространяемая ложная информация**, которую специально создают, чтобы запутать, ввести в заблуждение или посеять панику среди людей.

**1. Оригинал всегда лучше любого пересказа.** Очень важно искать оригинальный источник новости. Подумай, можешь ли ты доверять этому источнику? Если это «желтое СМИ» или сайт, специально собирающий громкие заголовки, то доверять такому источнику нельзя!

**2. Обрати внимание на текст.** У реальной новости всегда много свидетелей и участников, которые рассказывают о событиях своими словами. По этой причине разные СМИ напишут про одну и ту же новость по-разному. Фейки – наоборот, не отличаются разнообразием. Фейковые новости, даже опубликованные на разных сайтах, мало отличаются друг от друга, а иногда и вовсе могут быть написаны «под копирку». Фейк придуман одним источником, откуда его скопировали другие сайты.

**3. Настоящая новость никогда не пройдет мимо популярных, известных и авторитетных СМИ.** Крупные газеты, сайты и телеканалы беспокоятся о своей репутации, поэтому тщательно проверяют любую информацию. Фейки распространяют небольшие издания, которые могут не проверить информацию, а иногда и заведомо опубликовать ложные сведения.

**4. Проверь факты и цитаты из новости.** Не важно, кому принадлежит цитата, насколько это уважаемый и популярный человек. Недобросовестные СМИ могут подделывать или вырывать из контекста любые слова для создания фейковой новости.

**5. Обращай внимание на основную суть новости, а не на мелкие детали в ней.** Обычно в фейках указывают очень много подробностей, которые создают иллюзию правдоподобности отвлекают внимание от основного смысла.

**ЕСЛИ ТЫ НАШЕЛ ИЛИ ПОЛУЧИЛ НЕДОСТОВЕРНУЮ ИНФОРМАЦИЮ, НЕ ПЕРЕСЫЛАЙ ЕЕ ДРУЗЬЯМ И РОДНЫМ! СНАЧАЛА ДОЖДИСЬ ОФИЦИАЛЬНОГО ОПРОВЕРЖЕНИЯ ИЛИ ПОДТВЕРЖДЕНИЯ.**



- 1. Сокращай время пользования Интернетом!** Для общения с друзьями и развлечения нужно не так много времени. Вовсе не обязательно торчать в соцсетях весь день.
- 2. Анонимность в сети – МИФ. Все, что мы выкладываем в Интернете, остается там навсегда.**
- 3. Проводи больше времени в реальной жизни.** Общайся с друзьями, родителями, читай, занимайся спортом и хобби.
- 4. Будь бдителен!** В Интернете много мошенников и преступников, которые охотятся за твоими деньгами или данными.
- 5. Не выкладывай свои персональные данные в Интернет.** Помни, что отправлять их не стоит даже друзьям.
- 6. Закрой свои страницы в соцсетях от посторонних.** Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и прекрати общение.
- 7. Не бойся рассказать родителям о своих проблемах.** Если кто-то решит тебя обижать, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.
- 8. Помни, что из Интернета ничего не удаляется.** Если ты не хочешь, чтобы твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.
- 9. Не верь всему, что написано в Интернете.** В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.
- 10. Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни.** Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

# КИБЕРУГРОЗЫ: ЗНАНИЕ О ФАКТОРАХ ОПАСНОСТИ – ВАША БЕЗОПАСНОСТЬ!

## Ключ в виртуальный мир

Современный смартфон – полноценный персональный компьютер. Он обладает всеми теми же функциями, что и домашний компьютер или ноутбук, а в чем-то даже их превосходит. В отличие от домашнего компьютера смартфон имеет постоянный доступ в Интернет, он работает 24 часа в сутки, имеет продвинутую камеру и микрофон, а также датчики движений, что позволяет ему круглосуточно записывать всю информацию о своем пользователе. Так, смартфон является нашим ключом в виртуальную реальность.



## Ключевой вопрос

Как сделать свой смартфон безопасным?

