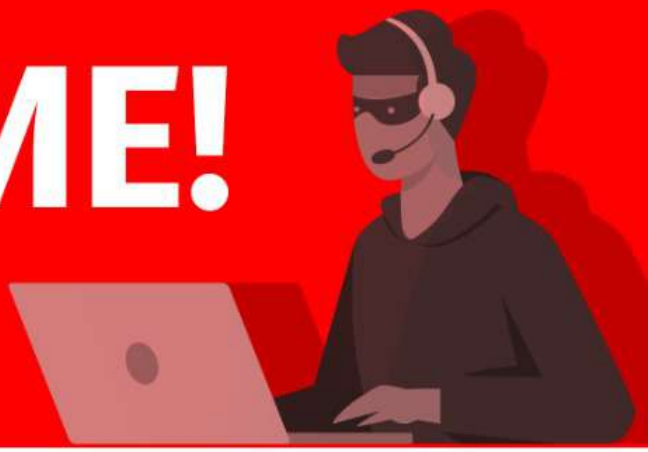
ВНИМАНИЕ!

МВД предупреждает: телефонные мошенники!



Финансовые аферисты постоянно меняют сценарии обмана. Однако есть фразы, которые выдают преступников. Вот некоторые из них:

«Оформлена заявка на кредит»
Если вы не оставляли заявку, а вам сообщают о предварительно одобренном кредите, то **просто кладите трубку**. Не продолжайте разговор — иначе, сказав лишнего, вы точно поможете мошенникам оформить на вас кредит и похитить деньги.

«Сотрудник Центробанка»
Настоящие работники Банка России **не звонят и не пишут гражданам** для совершения каких-либо банковских операций. Так поступают лжесотрудники мегарегулятора.

«Специальный или безопасный счет»
Распространенная легенда аферистов, которые убеждают людей перевести сбережения на «специальный» счет — якобы для сохранности денег. **Однако «специальных» («безопасных», «защищенных» и др.) счетов не существует.**

«Вас беспокоит специалист финансовой безопасности, сотрудник службы безопасности банка»
Отличить аферист от настоящего специалиста службы безопасности легко: первый будет **интересоваться данными вашей карты или кодом из СМС**. К тому же он **не сможет** сообщить вам актуальный остаток по счету.

«Идут следственные действия, помогите задержать мошенников и не разглашайте информацию»
Работники правоохранительных органов **не проводят** процессуальные действия по телефону, **не запрашивают** финансовые данные и **не предлагают** поучаствовать в задержании мошенников.

«Ваши деньги пытаются похитить, зафиксирована подозрительная операция»
Банки могут приостановить такие операции **без участия клиента**. Если у банка возникнут сомнения, его представитель может написать вам в онлайн-банке или позвонить для подтверждения операции. Но, в отличие от жулика, настоящий работник банка звонит только с официального номера банка и никогда не просит совершить операции по карте.

«Истекает срок действия сим-карты»
Не сомневайтесь, вы разговариваете с мошенником: у сим-карты мобильного оператора **нет срока годности** и она не нуждается в замене по этой причине.

«Продиктуйте код из СМС-сообщения»
Код из СМС — это аналог вашей собственноручной подписи. Его **никогда и никому нельзя сообщать или пересылать**.

МВД по Республике Башкортостан напоминает:
проявляйте максимальную осторожность при общении с неизвестными Вам лицами по телефону или в мессенджерах. Не доверяйте обещаниям быстрого заработка! Не переводите и не передавайте незнакомцам деньги!
02.мвд.рф

!!! **Отключите уведомления на заблокированном экране.** Это помешает злоумышленникам видеть письма и сообщения;

!!! **Установите приложение, блокирующее звонки с неизвестных номеров;**

!!! **Пользуйтесь только официальными и проверенными приложениями.** Использование сторонних приложений делает ваше устройство уязвимым к несанкционированному доступу;

!!! **Не перезванивайте на незнакомые номера**, даже если любопытно;

!!! **Не переходите по сомнительным ссылкам и не скачивайте файлы от незнакомых отправителей**.

ТАКЖЕ НЕОБХОДИМО ПОМНИТЬ:

!!! **Не верьте в выигрыш, за который нужно платить;**

!!! **Прервите разговор с незнакомцем**, перепроверьте полученную информацию посредством имеющихся приложений и сервисов, а также посещения непосредственной организации, предприятия, офиса или силовых структур;

!!! **Проверяйте телефонные счета на предмет несанкционированного списания со стороны мошенников**.

Помните! Киберпреступники не стоят на месте и придумывают все новые и новые мошеннические схемы и различные ухищрения, чтобы завладеть вашими денежными средствами или конфиденциальной информацией!!!

МВД ПО РЕСПУБЛИКЕ БАШКОРТОСТАН НАПОМИНАЕТ:

- **если поступает звонок с неизвестного номера — отклоните вызов;**
- **прежде чем перевести кому-либо деньги, обязательно посоветуйтесь с близкими.**

Помните, что мошенники могут использовать подложные номера. Будьте внимательны!

Телефон доверия:
8 (347) 279-32-92

@BASHMOSHKI

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ БАШКОРТОСТАН

ЗАЩИТИТЕ СЕБЯ И СВОИХ БЛИЗКИХ ОТ КИБЕРМОШЕННИКОВ

ПАМЯТКА ДЛЯ ГРАЖДАН
ПО ЗАЩИТЕ АБОНЕНТСКИХ НОМЕРОВ
ОТ КИБЕРПРЕСТУПНИКОВ

Мобильный телефон стал неотъемлемой частью нашей жизни.

В нем мы храним самые важные для нас сведения: фотографии, документы, учетные записи от банков и электронной почты, конфиденциальную информацию, в том числе персональные данные и т.д.

Мобильные мошенники пытаются войти в доверие и вынудить вас заразить свое устройство или передать им конфиденциальную информацию (в том числе персональные данные).

РАСПРОСТРАНЕННЫЕ ВИДЫ МОБИЛЬНОГО МОШЕННИЧЕСТВА:

► Сообщения о заражении мобильного телефона вредоносной программой.

На экране телефона отображается поддельное сообщение, например: «В ходе сканирования телефона было обнаружено вредоносное программное обеспечение, требуется срочно скачать/загрузить «антивирус».

Результат: При загрузке «антивируса» вы рискуете загрузить вредоносную или шпионскую программу.

► Мошенничество с помощью телефонных звонков («вишинг»).

В ходе звонка мошенник пытается убедить вас предоставить/сообщить ему свои личные персональные данные или перевести денежные средства. При этом он просит совершить какие-либо действия во время звонка, не прерывая разговор.

Результат: Перевод денежных средств мошенникам (включая личные накопления и кредитные средства). Утечка конфиденциальной информации, которой могут воспользоваться мошенники в преступных целях.

► Мошенничество по SMS, включая рассылку вредоносных ссылок («SMS-фишинг», «смишинг»).

Призыв к действию с помощью текстового сообщения, которое вынуждает перезвонить, загрузить по ссылке вредоносную или шпионскую программу, оформить подписку или выдать персональные данные.

Результат: При переходе по ссылке происходит загрузка вредного или шпионского ПО. Перевод денежных средств мошенникам. Утечка конфиденциальной информации, которыми могут воспользоваться в преступных целях.

► Сбрасывающиеся звонки. Призыв перезвонить на подозрительный платный номер.

Результат: Съем денежных средств.

РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СВОЕГО ТЕЛЕФОНА ОТ ДЕЙСТВИЙ МОШЕННИКОВ:

!!! Уберите автоматическое подключение к Wi-Fi и старайтесь не подключатся к публичным сетям Wi-Fi. Они плохо защищены и через них злоумышленники могут получить доступ ко всем вашим данным;

!!! Установите сложные пароли. Пароль должен содержать буквы, цифры и специальные символы. Используйте уникальные пароли на разные аккаунты, приложения и сайты;

!!! Не позволяйте посторонним пользоваться вашим телефоном;

!!! Не делитесь своими паролями и учетными записями. Ими могут воспользоваться без вашего ведома;

!!! Не вводите логины и пароли на незнакомых сайтах и чужих устройствах. Возможна утечка паролей и учетных записей;

