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!
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

Научись пользоваться интернетом правильно!

1. **не сообщай незнакомцам свой логин и пароль**
2. **не открывай файлы из непроверенных источников**
3. **не заходи на сайты, которые защита компьютера считает подозрительными**

не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102

Научись пользоваться интернетом правильно!

Безопасный интернет для детей

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

НЕ отправляй незнакомцам свои фото и видео

Злоумышленники могут узнать что-то нужное 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

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

не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102

научись пользоваться интернетом правильно!

БЕЗОПАСНЫЙ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

не сообщай незнакомцам свой логин и пароль

не открывай файлы из непроверенных источников

не заходи на сайты, которые защита компьютера считает подозрительными

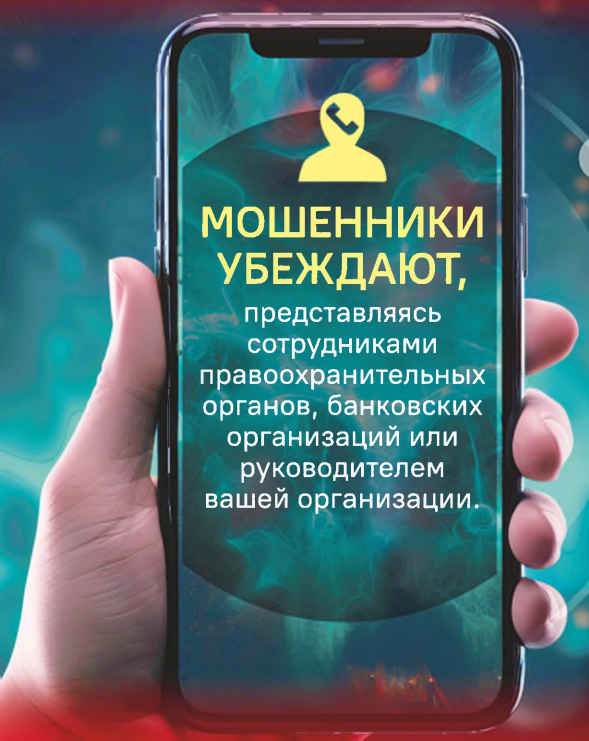
не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102


ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ
ЧТО ДЕЛАТЬ:
ВАШ БЛИЗКИЙ РОДСТВЕННИК (СЫН, ВНУК, МУЖ) ПОПАЛ В БЕДУ (АВАРИЮ, ОГРАБЛЕН, АРЕСТОВАН), И ЧТОБЫ «ВЫПУТАТЬСЯ» ИЗ ИСТОРИИ, ОН ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ ЧЕЛОВЕКУ, КОТОРЫЙ ПОМОЖЕТ
ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ
У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ
ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ
ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА
НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ
ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ
НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ
С ВАШЕЙ БАНКОВСКОЙ КАРТЫ БЫЛА ПОПЫТКА ПЕРЕВЕСТИ ДЕНЬГИ, И БАНК ЕЕ ЗАБЛОКИРОВАЛ; ЗВОНИТ ЯКОБЫ ПРЕДСТАВИТЕЛЬ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА И ПРЕДЛАГАЕТ РАЗБЛОКИРОВАТЬ КАРТУ, НО ДЛЯ ЭТОГО ЕМУ НУЖНО СООБЩИТЬ ЕЕ НОМЕР И КОД, ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ
– СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ;
– НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ СМС;
– НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ;
– ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВАНИВАЙТЕ В БАНК ВСТРЕЧНЫМ ЗВОНКОМ. МОЖНО ПЕРЕЗВОНИТЬ В БАНК ПО ОФИЦИАЛЬНОМУ НОМЕРУ (ОН УКАЗАН НА КАРТЕ) И СООБЩИТЬ О ЗВОНКЕ
ВАЖНО!
МОШЕННИКИ ВОРУЮТ БАЗЫ ДАННЫХ И НАЗЫВАЮТ ВАС ПО ИМЕНИ-ОТЧЕСТВУ, А В ТЕЛЕФОНЕ ВИДЕН НОМЕР ВАШЕГО БАНКА
БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:



МОШЕННИКИ УБЕЖДАЮТ, представляясь сотрудниками правоохранительных органов, банковских организаций или руководителем вашей организации.

