Как не стать жертвой киберпреступника. 6 правил информационной безопасности.

6 правил информационной безопасности

КАК НЕ СТАТЬ ЖЕРТВО 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 симво
× Хранить пароли на бумажных но
× Использовать в качестве парол (имя пользователя, учетная запи
× Сохранять пароль автоматическ 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 до учетной записи (странице) или с банковского обслуживания при подключении к бесплатным (отк точкам Wi-Fi в кафе, транспорте центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

6 правил информационной безопасности

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизв отправителя: скорее всего это с мошенники
× Открывать подозрительное влож к письму: сначала позвоните отп и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕР

+ 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

× Размещать персональную и конт информацию о себе в открытом
× Использовать указание геолока на фото в постах
× Отвечать на обидные выражени и агрессию в соцсетях – лучше н об этом администратору ресурса
× Употреблять ненормативную лек при общении
× Устанавливать приложения с ни рейтингом и отрицательными от

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ

+ 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

× Хранить пин-код вместе с карточ на карточке
× Сообщать CVV-код или отправля его фото
× Распространять свои паспортны (информацию личного характера мобильного телефона), «логин»