!!! Используйте двухфакторную проверку на телефоне. Удобнее и надежнее пользоваться специальными приложениями;

!!! Используйте длинный ПИН-код, это повысит безопасность;

!!! Храните пороли и ПИН-коды в местах, куда злоумышленники не доберутся. Не храните пароли на бумажных носителях, которые носите с собой, не сохраняйте в браузере, при использовании облачного хранилища создавайте максимально сложный пароль;

!!! Отключите автозаполнение паролей на телефоне и браузерах. Так посторонние не смогут войти в приложения, которыми вы пользуетесь;

!!! Ограничьте/запретите доступ приложений к вашим личным данным (к аккаунтам, фотографиям, SMS, контактам и тд.). Этим смогут воспользоваться злоумышленники;

ПОСТАВЬТЕ ЩИТ ОТ КИБЕРМОШЕННИКОВ

► **Подключите сервисы** сотовых операторов **для защиты от нежелательных звонков**;

► **Подключите определитель номера**. При звонке высвечивается информация о том, что звонок является нежелательным, возможно звонят мошенники;

► **Настройте телефон. Заблокируйте входящие звонки от неизвестных абонентских номеров**, в том числе в мессенджерах. Это особенно актуально для лиц пожилого возраста и пенсионеров.

МВД ПО РЕСПУБЛИКЕ БАШКОРТОСТАН НАПОМИНАЕТ:

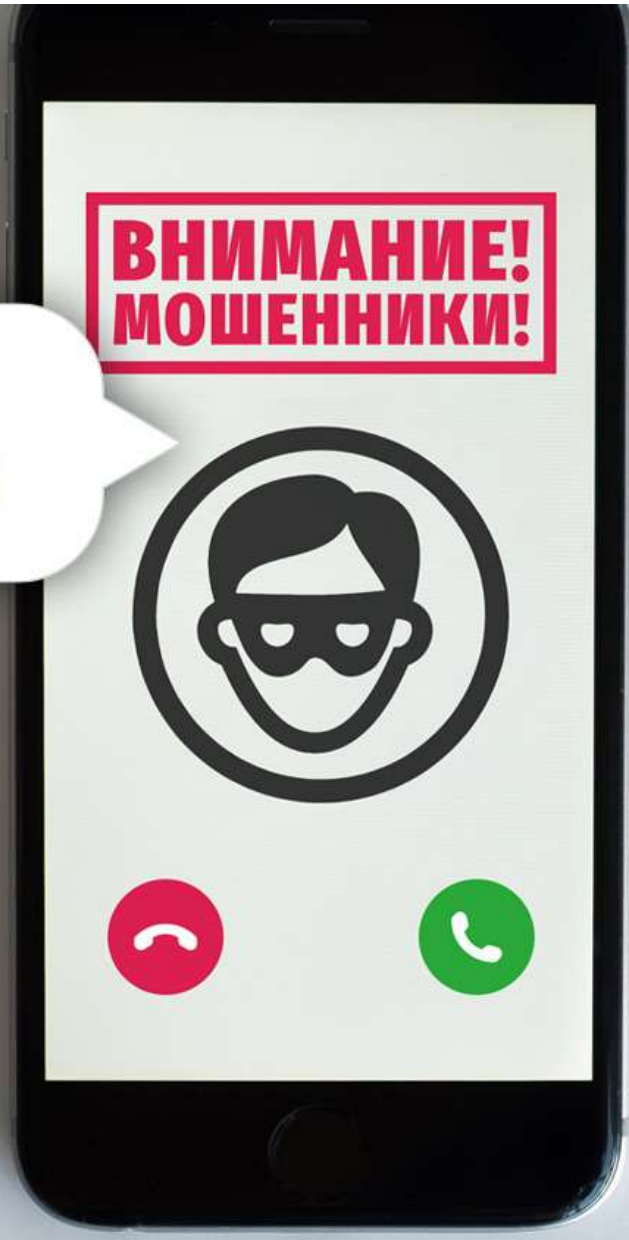
- если поступает звонок с неизвестного номера — отклоните вызов;
- прежде чем перевести кому-либо деньги, обязательно посоветуйтесь с близкими.