# Источники проблемы

- **Огромное количество навязчивой рекламы** – сайты, приложения, соцсети и игры – все это содержит огромное количество рекламы, на которой зарабатывают их разработчики. По данным Всероссийского центра изучения общественного мнения 29% россиян получают спам ежедневно.
- **Информационный шум** – в цифровом мире множество неконтролируемых уведомлений, которые приходят на телефон практически ежеминутно. Большинство пользователей не хотят тратить время на их отключение и удаление. А они содержат часто совсем ненужные рекламные предложения, приманки и являются способом вымогательства денег пользователя.
- **Установка нежелательного и вредоносного программного обеспечения** – при переходе по новой ссылке, скачивании файлов, установке приложений (даже из проверенных источников!) существует вероятность установки вирусов, шпионских или рекламных программ. Опасность могут представлять даже приложения, скачанные из официальных магазинов смартфонов. По данным ВЦИОМ, лишь 16% родителей устанавливают на устройство их ребенка антивирус.
- **Утечка персональных данных владельца** – все, что содержится в смартфоне, начиная от логинов и паролей, заканчивая фотографиями, банковскими реквизитами и даже перепиской, может не только попасть в руки к мошенникам, но и стать достоянием общественности.

## Внимание!

Чем активнее используется устройство, тем больше данных о своем владельце оно накапливает. К таким данным относятся не только ваши фото, видео, переписки, но и такие данные, как:

- история установки и использования приложений;
- история энергопотребления, то есть циклов и времени зарядки, интенсивности работы;
- история уведомлений и действий;
- история магазина приложений;
- история браузера;
- история перемещений по городу и многое другое.

## Надо знать!

**Вредоносные приложения на смартфонах пытаются заработать на пользователе – вытянуть деньги, внимание пользователя, показывая ему рекламу или перенаправляя на сайты, украсть персональные данные или профиль пользователя, передать мошенникам доступ к самому устройству.**

**Вредоносные приложения бывают разными:**

- **Фальшивые приложения** – копия настоящих приложений, как правило, банковских или приложений мобильных операторов. Их задача – полностью замаскировавшись под настоящее приложение, украсть у пользователя данные от личного кабинета и получить доступ к мобильному или банковскому счету.
- **Приложения-вымогатели** – блокируют устройство и требуют перечисление денег за разблокировку.
- **Денежные «пиявки»** – программы со скрытой подпиской. Однажды купив подобную программу или совершив покупку с её помощью, можно обнаружить, что она оформила «полноценную» подписку и деньги теперь списываются регулярно. Как правило, всегда можно отказаться от «денежной пиявки» и отменить такую подписку. Следите за своими расходами в сети.

## Информация к размышлению

**Вредоносные программы можно разделить на две большие категории:**

- **Вирусы** – вредоносные программы, которые напрямую вредят устройству, установленным программам. Распространяются по Интернету и заражают устройства.
- **Трояны** – маскируются под настоящие программы, а иногда даже могут выполнять некоторые полезные функции. Похищают данные пользователя, рассылают спам, создают трафик на сайты.

## Как вирусы попадают на устройство?

- **Из зараженного электронного письма** или файла, приложенного к письму – нельзя открывать письма, пришедшие из неизвестных источников, а особенно скачивать и запускать файлы, прикрепленные к этим письмам. Вирусы могут распространяться даже через текстовые файлы, например в формате .pdf.
- **Через зараженный сайт** – многие сайты способны самостоятельно устанавливать на компьютеры вирусы. Для этого бывает достаточно просто открыть страницу. Это особенно актуально для нелегальных сайтов, например, с пиратским контентом.
- **Через установку неизвестных приложений** с неизвестного сайта – если вы скачиваете что-либо из Интернета, убедитесь, что источник надежен. Программы лучше скачивать с официальных сайтов разработчиков этих программ.

## Как защитить себя от киберугроз:

- Не открывайте письма и сообщения от незнакомых отправителей;
- Не скачивайте пиратский контент;
- Внимательно проверяйте адреса веб-сайтов, которые вы посещаете;
- Не устанавливайте на телефон или компьютер, приложение из непроверенного источника;
- Не давайте приложениям разрешения, которые не нужны им для работы – приложению «калькулятор» не нужен доступ к микрофону смартфона;
- Следите за своими расходами в сети и за тем, какие подписки оформляют приложения;
- В настройках телефона отключите уведомления от приложений, которые вы не хотите получать;
- Установите на компьютер и телефон антивирус;
- Храните на телефоне как можно меньше информации о себе. Так вы защититесь от утечки данных;
- Подключите на телефоне функцию защиты от спама. На некоторых устройствах она доступна в настройках или ее можно подключить у мобильного оператора.

## Личный пример

**Не открывайте MMS и сообщения, присланные с незнакомых номеров!**



**НАЦИОНАЛЬНЫЙ  
ЦЕНТР ПОМОЩИ**  
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ  
НАЙТИРЕБЕНКА.РФ



**лига  
безопасного  
интернета**



**Сайт**  
**ligainternet.ru**

