



# КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

## НАДЕЖНЫЕ ПАРОЛИ

01

### НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам
- + Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
- + Доверять только проверенным менеджерам паролей

### НЕ РЕКОМЕНДУЕТСЯ:

- ✗ Использовать повторения символов
- ✗ Хранить пароли на бумажных носителях
- ✗ Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
- ✗ Сохранять пароль автоматически в браузере
- ✗ Использовать биографическую информацию в пароле

## БЕЗОПАСНЫЙ WI-FI

02


- + Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
- + Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
- + Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

- ✗ Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

## ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

03

- + Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

- ✗ Переходить по непроверенным ссылкам
- ✗ Вводить информацию на сайтах, если соединение не защищено (нет https и )