Помните, что мошенники могут использовать подложные номера. Будьте внимательны!

02.мвд.рф

Министерство внутренних дел по Республике Башкортостан
Управление МВД России по городу Уфе

Ваш родственник находится в полиции



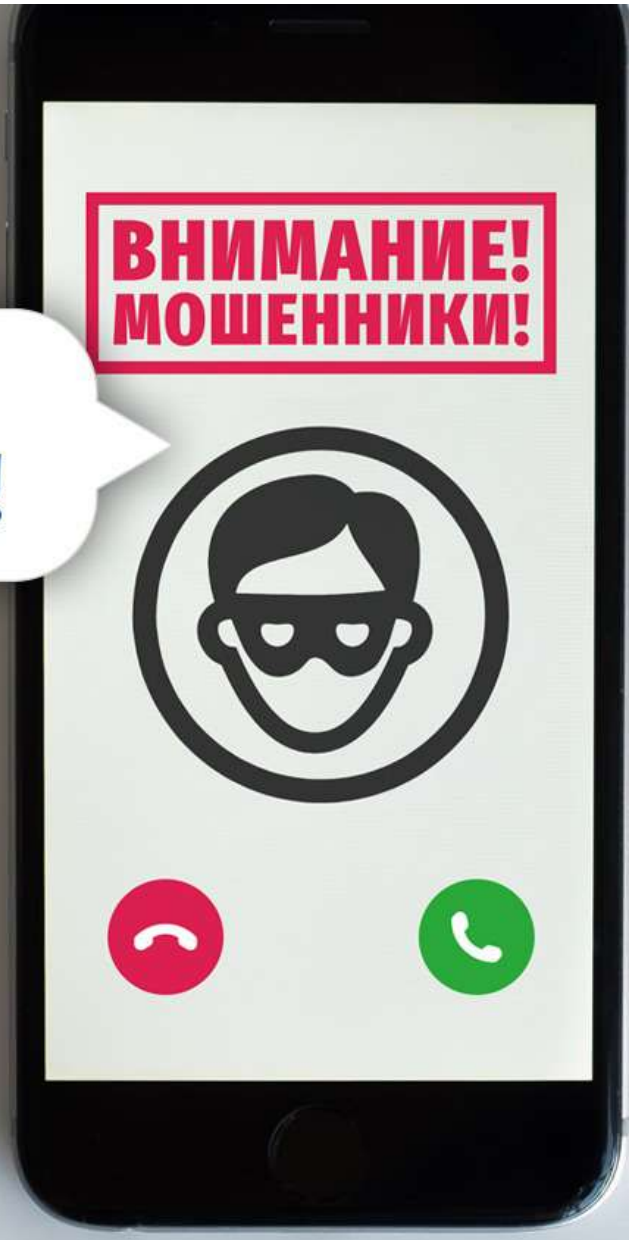
НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР!

Позвоните родственнику!

БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

02.мвд.рф

Министерство внутренних дел по Республике Башкортостан
Управление МВД России по городу Уфе



Ваш сын попал в ДТП! Срочно нужны деньги!

