



ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

КОМИТЕТ ПО ОБРАЗОВАНИЮ

пер. Антоненко, дом 8, Санкт-Петербург, 190031

Тел.(812) 417-34-54, Факс (812) 417-34-56

E-mail: kobr@gov.spb.ru

www.k-obr.spb.ru

Комитет по образованию

№ 03-16-470/19-0-1

от 02.12.2019



**Заместителям глав
администратий районов
Санкт-Петербурга,
курирующим вопросы
образования**

**О направлении методических
материалов**

Уважаемые руководители!

Информируем Вас, что Управлением Роскомнадзора по Северо-Западному федеральному округу подготовлены информационно-методические материалы для несовершеннолетних по вопросам кибербезопасности в сети «Интернет»:

- памятка по кибербезопасности;
- правила поведения в сети Интернет;
- презентация по кибербезопасности.

Просим Вас рассмотреть возможность использования указанных методических материалов в подведомственных общеобразовательных организациях при проведении мероприятий по обеспечению информационной безопасности детей и подростков, а также разместить указанные материалы на сайтах органов управления образованием и образовательных организаций Санкт-Петербурга.

Приложение: на 24 л. в 1 экз.

**С уважением,
заместитель председателя Комитета**

А.А. Борщевский

Горина М.А.,
(812) 576-18-27



РОСКОМНАДЗОР

**РОЛЬ И МЕСТО ЗАЩИТЫ ПРАВ СУБЪЕКТОВ
ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЕСПЕЧЕНИИ
КИБЕРБЕЗОПАСНОСТИ**

КИБЕРУГРОЗЫ В СЕТИ ИНТЕРНЕТ

- ✓ МОШЕННИЧЕСТВО
- ✓ СЛЕЖКА
- ✓ КИБЕРБУЛЛИНГ,
ТРОЛЛИНГ
- ✓ ШАНТАЖ
- ✓ ВЫМОГАТЕЛЬСТВО
- ✓ АГРЕССИВНЫЙ МАРКЕТИНГ



ИСТОЧНИКИ КИБЕРУГРОЗ

- ПРАКТИКА ПРИНЯТИЯ условий пользовательского соглашения по умолчанию
- ХИЩЕНИЕ ПД
- ИСПОЛЬЗОВАНИЕ «серых» мобильных приложений
- ФИШИНГ
- ПОВСЕМЕСТНОЕ ИСПОЛЬЗОВАНИЕ видеонаблюдения
- ПРОСКОМНАДЗОР
- ПЕРЕДАЧА ПД по незащищенным каналам связи
- ИСПОЛЬЗОВАНИЕ геолокационных сервисов
- РАСПРОСТРАНЕНИЕ ПД в открытых источниках
- ОБЩЕНИЕ с виртуальными друзьями

ПОСЛЕДСТВИЯ КИБЕРУГРОЗ



- ПРИСВОЕНИЕ ЛИЧНОГО ИМУЩЕСТВА ГРАЖДАН ОБМАННЫМ ПУТЁМ

- Принуждение к выполнению воли третьих лиц

- Вред психическому, нравственному и духовному здоровью граждан

- Монетизация пользователя сети Интернет, т.е. пользователь становится товаром

- Нарушение права на личную жизнь

Манипулирование субъектом персональных данных



ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1 КОНВЕНЦИЯ СОВЕТА ЕВРОПЫ

О защите физических лиц при автоматизированной обработке персональных данных ETS № 10

2 ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ

«О персональных данных»

3 ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ

«Об информации, информационных технологиях и о защите информации»

(в части порядка блокировки информации в сети Интернет)

4 ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

«О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»

РОСКОМНАДЗОР

НАРУШЕНИЯ ПОРЯДКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

- ☐ Нерегулируемый оборот информации, содержащей персональные данные
- ☐ Несоответствие обработки персональных данных декларируемым в пользовательских соглашениях Интернет-компаний целям обработки персональных данных
- ☐ Сбор и анализ персональной информации пользователей, в том числе, персонифицированной заинтересованности пользователя к определенным товарам
- ☐ Использование персональных данных пользователя сети Интернет с целью продвижения товаров, работ, услуг на рынке
- ☐ Создание фальшивых аккаунтов в социальных сетях
- ☐ Использование персональных данных в коммерческих целях
- ☐ Общедоступность личной информации

ПОЛНОМОЧИЯ РОСКОМНАДЗОРА ПО КОНТРОЛЮ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

АИС «Реестр нарушителей прав субъектов персональных данных»

ЦЕЛЬ:

**ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ С НАРУШЕНИЕМ
ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**



НАЛИЧИЕ СИСТЕМЫ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ СПОСОБСТВУЕТ

Достижению БАЛАНСА интересов

Личности, общества и государства

СОХРАНЕНИЮ

**неприкосновенности частной
жизни**

Сохранению

психологического

Здоровья граждан

РОСКОМНАДЗОР

**Информационная памятка для несовершеннолетних по вопросам
кибербезопасности
в сети «Интернет»**

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоём персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефiatные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StRong!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Веди себя вежливо;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
7. Периодически проверяй какие платные услуги активированы на твоём номере;

8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Фишинг или кража личных данных

Главная цель фишинг - вида Интернет-мошенничества, состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получают доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Правила безопасного
поведения
в сети Интернет





my name

КАК ТЕБЯ ЗОВУТ?

10.5

СКОЛЬКО ТЕБЕ ЛЕТ?



КАКОГО ЧИСЛА У ТЕБЯ
ДЕНЬ РОЖДЕНИЯ?

КАКОМУ ТЕБЯ НОМЕР
ТЕЛЕФОНА?

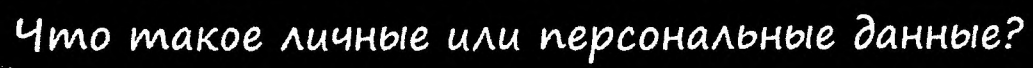


В КАКОМ КЛАССЕ И КАКОЙ
ШКОЛЕ ТЫ УЧИШЬСЯ?



ГДЕ ТЫ ЖИВЕШЬ?







Какую информацию мы чаще всего размещаем о себе?

ФОТОГРАФИИ,
ИМЯ И ВОЗРАСТ

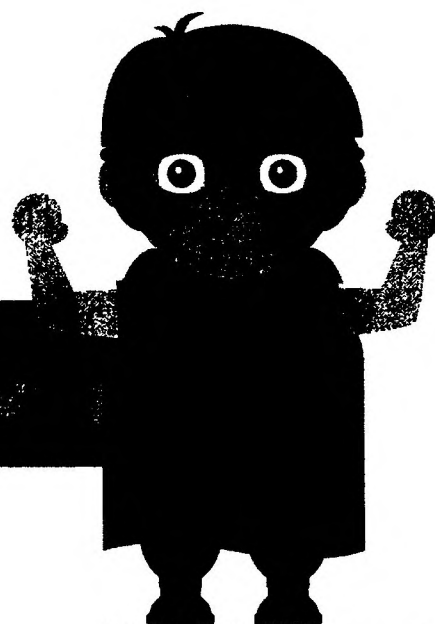


НОМЕР
БАНКОВСКОЙ
КАРТЫ

ГДЕ ЖИВЕМ, В КАКОМ
КЛАССЕ И ШКОЛЕ
УЧИМСЯ

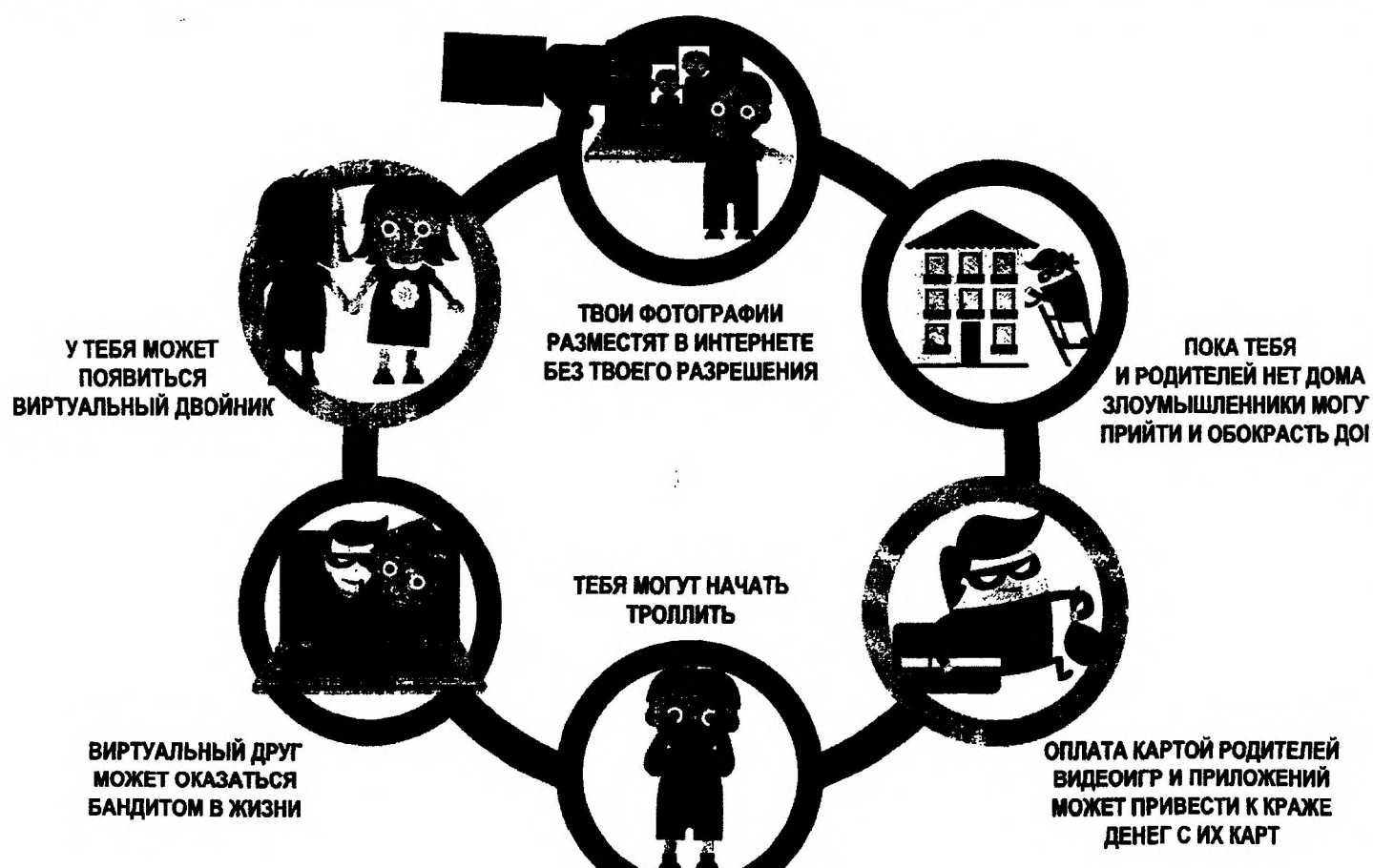


КУДА И КОГДА
ИЗЖАЕМ ОТДЫХАТЬ





Какие угрозы влечет беспечное отношение к личным данным?





Правила защиты персональных данных

Используй
вместо имени
ник, картинку
вместо фото и
устойчивые пароли



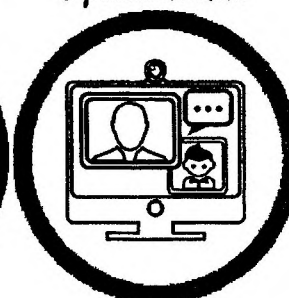
Не указывай
в Сети,
где ты живешь и



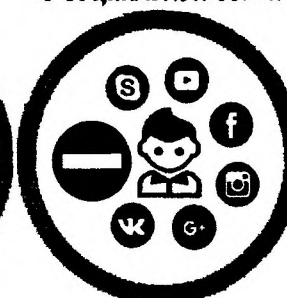
Не оставляй
личную
информацию о себе
в социальных сетях



Если тебе предлагает
встретиться
виртуальный друг –
посоветуйся
с родителями



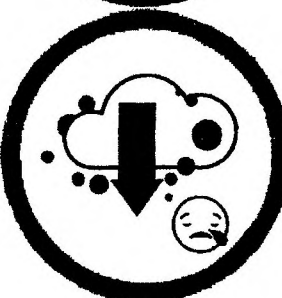
Ограничь доступ
к своему профилю
в социальной сети



