Безопасность мобильного устройства

7 ГЛАВА

Особенность мобильных гаджетов с точки зрения киберугроз

Количество пользователей смартфонов и планшетов растет с каждым годом. Растет и число вредоносных программ, разработанных для мобильных устройств. Разработчики антивирусов Zimperium Labs в начале 2015 года подсчитали, что 95% устройств Android можно взломать с помощью простого текстового сообщения.

Какие зловредные программы создаются для мобильных устройств?

1. Для сбора логинов и паролей, которые используются для входа в банковские системы.
2. Программы-вымогатели, которые блокируют доступ к важным файлам, к фото и видео пользователя.
3. Рекламные программы, которые также занимаются сбором информации о вас и передают ее третьим лицам. Главная цель – показать вам баннер, который бы заставил принять рекламное предложение. Особенно распространено так называемое сталкерское программное обеспечение. Оно легально, но также занимается наблюдением за пользователем и сбором личных сведений.
4. СМС-троянцы, которые отправляют с вашего номера сообщения на платные номера.
5. Вирусы, которые действуют через специальные программы для людей с ограниченными возможностями.

Постоянно появляются новые и новые варианты программ, которые ставят под угрозу безопасность ваших данных на мобильном телефоне или планшете.

К тому же есть риск потерять смартфон или планшет, или устройства могут украсть, а с ними пропадут и все ваши данные.

Конечно, сегодня можно настроить удаленное управление мобильным устройством и так же удаленно стереть с него данные.

Подробнее об управлении мобильным устройством через Google-аккаунт в главе 3 «Основы работы с приложениями. Настройки.» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета».

Как действуют вирусные программы на мобильных устройствах:

1. Собирают данные ваших логинов и паролей.
2. Блокируют доступ к личным данным с целью вымогательства.
3. Собирают о вас информацию для маркетологов и рекламистов.
4. Удаленно управляют вашими учетными записями.
5. Отправляют сообщения на номера телефонов с оплатой за счет отправителя.

Основные рекомендации для безопасной работы на мобильном устройстве

Чтобы максимально обезопасить себя, будьте внимательны, когда используете мобильное устройство:

- не скачивайте программы и приложения с подозрительных сайтов в интернете;
- не подключайте в телефоне функцию бесконтактных платежей: это удобно, но менее безопасно;
- не сохраняйте данные банковской карты ни в аккаунте смартфона, ни в браузере;
- правильно настраивайте доступ приложений к другим вашим данным. Они должны быть логичными. Понятно, почему Вайбер запрашивает доступ к контактам, но если такое же разрешение просит приложение Лупа или Фонарик – это, как минимум, странно. Удаляйте такие приложения;
- после работы на мобильном устройстве всегда выключайте его, блокируйте экран доступа, ведь иногда мошеннику достаточно тридцати секунд, чтобы получить доступ к вашим данным;
- не переходите по ссылкам, присланным в сообщениях в мессенджерах или социальных сетях и электронной почте незнакомцами;
- проверьте настройки конфиденциальности и безопасности в приложении-браузере и аккаунте, который привязан к мобильному устройству. Обязательно поставьте запрет на скачивание приложений из неизвестных источников;

Подробнее о настройках безопасности в главе 3 «Основы работы с приложениями. Настройки» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета»

- отключайте Bluetooth и Wi-Fi, если вы ими не пользуетесь;
- не заходите в личные аккаунты и не проводите платежи в общественных сетях Wi-Fi;
- установите антивирус на мобильный телефон. При этом убедитесь, что в него встроена услуга на случай кражи устройства (возможность управлять удаленно);
- настройте блокировку экрана, желательно используя биометрические данные;
- для защиты приложений можно использовать программы-защитники данных. Например, App Lock (можно скачать из магазина приложений), или встроенную в смартфоны Samsung папку Knox. Принцип работы один. Это приложение, куда вы можете перенести файлы с ценной информацией, а также другие важные приложения, например, банковское. Доступ будет под паролем. Это практически так же, как если бы вы в большой сейф спрятали еще один маленький сейф с важными документами.

Биометрия для телефона

Блокировка экрана – одна из самых важных функций для безопасности вашего смартфона. Суть в том, что, если вы где-то оставили свое устройство, никто из посторонних не сможет получить доступ к вашей информации. Если для того, чтобы перейти к приложениям, достаточно просто провести по экрану пальцем, это значит, что у вас нет защиты. Обязательно установите ее. Это могут быть биометрические данные, графический ключ или пароль.

Подробнее об установке пароля на экран блокировки в главе 3 «Начало работы на планшетном компьютере» модуля 6 «Основы работы на планшетном компьютере» расширенного курса «Азбука интернета»

Специалисты считают, что одна из самых надежных технологий – использование биометрических данных. В современных смартфонах есть возможность настроить вход по отпечатку пальца (Touch ID – Тач Ай Ди) или по распознаванию вашего лица (Face ID – Фэйс Ай Ди). Наиболее удобный способ – отпечаток пальца.

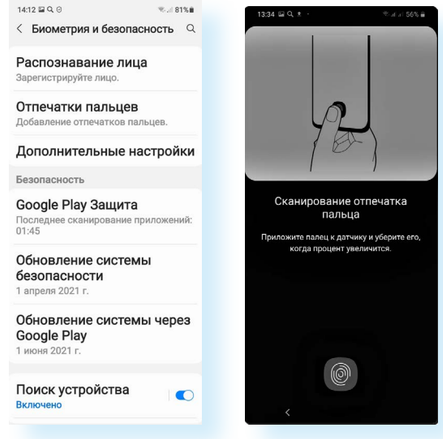
Для того, чтобы настроить блокировку экрана по биометрическим данным:

- перейдите в раздел «Настройки»;
- выберите пункт «Биометрия и безопасность» (название опции может отличаться на разных устройствах);
- определите, какой тип биометрии вам подойдет (распознавание лица или отпечаток пальца).

Например, вы выберете «Отпечатки пальцев». Далее вам потребуется ввести графический код разблокировки или пароль. Дело в том, что будут работать два варианта разблокировки экрана. Если по каким-то причинам у вас не получается войти по отпечатку пальца, вы сможете получить доступ к смарфтону другим способом – путем ввода пароля или графического ключа. Далее вас попросят приложить палец, которым вы будете делать разблокировку смартфона, к сканеру. На экране будет отмечено это место 7.1.

Для настройки экрана блокировки с использованием биометрии:

1. Перейдите в раздел «Настройки».
2. Выберите пункт «Биометрия и безопасность» (название опции может отличаться на разных устройствах).
3. Определите, какой тип биометрии вам подойдет.
4. Следуйте инструкциям для полной настройки.



7.1

(Есть модели, где для сканирования отпечатка необходимо приложить палец к фронтальной камере или к кнопке навигации. Внимательно читайте инструкции на экране). После того, как будет создан отпечаток вашего пальца, завершите настройку. Теперь, чтобы разблокировать смартфон, вам нужно будет приложить палец к обозначенному внизу экрана сканеру.

Обратите внимание, что теперь вы сможете использовать вход по отпечатку пальца и в другие приложения, установленные на смартфоне. Например, на портал «Госуслуг», в онлайн-банк, в личный кабинет «Ростелекома». Данную функцию нужно включить в настройках приложения.

Работа в публичных точках доступа Wi-Fi

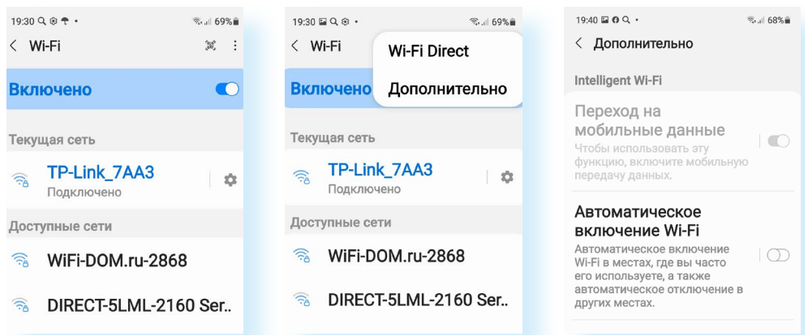
В ходе недавнего опроса 70% владельцев планшетов и 53% владельцев смартфонов и мобильных телефонов заявили, что они используют общедоступные точки доступа Wi-Fi. Такую информацию приводит «Лаборатория Касперского». Можно считать, что более половины владельцев мобильных устройств фактически отдают свои личные данные в руки мошенников.

Мы уже выясняли, что с помощью трекеров (программ, которые собирают данные для маркетологов и рекламщиков) в общедоступной сети Wi-Fi очень просто отследить ваши перемещения. Не удивляйтесь, если в продуктовом магазине, в торговом центре вам вдруг пришло сообщение о низкой цене на какие-то продукты. Скорее всего, ваш смартфон настроен так, что автоматически ищет и подключается ко всем общественным Wi-Fi сетям. Лучше отключить эту функцию.

Для этого:

- перейдите в «Настройки»;
- зайдите в раздел «Подключения»;
- нажмите на строку Wi-Fi;
- затем вверху зайдите в настройки Wi-Fi (это три точки, расположенные вертикально);
- в блоке «Автоматическое включение Wi-Fi» передвиньте ползунок влево (положение «Выключено») 7.2;

7.2



- в блоке «Hotspot 2.0» (подключение к другим устройствам, раздающим интернет) также поставьте ползунок в положение «Выключено».

Названные выше разделы «Настроек» могут отличаться в зависимости от модели и версии операционной системы.

Если вам срочно понадобилось выйти в интернет, то используйте интернет мобильного оператора, либо выходите в интернет через VPN. Это безопаснее, чем подключаться к общественным Wi-Fi сетям.

Работа в Bluetooth

Многие гаджеты сегодня работают по **Bluetooth**(Блютуз)-соединению. Это формат беспроводного соединения между компьютерными устройствами и различными электронными гаджетами. Как правило, оно работает на расстоянии от 10 до 100 метров.

Подробнее о Bluetooth-подключении в главе 3 «Начало работы на планшетном компьютере» модуля 6 «Основы работы на планшетном компьютере» расширенного курса «Азбука интернета»

По Блютуз подключаются беспроводные наушники, выносные акустические колонки, «умные вещи», смарт-часы, поэтому очень часто соединение Блютуз остается в мобильном устройстве активированным. Включенный Блютуз может стать для хакеров лазейкой к вашим данным. Это беспроводное соединение имеет слабый уровень защищенности. Взлом Блютуз позволит получить доступ к вашим контактам, личной почте, аккаунтам в социальных сетях и даже платежным данным. Данную технологию также используют для слежки за покупателем, изучения его предпочтений. Собранные данные передаются рекламщикам.

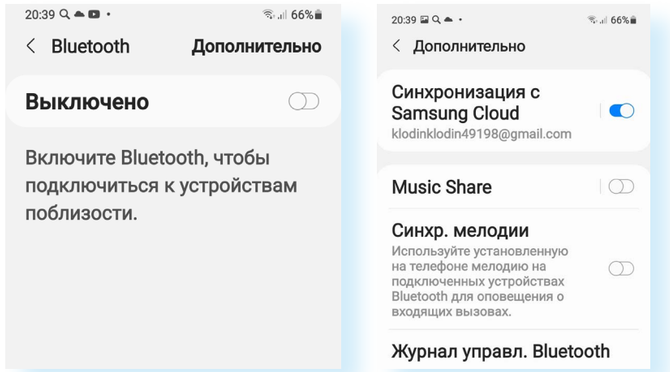
Поэтому отнеситесь внимательно к использованию такого соединения. Эксперты рекомендуют отключать Блютуз, когда вы его не используете.

На мобильном устройстве практически нет настроек Блютуз, помогающих защитить соединение.

В телефонах Samsung появилась технология Music Share, которая позволяет делиться с друзьями музыкой объемом до 2 ГБ.

Желательно также отключить ее, если не используете:
- перейдите в «Настройки»;
- выберите «Подключения»;
- затем нажмите «Bluetooth»;
- вверху кликните «Дополнительно»;
- далее передвиньте ползунок в неактивное положение напротив надписи «Music Share» 7.3.