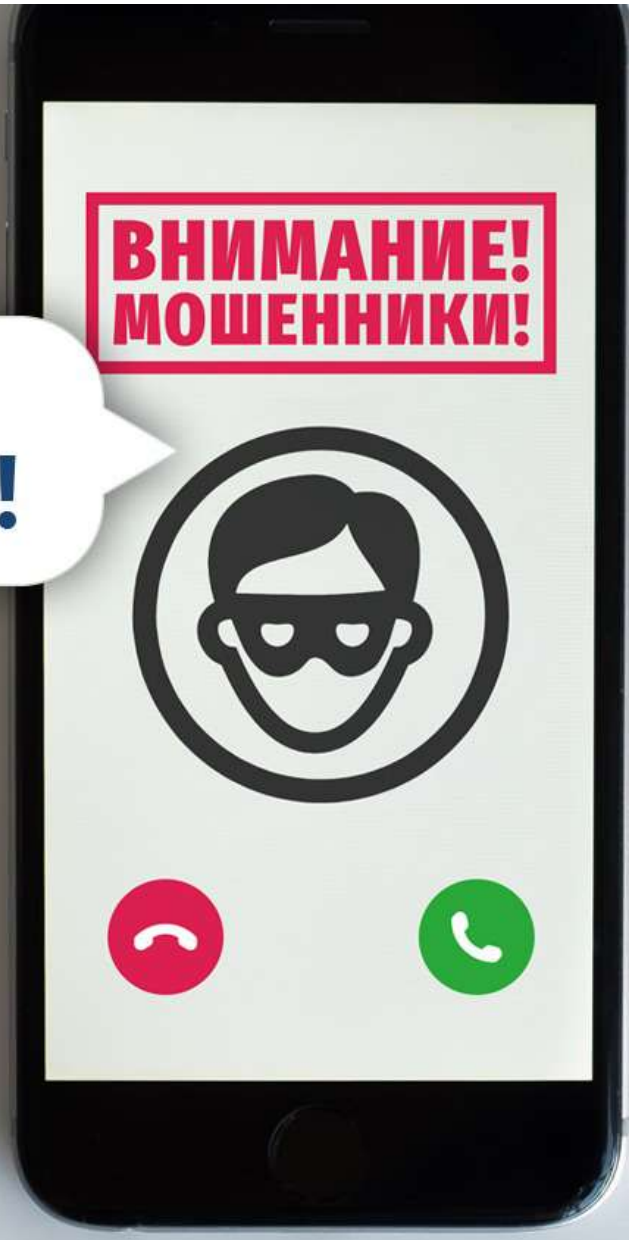
НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР!

Позвоните родственнику!

БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

02.мвд.рф

Министерство внутренних дел по Республике Башкортостан
Управление МВД России по городу Уфе



Алло, это служба безопасности банка!

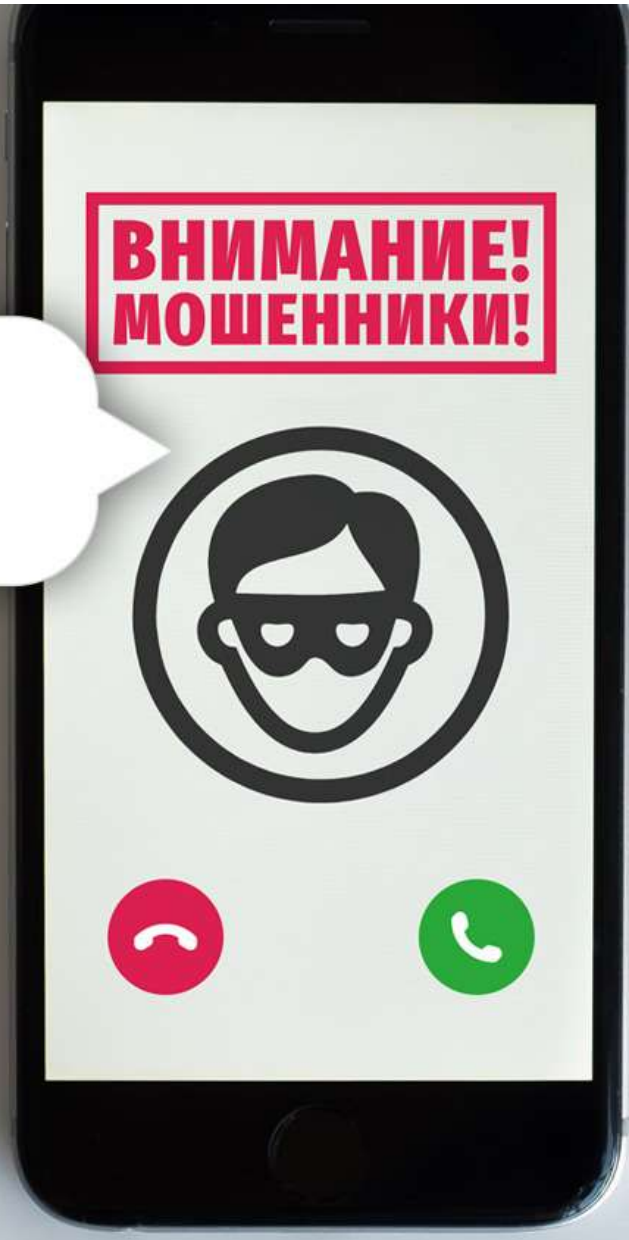
ПОСТУПИЛ ЗВОНОК ОТ «СОТРУДНИКА БАНКА»?