- **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, 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

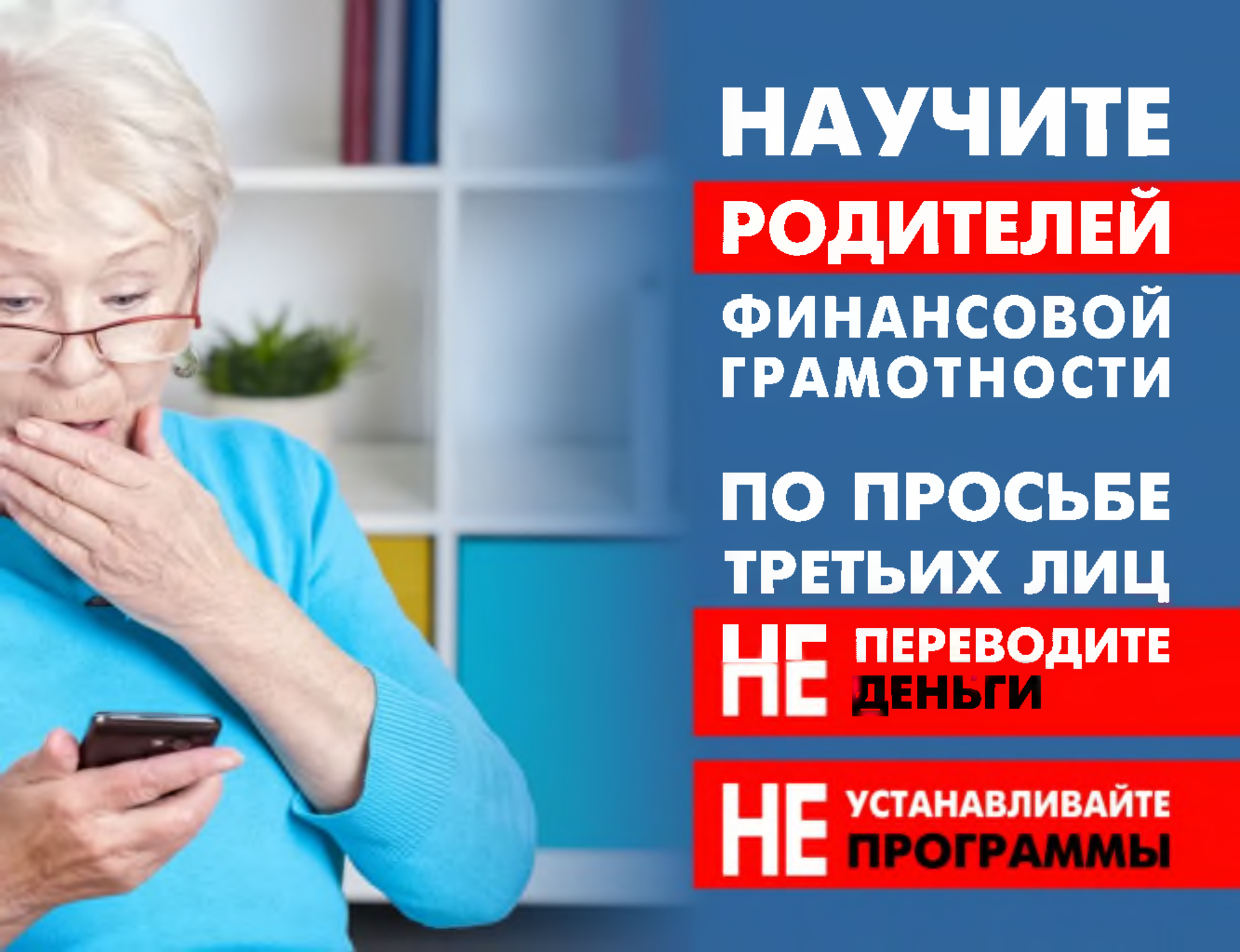
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Если вы или ваши близкие стали жертвами мошенников, или вы подозреваете, что в отношении вас планируются противоправные действия

НЕЗАМЕДЛИТЕЛЬНО СООБЩАЙТЕ В МИЛИЦИЮ!

