БЕЗОПАСНОЕ ПОВЕДЕНИЕ

В СЕТИ ИНТЕРНЕТ

Молодёжь

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

Это отрасль компьютерной безопасности, связанная специальным образом не только с Интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом

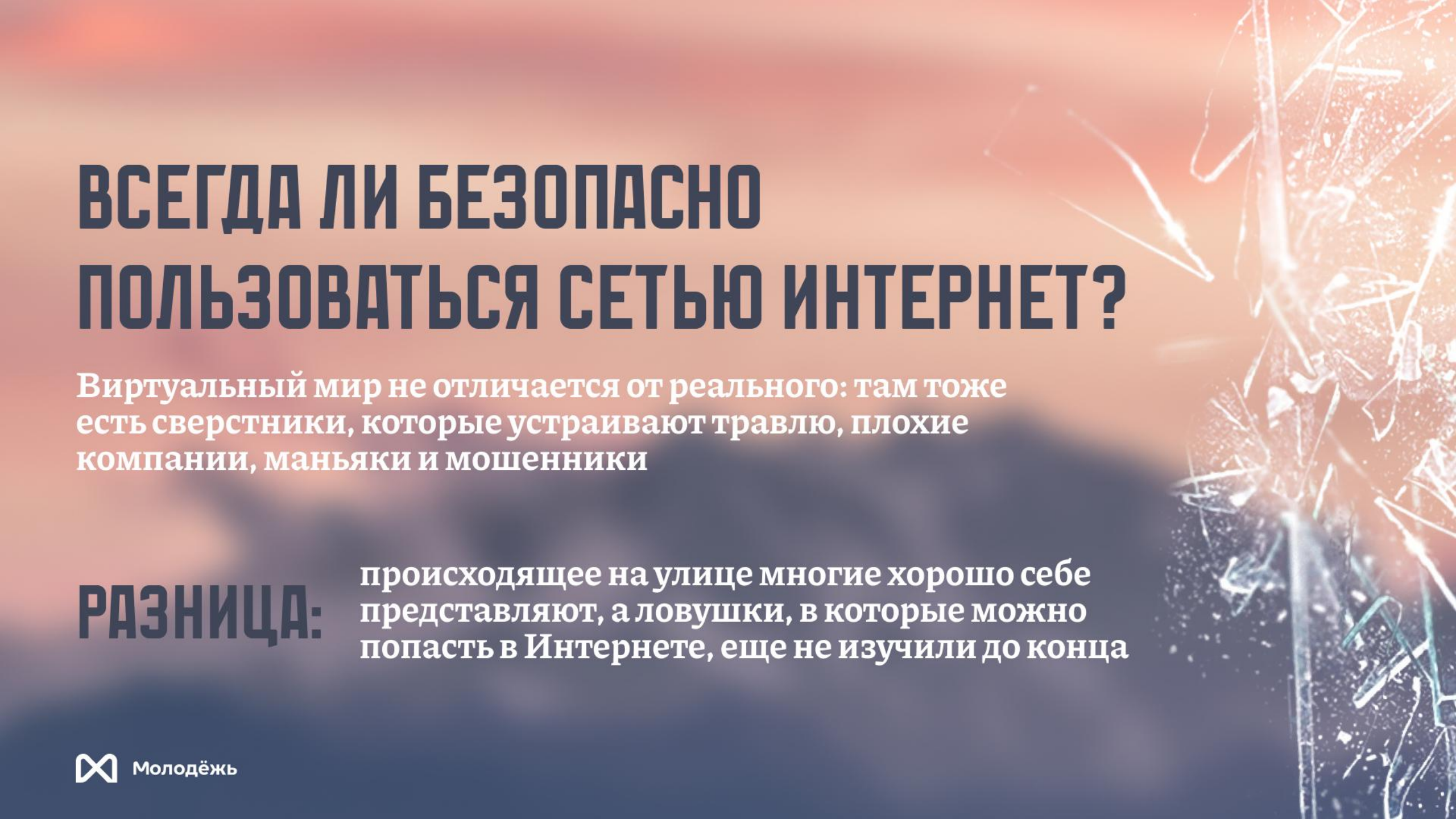
ЦЕЛЬ: **Установить правила и принять меры для предотвращения атак через Интернет**

Молодёжь

ВСЕГДА ЛИ БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СЕТЬЮ ИНТЕРНЕТ?