НЕМЕДЛЕННО
прекратите разговор!

БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

02.мвд.рф

Министерство внутренних дел по Республике Башкортостан
Управление МВД России по городу Уфе



Переведите деньги на безопасный счет

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ НЕЗНАКОМЫМ ЛЮДЯМ!

Учтите, что с Вами могут общаться **МОШЕННИКИ!**

БУДЬТЕ БДИТЕЛЬНЫ!
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

02.мвд.рф

ЗАЩИТИТЕ СЕБЯ И СВОИХ БЛИЗКИХ ОТ КИБЕРМОШЕННИКОВ

Мобильный телефон стал неотъемлемой частью нашей жизни.

В нем мы храним самые важные для нас сведения: фотографии, документы, учетные записи от банков и электронной почты, конфиденциальную информацию, в том числе персональные данные и тд.

Лучшая защита от кибермошенников — соблюдение правил цифровой безопасности:

- **Уберите автоматическое подключение** к Wi-Fi и старайтесь не подключатся к публичным сетям Wi- Fi. Они плохо защищены и через них злоумышленники могут получить доступ ко всем вашим данным;
- **Установите сложные пароли**. Пароль должен содержать буквы, цифры и специальные символы. Используйте разные пароли к разным аккаунтам, приложениям и сайтам;
- **Не делитесь своими паролями** и учетными записями;
- **Отключите автозаполнение паролей** на телефоне и браузерах;
- **Используйте двухфакторную проверку** на телефоне;
- **Пользуйтесь только официальными и проверенными приложениями**;
- **Не перезванивайте на незнакомые номера**;
- **Не переходите по сомнительным ссылкам** и не скачивайте файлы от незнакомых отправителей.

МВД ПО РЕСПУБЛИКЕ БАШКОРТОСТАН НАПОМИНАЕТ:

- **если поступает звонок с неизвестного номера — отклоните вызов;**
- **прежде чем перевести кому-либо деньги, обязательно посоветуйтесь с близкими.**

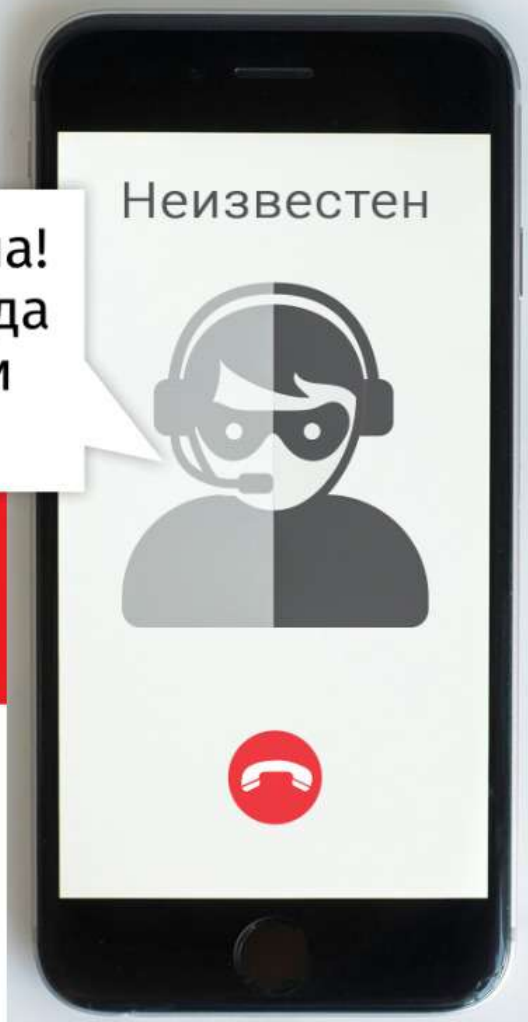
Помните, что мошенники могут использовать подложные номера. Будьте внимательны!

