



# КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

## НАДЕЖНЫЕ ПАРОЛИ

### 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
- × Хранить пароли на бумажных носителях
- × Использовать в качестве пароля имя пользователя, учетную запись или номер телефона (имя пользователя, учетная запись)
- × Сохранять пароль автоматически в браузере
- × Использовать биографическую информацию в пароле

## БЕЗОПАСНЫЙ WI-FI

- + 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 учетной записи (странице) при использовании банковского обслуживания при подключении к бесплатным точкам Wi-Fi в кафе, транспортных центрах и т.д.

## ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

- + 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 (https)

{backbutton}