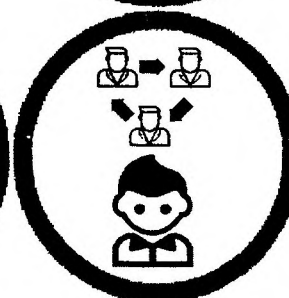
Не отправляй смс на
короткие номера, не
сообщай номера
банковских карт,
своей или родителей



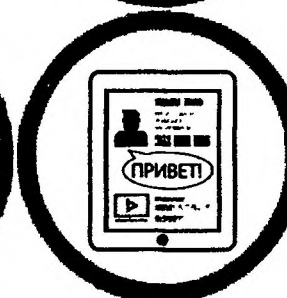
Не ставь
геолокацию
под своими
постами



Не скачивай
приложения
с непроверенных
сайтов, установи
антивирус



Не рассказывай,
когда
и куда едешь
с родителями
отдыхать



Не знакомься
в интернете



ЧТО ДЕЛАТЬ, ЕСЛИ ТЕБЯ ОБИЖАЮТ В СЕТИ?



ТРОЛЛИНГ – вид хулиганства в сети, форма провокации или издевательства. Троль питается негативными эмоциями, он задает обидные вопросы, может оскорблять, издеваться, высмеивать внешний вид, рост, вес, писать обидные слова про родных и друзей

Если тебя обижают в сети, то помни **ГЛАВНОЕ ПРАВИЛО – НЕ КОРМИ ТРОЛЯ**

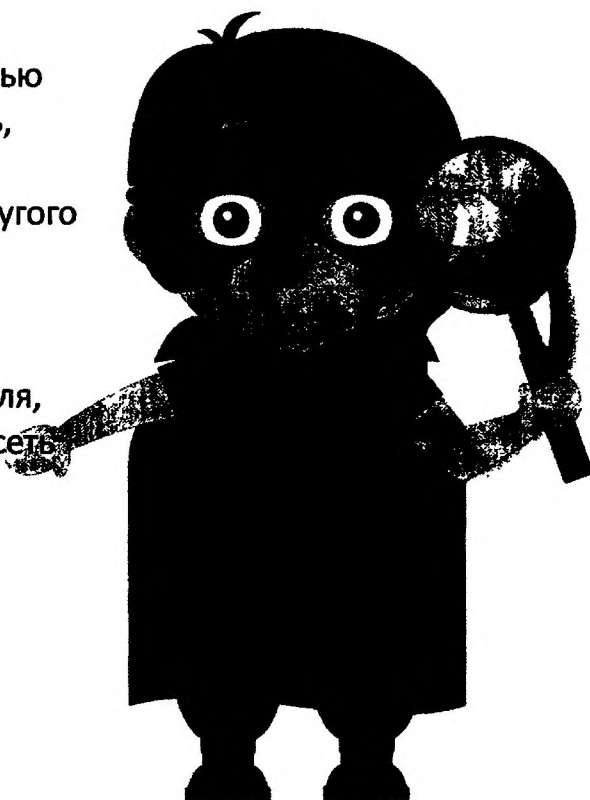
Как только перестанешь реагировать на него, он очень быстро потеряет интерес. Можешь пожаловаться на него или сообщить о троллинге администратору сайта



Что такое кибербуллинг?

КИБЕРБУЛЛИНГ – это использование современных технологий с целью обидеть, унижить, запугать или преследовать другого человека

Говоря простым языком, это травля, перенесенная в сеть Интернет



- Никогда не принимай сам участие в интернет-травле кого-либо
- Установи настройки приватности, чтобы незнакомые люди не могли писать тебе или оставлять комментарии под твоими фото
- Никогда не отвечай на буллинг
- Делай скриншоты всех сообщений и сообщи о травле администратору ресурса – зачинщика травли заблокируют
- Добавь его в черный список
- Поговори о проблеме с кем-нибудь из взрослых, лучше с родителями – они поддержат и помогут собрать доказательства и найти выход из сложившейся ситуации



ЧТО ТЫ ЗНАЕШЬ О ЗАЩИТЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ?



ПЕРСОНАЛЬНЫЕ ДАННЫЕ

