

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с неизвестного
номера

2 

звонящий
представляется
вашим
родственником

3 

он говорит,
что ~~был~~ человек
или из-за него
человек
попал в ДТП

4 

он просит денег,
как компенсацию
за ~~убыток~~ или
чтобы ~~закрыть~~ дело

5 

затем звонит
милиционеру/
следователю
и подтверждает
легенду

6 

за деньгами
приезжает
курьер

Мама, папа, я
в беде!

Нужны деньги!
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102

КАК ОБЕЗОПАСИТЬ СВОЮ БАНКОВСКУЮ КАРТУ

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.

**ВНИМАНИЕ!!!
МОШЕННИКИ**

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.**



ВНИМАНИЕ! **ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!**



НЕ СОВЕРШАЙТЕ НИКАКИХ ДЕЙСТВИЙ НА СМАРТФОНЕ ПО ПРОСЬБЕ ПОСТОРОННИХ ЛЮДЕЙ! ТЕМ БОЛЕЕ, НЕ СООБЩАЙТЕ ИМ КОДЫ, ПАРОЛИ, И ДР.ИНФОРМАЦИЮ

НЕ СОХРАНЯЙТЕ В ПРИЛОЖЕНИЯХ И БРАУЗЕРАХ ПАРОЛИ, КОДЫ, ЛОГИНЫ. ПРЕСТУПНИК МОЖЕТ УЗНАТЬ КОД ИЗ ПРИСЛАННОГО SMS-СООБЩЕНИЯ



128 293 154

ПРЕСТУПНИК ПО ТЕЛЕФОНУ ПРОСИТ ВАС УСТАНОВИТЬ ПРОГРАММУ НА ТЕЛЕФОН ДЛЯ ДИСТАНЦИОННОГО ДОСТУПА И СООБЩИТЬ ЕМУ ПАРОЛЬ И КОД



УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ



Хранить пинкод вместе с картой



Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

НЕЛЬЗЯ



Сообщать CVV-код или отправлять его фото



Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.



Сохрани эту информацию и поделись с другими

Безопасный интернет для детей

**СОХРАНИ
ИНФОРМАЦИЮ**

**не сообщай незнакомцам
свой логин и пароль**

**не открывай файлы из
непроверенных источников**

**не заходи на сайты, которые
защита компьютера считает
подозрительными**



**НЕ отправляй незнакомцам
свои фото и видео**

Злоумышленники могут узнать что-то
нужное им о твоей жизни



**НЕ встречайся с людьми,
с которыми знаком только
в интернете**

За маской онлайн-собеседника
может скрываться злоумышленник



**НЕ сообщай в интернете
свой реальный
адрес и телефон**

Злоумышленник может встретить
тебя с недобрыми намерениями



**НЕ отправляй личные данные
для участия в конкурсах
на малоизвестных сайтах**

Информацией могут завладеть и
воспользоваться недоброжелатели

**РОДИТЕЛИ!
научите детей
пользоваться
интернетом
правильно!**



**Всегда важно помнить: неправильное поведение
в интернете может принести большой вред.**

не дай себя обмануть!



**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ**

**круглосуточный
единый
номер**

102

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки



НЕ верьте обещаниям внезапных выигрышей

**УСТАНОВИТЕ АНТИВИРУС НА ВСЕ
ВАШИ УСТРОЙСТВА**



НЕ сообщайте свои персональные данные и данные банковской карты



НЕ указывайте личную информацию в открытых источниках



НЕ используйте одинаковые пароли для всех аккаунтов



Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

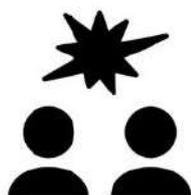


Размещать персональную и контактную информацию о себе в открытом доступе



Использовать указание геолокации на фото в постах

НЕЛЬЗЯ



Отвечать на агрессию и обидные выражения



Реагировать на письма от неизвестного отправителя



Открывать подозрительное вложение к письму



Сохрани эту информацию и поделись с другими

ОСТОРОЖНО! МОШЕННИКИ!

Телефонные мошенники представляются сотрудниками правоохранительных органов или банка. Под различными предложениями 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

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!



ОН

МОЖЕТ ПОПРОСИТЬ:

МОШЕННИК МОЖЕТ И НАЗВАТЬ
ПРЕДСТАВИТЬСЯ:

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

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

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

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! ОПЕРАЦИЯ «ВИШИНГ»!

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



АФЕРИСТ МОЖЕТ
ПРЕДСТАВИТЬСЯ
БАНКОВСКИМ РАБОТНИКОМ И
ВЫМАНИТЬ
КОНФИДЕНЦИАЛЬНЫЕ
ДААННЫЕ



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
ДААННЫЕ (ДВУХФАКТОРНАЯ
АВТОРИЗАЦИЯ,
СМС-ОПОВЕЩЕНИЕ, И Т.Д.)

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

ГУПК КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

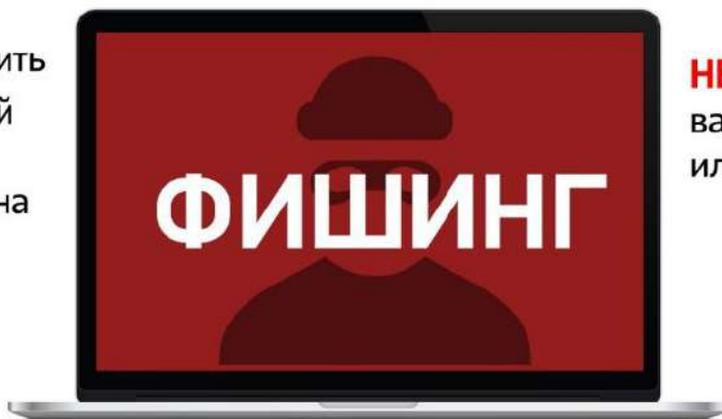
ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



НЕ пользуйся открытыми вай-фай-сетями в кафе или на улице



Не спеши переходить по ссылке: введи адрес вручную



Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении



Сохрани эту информацию и поделись с другими

ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ



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 обратной стороны карты для получения денежных средств



Управление по противодействию
киберпреступности криминальной милиции
УВД Витебского облисполкома