

- 01 НАДЕЖНЫЕ ПАРОЛИ
- 02 БЕЗОПАСНЫЙ WI-FI
- 03 БРАУЗЕРЫ И САЙТЫ
- 04 ЗАЩИТА ОНЛАЙН-БАНКИНГА
- 05 ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ
- 06 БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

6

правил
информационной
безопасности

|GROUP|IB|



КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕР- ПРЕСТУПНИКА

|GROUP|IB|



НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам и менять их каждые 3 месяца
- + Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные буквы, знаки пунктуации
- + 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

НЕОБХОДИМО:

- + Отключить общий доступ к вашей Wi-Fi сети и использовать надежный пароль к ней
- + Обновить прошивку роутера и сменить пароль к административной панели
- + Запретить автоматическое подключение своих устройств к открытым Wi-Fi точкам

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.

НЕОБХОДИМО:

- + Обновлять браузер и плагины
- + Использовать VPN

НЕ РЕКОМЕНДУЕТСЯ:

- Переходить по непроверенным ссылкам
- Вводить информацию на сайтах, если соединение не защищено (нет https и )
- Сохранять персональные данные в браузере

НЕОБХОДИМО:

- + Хранить в тайне пин-код карты и другие банковские данные
- + Прикрывать ладонью клавиатуру при вводе пин-кода
- + Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- + Использовать лимиты на максимальные суммы онлайн-операций
- + Скрыть CVV-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 для доступа к системе интернет-банкинга
- Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

НЕОБХОДИМО:

- + Устанавливать приложения только из официальных магазинов
- + Обращать внимание, к каким функциям устройства 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
- Указывать геолокацию 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 негативными отзывами

НЕОБХОДИМО:

- + Подключить двухфакторную аутентификацию
- + Использовать разную почту для переписок и для регистраций на сайтах
- + Использовать спам-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

- Реагировать на письма от неизвестного отправителя – скорее всего это спам или мошенники
- Открывать подозрительное вложение к письму – сначала позвоните отправителю и узнайте, что это за файл