Виртуальный мир не отличается от реального: там тоже есть сверстники, которые устраивают травлю, плохие компании, маньяки и мошенники

РАЗНИЦА: происходящее на улице многие хорошо себе представляют, а ловушки, в которые можно попасть в Интернете, еще не изучили до конца



Молодёжь

1. ХРАНИТЕ ТАЙНЫ

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. И только в том случае, если соединение устанавливается по протоколу https.
Слева от адреса сайта должен появиться значок в виде зеленого замка – это означает, что соединение защищено

Важно помнить, что ни в коем случае нельзя передавать через Сеть данные любых документов и банковских карт.

Тем более если кто-то об этом просит, старается убедить в том, что возникла критическая ситуация, торопит и повторяет, что нужно срочно прислать информацию

Молодёжь

2. БУДЬТЕ АНОНИМНЫ

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним

Не стоит ставить свою фотографию на аватар, если вам не исполнилось хотя бы 15-16 лет

Молодёжь

3. НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЦАМИ

**Несколько главных опасностей,
с которыми можно столкнуться в Интернете:**

1. **Буллинг.** Вас могут начать обзывать или травить в интернете – чаще всего без какой-либо причины, "потому что так захотелось". К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях
2. **Педофилы.** Просят прислать личные фотографии, а при отказе угрожают расправой над членами семьи или шантажируют другими способами
3. **Мошенники.** Пытаются завладеть данными пользователя или втянуть Вас в опасную финансовую авантюру

Главное средство защиты от всех этих угроз – конфиденциальность!

Молодёжь

4. РАСПОЗНАЙТЕ ЗЛОУМЫШЛЕННИКА

На что надо обратить внимание прежде, чем вступить в диалог?

- **Вы не знакомы с этим человеком в реальной жизни**
- **Ваш собеседник явно взрослее вас**
- **У него нет или очень мало друзей в соцсети**
- **Собеседник о чем-то просит: сфотографироваться, прислать какие-то данные и прочее**

Молодёжь

5. НЕ СООБЩАЙТЕ СВОЕ МЕСТОПОЛОЖЕНИЕ

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Отследить местоположение человека теперь не составляет труда

Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на "искабельных" объектах – особенно на фотографиях

Молодёжь

6. ВНИМАНИЕ — НА ИГРЫ

В онлайн-играх человек более уязвим, поскольку им проще манипулировать:

игровые объекты, членство в командах, внутриигровые социальные связи – все это может стать механизмом манипуляции для мошенников, педофилов или даже вербовщиков различных экстремистских группировок

Молодёжь

7. УЧИТЕСЬ ЗАМЕЧАТЬ ПОДДЕЛЬНЫЕ САЙТЫ

Фишинг – это способ выманивать у человека его данные: логин, название учетной записи и пароль

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети

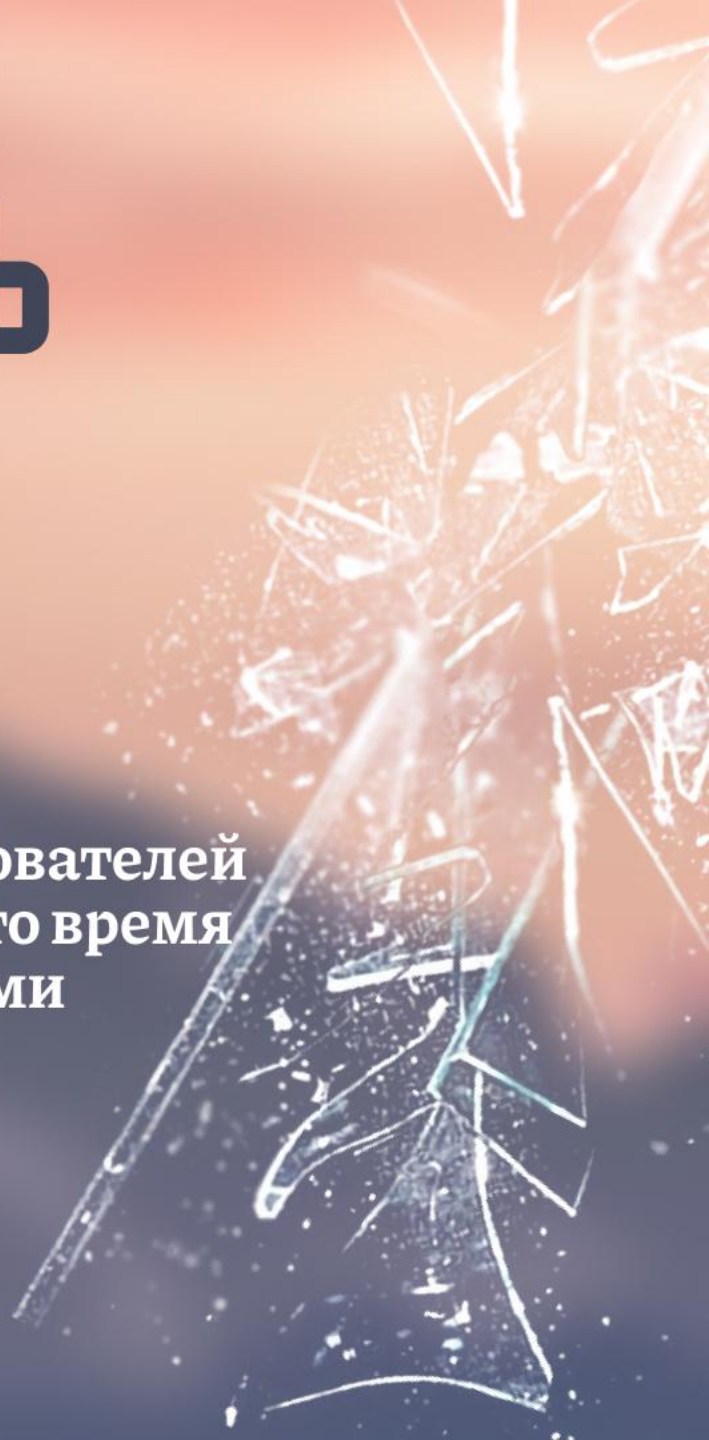
Например, для mail.ru это может быть "meil.ru", а для vk.com — "vk-com.com"

Молодёжь

8. ТРЕНИРУЙТЕ ПАМЯТЬ

Почему не следует пользоваться сервисами, которые сохраняют пароли?

- Онлайн-сервисы для хранения паролей ненадежны
- Их часто взламывают и копируют оттуда пароли пользователей
- Чаще всего жертвы узнают об этом лишь спустя какое-то время
- Нередко такие сайты и сервисы создаются мошенниками специально для того, чтобы собирать пароли



9. АККУРАТНЕЕ С ПОКУПКАМИ

Основные финансовые потери обычно происходят через телефон. Необходимо подключить услуги блокировки платного контента, не класть много денег на счет телефона и контролировать расходы

Все сервисы, которые принимают деньги, должны иметь зеленый значок "https" рядом с названием. Если такого значка нет, лучше не пользоваться страницей