7.3



Феномен и риски селфи

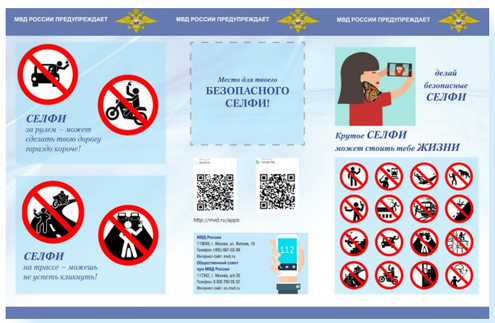
Слово селфи («selfie») в 2012 году по версии журнала «Тайм» вошло в топ-10 самых модных словечек года. По сути **селфи** – это автопортрет, который делается с расстояния вытянутой руки.

Селфи – это удобно, потому что не нужно просить кого-то фотографировать себя в путешествии, и, с одной стороны, в этом нет ничего плохого. Это такой новый способ общения с внешним миром. Но психологи считают постоянное желание делать селфи новой формой психологической зависимости. При этом человек ждет позитивных отзывов, лайков, и, если этого не происходит, у автора паблика может даже возникнуть расстройство психики.

В погоне за яркими селфи и большим количеством лайков и комментариев пользователи (в основном молодые люди) делают такие автопортреты, рискуя жизнью.

Министерство внутренних дел России разработало специальную методичку «Безопасное селфи» 7.4.

7.4



Также ваше селфи – это говорящее фото. Можно увидеть, где и с кем вы находитесь, обстановку в вашем доме. Эта информация может быть полезна мошенникам, которые вполне могут уже иметь ваши личные данные, а по вашей ленте в соцсетях можно определить ваши маршруты и узнать о поездках.

Поэтому чрезмерно не увлекайтесь автопортретами на мобильный телефон, не рискуйте в погоне за суперселфи, и лучше всего выкладывайте свои фото несколько позже, чем была ситуация, запечатленная на селфи.

Чьи в семье сим-карты?

Симки для телефонов доступны всем, и очень часто их может быть у человека несколько. А еще бывает так, что номер телефона оформлен на одного человека, а пользуется им другой: родственник, супруг, ребенок или просто знакомый. Скажем, брали симку в салоне и забыли паспорт. Не возвращаться же. Попросили оформить своего друга, у которого паспорт при себе. Теперь номер ваш, но оформлен на другого. А это уже может привести к проблемам.

В России в 2018 году вступил в силу закон, по которому номером телефона должен пользоваться именно тот человек, на кого оформлен договор. Узнать, на вас ли оформлена сим-карта, можно в салоне связи, но нужно иметь в виду – если оператор узнает, что номером пользуется другой человек, будет 15 дней, чтобы предоставить свои данные, иначе номер будет заблокирован.

Что может сделать владелец сим-карты? Он может обратиться к сотовому оператору и расторгнуть договор. И вы рискуете оказаться без связи, возможно, не в самый подходящий момент.

А еще владелец номера может перевыпустить симку, и тогда звонки будут приходить ему, а не вам. А это и информация о платежных операциях, уведомления с сайтов и приложений, где есть ваш личный кабинет. Вы не сможете восстановить пароли от ряда сервисов, где подтверждение о смене пароля проверяется кодом из смс. А между тем реальный владелец симки сможет узнать, какими сервисами вы пользуетесь, где совершаете покупки и на какие суммы.

Более того, он может забрать себе некоторые учетные записи, которые привязаны к номеру телефона. Например, ваши сообщения в мессенджерах. А вот получить доступ к вашему банковскому счету для владельца номера телефона будет сложнее. Ведь банки запрашивают дополнительные данные с клиента: номер карты или секретный вопрос.

Так что обязательно постарайтесь разобраться, чьими симками вы пользуетесь 7.5.

7.5

Затем нужно будет переоформить их на себя. Сделать это нужно вместе с владельцем номера. Понадобится заполнить заявление. Переоформить номер можно и в том случае, если человек, на которого оформлен номер, находится в другом городе. И даже если вы не знаете о его местонахождении, можно попробовать обратиться с заявлением к оператору сотовой связи. Есть шансы, что вашу просьбу удовлетворят.

Если люди находятся в разных городах, оператор может предложить обратиться в салон связи по месту жительства и составить заявление. Первым в любом случае должен обратиться текущий владелец номера, то есть тот, на кого оформлен договор.

