



КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ

01

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 пароль автоматически в браузере
- ✗ Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI

02

- + 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 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

03

- + 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 (нет https и )

6

правил
информационной
безопасности



|GROUP|IB|

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

04

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 неизвестного отправителя: скорее всего это спам или мошенники
- ✗ Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

05

- + 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 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 отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ

06

- + 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 CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

- ✗ Хранить пин-код вместе с картой / 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.

Как не стать жертвой киберпреступника. ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:



хранить в тайне пин-код карты



прикрывать ладонью
клавиатуру при вводе
пин-кода



оформлять
отдельную
карту для
онлайн-покупок



деньги зачислять
только в размере
предполагаемой покупки



использовать услугу 3-D Secure* и лимиты на
максимальные суммы онлайн-операций



скрыть CVV-код на карте (трехзначный номер на
обратной стороне), предварительно сохранив его



подключить услугу "SMS-оповещение"



Не рекомендуется

123 хранить пин-код вместе
с карточкой/на карточке

546 сообщать CVV-код или
отправлять его фото



распространять личные
данные (например
паспортные), логин
и пароль доступа к системе
"Интернет-банкинг"



SMS сообщать данные,
полученные в виде
SMS-сообщений, сеансовые
пароли***, код авторизации,
пароли 3-D Secure

* Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).

** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенней для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.

*** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.



Источник: МВД Беларуси.

© Инфографика

БЕЗОПАСНЫЙ WI-FI

Рекомендуется:



отключить общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет;



использовать надежный пароль для доступа к своей точке Wi-Fi;



выключить автоматическое подключение своих устройств к точкам Wi-Fi.

ВАЖНО ПОНИМАТЬ,

что многие уязвимости в защите возникают из-за устаревшего ПО, поэтому обязательно установите все последние обновления для своего ноутбука или телефона.



Не рекомендуется:

доверять открытым точкам Wi-Fi: именно такие сети используют злоумышленники для воровства личных данных пользователей;



вводить свой логин и пароль доступа к учетной записи или системе банковского обслуживания при подключении к бесплатным точкам Wi-Fi.



ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!



Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...



... в котором говорится, что банковская карта заблокирована и предлагается разблокировать ее, пройдя по ссылке...



... ни в коем случае не переходите по ссылке!
Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:



- не переходите по прикрепленной ссылке;
- никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.



Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь

