



МОБИЛЬНЫЙ ИНТЕРНЕТ И WI-FI

цифровой
диктант.рф



ПРИ ПОДДЕРЖКЕ
**ФОНДА
ПРЕЗИДЕНТСКИХ
ГРАНТОВ**

Проект реализован с использованием гранта
Президента Российской Федерации на развитие
гражданского общества, предоставленного Фондом
президентских грантов

МОБИЛЬНЫЙ ИНТЕРНЕТ И WI-FI

Трудно представить себе использование современного смартфона без подключения к интернету. На интернете завязано все – например, социальные сети и банковские приложения. Без интернета невозможно установить обновления на смартфон, узнать информацию о погоде за окном и послушать новый музыкальный альбом.

ИНТЕРНЕТ В СМАРТФОНЕ

Интернет в смартфоне нужен для выполнения большого количества функций, например:

- > Обновление операционной системы
- > Загрузка и обновление приложений
- > Интернет-серфинг
- > Использование приложений с функциями, требующими подключение к интернету
- > Онлайн-просмотр фотографий и видео
- > Прослушивание музыки
- > Общение в социальных сетях и мессенджерах
- > Онлайн-покупки, включая заказ еды и заказ такси



Основные два способа подключения смартфона к интернету – с использованием мобильной сети (мобильная передача данных) и через Wi-Fi-сети.



МОБИЛЬНАЯ ПЕРЕДАЧА ДАННЫХ



При использовании режима мобильной передачи данных смартфон будет получать интернет-трафик от мобильного оператора, чья SIM-карта в нем установлена. Стоимость мобильного интернета при этом будет тарифицироваться мобильным оператором, то есть использование мобильной передачи данных в большинстве случаев не является бесплатным.

С помощью мобильной передачи данных совершаются VoLTE-звонки. VoLTE – технология передачи голоса по сети LTE, она нужна для увеличения качества и четкости звучания передаваемого голоса. В России эта технология пока что недостаточно распространена, практически все крупные мобильные операторы поддерживают VoLTE-звонки только в Москве, и только один – в других городах.



Если на вашем смартфоне установлено несколько SIM-карт, вы можете выбрать ту, с помощью которой вы будете подключаться к интернету.

ПРЕИМУЩЕСТВА МОБИЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ:

-  Работает практически везде, где есть мобильная связь
-  При хорошем подключении работает быстрее, чем подключение по Wi-Fi

НЕДОСТАТКИ МОБИЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ:

- **Низкая скорость передачи данных в некоторых ситуациях.** Если в месте, где находится смартфон, нестабильное покрытие мобильной связи, интернет будет работать очень медленно.
- **Использование мобильного трафика – платная услуга.** Если на вашем мобильном тарифе, например, нет функции безлимитного интернета, то онлайн-просмотр кино может оказаться очень дорогим.
- **Возможен дорогой роуминг.** Если вы находитесь в другой стране, использовать мобильную передачу данных может быть дорого из-за роуминга – процедуры предоставления услуг абоненту вне зоны обслуживания «домашней» сети абонента с использованием ресурсов другой сети.
- **Ограничение размера приложений, которые можно скачать из официальных магазинов.** При использовании мобильного интернета вы не сможете скачать «тяжелые» приложения на смартфон из официальных магазинов. Например, в App Store существует ограничение в 200 мегабайт.
- **Большее энергопотребление** в сравнении с передачей данных по Wi-Fi-сети.

КАК СЭКОНОМИТЬ НА МОБИЛЬНОМ ТРАФИКЕ

Мобильный трафик – общее количество данных, которые загружаются на устройство или с его помощью передаются в интернет. Существуют несколько советов, воспользовавшись которыми можно снизить количество передаваемых данных. Это будет особенно актуально, если на вашей SIM-карте установлен тарифный план с дорогим мобильным интернетом.

→ ПРОВЕРЯЙТЕ РАСХОД МОБИЛЬНОГО ТРАФИКА

Если вы заметили подозрительную активность (например, большое количество трафика загружается ночью, когда вы спите), это может быть сигналом – ваш смартфон может быть заражен вирусом. Для экономии трафика вирус нужно будет найти и удалить.

→ ИСПОЛЬЗУЙТЕ РЕЖИМ ЭКОНОМИИ ТРАФИКА

Если данный режим включен, фоновая передача данных для большинства сервисов и приложений возможна только по Wi-Fi. При этом активные сервисы и приложения могут использовать мобильное подключение.

→ УСТАНОВИТЕ ЛИМИТ ИСПОЛЬЗУЕМОГО ТРАФИКА

Вы можете настроить предупреждение, которое будет появляться при достижении определенного объема мобильного трафика на устройстве.

→ ОТКЛЮЧАЙТЕ МОБИЛЬНЫЙ ИНТЕРНЕТ, КОГДА ВЫ ИМ НЕ ПОЛЬЗУЕТЕСЬ

Запретите приложениям скачивать и отправлять информацию через мобильную сеть.



→ ОТКЛЮЧИТЕ АВТОСИНХРОНИЗАЦИЮ ПРИЛОЖЕНИЙ

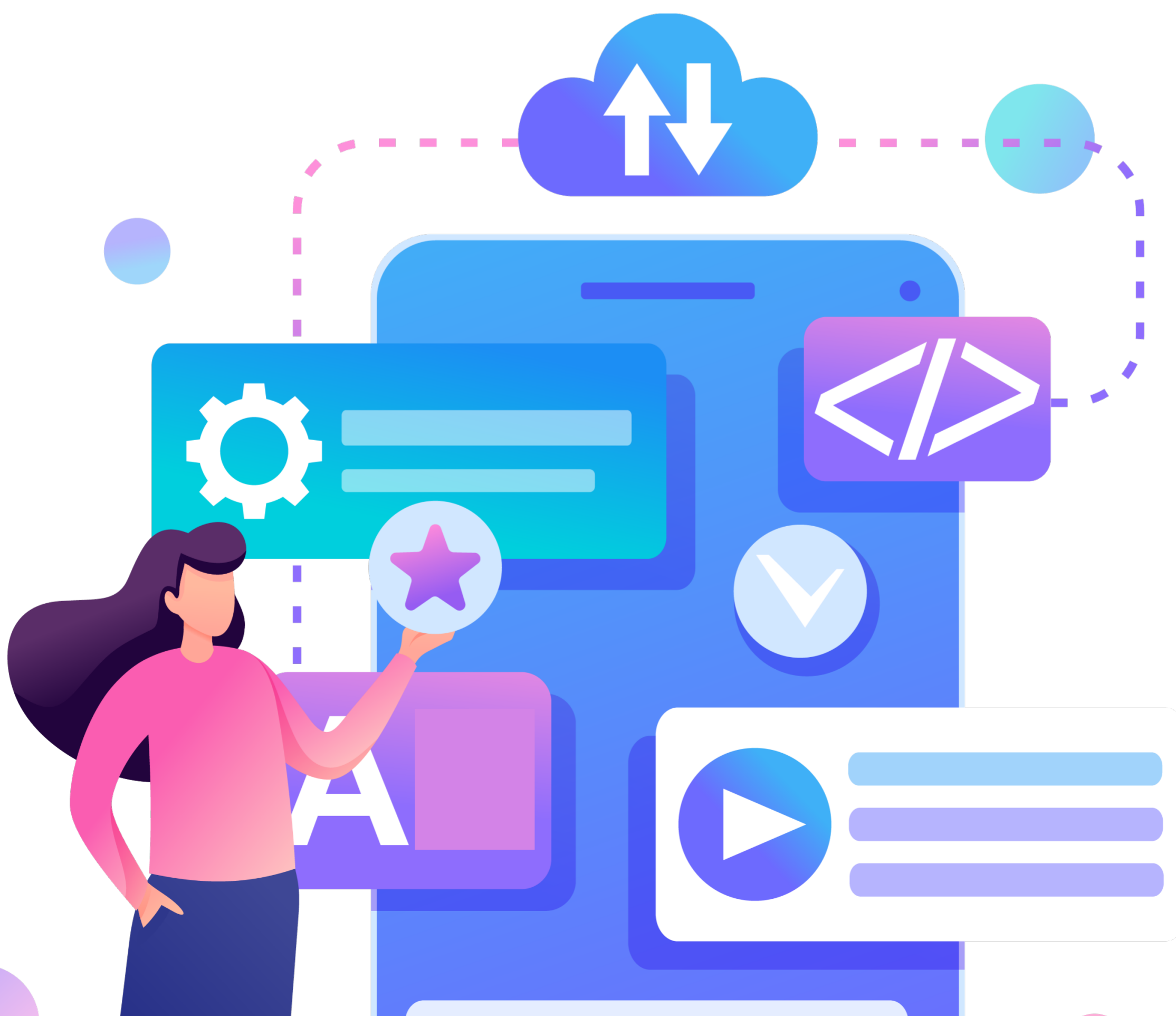
Когда автосинхронизация включена, данные приложений обновляются без вашего участия. Отключите автосинхронизацию приложений для экономии трафика. Но тогда вам понадобится синхронизировать приложения вручную.

→ ОГРАНИЧИВАЙТЕ ФОНОВЫЙ ТРАФИК ДЛЯ ПРИЛОЖЕНИЙ

Некоторые приложения передают данные в фоновом режиме, они могут скачивать информацию даже тогда, когда вы с ними не работаете. Ограничение фонового трафика также позволит уменьшить общий объем передаваемых данных.

→ ОТКЛЮЧАЙТЕ ИЛИ ОГРАНИЧИВАЙТЕ ПЕРЕДАЧУ ДАННЫХ В РОУМИНГЕ

Когда вы находитесь в другой стране, вы можете подключаться к сетям других мобильных операторов с помощью функции интернет-роуминга. Большинство мобильных операторов взимают за это дополнительную плату. Для того, чтобы снизить расходы и сэкономить трафик, отключите интернет-роуминг.



WI-FI СЕТИ

Wi-Fi – современная технология беспроводной сети. В каждой сети Wi-Fi присутствуют:



ТОЧКИ ДОСТУПА

устройства, которые делятся Wi-Fi-трафиком (например, Wi-Fi-роутеры)



КЛИЕНТЫ

устройства, которые получают Wi-Fi-трафик

К одной точке доступа может подключаться несколько клиентов (их количество ограничено возможностями устройства). Wi-Fi-роутеры можно встретить практически везде: в офисах, торговых центрах, университетах, жилых квартирах, даже в метро.

Каждая Wi-Fi-сеть имеет название и метод шифрования (WEP, WPA, WPA2 и другие). Если в Wi-Fi сети используется шифрование, она будет защищена паролем. Длина такого пароля – минимум 8 символов.



Советуем всегда защищать ваши домашние и рабочие Wi-Fi сети паролями, чтобы злоумышленники не могли использовать их в своих преступных целях. Если с открытой Wi-Fi сети совершается компьютерное преступление (например, кража денег с банковских счетов), правоохранительные органы в первую очередь обратятся к ее владельцу.

Если вы знаете пароль от Wi-Fi-сети, вы можете подключиться к ней со своего смартфона. Для этого необходимо открыть настройки устройства, перейти в раздел беспроводных сетей, открыть Wi-Fi-сети, выбрать нужную и ввести пароль.

ПРЕИМУЩЕСТВА МОБИЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ:

- +** **Wi-Fi-сети могут присутствовать там, где нет мобильной связи.** Например, внутри вагонов метрополитена, зданий с толстыми стенами или на подземных этажах зданий.
- +** **Вы можете подключать устройства, которые не поддерживают SIM-карты.** Ноутбуки, планшеты, различные “умные устройства” – всё это будет иметь доступ в интернет, если вы настроите подключение по Wi-Fi.
- +** **Меньший расход батареи.** При подключении к Wi-Fi-сетям у цифровых устройств тратится меньше заряда батареи, чем при подключении к мобильным сетям.
- +** **Не тарифицируется мобильным оператором (если вы не используете Wi-Fi-роутер с SIM-картой).** Если вы используете публичный Wi-Fi (в торговых центрах, офисах и других заведениях) с бесплатным доступом, вам не придется оплачивать интернет-трафик. Даже при использовании домашнего Wi-Fi с подключением к городским интернет-сетям тарификация чаще всего может быть ниже, чем при использовании мобильного интернета.
- +** **Подключение к другим устройствам.** Если в сети Wi-Fi, к которой подключен смартфон, присутствуют другие цифровые устройства, то смартфон может с ними взаимодействовать. Например, включать музыку через умные колонки или демонстрировать изображение экрана через умные телевизоры.
- +** **Распространенность.** Wi-Fi является общемировым стандартом, поэтому вы сможете найти и подключиться к Wi-Fi-сети практически в любой стране. Обычно это намного дешевле и выгоднее, чем оплачивать мобильный роуминг.

НЕДОСТАТКИ ПЕРЕДАЧИ ДАННЫХ WI-FI:

- **Нестабильная скорость передачи трафика.** Если к Wi-Fi-сети подключено большое количество людей, или между точкой доступа и клиентом есть большое физическое препятствие (например, стена), подключение становится нестабильным, и скорость передачи трафика может снизиться.
- **Опасность публичных сетей.** Публичные Wi-Fi-сети могут использоваться злоумышленниками для взлома устройств, подключенных к этим сетям, и кражи различных данных.

В качестве точки доступа может выступать даже ваш смартфон. Для этого необходимо включить режим точки доступа (или режим модема) в настройках. В этом режиме ваш смартфон сможет обмениваться трафиком с другими цифровыми устройствами.

Также многие смартфоны умеют одновременно использовать мобильную передачу данных и передачу данных через Wi-Fi для того, чтобы подключение к интернету было бесперебойным и наиболее быстрым.



ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ

→ ПЕРИОДИЧЕСКИ ПРОВЕРЯЙТЕ КОЛИЧЕСТВО ПЕРЕДАВАЕМОГО ИНТЕРНЕТ-ТРАФИКА

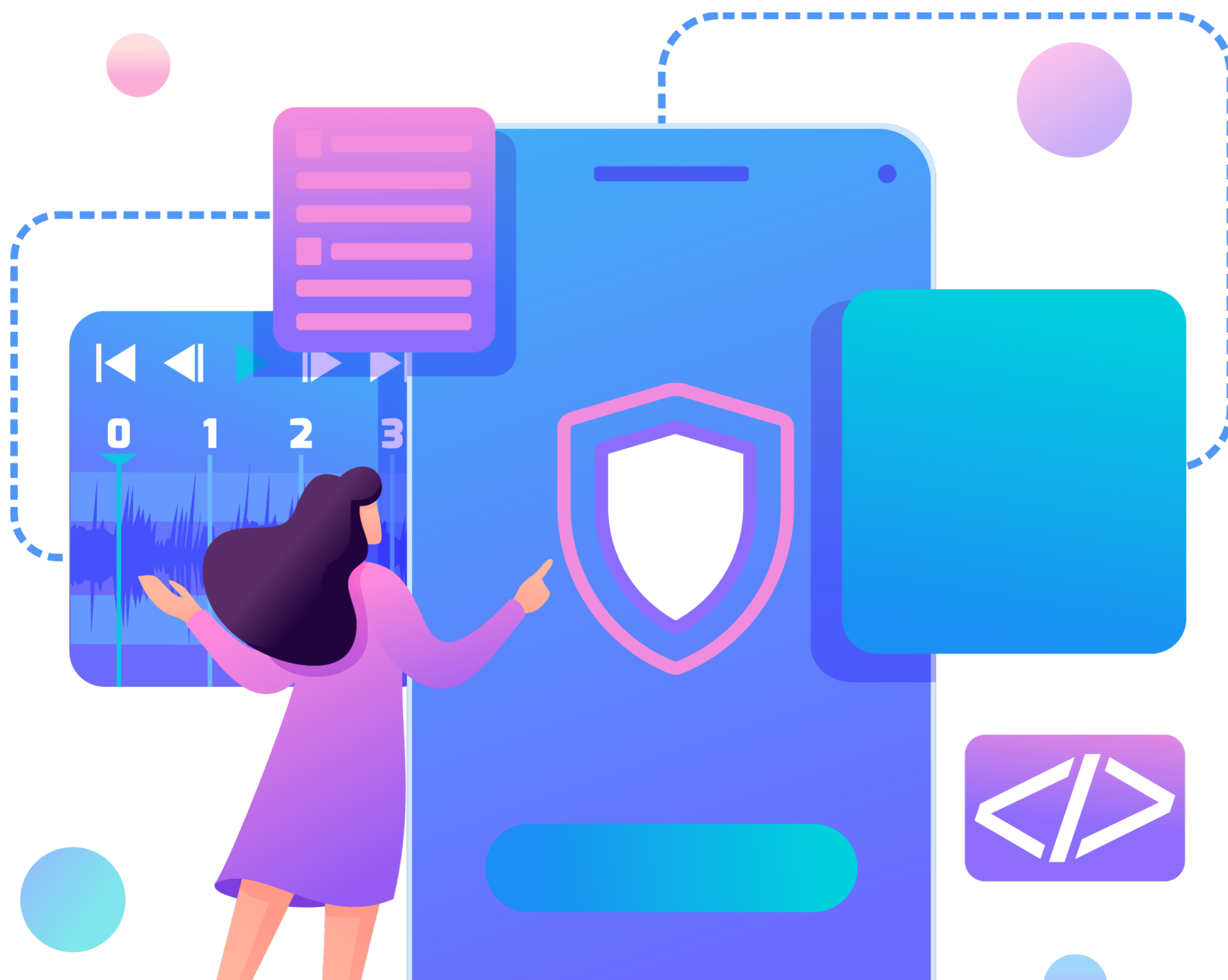
Если вы заметите что-то подозрительное, проверьте ваше цифровое устройство на вирусы.