Сим-карты часто продают с рук безо всякой регистрации. Это незаконная деятельность. За использование такой симки по закону взимается штраф до 2 тысяч рублей для физического лица. Такая симка может перестать работать в любой момент. Вы не сможете восстановить ее в салоне. Могут возникнуть проблемы с привязкой симки к банковскому счету. Бывает, что анонимные сим-карты продают мошенники. Они ждут, когда на номер будет положена определенная сумма денег и блокируют номер, перевыпустив симку. Но даже если это не мошенники, в любом случае у таких сим-карт уже есть владелец. Часто это юридическое лицо, фирма, которая якобы закупила симки для своих сотрудников.

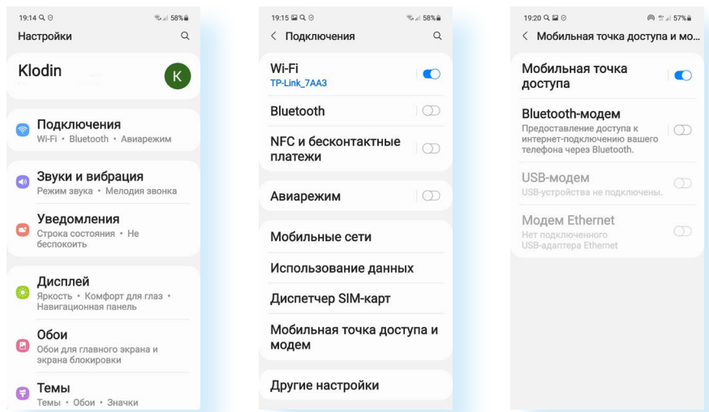
Безопасная работа смартфона в режиме «Точки доступа»

Каждый смартфон может работать как мобильный модем, ведь он выходит в интернет через сотовую связь и может делиться интернет-соединением с другими устройствами по Wi-Fi. Например, смартфон может быть точкой доступа в интернет для ноутбука или планшета.

Это полезная функция. Чтобы подключить ее, нужно:

1. Зайти в смартфоне в «Настройки».
2. Выбрать «Подключения».
3. Перейти в раздел «Мобильная точка доступа».
4. Передвинуть ползунок напротив надписи «Мобильная точка доступа» 7.6.

7.6



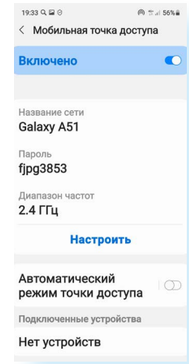
Вы включили передачу данных. Теперь другое устройство по Wi-Fi может подключиться к вашему смартфону и получить ваш доступ в интернет.

Конечно, это небезопасно. На что обратить внимание? Обязательно настраивайте раздачу по паролю.То есть, чтобы подключиться к вашему интернету на другом устройстве, нужно будет ввести пароль.

Если нет необходимости в раздаче интернет-соединения, отключайте данную опцию в смартфоне. Периодически проверяйте настройки вашей точки доступа на телефоне. Там вы сможете увидеть, сколько устройств используют ваше интернет-соединение.

Чтобы настроить точку доступа в смартфоне, нужно:

1. Зайти в «Настройки».
2. Перейти в раздел «Подключения».
3. Далее выбрать «Мобильная точка доступа и модем».
4. Нажать на надпись «Мобильная точка доступа».
5. Здесь вы увидите название сети, пароль к вашей точке доступа, а также подключившиеся к вам устройства 7.7.



7.7

Нажав «Настроить», вы сможете изменить пароль, название своего устройства. Также можно установить дополнительную защиту от чужих подключений, включив опцию «Защищенные кадры управления».

Чтобы подключить точку доступа, нужно:

1. Зайти в смартфоне в «Настройки».
2. Выбрать «Подключения».
3. Перейти в раздел «Мобильная точка доступа».
4. Передвинуть ползунок напротив надписи «Мобильная точка доступа».

Контрольные вопросы

1. Каковы особенности мобильных телефонов с точки зрения кибербезопасности?
2. На какие правила безопасности стоит обращать внимание при работе на мобильных устройствах?
3. Почему опасно работать в личных кабинетах приложений и проводить платежи со смартфона, подключившись к общественным сетям Wi-Fi?
4. Почему Bluetooth после использования нужно отключать?
5. Почему важно настроить экран блокировки на мобильном устройстве?
6. Чем могут быть опасны селфи?
7. Почему важно оформлять свои сим-карты на себя?