02.мвд.рф

ВНИМАНИЕ!

Телефонные мошенники!

Ваша заявка на кредит одобрена! Иван Петров — это Вы? Нет? Тогда я вынужден сообщить, что Ваши счета в опасности.



Прервите разговор! Вам позвонили мошенники!

СХЕМА МОШЕННИЧЕСТВА:

Аферисты под видом сотрудников Банка России (ФСБ, МВД, Следственного комитета, Госуслуг), сообщают жертве о том, что **кто-то пытается похитить деньги с ее счета**. Чтобы их спасти, надо **перевести средства на «безопасный» счет** в ЦБ РФ. По легенде это временная мера — на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве.

ВАЖНО

Пользуйтесь только **официальными ресурсами** финансовых организаций!

Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, **перезвоните на официальный номер**, размещенный на сайте финансовой организации.

Там же вы можете найти ссылки на официальные банковские приложения и скачать их.

ЗАПОМНИТЕ!

Настоящего представителя банка всегда можно проверить: просто положите трубку и перезвоните по номеру телефона финансовой организации. Он есть на официальном сайте и на оборотной стороне карты. Поинтересуйтесь, мог ли сотрудник банка связываться с вами, и зачем.

Если вас просят перевести средства на счет или заплатить за что-то, то, скорее всего, вы столкнулись с мошенниками.

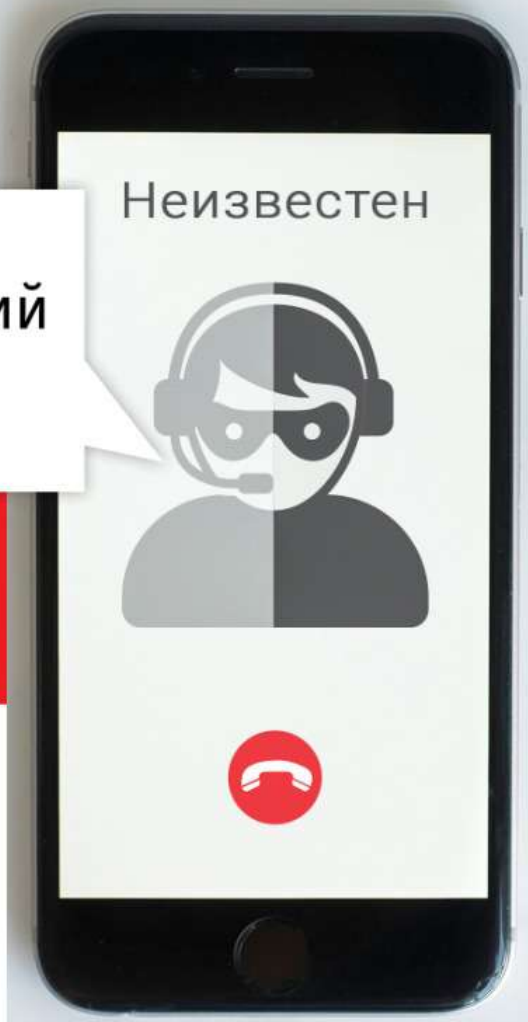
МВД по Республике Башкортостан напоминает:
не переводите деньги незнакомым людям. В случае поступления звонка якобы от сотрудника банка положите трубку. Помните, что мошенники могут использовать подложные номера. Будьте внимательны!

02.мвд.рф

ВНИМАНИЕ!

Телефонные мошенники!

Я специалист по инвестициям и помогу Вам получить высокий доход с минимальными вложениями!



Прервите разговор! Вам позвонили мошенники!

СХЕМА МОШЕННИЧЕСТВА:

Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое — нужно лишь открыть «брокерский» счет и инвестировать от 10 000 рублей. Доход — не меньше миллиона.

Для открытия такого счета мошенники **требуют установить приложение**.

Далее программа **имитирует** якобы рост доходов от инвестиций, в том числе в криптовалюту. **Как только у «инвестора» возникает желание вывести деньги со счета — начинаются проблемы.** Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства.