→ ОТКЛЮЧАЙТЕ МОБИЛЬНУЮ ПЕРЕДАЧУ ДАННЫХ В РОУМИНГЕ

Если вы не настроили специальный тарифный план, который позволит вам не тратить огромное количество денег на мобильную связь, лучше её отключить. Даже если вы не будете заходить в интернет, ваш телефон может решить, что приложения требуют обновления, и на это будет потрачено большое количество денег.

→ НЕ ИСПОЛЬЗУЙТЕ МОБИЛЬНУЮ ПЕРЕДАЧУ ДАННЫХ ДЛЯ СКАЧИВАНИЯ БОЛЬШИХ ФАЙЛОВ

Для этого лучше подойдет Wi-Fi.



ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ WI-FI

→ С ОПАСКОЙ ПОДКЛЮЧАЙТЕСЬ К НЕЗАПАРОВАННЫМ WI-FI СЕТЯМ

Эти сети могут использовать мошенники для воровства личных данных.

→ ОТКЛЮЧИТЕ ОБЩИЙ ДОСТУП

Не разрешайте другим устройствам, подключенным к вашей Wi-Fi-сети, обнаруживать ваше цифровое устройство и просматривать список ваших файлов.

→ ОТКЛЮЧАЙТЕ WI-FI, ПОКА ВЫ ИМ НЕ ПОЛЬЗУЕТЕСЬ

Это позволит вам сэкономить заряд вашего устройства, а также не позволит "вычислить" ваше устройство в тот момент, когда оно будет автоматически сканировать находящиеся рядом сети.

→ ЗАЩИТИТЕ СВОИ ПЕРСОНАЛЬНЫЕ И БАНКОВСКИЕ ДАННЫЕ

Не заходите на критические важные сайты (банки, госуслуги и другие) или в приложения, а также не вводите пароли в почтовые сервисы и социальные сети, когда вы подключены к публичному Wi-Fi.

→ ПОДКЛЮЧАЙТЕСЬ К WEB-САЙТАМИ ПО HTTPS

HTTPS-соединение является более защищенным, при таком соединении потенциальному злоумышленнику будет намного сложнее получить доступ к вашим паролям и личным данным.

→ ИСПОЛЬЗУЙТЕ VPN

При использовании VPN весь ваш интернет-трафик будет проходить через безопасную виртуальную сеть. Советуем использовать платные VPN-сервисы, они быстрее работают и являются более надежными.

→ ВКЛЮЧИТЕ БРЭНДМАУЭР И АНТИВИРУС

Эти приложения будут отслеживать все входящие и исходящие соединения и предупредят вас в случае подозрительной интернет-активности на вашем устройстве.



© Региональная общественная организация "Центр интернет-технологий" (РОЦИТ), 2019

Не для продажи. Ссылки на сайты приведены в информационных целях и не являются рекламой.