

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>

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 SMS, 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 SMS, 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





МОШЕННИЧЕСТВО В INSTAGRAM



Купить технику по низким ценам



ПОКУПАЯ ТОВАРЫ В СОЦ. СЕТИ INSTAGRAM
ВЫ РИСКУЕТЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЯ

Схемы интернет-мошенников в социальной сети Instagram

А можно при получении оплатить?

19:27 ✓✓

Yarik

А можно при получении оплатить?

Мы не работаем с оплатой при
получении

19:27

У нас оплата производится сразу

19:27

ПРЕДОПЛАТА ЗА ТОВАР

Покупка товара по полной либо частичной
ПРЕДОПЛАТЕ приводит к потере
Ваших денежных средств.
Данная сделка ничем не гарантирована

Европочтой 08:44 ✓✓

13 октября

<https://evropochta.by/pay-delivery>

Оплачивайте доставку, после оплаты
сохраняйте чек

10:52

Пропущенный звонок

16:44

Отменяем заказ?

16:53

ОПЛАТА ДОСТАВКИ ПО ССЫЛКЕ

Злоумышленники, под предлогом оплаты
доставки отправляют ССЫЛКУ, где
необходимо ввести реквизиты карты.
В данном случае мошенники спишут все
денежные средства с вашего счёта

Признаки мошеннического интернет-магазина



ПРЕДОПЛАТА

Откажись от покупок
в интернете по предоплате!



ОЧЕНЬ НИЗКИЕ ЦЕНЫ

Цена занижена в несколько раз для
привлечения жертв преступления



ЗАКРЫТЫЕ КОММЕНТАРИИ

Мошенники закрывают
комментарии под публикациями!



ОБЩЕНИЕ В TELEGRAM

Для заказа товара Вас просят
перейти в мессенджер Telegram

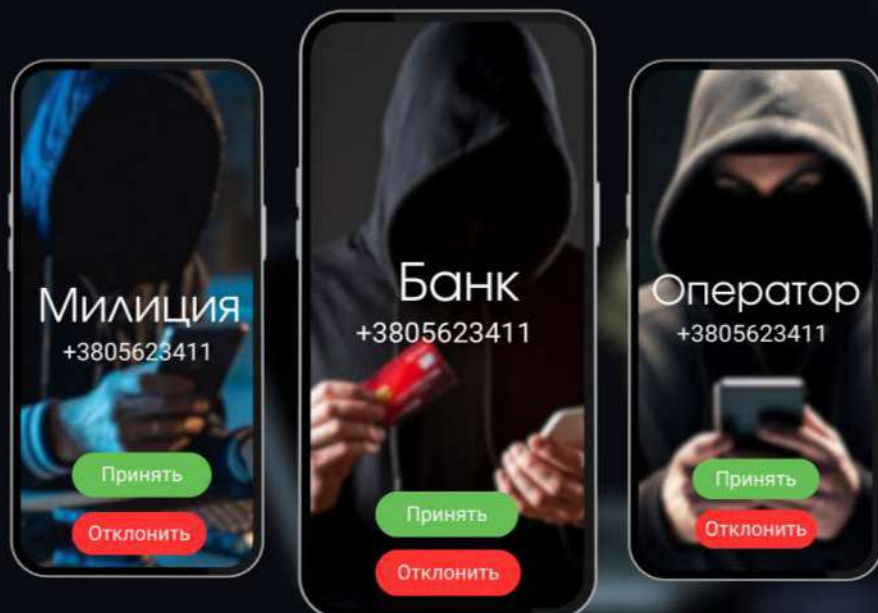


УВД Бобруйского горисполкома

г. Бобруйск, ул. Минская, 130А

МИЛИЦИЯ ПРЕДУПРЕЖДАЕТ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

Внимание! Мошенники
представляются **сотрудниками** !



Не выполняйте инструкции неизвестных
Вам людей! Будьте бдительны!

Мошенники убеждают!



ПЕРЕВЕДИТЕ ДЕНЬГИ



ВАМ ГРОЗИТ УГОЛОВНАЯ
ОТВЕТСТВЕННОСТЬ



УСТАНОВИТЕ ПРИЛОЖЕНИЕ



НА ВАШЕ ИМЯ
ОФОРМЛЕНА ЗАЯВКА



ЗАДЕКЛАРИРУЙТЕ
ДЕНЕЖНЫЕ СРЕДСТВА



НАЗОВИТЕ ПАСПОРТНЫЕ
ДАННЫЕ И СМС-КОД



ВОЗЬМИТЕ КРЕДИТ

🔍 НА ЧТО СТОИТ ОБРАТИТЬ ВНИМАНИЕ? ✕

СОТРУДНИКИ НЕ ЗВОНЯТ В МЕССЕНДЖЕРАХ!



Используя мессенджер, злоумышленникам проще ввести Вас в заблуждение!

ОБРАТИТЕ ВНИМАНИЕ НА АБОНЕНТСКИЙ НОМЕР!

+375

Абонентские номера в Республики Беларусь начинаются с кода-страны

СОТРУДНИКИ НЕ СПРАШИВАЮТ ВАШИ ДАННЫЕ!

Сотрудники владеют всей необходимой информацией без Вашей помощи!



УВД Бобруйского горисполкома

г. Бобруйск, ул. Минская, 130А

Десять правил безопасности для детей в интернете

1. Посещайте Сеть вместе с детьми, побуждайте их делиться опытом использования интернета.
2. Научите детей доверять интуиции – если их в интернете что-либо беспокоит, пусть сообщают вам.
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты.
4. Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки.
5. Объясните детям, что в интернете и реальной жизни разница между правильным и неправильным одинакова.
6. Детям никогда не следует встречаться с друзьями из интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают.
7. Скажите детям, что далеко не все, что они читают или видят в интернете, – правда, приучите их спрашивать вас, если они не уверены.
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает.
9. Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ – кража.
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде – даже в виртуальном мире.