

ВНИМАНИЕ!

ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!



НЕ СОВЕРШАЙТЕ НИКАКИХ ДЕЙСТВИЙ НА СМАРТФОНЕ ПО ПРОСЬБЕ ПОСТОРОННИХ ЛЮДЕЙ! ТЕМ БОЛЕЕ, НЕ СООБЩАЙТЕ ИМ КОДЫ, ПАРОЛИ, И ДРУГУЮ ИНФОРМАЦИЮ

НЕ СОХРАНЯЙТЕ В ПРИЛОЖЕНИЯХ И БРАУЗЕРАХ ПАРОЛИ, КОДЫ, ЛОГИНЫ. ПРЕСТУПНИК МОЖЕТ УЗНАТЬ КОД ИЗ ПРИСЛАННОГО SMS-СООБЩЕНИЯ



128 293 154

ПРЕСТУПНИК ПО ТЕЛЕФОНУ ПРОСИТ ВАС УСТАНОВИТЬ ПРОГРАММУ НА ТЕЛЕФОН ДЛЯ ДИСТАНЦИОННОГО ДОСТУПА И СООБЩИТЬ ЕМУ ПАРОЛЬ И КОД



УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

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

научись пользоваться интернетом правильно!

БЕЛАРУСЬ
ИНФОРМАЦІЮ



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
единный
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*

**СОХРАНИ
ИНФОРМАЦИЮ**



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 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**

ТЕЛЕФОННЫЕ МОШЕННИКИ

представляются работниками:

коммунальных служб

(энергонадзора, водоканала, газовой службы),

организаций связи (Белтелеком, Белпочта, МТС, А1),

правоохранительных органов и банков


продавцами, инвесторами, брокерами

ЗАПУГИВАЮТ ИЛИ ЗАВЛЕКАЮТ:

- ✓ ПОДОЗРЕНИЕМ В ПРЕСТУПЛЕНИИ, ПРОВЕДЕНИЕМ ОБЫСКА
- ✓ СЛОЖНОЙ СИТУАЦИЕЙ С РОДСТВЕННИКОМ
- ✓ БЫСТРЫМ ЗАРАБОТКОМ И ПОЛУЧЕНИЕМ ПРИБЫЛИ
- ✓ ОКОНЧАНИЕМ ДЕЙСТВИЯ ПРИБОРА УЧЕТА
- ✓ ОКОНЧАНИЕМ ДЕЙСТВИЯ ДОГОВОРА ИЛИ УСЛУГИ СВЯЗИ
- ✓ ДЕЙСТВИЕМ АКЦИЙ, СКИДОК, ПРОВЕДЕНИЕМ РОЗЫГРЫШЕЙ

УБЕЖДАЮТ:

- ✗ ОФОРМИТЬ «ВСТРЕЧНЫЙ» КРЕДИТ
- ✗ ПЕРЕВЕСТИ ДЕНЬГИ НА «БЕЗОПАСНЫЙ» СЧЕТ
- ✗ СООБЩИТЬ ЛИЧНЫЕ ДАННЫЕ И КОД ИЗ УВЕДОМЛЕНИЯ
- ✗ СКАЧАТЬ И УСТАНОВИТЬ ФАЙЛ ПРИЛОЖЕНИЯ (*.APK)
- ✗ ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР ИЛИ УСЛУГ
- ✗ ВНЕСТИ СУММУ НА СЧЕТ ДЛЯ НАЧАЛА ИНВЕСТИРОВАНИЯ

 **УБЕДИТЕСЬ В
ДОСТОВЕРНОСТИ
ЗВОНКА
ПО ДРУГИМ
КАНАЛАМ СВЯЗИ**



Главное управление
по противодействию
киберпреступности
МВД Республики Беларусь



ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с **неизвестного**
номера

2 

звонящий
предлагает
выдать
родственником

3 

он говорит,
что **сбил человека**
или **из-за него**
человек
попал в ДТП

4 

он просит денег
как **компенсацию**
вреда или
чтобы **закрыть дело**

5 

звоня звонит
милиционеру/
следователю
и подтверждает
легенду

6 

он **высылает**
привозит
курьер

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 ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**

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 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

**РОДИТЕЛИ!
научите детей
пользоваться
интернетом
правильно!**

**ГЛАВНЫЕ
ПРАВИЛА
ЦИФРОВОЙ
ГИГИЕНЫ**



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

не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**

ГЛАВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГМЕНЫ ДЛЯ ДЕТЕЙ

НЕ СООБЩАЙ ЛИЧНУЮ ИНФОРМАЦИЮ НЕЗНАКОМЦУ. И, ВОобще, В ИНТЕРНЕТЕ НЕ РАЗМЕЩАЙ СВЕДЕНИЯ О СЕБЕ И СЕМЬЕ

СОВЕТУЙСЯ С РОДИТЕЛЯМИ, КАК ПРАВИЛЬНО ПОСТУПИТЬ, ЕСЛИ СТОЛКНУЛСЯ С ЧЕМ-ТО НЕПОНЯТНЫМ ИЛИ ПУГАЮЩИМ

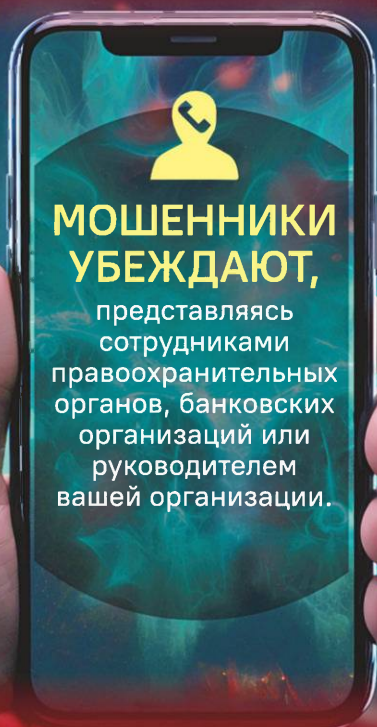
ПОМНИ, ЧТО В ИНТЕРНЕТЕ НАДО БЫТЬ ОЧЕНЬ-ОЧЕНЬ ВНИМАТЕЛЬНЫМ. СТАРАЙСЯ ИЗБЕГАТЬ ОБЩЕНИЯ С НЕЗНАКОМЫМИ ЛЮДЬМИ В ОНЛАЙН-ИГРАХ И СОЦСЕТАХ, НЕ ВЫПОЛНЯЙ БЕЗДУМНО ТО, ЧТО ОНИ ПОПРОСЯТ ТЕБЯ СДЕЛАТЬ



ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД



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
на сайте
<https://mvd.gov.by>



Главное управление
по противодействию киберпреступности
КМ МВД Республики Беларусь

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
киберпреступности МВД Республики Беларусь





НАУЧИТЕ

РОДИТЕЛЕЙ

**ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ**

Телефонные мошенники

ПРЕДСТАВЛЯЮТСЯ:



- сотрудниками гос. органов и банков
- продавцами, инвесторами, брокерами
- работниками служб связи (Белпочта, Белтелеком, А1, МТС)
- работниками коммунальных служб (энергонадзора, водоканала, газовой службы)

УГРОЖАЮТ И ЗАПУГИВАЮТ:

- подозрением в преступлении и проведением обыска
- сложной ситуацией с родственником
- окончанием действия прибора учета или услуги

УБЕЖДАЮТ И ЗАСТАВЛЯЮТ:

- под предлогом декларирования перевести деньги на “безопасный” счет
- внести предоплату за товар или взнос в инвестиционный проект
- передать личные данные и коды из сообщения, установить приложение



Не дайте себя обмануть!



Главное управление по противодействию киберпреступности
КМ МВД Республики Беларусь

Законные сделки с криптовалютой



Убедитесь, что Ваши сделки соответствуют действующему законодательству Республики Беларусь

Порядок осуществления сделок с криптовалютой определен Декретом Президента Республики Беларусь от 21 декабря 2017 г. №8 «О развитии цифровой экономики» и Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)»

В Республике Беларусь физическим лицам:

✓ РАЗРЕШЕНО

Добыча криптовалюты в результате майнинга
(как на территории Республики Беларусь, так и на территории иностранного государства)

Продажа (покупка) криптовалюты за денежные средства на белорусских криптоплатформах, являющихся резидентами Парка высоких технологий

Обмен криптовалюты на иные токены
(на белорусских и иностранных криптоплатформах)

Получение криптовалюты в дар или наследство

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
[CYBER_FORTRESS_BREST](#)



КИБЕРКРЕПОСТЬ

✗ ЗАПРЕЩЕНО

Продажа (покупка) криптовалюты за денежные средства на иностранных криптоплатформах

Продажа (покупка) криптовалюты за денежные средства напрямую между физическими лицами










Главное управление
по противодействию
киберпреступности

КМ МВД Республики Беларусь

ПОЛЬЗУЙТЕСЯ 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>

ВИРУСНЫЕ АРК-ФАЙЛЫ

Что такое АРК-вирус?

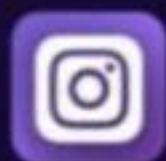
АРК-вирусы — это вредоносные программы, скрывающиеся в АРК-файлах, которые могут нанести ущерб вашему устройству и данным.

Твой профиль



Их мишень!

Где скрываются АРК-вирусы?



1. Социальные сети и мессенджеры
- Фальшивые версии популярных приложений.



2. Операторы сотовой связи
- Фальшивые версии приложений сотовых операторов.



3. Финансовые приложения
- Поддельные банковские приложения.



4. Медиаприложения
- Неофициальные загрузчики музыки и видео.



Как защитить себя?



- Скачивайте приложения только из официальных источников (Google Play, App Store).
- Проверяйте отзывы и рейтинги перед установкой.
- Используйте антивирусное ПО для защиты вашего устройства.
- Регулярно обновляйте систему и приложения для повышения безопасности.

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
CYBER_FORTRESS_BREST



КИБЕРКРЕПОСТЬ



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



МОШЕННИКИ И КОД ОТ ДОМОФОНА:



как
работает
новая
схема
обмана



Милиция Могилевщины



МОШЕННИКИ И КОД ОТ ДОМОФОНА:



как
работает
новая
схема
обмана



Милиция Могилевщины

ЧТО ПРОИСХОДИТ:



1 Аферисты звонят

представляются



2 сотрудниками компаний
по установке домофонов

3 предлагают бесплатную
замену ключей



Милиция Могилевщины

КРОМЕ ЭТОГО:



Под видом «плановой замены чипов» запрашивают личные данные человека. Если «клиент» соглашается, то следом они запрашивают код из SMS, который направляется якобы «от компании» и будет использован для открытия домофонной двери.



Позже с другого номера звонит лжеправоохранитель, сообщая о взломе системы, и под предлогом предотвращения мошенничества убеждает жертву сообщить личные данные и банковские реквизиты. Получив доступ к аккаунтам, злоумышленники могут оформлять кредиты и похищать деньги со счетов.

Милиция Могилевщины



- Жительница Могилева
поверила аферистам и лишилась
5000 рублей

РЕАЛЬНЫЕ СЛУЧАИ:



- Бобруйчанку "развели" по этой
схеме, как итог: у нее было
украдено также более
5000 рублей

Милиция Могилевщины

ЧТО ДЕЛАТЬ:



- **НИКОГДА НЕ СООБЩАЙТЕ** одноразовые SMS-коды посторонним;
- **СТОИТ ПОМНИТЬ, ЧТО СОТРУДНИКИ** правоохранительных органов, банковских и иных учреждений не связываются в мессенджере с просьбой о конфиденциальных данных;
- **ВАЖНО НЕЗАМЕДЛИТЕЛЬНО ПРЕКРАЩАТЬ** разговор с **НЕЗНАКОМЦЕМ;**
- **ОБРАЩАТЬСЯ К ПРЕДСТАВИТЕЛЯМ** банков, в государственные органы и учреждения только через официальные сайты и контактные телефоны, размещенные на них;
- **НЕ ПЕРЕХОДИТЬ ПО ПОДОЗРИТЕЛЬНЫМ** ссылкам и не скачивать приложения из неизвестных источников.



Милиция Могилевщины



БУДЬТЕ ОСТОРОЖНЫ!

Если незнакомцы по телефону требуют от Вас совершить какие-либо манипуляции с финансами (задекларировать, положить на безопасный счет и т.д.) - немедленно прекратите разговор

**И сообщите об этом
В милицию!**



Милиция Могилевщины

НОВАЯ



СХЕМА

ОБМАНА:

ШЛАГБАУМЫ И
"БЕСПЛАТНЫЕ" КЛЮЧИ



МИЛИЦИЯ МОГИЛЕВЩИНЫ

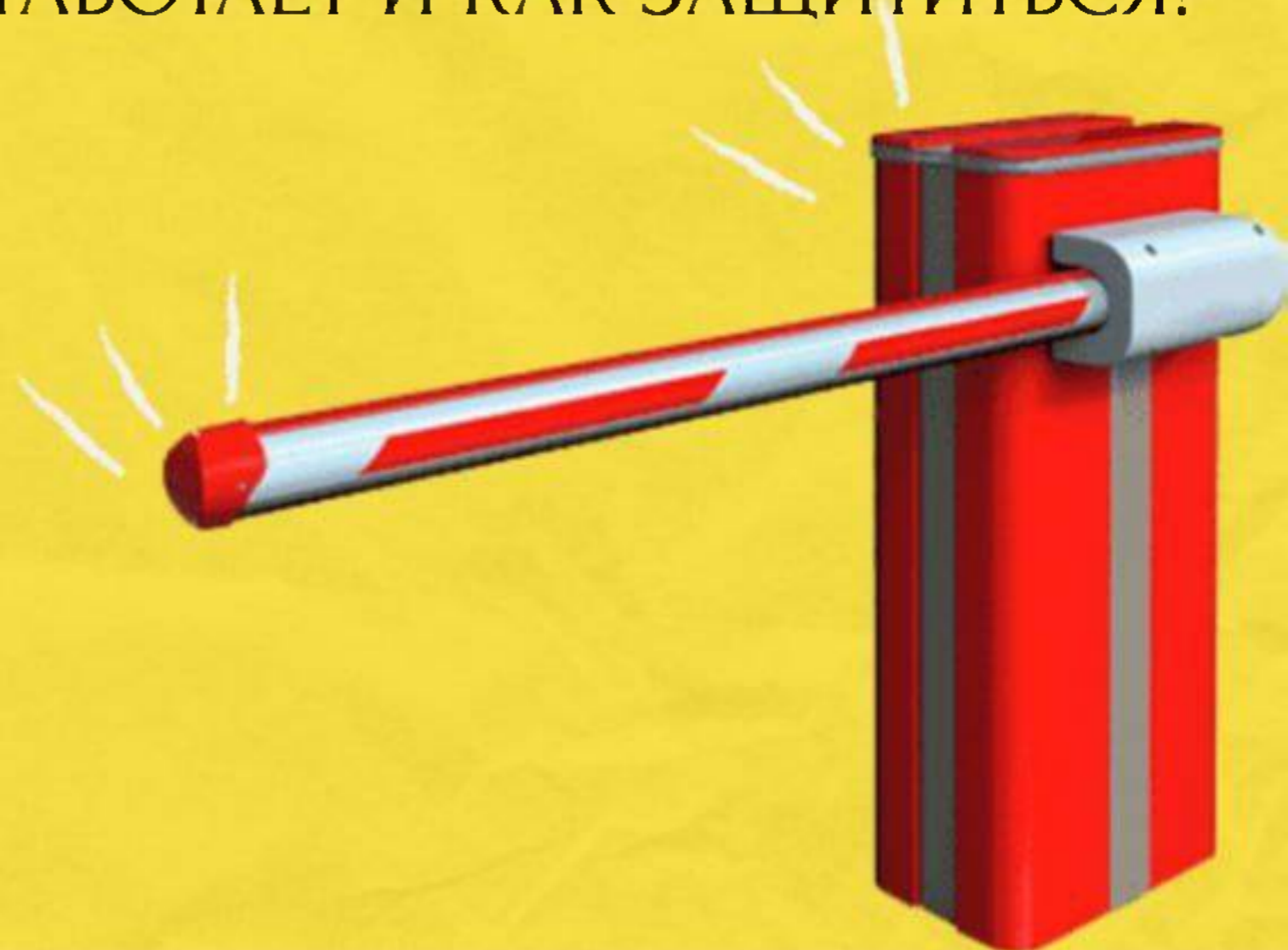
СВЕЖЖАЯ УЛОВКА:



ЗЛОУМЫШЛЕННИКИ НЕ СТОЯТ НА МЕСТЕ И ПРИДУМЫВАЮТ ВСЕ НОВЫЕ СПОСОБЫ "РАЗВОДА".

