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

БЕЗОПАСНЫЙ WI-FI

НЕОБХОДИМО

- ❖ 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

НЕ РЕКОМЕНДУЕТСЯ

- ❖ 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

НЕОБХОДИМО

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

НЕ РЕКОМЕНДУЕТСЯ

- ❖ Переходить по непроверенным ссылкам
- ❖ Вводить информацию на сайтах, если соединение не защищено

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

НЕОБХОДИМО

- ❖ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
- ❖ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
- ❖ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.

НЕ РЕКОМЕНДУЕТСЯ

- ❖ Размещать персональную и контактную информацию о себе в открытом доступе
- ❖ Использовать указание геолокации на фото в постах
- ❖ Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
- ❖ Употреблять ненормативную лексику при общении
- ❖ Устанавливать приложения с низким рейтингом и отрицательными

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ

НЕОБХОДИМО

- ❖ Хранить в тайне пин-код карты
- ❖ Прикрывать ладонью клавиатуру при вводе пин-кода
- ❖ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- ❖ Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций
- ❖ Скрыть CCV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

НЕ РЕКОМЕНДУЕТСЯ

- ❖ Хранить пин-код вместе с карточкой/на карточке
- ❖ Сообщать CVV-код или отправлять его фото
- ❖ Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона) «логин» и «пароль» доступа к системе «Интернет-банкинг»
- ❖ Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.