Автор: Administrator
21.09.2019 01:12 -

После покупки нового смартфона владелец старается заполнить его разными приложениями. При этом забывает о том, что телефон может легко поймать вирус, если не уделять особое внимание безопасности гаджета. Установка антивируса – дело несложное. Но и без него можно эффективно защитить смартфон.

Не подключайтесь к общедоступному WiFi

В общественных местах, на остановках и вокзалах часто доступен Wi-Fi. Но следует

хорошо подумать, прежде чем подключаться к нему:

- бесплатный доступ в интернет в кафе, аэропортах и отелях является хорошей возможностью оказаться во всемирной паутине, но это может быть небезопасно;
- через общедоступные WiFi-сети нельзя вводить логины и пароли доступа. А также не рекомендуется использовать публичный WiFi для передачи конфиденциальных данных, например, выхода в электронную почту или социальные сети.

Кроме того, нельзя допускать без согласия пользователя автоматического подключения смартфона к сетям Wi-Fi, поэтому в мобильном телефоне следует отключить функцию “Подключение к Wi-Fi автоматически”.

Ведь открытая незапароленная точка доступа – любимый способ хакеров. Опасным может даже быть Wi-Fi, имеющий пароль. После подключения к телефону взломщик может получить всю информацию, имеющуюся на гаджете, и увидеть, что делает собственник телефона в нем.

Чтобы выявить, не подвергался ли телефон взлому, нужно обратить внимание на следующие признаки:

- быстрая разрядка;
- самостоятельно закрывающиеся и открывающиеся приложения;
- большой расход мобильного трафика.

При наличии подобных признаков можно допустить мысль, что на телефон происходили атаки хакеров.

Не переходите по ссылкам, полученным от неизвестного отправителя

Нельзя переходить по нежелательным ссылкам, полученным от неизвестного отправителя. Мошенники могут обещать розыгрыш призов или использовать другие уловки. Подобным образом можно не только получить вирус, которым хакеры заражают телефон или компьютер, но и передать доступ к личным данным пользователя.

Нужно сразу удалять сообщения, полученные от незнакомых отправителей, особенно содержащие в тексте ссылки или запросы на личные данные. Не рекомендуется переходить на подозрительные сайты, обещающие вознаграждение за просмотр ролика или заполнение анкеты. Даже если ссылка поступила от знакомого человека. Возможно, его смартфон ранее уже был взломан.

Устанавливайте приложения только из официального магазина приложений

Следует внимательно относиться к источникам скачивания и информации о разработчиках приложений. Особенно касается это ссылок на бесплатную загрузку, случайным образом полученным в интернете. Доверять можно только проверенным источникам. Приложения рекомендуется устанавливать непосредственно из официального магазина.

В основном известные производители планшетов, смартфонов и других устройств на платформе Андроид устанавливают приложение Google Play. Но на некоторых моделях он не установлен.

Держитесь подальше от общедоступных зарядных устройств

Подсоединение умирающего смартфона к зарядному устройству в неизвестных местах является рискованным поступком. Может произойти следующее:

- благодаря скрытому устройству по другую сторону ящика можно потерять персональные данные (сохраненные пароли);
- параллельно получить вирус.

Таким образом, подсоединять смартфон к неизвестным кабелям является не лучшей идеей. Зарядные устройства, работающие в торговых центрах и аэропортах, обычно не представляют опасности. Но все же лучше всего носить зарядки с собой или не писать без конца посты в социальных сетях в интернете при нахождении вне дома.

Таким образом, можно пользоваться смартфоном без антивирусной программы, если следовать вышеперечисленным советам.