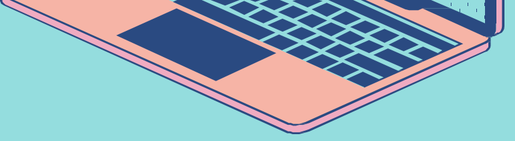
Информационная памятка для несовершеннолетних по вопросам кибербезопасности в сети «Интернет»



Компьютерный вирус

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию).

Какие методы защиты от вредоносных программ мы знаем?

Существуют компьютерные вирусы.
От них есть лекарства – антивирусы.

Попроси родителей установить антивирус на твой компьютер.

Какие методы защиты от вредоносных программ мы знаем?

Используй современные операционные системы

Постоянно устанавливай патчи

Работай на своем компьютере под правами пользователя

Используй антивирусные программные

Ограничь доступ к компьютеру для посторонних лиц

Используй внешние носители информации

Не открывай файлы из ненадёжных источников

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

Не передавай свою личную информацию через общедоступные Wi-Fi сети

При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам»

В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически»

Используй и обновляй антивирусные программы и брандмауэр

Не используй публичный WI-FI для передачи личных данных

Используй только защищенное соединение при наборе веб-адреса вводи именно «https://»

Социальная сеть

Социальные сети объединяют людей из разных уголков планеты.

Рассказывай родителям о своих друзьях в сети.

Основные советы по безопасности в социальных сетях:

Ограничь список друзей

Защищай свою частную жизнь.

Защищай свою репутацию

Не используй свою личную информации

Отключай местоположение фотографий в соц. сетях

Используй сложные пароли

Используй разные пароли для аккаунтов

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.

Основные советы по безопасной работе с электронными деньгами:

Привяжи к счету мобильный телефон.

Используй одноразовые пароли.

Не вводи свои личные данные на сайтах, которым не доверяешь

Выбери сложный пароль.

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.

Основные советы по безопасной работе с электронной почтой

Надо выбрать правильный почтовый сервис.

Не указывай в личной почте личную информацию.

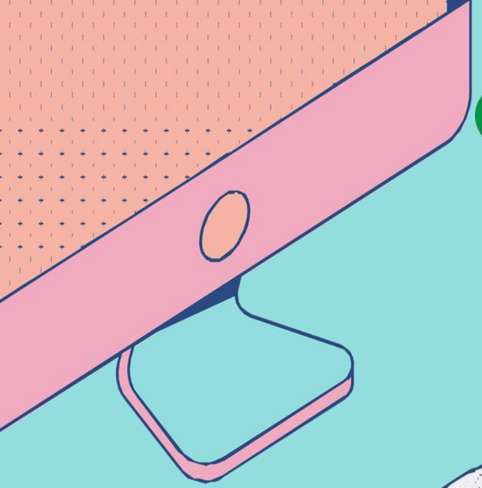
Используй двухэтапную авторизацию.

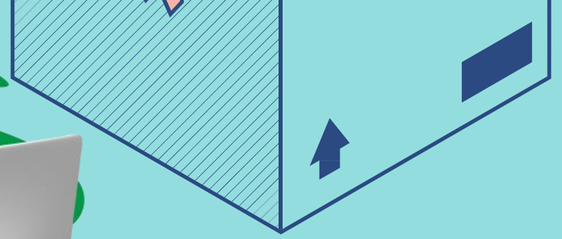
Выбери сложный пароль.

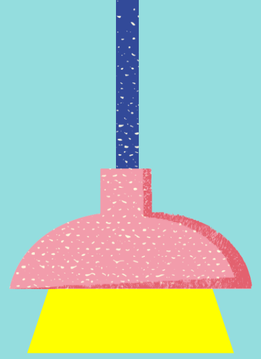
Используй несколько почтовых ящиков.

Не открывай сомнительные файлы

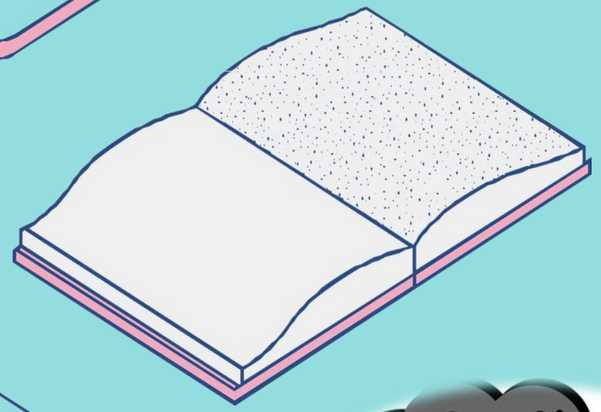
После окончания работы не забудьте **ВЫЙТИ** с почтового сервиса

