

ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ



НЕ следуй инструкциям
незнакомцев, позвонившим
с неизвестного номера



НЕ сообщай неизвестным
лицам свои персональные
данные



НЕ совершай никаких
действий на смартфоне по
просьбе посторонних лиц



НЕ переводи деньги
незнакомым людям в
качестве предоплаты



Сохрани эту информацию и поделись с другими

ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ



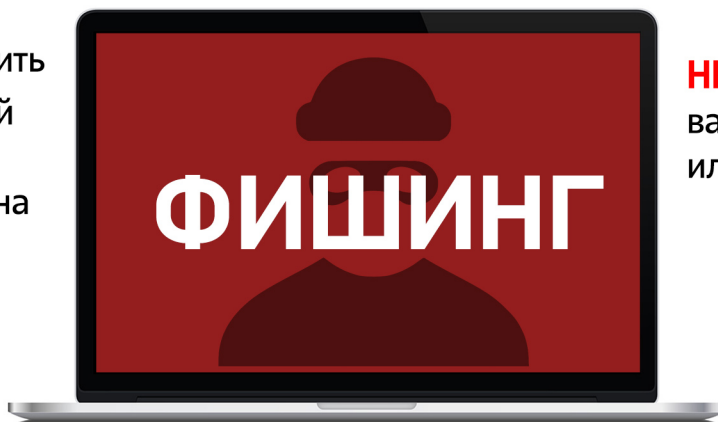
Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



Не спеши переходить по ссылке: введи адрес вручную



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



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



Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

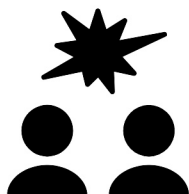


Размещать персональную
и контактную
информацию о себе в
открытом доступе



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

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 используйте одинаковые пароли для всех аккаунтов



НЕ сообщайте свои персональные данные и данные банковской карты



НЕ указывайте личную информацию в открытых источниках



Сохрани эту информацию и поделись с другими

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.

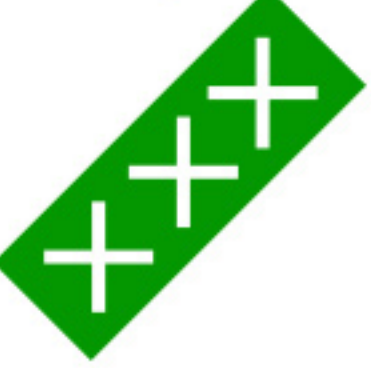


Сохрани эту информацию и поделись с другими

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.

© Инфографика 

! 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



102 - общегосударственный номер экстренной связи. В Беларуси действует единый номер 102. Информацию о номере 102 можно узнать по телефону 102 или на сайте mvd.gov.by

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 обратной 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>