Рекомендации по соблюдению мер информационной безопасности

Рекомендации по соблюдению мер «цифровой гигиены»

Необходимо:	Не рекомендуется:
Защита данных банковской платежной карточки	
Хранить в тайне пин-код, сведения с карточки сеансовых кодов	Хранить пин-код вместе с карточкой/на карточке
Прикрывать ладонью клавиатуру при вводе пин-кода	Сообщать кому-либо реквизиты карты или отправлять их фото по сети Интернет
Оформить отдельную карту для онлайн-покупок, выезда за границу, и не хранить на ней большие суммы. Для карты, используемой в Беларуси, рекомендуется ограничить возможность ее использования за пределами нашей страны	Распространять свои персональные данные (информацию личного характера, номер мобильного телефона), логин и пароль доступа к системе «Интернет-банкинг»
Использовать двухфакторную аутентификацию, установить лимиты на максимальные суммы операций, подключить смс-оповещение о проведении операций по карте	Сообщать данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Sequre» и т.д.
Скрыть CVV номер на карте (трехзначный номер на оборотной стороне), предварительно сохранив его	Пользоваться системой «Интернет-банкинг» на чужих компьютерах или мобильных устройствах
Вводить логин и пароль к системе «Интернет-банкинг» только на официальном сайте или в мобильном приложении банка	
В случае утери (кражи) карты, незамедлительно по телефону обратиться в банк для ее блокирования	
При обнаружении несанкционированного списания денежных средств с карт-счета, незамедлительно обратиться с заявлением в банк для их возврата по принципу «нулевой ответственности»	
Безопасность электронной почты	
Подключить двухфакторную аутентификацию	Реагировать на письма от неизвестного отправителя: скорее всего, это спам или «фишинговая» рассылка
Использовать минимум 2 типа e-mail адресов: закрытые (только для привязки устройств и средств защиты, интернет-банкинга и др.), открытые (отдельные для переписки, регистрации на форумах, оформления различных подписок и т.д.)	Открывать подозрительные вложения к письму: сначала позвоните отправителю и узнайте, что это за файл
Использовать спам-фильтры и соответствующее антивирусное программное обеспечение	Отправлять в открытом виде важные данные (фотоизображения документов, пароли и т.д.). В случае необходимости

	– заархивировать, установив сложный пароль
В случае подозрительных ситуаций проверить статистику подключений и изменить пароль	
Надежные пароли	
Создавать персональные (уникальные) пароли к разным сервисам	Хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо
Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и т.д.	Сохранять пароль автоматически в браузере
Доверять только проверенным менеджерам паролей	Использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т.д.)
Регулярно производить смену паролей	Использовать повторение символов, биографическую информацию и сведения, обнародованные в социальных сетях
Использование браузеров и сайтов	
Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать неблагоприятных последствий после посещения зараженных сайтов	Переходить по непроверенным ссылкам и посещать сайты сомнительного содержания
Производить регулярное обновление ПО, антивирусов и файерволов	Вводить информацию на сайтах, если соединение не защищено (нет https)
Обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта с целью «фишинга»)	Открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами ПО
Использование приложений, соцсетей и мессенджеров	
По возможности скрывать номер телефона, адрес электронной почты и другие сведения	Размещать персональную и контактную информацию о себе в открытом доступе
Обмениваться сообщениями в соцсетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения	Использовать указание геолокации на фото и постах
Устанавливать программное обеспечение только из достоверных источников	Отвечать на обидные выражения и агрессию в соцсетях – лучше написать об этом администратору ресурса
Безопасность мобильных устройств	
Использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.)	Передавать незнакомым мобильный телефон или сим-карту. В случае передачи – контролировать все действия, которые производятся с устройством

Своевременно обновлять операционную систему устройства, антивирус и др. ПО	Устанавливать приложения с низким рейтингом и отрицательными отзывами
Устанавливать приложения из PlayMarket, AppStore или только из проверенных источников	Перезванивать на незнакомые иностранные номера
Обращать внимание, к каким функциям гаджета приложение запрашивает доступ	Хранить важную информацию на мобильном устройстве
Включить встроенные функции устройства для определения его местонахождения	Делать полное снятие ограничения на устройстве («джейлбрейк», режим «суперюзера»)
В случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы	
При смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно)	
При продаже устройства произвести его сброс до заводских настроек	
Безопасный Wi-Fi	
После установки устройства для доступа к Wi-Fi сразу же поменять пароль и логин, установленные по умолчанию	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, торговом центре и т.д.
Использовать надежный пароль для доступа к вашей Wi-Fi точке	Включать общий доступ к своей Wi-Fi точке, даже если у вас безлимитный Интернет
Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам	