10 ПРАВИЛ
безопасного использования карты

1. ХРАНИТЕ ПИН-КОД ОТДЕЛЬНО ОТ КАРТЫ
2. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ СВОЙ ПИН-КОД ИЛИ CVV
3. В СЛУЧАЕ ПОТЕРИ КАРТЫ ИЛИ ПИН-КОДА НЕМЕДЛЕННО ОБРАТИТЕСЬ В БАНК ДЛЯ БЛОКИРОВКИ КАРТЫ
4. ПОДКЛЮЧИТЕ СМС-УВЕДОМЛЕНИЯ ОБ ОПЕРАЦИЯХ ПО КАРТЕ
5. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛЬ ДЛЯ ДОСТУПА В МОБИЛЬНЫЙ ИЛИ ИНТЕРНЕТ-БАНК
6. ХРАНИТЕ ПОД РУКОЙ КОНТАКТНЫЙ НОМЕР СЛУЖБЫ ПОДДЕРЖКИ ВАШЕГО БАНКА
7. РЕГУЛЯРНО ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
8. НЕ ОСТАВЛЯЙТЕ КАРТУ БЕЗ ПРИСМОТРА. ПРИКРЫВАЙТЕ РУКОЙ КЛАВИАТУРУ ПРИ ВВОДЕ ПИН-КОДА КАК В БАНКОМАТЕ, ТАК И ПРИ ОПЛАТЕ КАРТОЙ В МАГАЗИНЕ
9. УСТАНОВИТЕ ДОСТУПНЫЙ ЛИМИТ СПИСАНИЙ ПО КАРТЕ В ДЕНЬ
10. ОБРАЩАЙТЕ ВНИМАНИЕ НА ВНЕШНИЙ ВИД БАНКОМАТА. ЕСЛИ У ВАС ВОЗНИКЛИ СОМНЕНИЯ, СООБЩИТЕ ОБ ЭТОМ СОТРУДНИКАМ БАНКА И ВОСПОЛЬЗУЙТЕСЬ ДРУГИМ БАНКОМАТОМ. ЗВОНИТЕ В БАНК ТОЛЬКО ПО ОФИЦИАЛЬНОМУ НОМЕРУ БАНКА, УКАЗАННОМУ НА ОБОРОТНОЙ СТОРОНЕ КАРТЫ

ТЕЛЕФОННЫЕ МОШЕННИКИ

МОГУТ ПРЕДСТАВИТЬСЯ РАБОТНИКАМИ БАНКА или ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

НЕ сообщайте данные карты и коды из СМС

НЕ оформляйте кредиты по просьбе третьих лиц

НЕ устанавливайте программы по просьбе третьих лиц

НЕ переводите деньги на «защищенный счет»

НЕ переходите по ссылкам от незнакомцев

Больше информации в Telegram-канале Цифровая грамотность t.me/clfgram

ПЕРЕЗВОНИТЕ В БАНК!

- если убеждают установить программу на ваше устройство
- если просят назвать данные для отмены якобы оформленной доверенности на операции по вашему вкладу
- если предлагают отменить расходную операцию, которую вы не совершали
- если убеждают оформить кредит и перевести деньги на «защищенный» счет
- если вам одобрен кредит, который вы не оформляли

ПЕРЕЗВОНИТЕ В МИЛИЦИЮ!

- если просят поучаствовать в «разоблачении недобросовестного сотрудника банка»

УСТАНОВИТЕ В VIBER ЗАЩИТУ ОТ ЛИШНИХ ЗВОНКОВ

Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома

ООО "Дизайн-Центр", св-во ИИРПИ № 2/93 от 01.04.2014 г. Зак № 0165 (XI.2021) Т. 2500

ОСТОРОЖНО! МОШЕННИКИ!

Телефонные мошенники представляются сотрудниками правоохранительных органов или банка. Под различными предлогами убеждают участвовать в «спецоперации по разоблачению мошенников». Для этого уговаривают оформить кредиты и перевести деньги на «специальный защищенный счет».