ОДИН ИЗ НИХ — ПОД ВИДОМ УСТАНОВКИ ШЛАГБАУМОВ ДЛЯ "БЕЗОПАСНОСТИ ДВОРА".

РАЗБИРАЕМСЯ, КАК ЭТО РАБОТАЕТ И КАК ЗАЩИТИТЬСЯ!



МИЛИЦИЯ МОГИЛЕВЩИНЫ

КАК ДЕЙСТВУЕТ СХЕМА?



ТЕЛЕФОННЫЕ МОШЕННИКИ МОГУТ ПРЕДСТАВЛЯТЬСЯ СОТРУДНИКАМИ УПРАВЛЯЮЩИХ КОМПАНИЙ ИЛИ ТОВАРИЩЕСТВА СОБСТВЕННИКОВ ЖИЛЬЯ



ОНИ ПРЕДЛАГАЮТ БЕСПЛАТНО ОФОРМИТЬ МАГНИТНЫЙ КЛЮЧ ИЛИ ЧИП ДЛЯ ШЛАГБАУМА, ЧТОБЫ "ОБЕСПЕЧИТЬ ПОРЯДОК". ПОТОМ ПРОСЯТ ПРОДИКТОВАТЬ КОД ИЗ SMS "ДЛЯ АКТИВАЦИИ". НА ДЕЛЕ ЭТО КОД ОТ ВАШЕГО БАНКА — И ЗЛОУМЫШЛЕННИКИ ПОЛУЧАЮТ ДОСТУП К СЧЕТУ!

МИЛИЦИЯ МОГИЛЕВЩИНЫ

ПОЧЕМУ ЭТО СРАБАТЫВАЕТ?



СХЕМА ОБЕЩАЕТ НЕ УГРОЗУ, А "ВЫГОДУ" —
БЕСПЛАТНЫЙ ДОСТУП И БЕЗОПАСНОСТЬ.
ЭТО СНИЖАЕТ БДИТЕЛЬНОСТЬ, И ЛЮДИ
ДЕЙСТВУЮТ, НЕ ПРОВЕРЯЯ. А ВЕДЬ
НАСТОЯЩИЕ ОРГАНИЗАЦИИ **НИКОГДА** НЕ
ЗАПРАШИВАЮТ КОДЫ SMS, ДАННЫЕ КАРТ
ИЛИ ПАСПОРТА ПО ТЕЛЕФОНУ!



МИЛИЦИЯ МОГИЛЕВЩИНЫ

ЧТО ВАЖНО ЗНАТЬ?



- РЕШЕНИЕ ОБ УСТАНОВКЕ ШЛАГБАУМА ПРИНИМАЕТСЯ ТОЛЬКО НА ОБЩЕМ СОБРАНИИ СОБСТВЕННИКОВ (С ПРОТОКОЛОМ).
- ПЛАТЕЖИ — СТРОГО ПО ОФИЦИАЛЬНЫМ РЕКВИЗИТАМ ЮРЛИЦА, А НЕ НА КАРТУ ЧАСТНОГО ЛИЦА.
- БАНКОВСКИЕ СИСТЕМЫ НЕ ПОМОГУТ, ЕСЛИ ВЫ САМИ ПРОДИКТУЕТЕ КОД.

ЧТО ДЕЛАТЬ ПРИ ТАКОМ ЗВОНКЕ?



- НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР!
- ПОЗВОНИТЕ В УК ПО НОМЕРУ С КВИТАНЦИИ ИЛИ С ОФИЦИАЛЬНОГО САЙТА — УТОЧНИТЕ, ПРОВОДИЛИСЬ ЛИ РАБОТЫ.
- ЕСЛИ КОД УЖЕ ЗАПРАШИВАЛИ, СООБЩИТЕ В БАНК (НОМЕР НА ОБОРОТЕ КАРТЫ).
- НИКОГДА НЕ ДИКТУЙТЕ КОДЫ ИЗ SMS ИЛИ ПУШ-УВЕДОМЛЕНИЙ!



МИЛИЦИЯ МОГИЛЕВЩИНЫ



БУДЬТЕ БДИТЕЛЬНО!

БОЛЬШИНСТВО ТАКИХ СХЕМ СНАЧАЛА
ТЕСТИРУЮТ В СОСЕДНИХ СТРАНАХ, А ПОТОМ
РЕАЛИЗУЮТ У НАС. УЧИТЕСЬ НА ЧУЖИХ
ОШИБКАХ, А НЕ НА СВОИХ!

ВЫ ВСЕГДА МОЖЕТЕ
ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ
ПО ТЕЛЕФОНУ **102**

МИЛИЦИЯ МОГИЛЕВЩИНЫ



НОВАЯ СХЕМА

ОБМАНА

СБОР ДАННЫХ
ШКОЛЬНИКОВ ЧЕРЕЗ
ФЕЙКОВЫЕ САЙТЫ С
ДОМАШНИМ ЗАДАНИЕМ

МИЛИЦИЯ МОГИЛЕВЩИНЫ

ЧТО ПРОИСХОДИТ?



ЗЛОУМЫШЛЕННИКИ В
СОСЕДНИХ СТРАНАХ
"ОБКАТЫВАЮТ" НОВЫЙ СПОСОБ
ОБМАНА.



ЗНАЙТЕ ЗАРАНЕЕ ОБ
ОЧЕРЕДНОМ "РАЗВОДЕ",
КОТОРЫЙ МОЖЕТ
ПОЯВИТЬСЯ И У НАС



МИЛИЦИЯ МОГИЛЕВЩИНЫ





САЙТЫ С “ДОМАШКОЙ”

ПОЯВИЛИСЬ СОТНИ
САЙТОВ С ОДИНАКОВЫМ
КОНТЕНТОМ,
МАСКИРУЮЩИХСЯ ПОД
РЕСУРСЫ С “ГОТОВЫМИ
ДОМАШНИМИ
ЗАДАНИЯМИ”.



ОНИ ИСПОЛЬЗУЮТСЯ ДЛЯ СБОРА
НОМЕРОВ И ДАННЫХ ОБ
УЧЕНИКАХ УЧЕБНЫХ ЗАВЕДЕНИЙ.

МИЛИЦИЯ МОГИЛЕВЩИНЫ





ЦЕЛЬ МОШЕННИКОВ:

ЗАПОЛУЧИВ ИХ, АФЕРИСТЫ МОГУТ В ТОМ ЧИСЛЕ "РАЗВОДИТЬ" ДЕТЕЙ НА ТО, ЧТОБЫ ОНИ ПОДЕЛИЛИСЬ ЛИЧНОЙ ИНФОРМАЦИЕЙ О РОДИТЕЛЯХ - КАРТОЧКИ, CVV КОД И ТД

eeee

КАК РАБОТАЕТ СХЕМА ПОСЛЕ СБОРА ДАННЫХ?

"ПРОЗВОН" ОТ ШКОЛЫ: МОШЕННИКИ СОВЕРШАЮТ ЗВОНОК, ПРЕДСТАВЛЯЯСЬ ДИРЕКТОРОМ ШКОЛЫ.

ПОЛУЧЕНИЕ ДАННЫХ: ПОД ПРЕДЛОГОМ, НАПРИМЕР, РЕГИСТРАЦИИ В ЭЛЕКТРОННОМ ДНЕВНИКЕ ОНИ ПЫТАЮТСЯ ПОЛУЧИТЬ КОД ИЗ SMS ИЛИ ДРУГУЮ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ.

МИЛИЦИЯ МОГИЛЕВЩИНЫ





ЧТО ДЕЛАТЬ:

✧ ✧ ✧ ОБЪЯСНИТЕ СВОИМ ДЕТЯМ, ЧТО
НЕЛЬЗЯ ПЕРЕДАВАТЬ ЛИЧНЫЕ ДАННЫЕ
ПОСТОРОННИМ ИЛИ ВВОДИТЬ ИХ НА
НЕЗНАКОМЫХ САЙТАХ

✧ ✧ ✧ В СЛУЧАЕ ТАКИХ ЗВОНКОВ,
НЕОБХОДИМО ПРЕРВАТЬ РАЗГОВОР
И РАССКАЗАТЬ О НЕМ ВЗРОСЛЫМ
РОДСТВЕННИКАМ/УЧИТЕЛЮ

ДОВЕРИТЕЛЬНО РАЗГОВАРИВАЙТЕ
СО СВОИМИ СЫНОВЬЯМИ И
ДОЧКАМИ!



МИЛИЦИЯ МОГИЛЕВЩИНЫ





БУДЬТЕ ОСТОРОЖНЫ!

ПОМНИТЕ: ВЫ ВСЕГДА
МОЖЕТЕ ОБРАТИТЬСЯ
ЗА ПОМОЩЬЮ В
МИЛИЦИЮ ПО
ТЕЛЕФОНУ 102!



МИЛИЦИЯ МОГИЛЕВЩИНЫ



МОШЕННИКИ:

ЭТО НУЖНО ЗНАТЬ



Милиция Могилевщины





ВАЖНО!

ТИПИЧНАЯ СХЕМА:



КАК ОБМАНЫВАЮТ

- На городской телефон (часто пожилым людям) поступает звонок — в трубке слышны плач и крики, якобы родственник (дочь, сын, внук, невестка и т. д.) сообщает, что по его/её вине произошло ДТП. Разговор происходит на эмоциях и стрессе.

Милиция Могилевщины



ОБЫЧНО

- Потом лжеследователь информирует, что в аварии есть пострадавшие, а виновнику грозит уголовное дело. Чтобы избежать наказания, необходимо срочно передать деньги для «улаживания» ситуации.

Милиция Могилевщины



КАК ЗАБИРАЮТ ДЕНЬГИ

ЧАЩЕ ВСЕГО

- Мошенники просят жертв собрать нужную сумму в пакет или сумку и передать их курьеру, который скоро приедет. При этом они удерживают жертву на линии, запрещая прерывать разговор. Курьерами же становятся обычные люди, ищущие подработку, такие как таксисты и студенты. Их задача — забрать деньги и либо перевести их на указанный счет, либо передать куратору.



Милиция Могилевщины



ЧТО ДЕЛАТЬ?

ОБЯЗАТЕЛЬНО

- Если вам поступил подобный звонок, сразу прекратите разговор и перезванивайте родственнику, который якобы попал в ДТП. О попытке мошенничества незамедлительно сообщите в милицию.

Курьеры телефонных мошенников несут уголовную ответственность наравне с организаторами схемы и обязаны возместить ущерб потерпевшим.

Милиция Могилевщины

Новая схема!



@UVDMOGILEV

NFC- ОБМАН:

*Всё, что нужно знать,
чтобы не потерять
свои деньги*

Милиция Могилевщины

Наш телеграм: @uvdmogilev

КАК МОШЕННИКИ ПОХИЩАЮТ ДАННЫЕ ВАШЕЙ КАРТЫ?



** Это новая и опасная схема,
использующая технологию NFC
(Беспроводная передача данных на
коротком расстоянии).*



**ИЗНАЧАЛЬНО ЖЕРТВЕ
ПОСТУПАЕТ ЗВОНОК ОТ ЯКОБЫ
СОТРУДНИКОВ БАНКА ИЛИ
ПРАВООХРАНИТЕЛЬНЫХ
ОРГАНОВ**

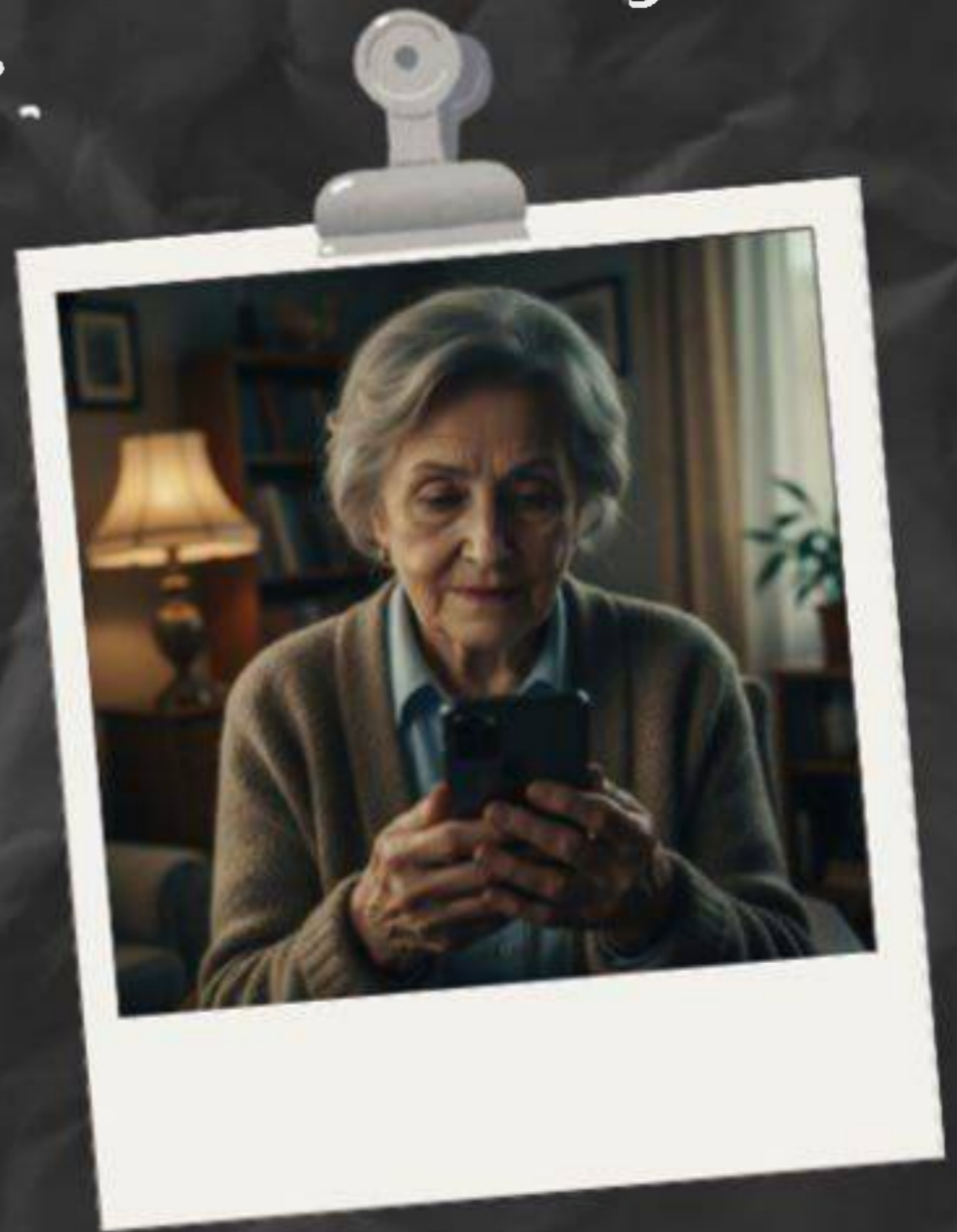
Милиция Могилевщины
Наш телеграм: @uvdmogilev

ЧТО ДАЛЬШЕ?



* Мошенники сообщают о
"подозрительных транзакциях" и
предлагают установить специальное
приложение на смартфон в качестве
"защиты". Они присылают ссылку для
скачивания.

✧
✧
**ЭТО
ОБМАН!**



Милиция Могилевщины
Наш телеграм: @uvdmogilev

КЛЮЧЕВОЙ ШАГ:



* Приложение требует, чтобы жертва приложила свою карту к телефону и ввела ПИН-код. Мошенники убеждают, что это безопасно, так как карта остается у владельца.



**ОДНАКО ТАК
ДЕЛАТЬ
НЕЛЬЗЯ!**

Милиция Могилевщины
Наш телеграм: @uvdmogilev

КРАЖЖА:



На самом деле, приложение считывает данные карты через NFC и передает их преступнику. Получив их, аферист прикладывает своё устройство к банкомату и снимает ваши деньги.

**БУДЬТЕ
БДИТЕЛЬНЫ!**

Милиция Могилевщины
Наш телеграм: @uvdmogilev

КАК

ЗАЩИТИТЬСЯ?



* Следуйте этим простым, но жизненно важным правилам, чтобы обезопасить себя и свои финансы:

НЕ УСТАНАВЛИВАЙТЕ ПРИЛОЖЕНИЯ ПО ССЫЛКАМ ИЗ СООБЩЕНИЙ, SMS ИЛИ МЕССЕНДЖЕРОВ. СКАЧИВАЙТЕ ТОЛЬКО ИЗ ОФИЦИАЛЬНЫХ МАГАЗИНОВ: APP STORE / GOOGLE PLAY.

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ ИЗ МЕССЕНДЖЕРОВ.

Милиция Могилевщины
Наш телеграм: @uvdmogilev

КАК ЗАЩИТИТЬСЯ?



✦ ✦ УСТАНОВИТЕ И РЕГУЛЯРНО
ОБНОВЛЯЙТЕ АНТИВИРУС НА ТЕЛЕФОНЕ.

✦ ✦ ВКЛЮЧИТЕ SMS ИЛИ
PUSH-УВЕДОМЛЕНИЯ О
ТРАНЗАКЦИЯХ. ЭТО
ПОМОЖЕТ ОПЕРАТИВНО
ОТРЕАГИРОВАТЬ!

*Не дайте себя
"развесить!"*



Милиция Могилевщины
Наш телеграм: @uvdmogilev



ПОМНИТЕ ГЛАВНОЕ ПРАВИЛО:



* Ни милиция, ни Банк **НИКОГДА**
не будут просить вас установить
приложение, ввести ПИН-код,
"проверить операции" таким
способом.

**ЕСЛИ ВАМ ПРЕДЛАГАЮТ ЧТО-ТО
ПОДОБНОЕ – СРАЗУ КЛАДИТЕ ТРУБКУ!
И ПОМНИТЕ: ВЫ ВСЕГДА МОЖЕТЕ
ОБРАТИТЬСЯ ЗА ПОМОЩЬЮ ПО
ТЕЛЕФОНУ 102**

Милиция Могилевщины
Наш телеграм: @uvdmogilev



ТОП-5

ПРИЗНАКОВ

что вас точно обманут в

Instagram



Милиция
Могилевщины



СЛИШКОМ ВЫГОДНЫЕ ПРЕДЛОЖЕНИЯ



Если кто-то предлагает
вам невероятные скидки
или подарки, которые
выглядят слишком хорошо,
чтобы быть правдой,
будьте осторожны!

Мошенники часто
используют заманчивые
предложения, чтобы
привлечь внимание.



Милиция
Могилевщины



НЕОБЫЧНЫЕ

АККАУНТЫ

Обратите внимание на аккаунты с низким/высоким количеством подписчиков, отсутствием публикаций или странными именами.

Часто это **признаки фейковых страниц**, созданных для обмана.



Милиция
Могилевщины



Если кто-то просит вас предоставить личные данные, такие как идентификационный номер паспорта, CVV код банковской карточки – это явный знак опасности. Настоящие компании никогда не будут запрашивать такую информацию через прямые сообщения.

ЗАПРОСЫ ЛИЧНОЙ ИНФОРМАЦИИ

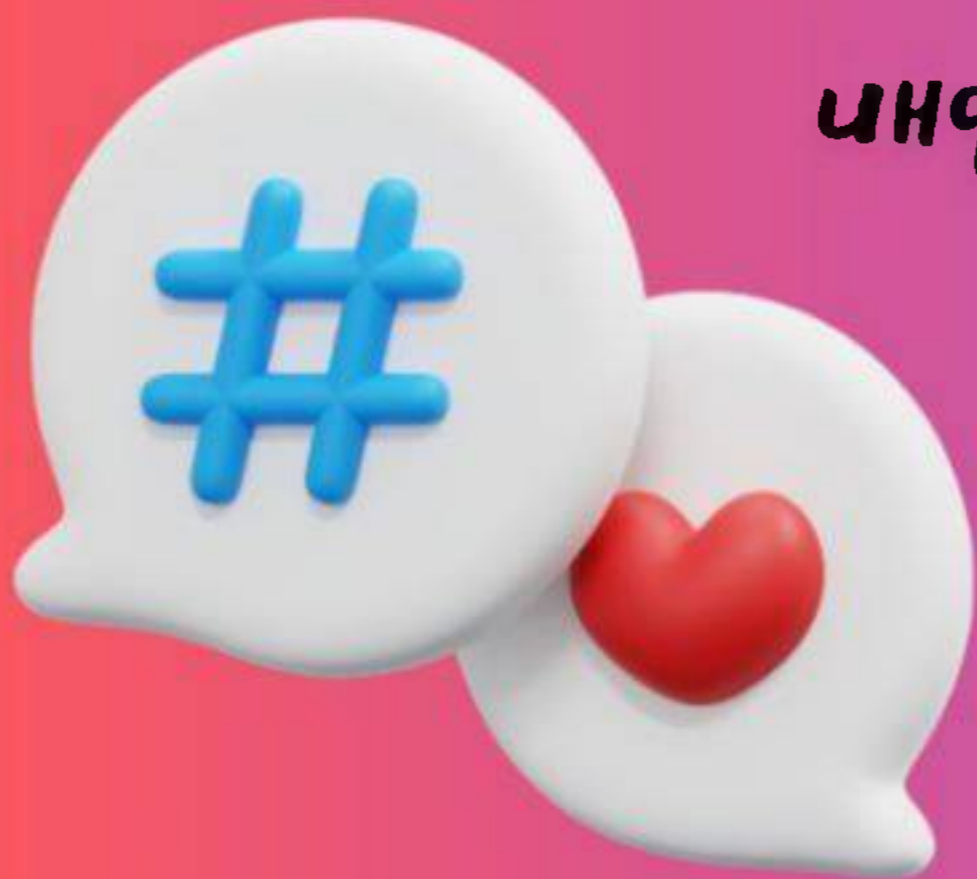
Милиция
Могилевщины





СРОЧНЫЕ ДЕЙСТВИЯ

Мошенники часто создают **искусственное** чувство срочности, заставляя вас действовать быстро. Если вам говорят, что предложение ограничено по времени, не спешите — лучше проверьте информацию.



Милиция
Могилевщины



НЕПРАВДОПОДОБНЫЕ ОТЗЫВЫ

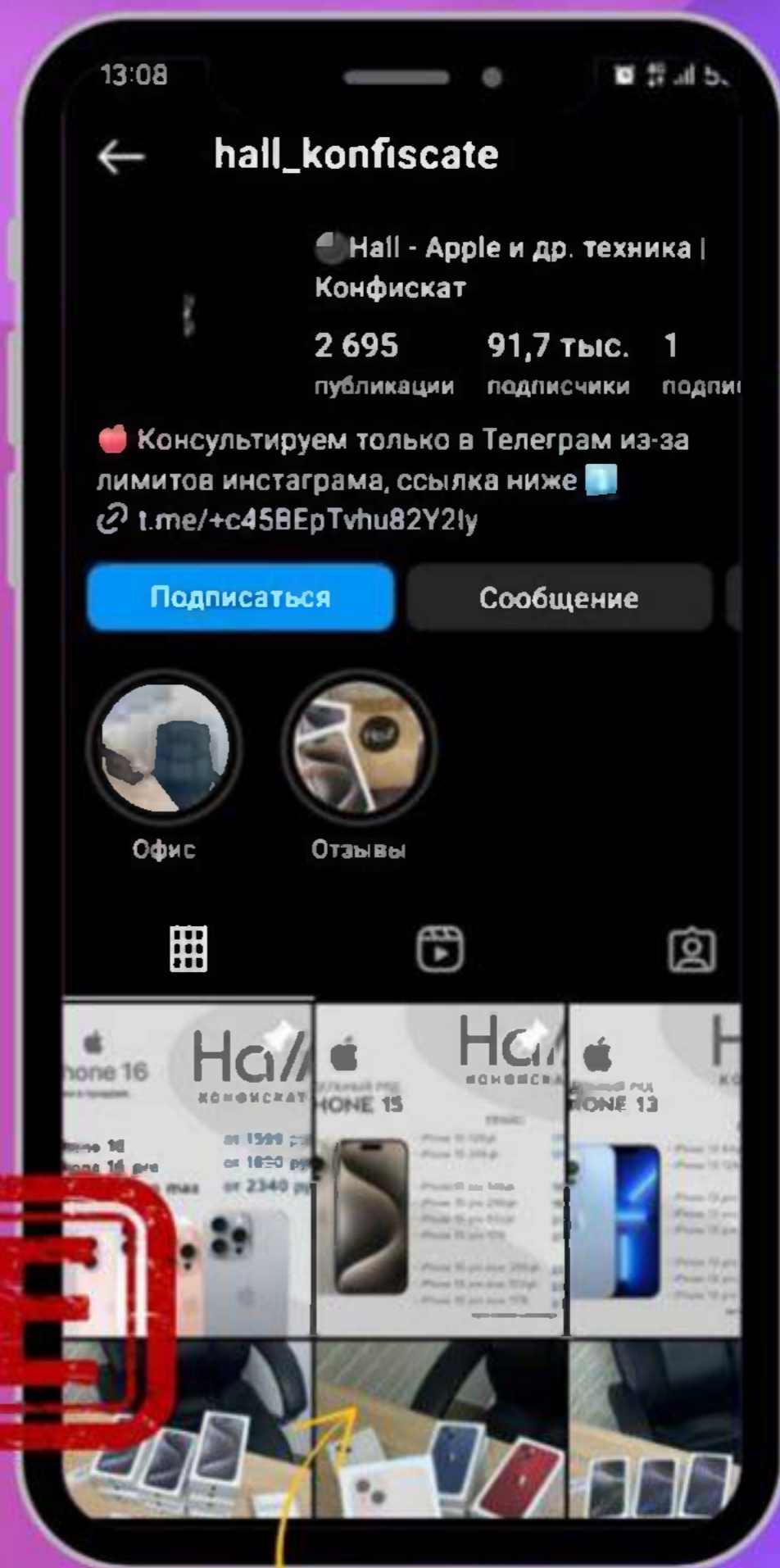
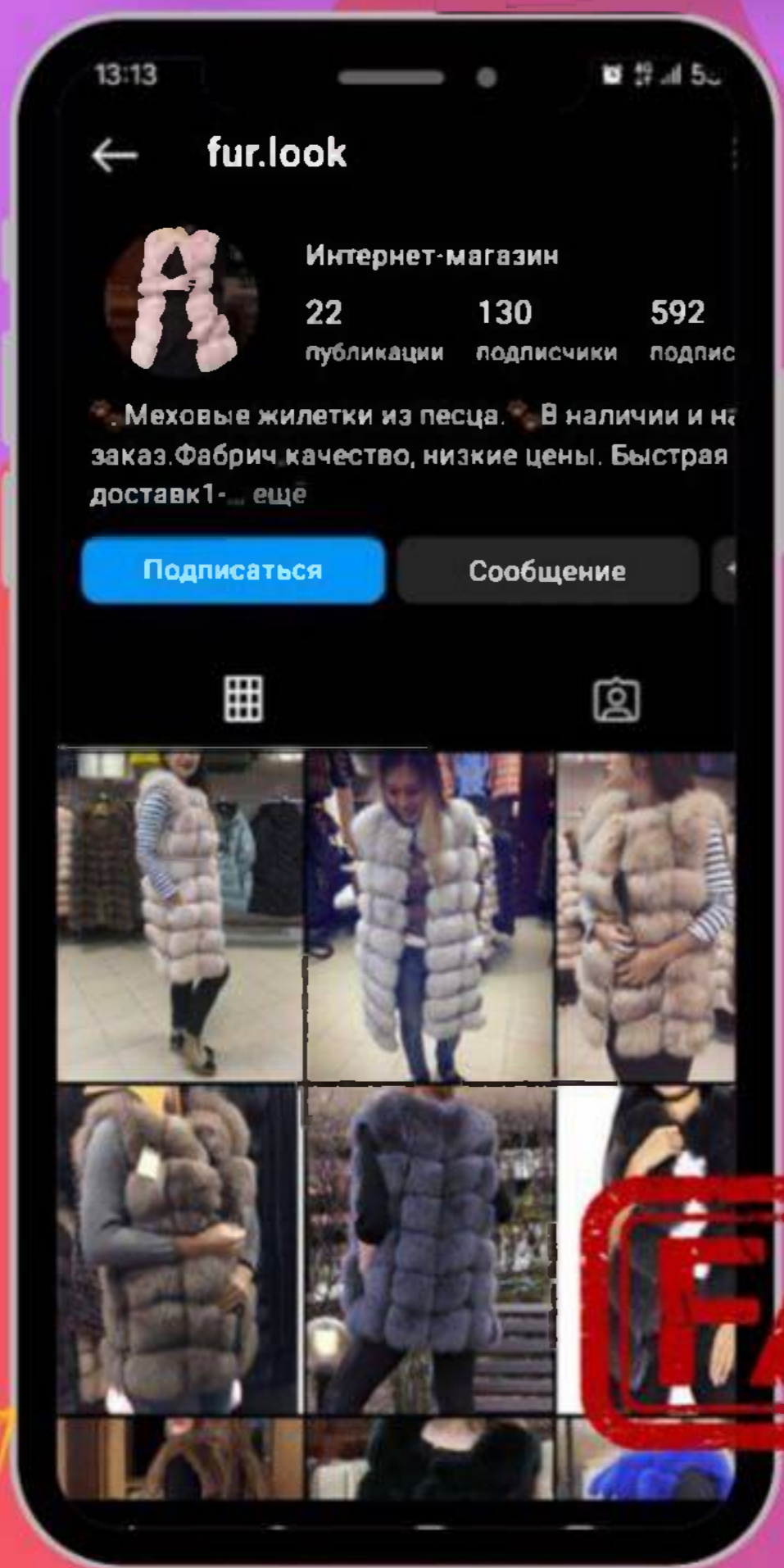
Если вы видите много положительных отзывов, но они выглядят слишком шаблонно или повторяются, **это может быть признаком подделанных комментариев.** Настоящие отзывы реальных пользователей всегда будут разнообразными и искренними.

Милиция
Могилевщины





ПРИМЕРЫ ФАЛЬШИВЫХ АККАУНТОВ



FAKE

ОДЕЖДА

Милиция
Могилевщины

ТЕХНИКА

БАНКОВСКАЯ



БЕЗОПАСНОСТЬ



ПО ВОЗМОЖНОСТИ ОФОРМИТЕ ОТДЕЛЬНУЮ ДЕБЕТОВУЮ КАРТУ ДЛЯ ОНЛАЙН-ОПЛАТЫ И ДЕРЖИТЕ НА НЕЙ МИНИМАЛЬНУЮ СУММУ.



ПИН-КОД: НИКОГДА НЕ ХРАНИТЕ ЕГО РЯДОМ С КАРТОЙ И НЕ ЗАПИСЫВАЙТЕ.



УСТАНОВИТЕ НИЗКИЕ ЛИМИТЫ НА СНЯТИЕ НАЛИЧНЫХ И ОНЛАЙН-ОПЕРАЦИИ.



МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV



ONLINE

ОБЪЯВЛЕНИЯ

ПОЖИЛЫХ



Как защитить бабушек и дедушек от мошенников

МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

ВАЖНО



ЗНАТЬ

В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ НАШИ САМЫЕ УЯЗВИМЫЕ РОДСТВЕННИКИ — ПОЖИЛЫЕ ЛЮДИ — ЧАСТО ЯВЛЯЮТСЯ ГЛАВНОЙ МИШЕНЬЮ КИБЕРМОШЕННИКОВ. СХЕМЫ СТАНОВЯТСЯ ВСЁ ИЗОЩРЕННЕЕ: ЗВОНКИ "ИЗ БАНКА", "ПОМОЩЬ" С ИНВЕСТИЦИЯМИ, ФЕЙКОВЫЕ КОМПЕНСАЦИИ.



Наша задача — защитить их. Сохраните и отправьте эту памятку своим родителям, бабушкам и дедушкам! Любо расскажите им эти правила сами.

МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

ПРАВИЛО



*"ПОЛОЖИТЕ ТРУБКУ
И ПЕРЕЗВОНИТЕ"*



ВСЕГДА

СОМНЕВАЙТЕСЬ В СРОЧНЫХ ЗВОНКАХ. МОШЕННИКИ ДАВЯТ НА ПАНИКУ ("ВАШ СЧЁТ АРЕСТОВАН", "СЫН ПОПАЛ В ДТП").

НИКОГДА

НЕ НАЗЫВАЙТЕ ПО ТЕЛЕФОНУ: ПИН-КОД, CVV-КОД, ПАРОЛИ И КОДЫ ИЗ СМС. СОТРУДНИКИ БАНКА ИХ НЕ СПРАШИВАЮТ!

*Спросите ФИО звонящего и положите трубку.
Сразу же перезвоните в официальный Банк или в
милицию по известному вам номеру (указанному
на карте или официальном сайте).*

— МИЛИЦИЯ МОГИЛЕВЩИНЫ —

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

ПРОВЕРЯЙТЕ



ССЫЛКИ И САЙТЫ

ОБЪЯСНИТЕ, ЧТО АДРЕС ЛЕГАЛЬНОГО САЙТА БАНКА ИЛИ ГОСУСЛУГ НАЧИНАЕТСЯ С HTTPS:// И ИМЕЕТ ЗНАЧОК ЗАМОЧКА СЛЕВА.

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ И НЕ СКАЧИВАЙТЕ ВЛОЖЕНИЯ ИЗ ПИСЕМ ОТ НЕИЗВЕСТНЫХ ОТПРАВИТЕЛЕЙ. ЕСЛИ ПИШУТ ОТ ИМЕНИ ГОСОРГАНА — ПОЗВОНИТЕ ТУДА И УТОЧНИТЕ ИНФОРМАЦИЮ.

ОСОБОЕ ВНИМАНИЕ К АКЦИЯМ: «ВЫ ВЫИГРАЛИ ПРИЗ!» — 99% ТАКИХ СООБЩЕНИЙ ВЕДУТ НА ФИШИНГОВЫЕ САЙТЫ.



МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

БАНКОВСКАЯ



БЕЗОПАСНОСТЬ



ПО ВОЗМОЖНОСТИ ОФОРМИТЕ ОТДЕЛЬНУЮ ДЕБЕТОВУЮ КАРТУ ДЛЯ ОНЛАЙН-ОПЛАТЫ И ДЕРЖИТЕ НА НЕЙ МИНИМАЛЬНУЮ СУММУ.



ПИН-КОД: НИКОГДА НЕ ХРАНИТЕ ЕГО РЯДОМ С КАРТОЙ И НЕ ЗАПИСЫВАЙТЕ.



УСТАНОВИТЕ НИЗКИЕ ЛИМИТЫ НА СНЯТИЕ НАЛИЧНЫХ И ОНЛАЙН-ОПЕРАЦИИ.



— МИЛИЦИЯ МОГИЛЕВЩИНЫ —

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

СЕМЕЙНЫЙ



КОНТРОЛЬ



**ПОМОГИТЕ ПОЖИЛОМУ ЧЕЛОВЕКУ
УСТАНОВИТЬ НАДЕЖНЫЙ
АНТИВИРУС НА КОМПЬЮТЕР ИЛИ
СМАРТФОН.**



**НАСТРОЙТЕ ДВУХФАКТОРНУЮ
АУТЕНТИФИКАЦИЮ (2FA): ВКЛЮЧИТЕ ЭТУ
ФУНКЦИЮ ВЕЗДЕ, ГДЕ ЭТО ВОЗМОЖНО
(СОЦСЕТИ, ПОЧТА, БАНКИ). ЭТО УСЛОЖНИТ
ВЗЛОМ.**



МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV



БУДЬТЕ

БДИТЕЛЬНЫ!

**РЕГУЛЯРНО ГОВОРИТЕ СО СВОИМИ ПОЖИЛЫМИ
РОДСТВЕННИКАМИ О НОВЫХ ВИДАХ МОШЕННИЧЕСТВА.
ЕСЛИ У НИХ ВОЗНИКЛИ СОМНЕНИЯ — ПУСТЬ ЗВОНЯТ
ВАМ, А НЕ ЗЛОУМЫШЛЕННИКАМ!**

*Помните: вы всегда можете
обратиться за помощью по телефону*

102!

МИЛИЦИЯ МОГИЛЕВЩИНЫ

НАШ ТЕЛЕГРАМ: @UVDMOGILEV

Как не превратить iPhone в «кирпич»

Мошенники используют различные уловки, чтобы заблокировать ваше устройство, вынуждая войти в их учётную запись Apple (iCloud)

Основные схемы обмана

- ✗ **«Помощь с файлами»**
Ссылаясь на «неисправное устройство», просят помощи в доступе к файлам (фотографиям, документам и т.д.) из облачного хранилища iCloud путем авторизации в мошеннической учётной записи
- ✗ **«Бесплатные игры и приложения»**
Рекламируют доступ к играм («PUBG Mobile», «Standoff 2») и приложениям («AioGram») в TikTok или Telegram, предлагая установить их через предоставленный аккаунт Apple
- ✗ **«Работа/подработка»**
Обещают вакансию (часто связанную с тестированием приложений), но требуют входа в «корпоративный» аккаунт Apple

Как защитить себя

- ✓ не сообщайте никому свои учётные данные (логин и пароль) от аккаунта Apple (iCloud)
- ✓ не входите на своём мобильном устройстве в аккаунт Apple (iCloud), предоставленный незнакомцами из Интернета
- ✓ не переходите по неизвестным ссылкам и не вводите данные Apple ID на посторонних сайтах

ВАЖНО!

Если ваш аккаунт заблокирован мошенником, сервисные центры не помогут. Разблокировка возможна только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
CYBER_FORTRESS_BREST



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь

КИБЕРОХОТА за несовершеннолетними

1

Мошенники звонят от лица милиции или других служб, сообщая о "чрезвычайной ситуации", и убеждают детей передать деньги родителей.

2

Злоумышленники создают фальшивые акции и розыгрыши в онлайн-играх, просят ввести данные банковских карт для получения "призов" или предлагают купить игровую валюту.

3

Аферисты убеждают установить программы удаленного доступа, получая контроль над смартфонами родителей и их банковскими приложениями.



БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
[CYBER_FORTRESS_BREST](https://t.me/CYBER_FORTRESS_BREST)



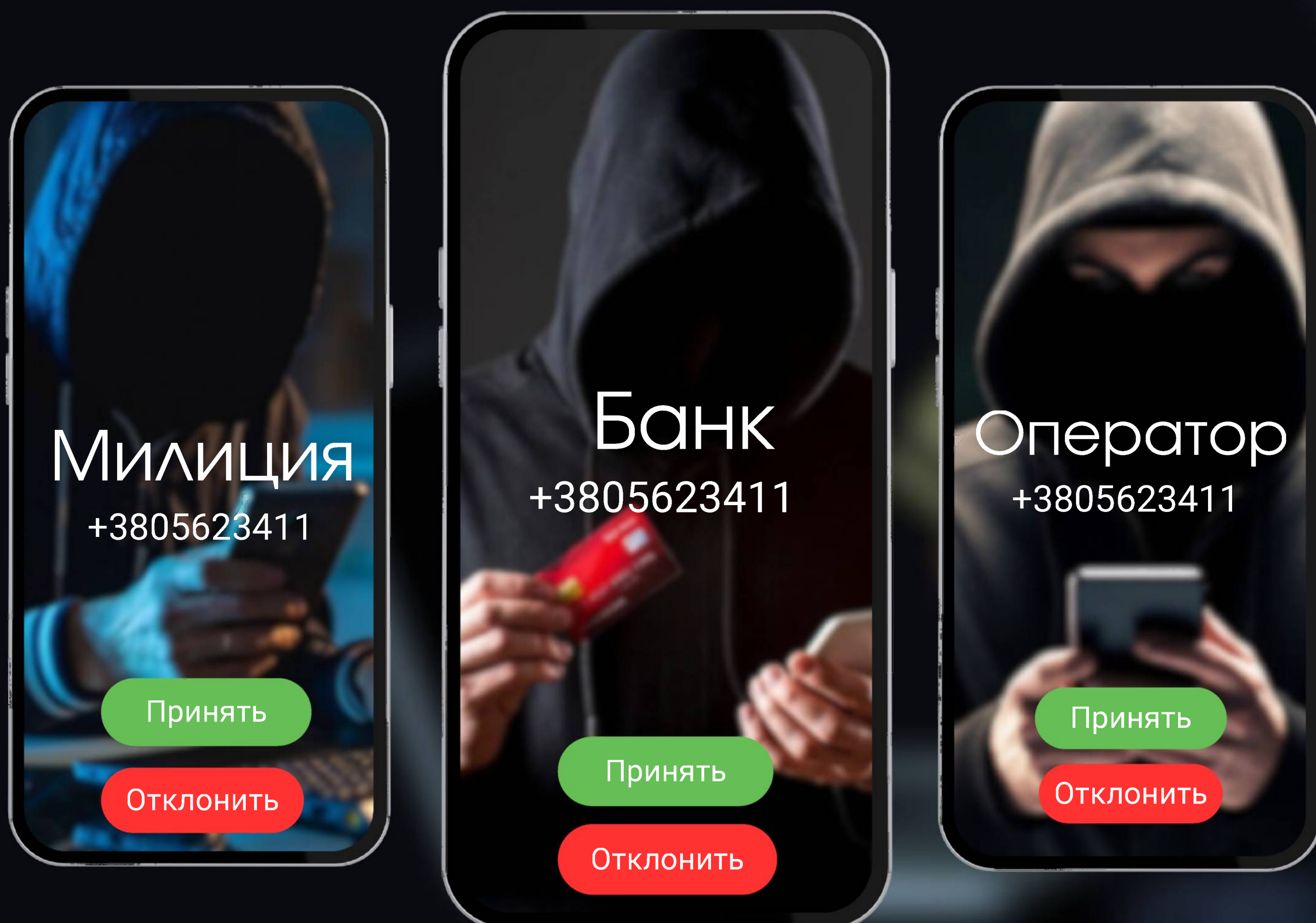
КИБЕРКРЕПОСТЬ



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь

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

МИЛИЦИЯ ПРЕДУПРЕЖДАЕТ! УЧАСТИЛИСЬ СЛУЧАИ МОШЕННИЧЕСТВА В СОЦ. СЕТИ **INSTAGRAM**



🔍 Купить технику по низким ценам ✕

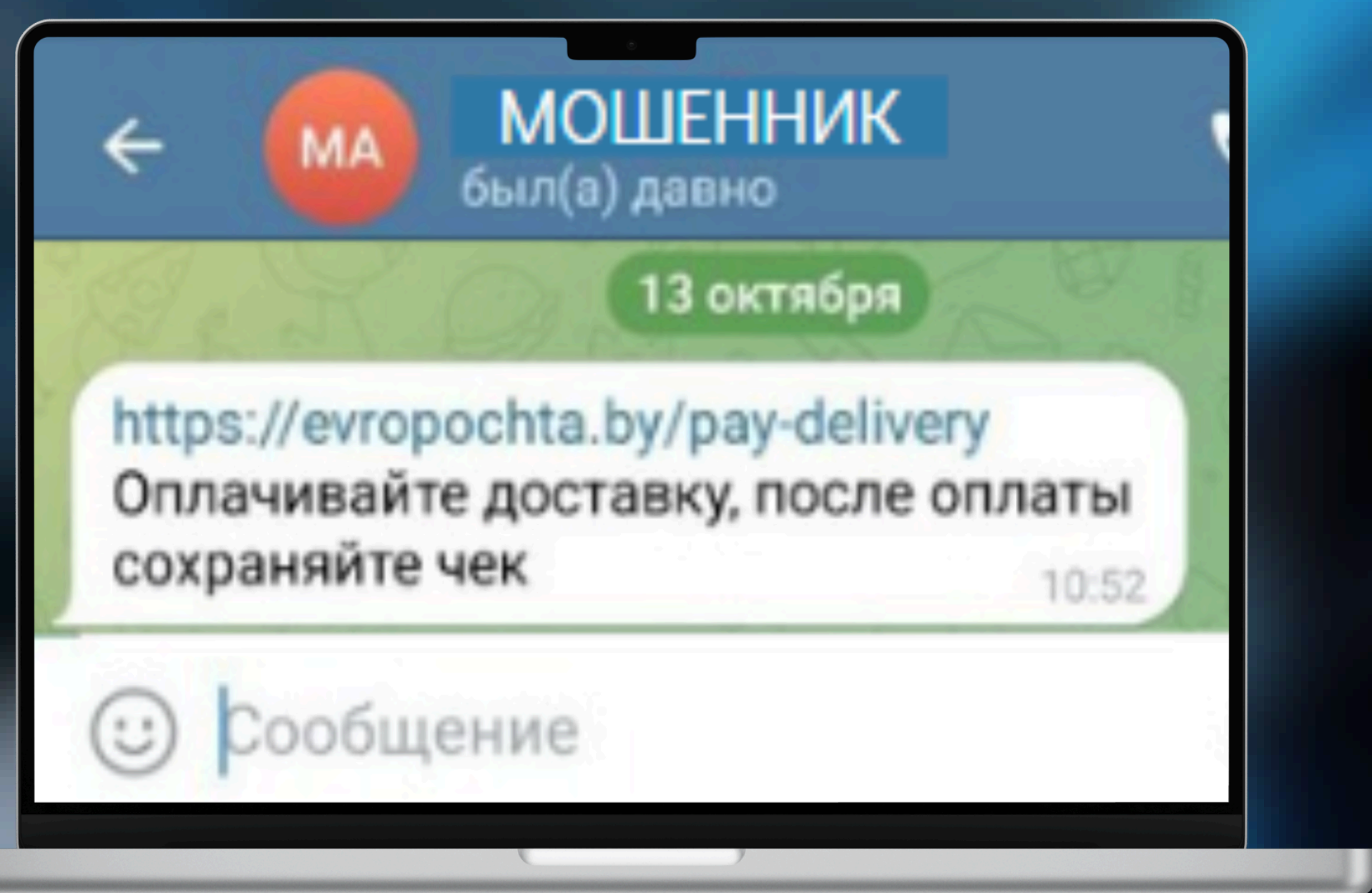
ПОКУПАЯ ТОВАРЫ В СОЦ. СЕТИ INSTAGRAM
ВЫ РИСКУЕТЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЯ

Схемы интернет-мошенников в социальной сети Instagram



ПРЕДОПЛАТА ЗА ТОВАР

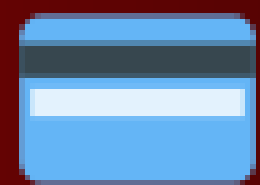
Покупка товара по полной либо частичной
ПРЕДОПЛАТЕ приводит к потере
Ваших денежных средств.
Данная сделка ничем не гарантирована



ОПЛАТА ДОСТАВКИ ПО ССЫЛКЕ

Злоумышленники, под предлогом оплаты д
оставки отправляют **ФИШИНГОВУЮ 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