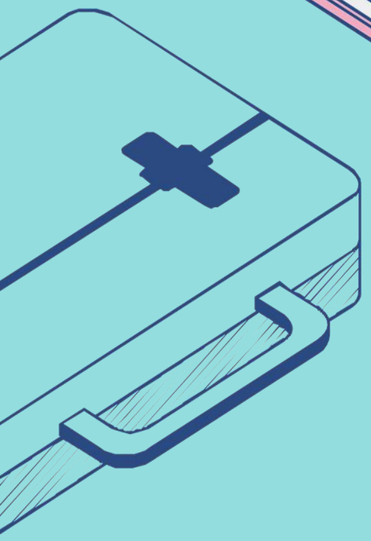






Кибербуллинг или виртуальное издевательство





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

Основные советы по борьбе с кибербуллингом:

Не бросайся в бой.

Управляй своей киберрепутацией

Анонимность в сети мнимая.

Если ты свидетель кибербуллинга.

Не стоит вести хулиганский образ виртуальной жизни.

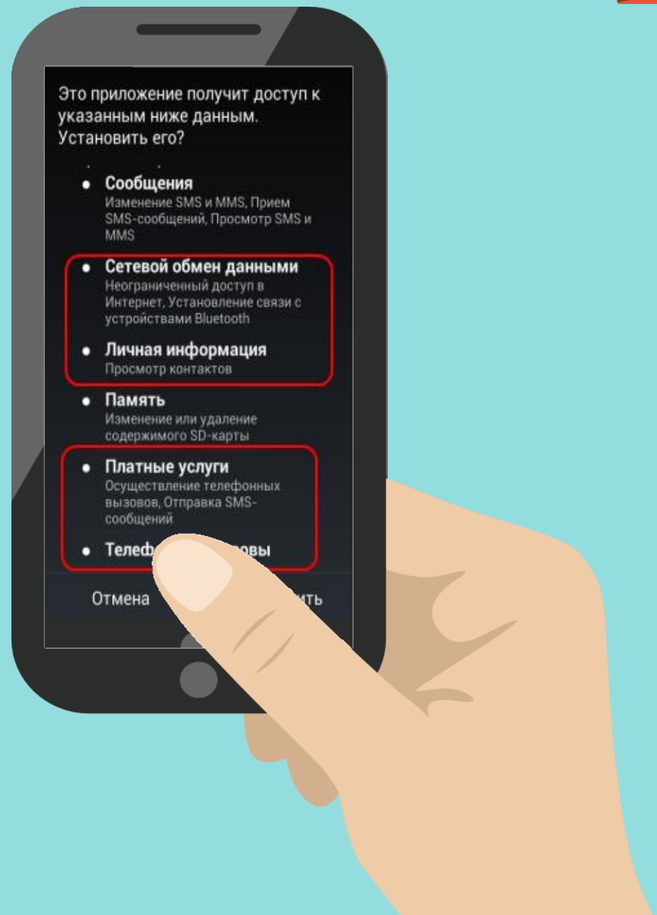
Веди себя вежливо.

Игнорируй единичный негатив

Бан агрессора

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.



Основные советы для безопасности мобильного телефона:

Будь осторожен, когда тебе предлагают бесплатный контент

Используй антивирусные программы для мобильных

Регулярно проверяй активированные услуги

Думай, что отправляешь

Не загружай приложения от неизвестного источника

Давай номер мобильного телефона только проверенным людям

Обновлять операционную систему смартфона

Удали cookies

Bluetooth должен быть выключен, когда ты им не пользуешься

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 для безопасности мобильного телефона:

Следи за своим аккаунтом.

Используй безопасные веб-сайты

Используй сложные и разные пароли.

Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей

Если тебя взломали, то необходимо предупредить всех своих знакомых

Установи надежный пароль (PIN)

Отключи сохранение пароля в браузере

ЗАКРЕПИМ ПРОЙДЕНЫЙ МАТЕРИАЛ

1. *Какие методы защиты от вредоносных программ мы знаем?*
2. Какие советы по безопасности работы в общедоступных сетях Wi-fi мы знаем?
3. Какие советы по безопасности в социальных сетях мы знаем?
4. Что мы знаем о кибербулинге и как с ним справиться?
5. Что мы знаем о «Фишинге» и как защитить личные данные?

ВОЛОНТЕРЫ КИБЕРБЕЗОПАСНОСТИ

Наши контакты:

@volinfo_bezopasnosti

kibervol05@mail.ru

@sh.krumov

Руководитель проекта: Крумов Шевкет

Главный специалист-эксперт отдела по гражданско-патриотическому и духовно-нравственному воспитанию Министерства по делам молодежи Республики Дагестан