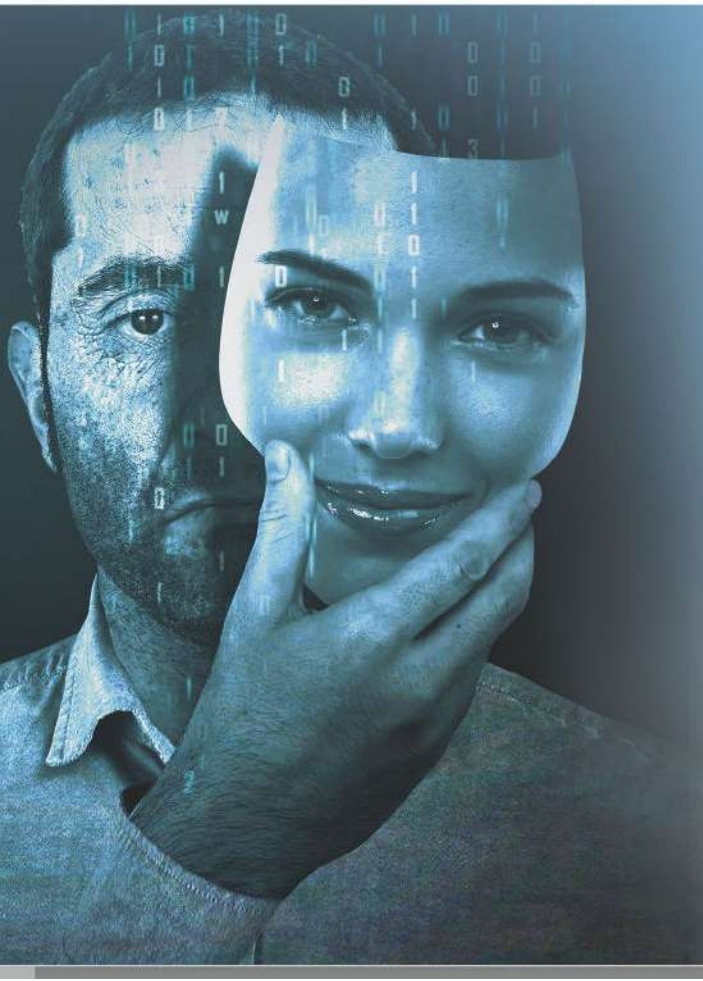
ПО ПРОСЬБЕ НЕЗНАКОМЫХ ЛИЦ:

- **НЕ сообщайте данные карты и коды из СМС-сообщений от банка, логины и пароли доступа к сервисам**
- **НЕ устанавливайте программы не передавайте коды регистрации**
- **НЕ оформляйте кредиты**
- **НЕ переводите деньги на «защищенный счет»**

Больше информации в Telegram-канале Цифровая грамотность t.me/cifgram

Если вам поступил звонок из «банка», завершите разговор и перезвоните в банк

Установите в Viber защиту от лишних звонков



БУДЬТЕ БДИТЕЛЬНЫ!

НЕ СТАНЬТЕ ЖЕРТВОЙ ОБМАНА!

Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома

ООО "Дизайн-Центр", св-во ИИРПИ № 2/93 от 01.04.2014 г. Зак № 0165 (XI.2021) Т. 2500

ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ

https:// оплата .by/
https:// банк
https:// доставка

ПОЛЬЗУЙСЯ БЕЗОПАСНО

- Пользуйтесь мобильными приложениями банка
- Переходите в интернет-банкинг только с официального сайта банка
- Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/
- Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)
- Не переходите в интернет-банкинг по ссылкам в поисковых системах
- Не используйте SMS-коды от банка и код с оборотной стороны карты для получения денежных средств

Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

ОН МОЖЕТ ПОПРОСИТЬ:

И НЕ ВЕДИТЕСЬ НА НА СЛОВА!!! МОШЕННИКА:

