

ПОЛЬЗУЙСЯ БЕЗОПАСНО «БАНК».by



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



Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



Больше информации
на сайте
<https://mvd.gov.by>

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет

Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет

Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске

Передать личные данные и код из СМС, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

Перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка

Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)

Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку

На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ,

представляясь продавцами, друзьями, партнерами по бизнесу, руководителями инвестиционных проектов



Больше информации
на сайте
<https://mvd.gov.by>



Главное управление
по противодействию киберпреступности
КМ МВД Республики Беларусь

ВНИМАНИЕ, МОШЕННИКИ!

Вам звонят посредством мессенджера
или с неизвестного номера...

ВАШИ ДЕЙСТВИЯ:

- не паникуйте и не верьте тому, что вам говорят
- не выполняйте никаких действий по просьбе третьих лиц
- прекратите разговор
- перезвоните родственникам и убедитесь, что ничего не случилось
- сообщите в милицию о звонке

ВАШ СЫН
ПОПАЛ В БЕДУ!
НУЖНЫ
ДЕНЬГИ!



mvd.gov.by



! ВНИМАНИЕ, ОПАСНОСТЬ !

ЗАЩИТИТЕ СЕБЯ ОТ МОШЕННИКОВ:

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

НЕ ВЕРЬТЕ обещаниям внезапных выигрышей

НЕ ИСПОЛЬЗУЙТЕ одинаковые пароли для всех аккаунтов

НЕ УКАЗЫВАЙТЕ личную информацию в открытых источниках

НЕ СООБЩАЙТЕ свои персональные данные и данные банковской карты



НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Если вы или ваши близкие стали жертвами мошенников, или вы подозреваете, что в отношении вас планируются противоправные действия **Незамедлительно сообщайте в милицию!**

102



mvd.gov.by





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
на сайте
<https://mvd.gov.by>

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



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь