ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

УГРОЗА
ДЛЯ ВЛАДЕЛЬЦЕВ WI-FI:

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВНЕДРИТЬ ВРЕДОНОСНЫЕ ПРОГРАММЫ НА ВАШЕ УСТРОЙСТВО ЧЕРЕЗ ОТКРЫТОЕ WI-FI-СОЕДИНЕНИЕ

- ВАШ ТРАФИК МОЖЕТ БЫТЬ ПЕРЕХВАЧЕН ЗЛОУМЫШЛЕННИКОМ, ВКЛЮЧАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, РЕКВИЗИТЫ КАРТ, И Т.Д.

- ВАШ КОМПЬЮТЕР МОЖЕТ БЫТЬ ПОДКЛЮЧЕН К БОТ-СЕТИ, ОСУЩЕСТВЛЯЮЩЕЙ DDOS-АТАКИ, ЧТО МОЖЕТ ПОВЛЕЧЬ УГОЛОВНУЮ ОТВЕТСТВЕННОСТЬ

УГРОЗА
ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

- ВВОДИМЫЕ ВАМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ ХАКЕРОМ (ПЛАТЕЖНАЯ ИНФОРМАЦИЯ, РЕВИЗИТЫ, КОНТАКТЫ НА ТЕЛЕФОНЕ, ПАРОЛИ)

- ЗЛОУМЫШЛЕННИК МОЖЕТ ПОЛУЧИТЬ ДОСТУП К ВАШИМ ПЕРСОНАЛЬНЫМ ДАННЫМ, ФОТО-ВИДЕО, ХРАНЯЩИМСЯ НА УСТРОЙСТВЕ, И Т.Д.

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВЗЛОМАТЬ ВАШИ ПРОГРАММЫ И СОЦИАЛЬНЫЕ СЕТИ, СОВЕРШАЯ ЗАТЕМ РАЗЛИЧНЫЕ ДЕЙСТВИЯ ОТ ВАШЕГО ИМЕНИ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЗОПАСНЫЙ WI-FI

Рекомендуется:

- отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;
- использовать надежный пароль для доступа к своей точке Wi-Fi;
- выключить автоматическое подключение своих устройств к точкам Wi-Fi.

ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.

Не рекомендуется:

- доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;
- вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