- Ваша карта заблокирована
- В отношении вашей карты предпринимаются мошеннические действия
- Вашему родственнику нужна помощь или лечение
- Вам положена отсрочка по кредиту или пособию

Данные карты:

- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

Пароль:

- от интернет-банка;
- из SMS-сообщения *(для входа в интернет-банк или подтверждения операции)*

Перевести деньги:

- на специальный счет или карту, где они будут в безопасности

НЕ

- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц

Безопасность при онлайн-платежах

МОЖНО

Указыватьномер своего телефона и электронную почту

Сообщать другим лицам номер вашей карты

Вводить в форму для оплаты на сайтах, начинающихся с https://, данные карты: номер, срок действия карты, ваше имя и фамилию, три цифры на обороте карты

Указывать при регистрации в платежной системе (типа WebMoney) паспортные данные

НЕЛЬЗЯ

Совершать любые операции с деньгами с чужого компьютера или пользуясь общественным wi-fi

Делать покупки на незнакомых сайтах

Давать другим какие-то сведения, помимо номера карты

Игнорировать современные браузеры со встроенной защитой и антивирусы

Сообщать кому-либо пин-коды ваших карт

УВД Витебского облисполкома

Осторожно - мошенники!

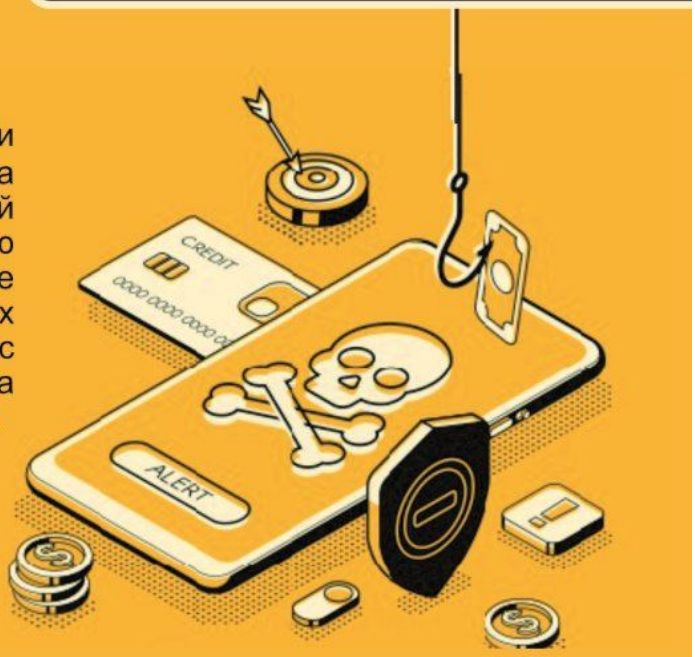
Как не стать жертвой киберпреступника

Помните! Никому нельзя сообщать: номер, срок действия, коды подтверждения на обороте карты, коды из СМС-сообщений, логины и пароли.

УВД Витебского облисполкома

КАК ОБЕЗОПАСИТЬ СВОЮ БАНКОВСКУЮ КАРТУ

ВНИМАНИЕ!!! МОШЕННИКИ



1 **НЕ РАССКАЗЫВАЙТЕ И НЕ ПОСЫЛАЙТЕ** никому — ни банковским служащим, ни покупателям, ни продавцам в сети — данные своей банковской карты, особенно секретный код с её оборотной стороны. Для пополнения карты достаточно знать только её номер.

2 **ПОДКЛЮЧИТЕ УСЛУГУ 3-D SECURE** и установите суточные лимиты на все виды совершаемых операций по вашей карте. Откройте отдельную карту для интернет-платежей и не храните на ней значительных денежных остатков. Не оплачивайте покупки с чужих электронных устройств и всегда выходите из всех платежных сервисов.

3 **НЕ ВВОДИТЕ ДАННЫЕ СВОЕЙ КАРТЫ** на страницах, полученных в мессенджере от непроверенных отправителей. Иногда страницы могут быть созданы для хищений денежных средств.

4 Если видите снятие денег без Вашего участия - **СРАЗУ ЖЕ БЛОКИРУЙТЕ КАРТУ НАБРАВ НОМЕР ВАШЕГО БАНКА САМОСТОЯТЕЛЬНО.**

УВД Витебского облисполкома

ВНИМАНИЕ!
АТАКА НА ГОСОРГАНИЗАЦИИ!

СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!

ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

НЕ НАДО:

... ОТКРЫВАТЬ ВЛОЖЕНИЯ ПОЧТОВЫХ СООБЩЕНИЙ ОТ НЕИЗВЕСТНЫХ ОТПРАВИТЕЛЕЙ

... ПЕРЕХОДИТЬ ПО ССЫЛКАМ, ПОЛУЧЕННЫМ ОТ НЕИЗВЕСТНЫХ

... ХРАНИТЬ И ПЕРЕДАВАТЬ В ОТКРЫТОМ ВИДЕ ВАЖНЫЕ ДАННЫЕ (ЗААРХИВИРУЙТЕ ИХ И УСТАНОВИТЕ ПАРОЛЬ)

... ПРИ РЕГИСТРАЦИИ ЯЩИКА УКАЗЫВАТЬ БИОГРАФИЧЕСКИЕ ДАННЫЕ, ИСПОЛЬЗОВАТЬ ПРОСТЫЕ ПАРОЛИ И ПОВТОРЯЮЩИЕСЯ СИМВОЛЫ

НАДО:

... ПОДКЛЮЧИТЬ 2-ФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

... РЕГУЛЯРНО МЕНЯТЬ ПАРОЛЬ ОТ ЭЛ.ПОЧТЫ

... ИСПОЛЬЗОВАТЬ НЕСКОЛЬКО ПОЧТОВЫХ ЯЩИКОВ ДЛЯ РАЗНЫХ РЕСУРСОВ (ПЕРЕПИСКА, РЕГИСТРАЦИЯ, ДЕЛОВАЯ ПОЧТА)

... ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ ИНТЕРНЕТ-РЕСУРСОВ

... ВВОДИТЬ ИНФОРМАЦИЮ ТОЛЬКО НА ЗАЩИЩЕННЫХ САЙТАХ (HTTPS)

ВНИМАНИЕ!

ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ - ЭТО ВАША БДИТЕЛЬНОСТЬ!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- 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, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

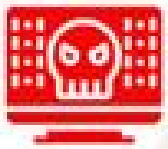
**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.

КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

В 2018-2020 ГГ ПРЕДПРИЯТИЯМ ПРИЧИНЕН УЩЕРБ НА СУММУ БОЛЕЕ 2 МЛН. РУБЛЕЙ

ОСНОВНЫЕ СХЕМЫ КИБЕРПРЕСТУПНИКОВ



Шифрование коммерческой информации

Хакеры получают доступ к данным организации, превращают их в бессмысленный набор символов и оставляют письмо с предложением расшифровать данные за деньги.

Подмена реквизитов для перевода средств

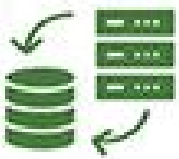
Эта криминальная схема используется в длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента, которые активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке. Когда у компаний намечается крупная сделка, со взломанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юрлица уведомляют партнеров об изменении реквизитов для перевода средств.

Фишинговое письмо

На электронную почту учреждения приходит письмо с вложением-вредоносом, способным превращать ценную для компании информацию в бесполезный набор символов.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРУГРОЗ

воспользоваться услугами профессионалов по защите данных



регулярно выполнять резервное копирование данных

пользоваться актуальными антивирусами

настроить специальное программное обеспечение, блокирующее таргетированные атаки на информационные системы

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РБ

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.

Главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь

ВНИМАНИЕ, ОПАСНОСТЬ!
ВРЕДОНОСНЫЕ РАСШИРЕНИЯ ДЛЯ БРАУЗЕРОВ!

ЧТО УМЕЮТ ДЕЛАТЬ ВИРУСНЫЕ РАСШИРЕНИЯ?

- Размещать навязчивую рекламу в вашем браузере

- Совершать действия от имени пользователя в соцсетях (лайкать нужные материалы, делать рекламные посты)

- Перенаправлять на фишинговые или зараженные сайты

- Незаметно для пользователя кликать на вредоносные или рекламные ссылки, активировать скрипты

- Подсовывать пользователю для скачивания вирусное ПО, или веб-приложения

- Самовосстанавливаться после удаления

- Подменять контент, видоизменять кнопки, интерфейс страницы, оформление

- Следить за серфингом пользователя в интернете: куда он ходит, какие сайты посещает, чем интересуется

КАК ОНИ ПОПАДАЮТ В ВАШ КОМПЬЮТЕР?

- В комплекте с другими программами (“в нагрузку” с какими-то нужным файлом или программой)

- Выдает себя за полезное ПО (наряду с полезными функциями программа может иметь и несколько “неполезных”)

- Обманом и шантажом (мошенники не дают пользователю уйти с их сайта, пока тот не установит программу или приложение)

В КАКИХ БРАУЗЕРАХ ОНИ УСТАНАВЛИВАЮТСЯ?

Дополнительные расширения поддерживают такие браузеры:

GOOGLE CHROME	OPERA
MOZILLA FIREFOX	EDGE
SAFARI	ЯНДЕКС.БРАУЗЕР
INTERNET EXPLORER	AMIGO, и др.

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

- Ваша карта заблокирована
- В отношении вашей карты предпринимаются мошеннические действия
- Вашему родственнику нужна помощь или лечение
- Вам положена отсрочка по кредиту или пособию

ОН МОЖЕТ ПОПРОСИТЬ:

Данные карты:

- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

Пароль:

- от интернет-банка;
- из SMS-сообщения *(для входа в интернет-банк или подтверждения операции)*

Перевести деньги:

- на специальный счет или карту, где они будут в безопасности

НЕ

- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

ОН МОЖЕТ ПОПРОСИТЬ:

И НЕ ВЕДИТЕСЬ НА НА СЛОВА!!! МОШЕННИКА:

- Ваша карта заблокирована
- В отношении вашей карты предпринимаются мошеннические действия
- Вашему родственнику нужна помощь или лечение
- Вам положена отсрочка по кредиту или пособию

Данные карты:

- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

Пароль:

- от интернет-банка;
- из SMS-сообщения *(для входа в интернет-банк или подтверждения операции)*

Перевести деньги:

- на специальный счет или карту, где они будут в безопасности

НЕ

- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц

Безопасность при онлайн-платежах

МОЖНО

Указыватьномер своего телефона и электронную почту

Сообщать другим лицам номер вашей карты

Вводить в форму для оплаты на сайтах, начинающихся с https://, данные карты: номер, срок действия карты, ваше имя и фамилию, три цифры на обороте карты

Указывать при регистрации в платежной системе (типа WebMoney) паспортные данные

НЕЛЬЗЯ

Совершать любые операции с деньгами с чужого компьютера или пользуясь общественным wi-fi

Делать покупки на незнакомых сайтах

Давать другим какие-то сведения, помимо номера карты

Игнорировать современные браузеры со встроенной защитой и антивирусы

Сообщать кому-либо пин-коды ваших карт

УВД Витебского облисполкома

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.

Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь

ВНИМАНИЕ

УВАЖАЕМЫЕ

Новополочане!!!

милиция предупреждает
о киберпреступниках,
которые орудуют в Интернете.
Чтобы обезопасить себя и свои
деньги помните о том, что:

- **Работники банка знают сведения о Вас, они не звонят по «VIBER» и не звонят из-за границы;**
- **Нельзя никому передавать СМС-пароли из банка. ВООБЩЕ НИКОМУ (даже если очень просят);**
- **Код с оборотной стороны карты нужен только для списания денег с неё;**
- **Для интернет покупок заведите отдельную карту;**
- **Не совершайте сомнительных сделок в интернете не убедившись в личности и намерениях покупателя или продавца;**
- **Будьте бдительны и осторожны, сохранность Ваших персональных данных и денег на карте в Ваших же интересах.**

Если Вы стали жертвой кибепреступников, обращайтесь в ОВД по тел.102

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

6 правил информационной безопасности

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 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.

6 правил информационной безопасности

GROUP-IB

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 🔒)

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

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- 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, предназначенной 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.

ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ ПОЗВОНИТЬ ПО ПОВОДУ ТОВАРА НА ТОРГОВОЙ ПЛОЩАДКЕ И ПРЕДЛОЖИТЬ СДЕЛКУ С ПРЕДОПЛАТОЙ

АФЕРИСТ МОЖЕТ ПРЕДСТАВИТЬСЯ БАНКОВСКИМ РАБОТНИКОМ И ВЫМАНИТЬ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

АФЕРИСТ СООБЩАЕТ, ЧТО РОДСТВЕННИК ЖЕРТВЫ ПОПАЛ В БЕДУ И ЕМУ НУЖНА ФИНАНСОВАЯ ПОМОЩЬ

ВИШИНГ - СПОСОБ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ТЕЛЕФОНА, КОГДА МОШЕННИК ПОД РАЗЛИЧНЫМ ПРЕДЛОГОМ ПЫТАЕТСЯ ВЫМАНИТЬ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ ЖЕРТВЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ ДЕНЕГ С ЕЕ БАНКОВСКОГО СЧЕТА

- НИКОГДА НЕ СООБЩАЙТЕ НЕЗНАКОМОМУ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ ТО, ЧТО ОТ ВАС ПРОСИТ СОБЕСЕДНИК. МОШЕННИКИ ОЧЕНЬ ИЗОБРЕТАТЕЛЬНЫ И УБЕДИТЕЛЬНЫ!

- НАДЕЖНО ЗАЩИЩАЙТЕ СВОИ ДАННЫЕ (ДВУХФАКТОРНАЯ АВТОРИЗАЦИЯ, СМС-ОПОВЕЩЕНИЕ , И Т.Д.)

- В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ КАРТЫ ЗАБЛОКИРУЙТЕ ЕЕ ПО ТЕЛЕФОНУ ИЛИ В БАНКЕ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

ФИШИНГ: КАК ЗАЩИЩИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ, ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества

Потенциальный покупатель вашего товара предлагает перейти в мессенджер, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок

Неизвестный в мессенджере присылает ссылку для перехода на интернет-сайт под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.

Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.

ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

БЫТЬ ХАКЕРОМ:
не развлечение, а преступление!

Уголовная ответственность за киберпреступления наступает:

Статья 212 УК Беларуси — **с 14 лет**

Хищение путем использования компьютерной техники или введения в компьютерную систему ложной информации наказывается вплоть до лишения свободы на срок **до 3 лет**.

Те же действия, совершенные **повторно или группой лиц по предварительному сговору**, наказываются лишением свободы на срок **до 5 лет**.

Если **хищение крупное**, то предусмотрено наказание в виде лишения свободы на срок **до 7 лет**.

За хищение, совершенное **организованной группой или в особо крупном размере**, грозит **до 12 лет** лишения свободы.

Статья 349 УК Беларуси — **с 16 лет**

Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, наказывается вплоть до лишения свободы на срок **до 2 лет**.

За несанкционированный доступ к компьютерной информации, повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные **тяжкие последствия**, грозит наказание вплоть до лишения свободы на срок **до 7 лет**.

Управление информации и общественных связей МВД Республики Беларусь