В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

КАК МОШЕННИКИ СЕБЯ ВЫДАЮТ

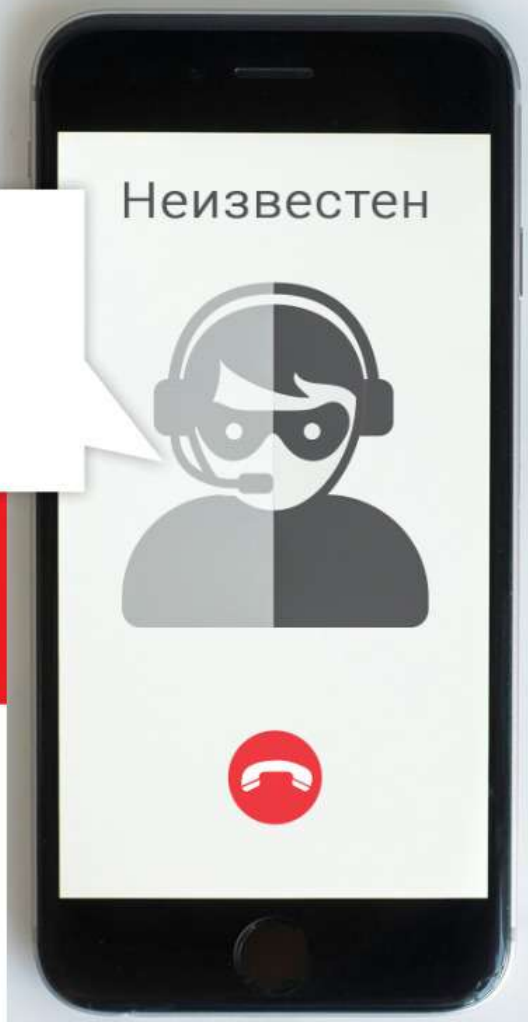
- обещают высокую доходность без рисков и за короткий срок;
- давят и требуют перечислить деньги прямо сейчас;
- общаются грубо и безграмотно;
- просят перевести деньги на личную карту или криптовалютные кошельки;
- делают публикации на странице частных лиц от имени известных организаций;
- предлагают установить на компьютер сторонние программы;
- убеждают продавать имущество, брать кредиты и инвестировать;
- их сайт выглядит небрежно.

МВД по Республике Башкортостан напоминает:
проявляйте максимальную осторожность при общении с неизвестными Вам лицами по телефону или в мессенджерах.
Не доверяйте обещаниям быстрого заработка!
Не переводите и не передавайте незнакомцам деньги!

02.мвд.рф

ВНИМАНИЕ!
Телефонные мошенники!

Вам звонят из ФСБ (МВД, Следственного комитета). Хочу сообщить, что у Вас большие проблемы…



Прервите разговор! Вам позвонили мошенники!

СХЕМА МОШЕННИЧЕСТВА:

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги», полиции.

Самая распространенная уловка — предложение **получить какую-либо государственную выплату**. Схема классическая: вы нам данные карты, мы вам — деньги.

Есть и другой сценарий. Например, звонок от представителей правоохранительных органов или финансовых учреждений **с угрозой блокировки счета**, по которому **якобы зафиксированы сомнительные операции и необходимо срочно перевести деньги на «безопасный» счет.**

Помните, что **подобные ведомства не наделены полномочиями** по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подобные письма и не звонят по телефону или в мессенджерах.

Если вы получили подобные сообщения — **проигнорируйте их** и обратитесь напрямую в государственную организацию!

ЗАПОМНИТЕ!

Реальные следователи не станут выяснять информацию по телефону, они вызовут в отделение с помощью повестки.

Не сообщайте никому личные данные: серию и номер паспорта, информацию о количестве денег на счетах, реквизиты счета. Сотрудники госструктур никогда не запрашивают такую информацию.

Не верьте, если вам говорят, что решить вопрос можно деньгами, например с помощью перевода на карту физлица.

МВД по Республике Башкортостан напоминает:
не переводите деньги незнакомым людям. В случае поступления звонка якобы от сотрудника правоохранительных органов положите трубку. Помните, что мошенники могут использовать подложные номера. Будьте внимательны!

02.мвд.рф