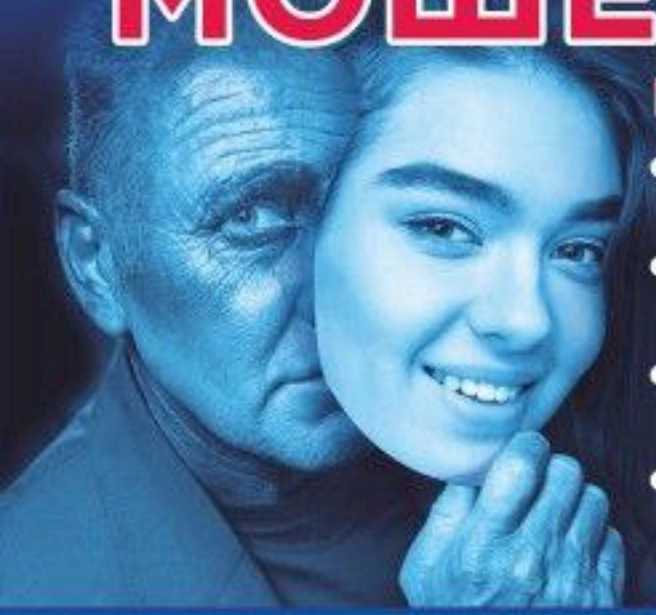
МОШЕННИКИ



МОГУТ ПРЕДСТАВИТЬСЯ:

- работниками госорганов и банков
- родственниками, знакомыми или продавцами
- руководителями организаций или учреждений
- кураторами криптовалютных бирж или инвестиционных проектов

- **НЕ сообщайте данные карты и коды из СМС-сообщений от банка, логины и пароли доступа к сервисам**
- **НЕ устанавливайте программы** по просьбе третьих лиц **и не передавайте коды регистрации**
- **НЕ оформляйте кредиты** по просьбе третьих лиц
- **НЕ переводите деньги на «защищенный счет»**
- **НЕ вводите данные карты и коды на страницах, открытых по ссылкам**
- **НЕ верьте обещаниям быстрого заработка на биржах**

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

БОЛЬШЕ ИНФОРМАЦИИ В ТЕЛЕГРАМ-КАНАЛЕ "ЦИФРОВАЯ ГРАМОТНОСТЬ" HTTP://t.me/cifgram

Управление
по противодействию
киберпреступности
УВД Витебского облисполкома

! 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

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 в Telegram-канале Цифровая грамотность t.me/cifgram

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КРИМИНАЛЬНОЙ МИЛИЦИИ 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 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)

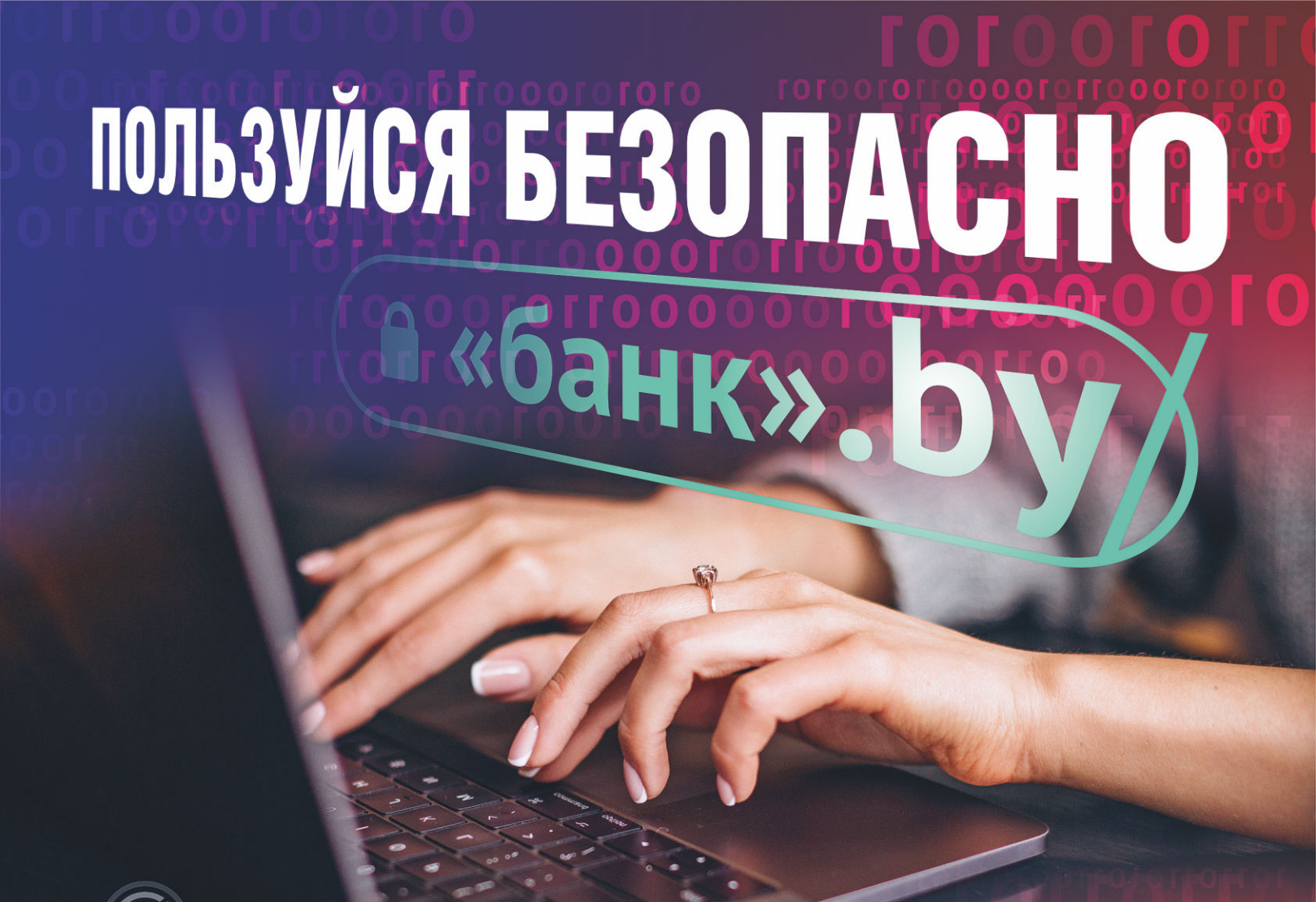
ВНИМАНИЕ!

ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ - ЭТО ВАША БДИТЕЛЬНОСТЬ!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

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

КИБЕР-ВИКТОРИНА!

ПРОЙДИ ТЕСТ

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

ПОДПИШИСЬ НА КАНАЛ