Молодёжь

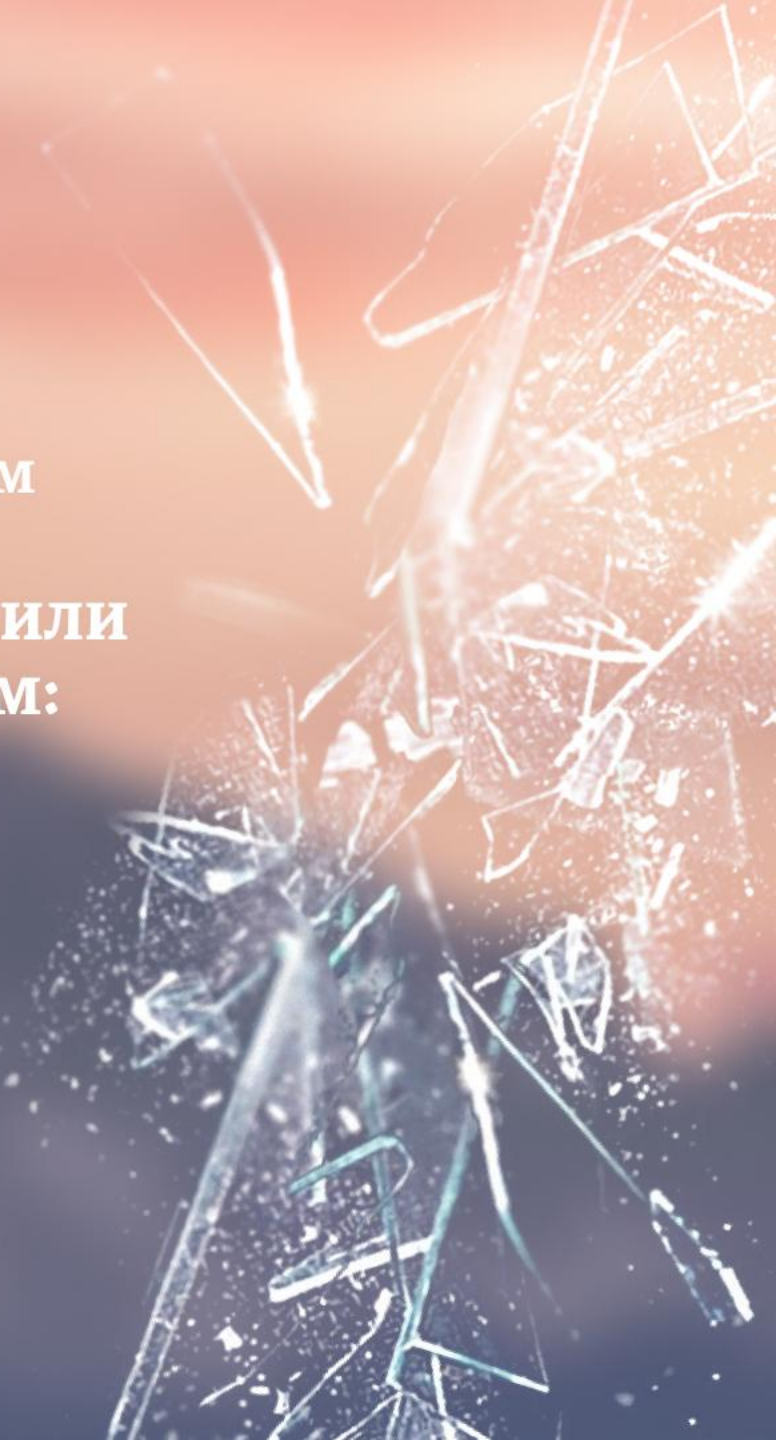
10. ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

Проверка информации – довольно сложный процесс, и даже взрослые люди далеко не всегда справляются с этим

Чтобы проверить информацию, которую вы получили в Интернете, следуйте следующим рекомендациям:

- **поищите еще два-три источника**
- **найдите первоисточник и задайте себе вопрос: "Можно ли ему доверять?"**
- **проверьте, есть ли в Сети другие мнения и факты, которые опровергают или подтверждают сказанное**

Если нужно узнать какой-то факт или выяснить, что значит непонятный термин, можно обратиться к "Рувики"



11. СОБЛЮДАЙТЕ СЕТЕВОЙ ЭТИКЕТ

Не оскорбляйте других, не будьте навязчивым, не позволяйте своим негативным эмоциям выходить из-под контроля, пишите грамотно

Как и в жизни, в Сети нам приходится бывать в разных сообществах, и правила общения могут различаться. Вежливый человек, попав в незнакомое общество, прежде всего попытается узнать его особенности

Существуют правила, актуальные для любых сообществ:

- **не привлекайте к себе внимание за счет эпатажа**
- **не отходите от темы разговора**
- **не игнорируйте вопросы собеседника, кроме явного троллинга или оскорблений**
- **никогда не участвуйте в травле**

Молодёжь

12. ГЛАВНЫЙ СЕКРЕТ БЕЗОПАСНОСТИ В СЕТИ

**Не нужно делать в Интернете ничего,
что бы вы не стали делать в физическом мире.**

Примеры, иллюстрирующие этот подход:

1. Личная информация
2. Коммуникации

Молодёжь

КИБЕРБУЛЛИНГ

Кибербуллинг – это форма травли, которая происходит через Интернет и цифровые устройства

Основные виды кибербуллинга:

1. Оскорбление
2. Троллинг
3. Шантаж
4. Изоляция
5. Фейковые аккаунты
6. Хейтинг
7. Публикация личных данных

Молодёжь

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРБУЛЛИНГ

Для несовершеннолетних правонарушителей, существует гражданско-правовая, административная и уголовная ответственность. За несовершеннолетних нарушителей в возрасте до 14 лет ответственность несут их родители и законные представители

В качестве ответственности за оскорбление, которое было размещено в социальной сети, зарегистрированной в качестве средства массовой информации, предусмотрен штраф – от 5 до 10 тыс. руб.

Молодёжь

ОТВЕТСТВЕННОСТЬ ЗА КИБЕРБУЛЛИНГ

Уголовная ответственность за "кибербуллинг" предусмотрена, в частности, ст. 110.1 Уголовного кодекса Российской Федерации (УК РФ) за склонение к совершению самоубийства или содействие совершению самоубийства.

А самое суровое наказание в соответствии со ст. 110 УК РФ установлено за доведение лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего. Такое деяние, если совершено в отношении несовершеннолетнего, или в информационно-телекоммуникационных сетях, включая сеть "Интернет", наказывается лишением свободы на срок от 8 до 15 лет

Уголовная ответственность за данные деяния наступает с 16 лет !

Молодёжь

КАК БОРОТЬСЯ С КИБЕРБУЛЛИНГОМ?

1. Игнорирование агрессора
2. Блокировка и жалобы
3. Сбор доказательств
4. Обращение за поддержкой
5. Психологическая помощь

Если вы не справляетесь с кибербуллингом самостоятельно, обязательно расскажите об этом кому-то из близких, кому доверяете, или обратитесь за помощью к психологу/педагогу в школе, учителю

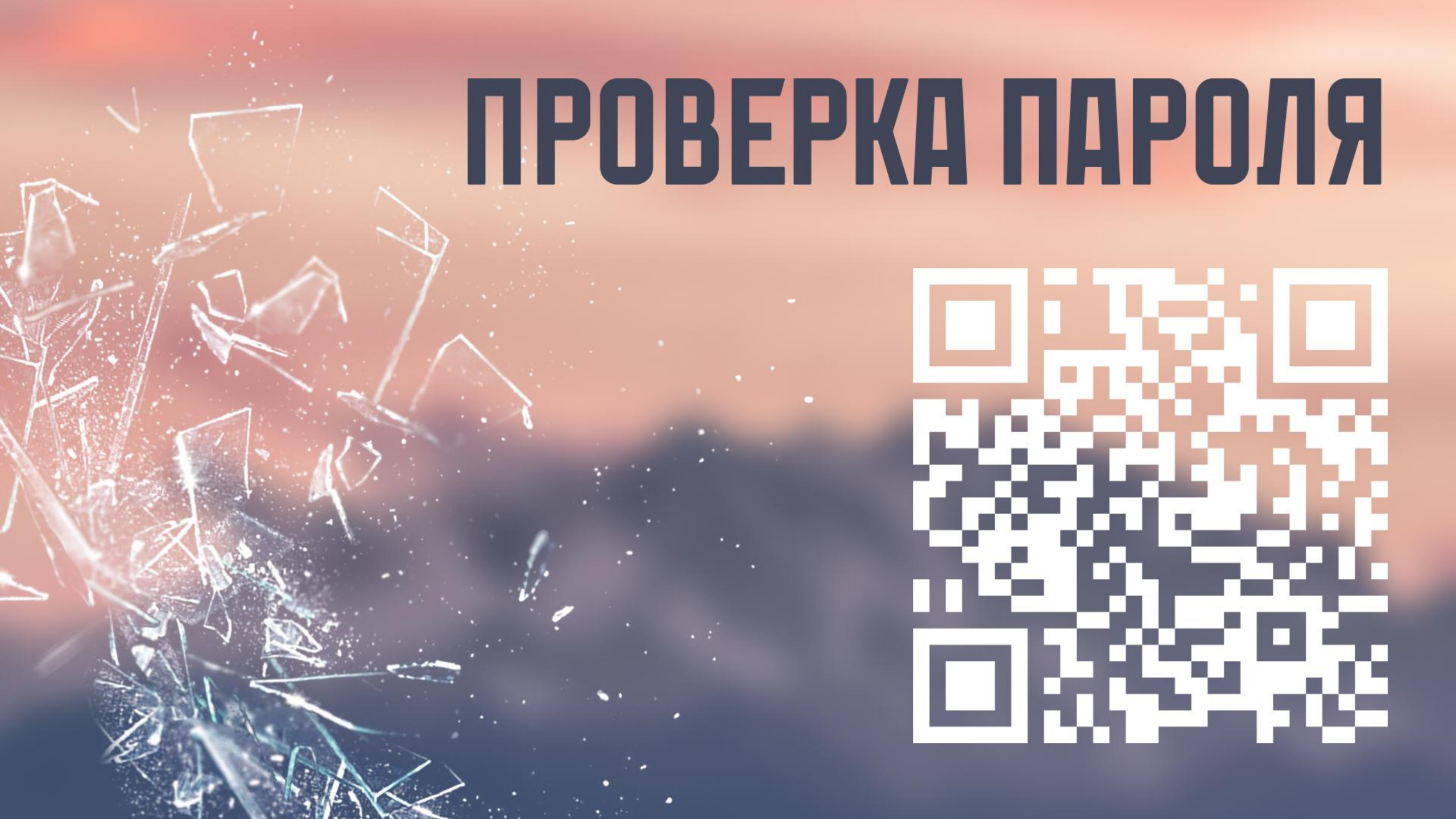
Также вы можете обратиться на бесплатный и анонимный Единый Общероссийский телефон доверия для детей, подростков и их родителей по телефону: 8 (800) 2000-122

Если травля переходит границы, угрожает вашей репутации, психическому состоянию или жизни, обратитесь в полицию

БЕЗОПАСНОЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ

Тест по безопасному поведению в сети Интернет

Молодёжь


ПРОВЕРКА ПАРОЛЯ

Надежный пароль должен соответствовать нескольким критериям, чтобы эффективно защищать ваши личные данные

Рекомендации по созданию надежного пароля:

1. **Длина пароля**
2. **Разнообразие символов**
3. **Уникальность**
4. **Избегание очевидных вариантов**
5. **Отсутствие личной информации**
6. **Регулярные обновления**

ПРОВЕРКА БЕЗОПАСНОСТИ САЙТА

ПОМНИТЕ ПРО БЕЗОПАСНОСТЬ!

Интернет – это мощный инструмент, который открывает перед нами огромные возможности, но требует ответственного подхода. Применяя на практике те знания, которые мы получили сегодня, вы сможете чувствовать себя уверенно и безопасно в цифровой среде

Молодёжь