

Приложение № 2
К письму Минобрнауки России
от 14.05.2018 г. № 08-1184

ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ПО БЕЗОПАСНОЙ РАБОТЕ С МОБИЛЬНЫМИ ТЕЛЕФОНАМИ

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. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги; Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона; Используй антивирусные программы для мобильных телефонов; Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение; После того как ты выйдешь с сайта, где вводил личную информацию, зайти в настройки браузера и удали cookies; Периодически проверяй, какие платные услуги активированы на твоем номере; Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь; Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.