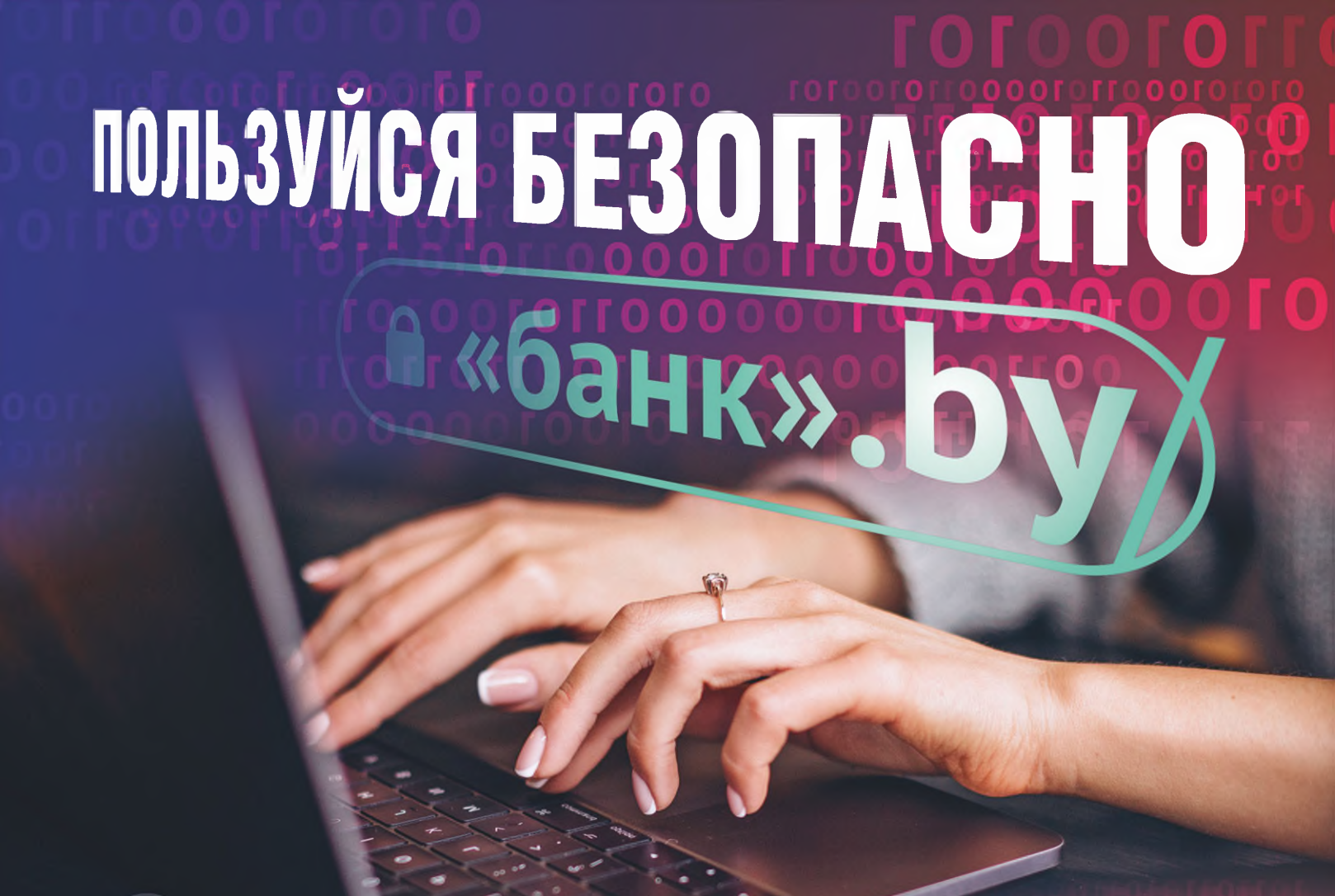
102

mvd.gov.by


НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ
ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ
НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ
НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

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