

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 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

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!

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

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

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! **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!**

научись пользоваться интернетом правильно!

СОВЕТЫ
ИНФОРМАЦИОННО



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

Безопасный Интернет для детей

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

НЕ отправляй незнакомцам свои фото и видео.
Злоумышленники могут узнать что-то важное о твоей жизни.

НЕ встречайся с людьми, с которыми знаком только в интернете.
За маской онлайн-общения может скрываться злоумышленник.

НЕ сообщай в интернете свои реальный адрес и телефон.
Злоумышленник может встретить тебя с неожиданными намерениями.

НЕ отправляй никому данные для входа в компьютер, не выполняй странных действий.
Информацией могут злоупотребить и восстановить твою личность.

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

не дай себя обмануть!

МИНИСТЕРСТВО ИНТЕРНАКТИКИ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единный
номер **102**

научись пользоваться интернетом правильно!

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*

**СОХРАНИ
ИНФОРМАЦИЮ**



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

У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ

ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА

ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ

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

ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ

ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ

НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ

НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ

- 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

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 ☎

Позвонили маме
с неизвестного
номера

2 👨‍👩‍👧

Вспышка
привлечения
внимания
родственников

3 🚗

Сказали, что
нужно срочно
перезвонить
родственнику

4 📄

Сказали, что
нужно срочно
перезвонить
родственнику

5 🧑

Сказали, что
нужно срочно
перезвонить
родственнику

6 📞

Сказали, что
нужно срочно
перезвонить
родственнику

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 ВНЕШНИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102

БУДЬ КИБЕРГЕРОЕМ!



Будь как ниндзя!
Не сообщай незнакомым людям в
Интернете свое настоящее имя,
адрес и номер телефона.
Будь осторожен с тем, что
пишешь о себе.



Придумай сложный
пароль, как у супергероя!
Никому его не говори, ведь
это твой секретный
ключ!

Помни, что в Интернете не все
те, кем кажутся!
Не добавляй в друзья людей,
которых не знаешь в реальной
жизни.



Будь как хакер!
Не кликай на
подозрительные
ссылки.



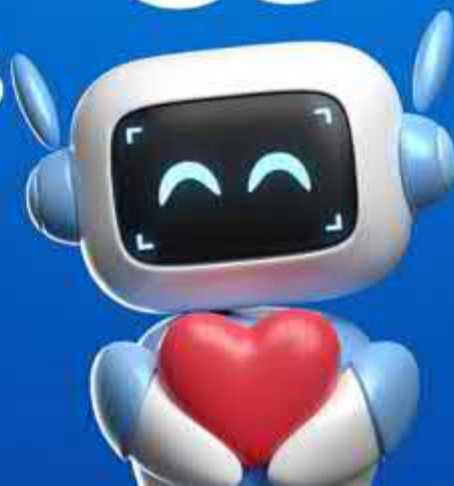
Будь осторожен, как на
минном поле!
Скачивай приложения только
из официальных магазинов.
Антивирус - твой верный
друг!



Не бойся просить о помощи!
Если тебя что-то тревожит в
Интернете, расскажи об этом
родителям или учителю.
Вместе вы сможете решить
любую проблему.



Интернет - это круто, но
помни о безопасности!
Соблюдая эти правила, ты
сможешь стать настоящим
кибергероем!



mvd.gov.by



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, 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



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 знакомишься 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

НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь



Главное управление по противодействию
изберпреступности МВД Республики Беларусь



**НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ**

10 правил безопасности в Интернете

Опасайся незнакомцев в Интернете.

Не все, что ты читаешь или видишь в Интернете, – правда, задавай вопросы родителям, уточняй.

Не делись своими личными данными и данными членов семьи (полное настоящее имя, адрес, район проживания, номер телефона, фото паспорта и прочие данные) в Интернете.

Ни в коем случае не встречайся с людьми, знакомство с которыми состоялось в Интернете, так как эти люди могут оказаться совсем не теми, за кого себя выдают.

Играя в онлайн-игры, соблюдай осторожность, не указывай реальные данные в профиле.

Соблюдай правила хорошего тона в Интернете, они ничем не отличаются от тех, которые действуют в реальном мире.

Не заходи на незнакомые сайты, не переходи по ссылкам, полученным в мессенджерах.

Не делай в Интернете того, что не сделал бы в реальной жизни.

Обязательно рассказывай взрослым о проблемах или подозрительных действиях в Интернете – они всегда помогут.

Помни: всё, что попадает в Интернет, там и остаётся (даже если было удалено).

РАСПИСАНИЕ ЗАНЯТИЙ

Понедельник

Вторник

Среда

Четверг

Пятница



«Учреждение К»
Министерство внутренних дел Республики Беларусь

MTE
Мультимедийное
www.mte-cyber.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



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>