

Министерство внутренних дел России представило список рекомендаций, которые помогут пользователям Android-устройств повысить уровень конфиденциальности и защитить личные данные.

В первую очередь, предлагается отключить автоматическое подключение к Wi-Fi, чтобы телефон не соединялся с неизвестными сетями без ведома пользователя. Также необходимо отказаться от использования устаревшего протокола WEP, так как он больше не считается безопасным.

Ведомство рекомендует отключать Bluetooth, если он не используется, чтобы снизить риск возможных атак через беспроводное соединение. Уведомления и конфиденциальную информацию на экране следует показывать только после разблокировки устройства, а тайм-аут экрана — установить на минимально удобное значение.

Для разблокировки экрана рекомендуется использовать PIN-код, пароль или графический ключ. Также стоит активировать мгновенную блокировку после бездействия или при нажатии кнопки питания. Приложениям следует ограничить доступ к микрофону, камере, геолокации и другим функциям, если это не требуется для их работы.

Дополнительно предлагается сбросить и удалить рекламный идентификатор, отключить показ паролей и передачу диагностических данных. Для повышения безопасности стоит установить PIN-код на SIM-карту и включить проверку приложений на вредоносное ПО.

Также рекомендуется запретить добавление новых пользователей с экрана блокировки, чтобы никто не мог получить доступ к устройству без разрешения владельца.