Памятка по профилактике мошеннических действий.
Внимание! МВД предупреждает: телефонные мошенники!

Ежедневно финансовые аферисты придумывают новые и новые способы мошенничеств:

1. **«Безопасный счет»**, звонки мошенников, которые представляются должностными лицами налоговой службы, полиции, ФСБ, прокуратуры, Пенсионного фонда, Госуслуг и др.

Его подвиды:

- «предоставление доступа к экрану телефона с последующим входом в различные приложения и хищением денежных средств»;

- «представление сотрудником госорганизации, оказывающей помощь по возврату ранее похищенных денежных средств»;

- «замена электросчетчика, установка соответствующего приложения в телефон и предоставление кодов из СМС»;

- «продление договоров обслуживания сим карт мобильных операторов связи, под предлогом улучшения качества связи» вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей или банковским реквизитам;

- «представление агентом страховой компании для перерегистрации медицинской страховки путем предоставления кодов по СМС»;

- «неоднократные звонки с разных номеров с информированием о взломе (попытки взлома) личного кабинета «Госуслуг», оформлением кредитов, переводом денежных средств на безопасный счет».

2. «Инвестиции» под видом финансовых экспертов мошенники в интернете рассказывают об уникальной схеме заработка.

3. «Заказ товаров в интернете, в том числе через сайты бесплатных объявлений Авито, Юла, Яндекс для продажи товаров и оказания услуг по подозрительно низкой цене».

4. «Взлом социальных страниц»

5. «Манипуляции под видом какого-либо крупного выигрыша».

6. «Родственник попал в ДТП, сбил человека и др.» мошенник под видом родственника, попавшего в ДТП, либо сотрудника правоохранительных органов просит деньги за возможность избежать наказания за противоправное деяние.

* * *

В 2024 г. жители Республики Башкортостан **ежедневно** переводили в среднем 12 млн рублей, **ежемесячно** – свыше 360 млн рублей, **за год** переведено более 4,4 млрд рублей.

* * *

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

–избегайте телефонных разговоров с подозрительными людьми, не бойтесь прервать разговор, просто кладите трубку;

– ни при каких обстоятельствах не сообщайте данные вашей банковской карты, а также секретный код на оборотной стороне карты;

– остерегайтесь «телефонных» мошенников, которые под видом сотрудником МВД, ФСБ, Центробанка и т.д. пытаются запугать Вас привлечением к уголовной ответственности, штрафами;

– никогда и никому не сообщайте пароли и секретные коды, которые приходят вам в СМС сообщении, и помните, что только мошенники их запрашивают;

– не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты;

- не передавайте деньги неизвестным лицам для решения возникших у Вас якобы проблемных вопросах;

– никогда не переводите денежные средства, если об этом вас просит сделать Ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– если Вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

- при смене номера телефона, отключите от него все мобильные банки и прочие сервисы, дающие доступ к Вашим финансам.

Министерство внутренних дел по Республике Башкортостан

Признаки мошенничества в инвестировании.

1. **«Гарантии высокой доходности без риска»** - легальные инвестиции всегда имеют определенный уровень риска. Если Вам обещают гарантированный высокий доход без потерь, возможно Вас пытаются обмануть.

2. **«Приведи друга – получи выгоду»** - если организация предлагает привлекать друзей и знакомых для радикального увеличения дохода – это с большой долей вероятности может быть мошенничество!

3. **«Отсутствие лицензии и регистрации»** - проверяйте наличие лицензии Центрального Банка РФ (ЦБ РФ). Список лицензированных организаций можно найти на сайте ЦБ: CBR.RU

4. **«Сложная и непрозрачная схема инвестирования»** - мошеннические компании часто избегают четких объяснений, куда именно будут направлены ваши средства.

5. **«Навязчивые звонки и давление»** - если Вас настойчиво уговаривают вложить средства прямо сейчас, используя срочность в качестве аргумента – это классический прием мошенников.

6. **«Платежи за обучение или доступ к эксклюзивной информации»** - под предлогом «Секретных методов» могут предлагать дорогостоящие курсы или платную подписку на якобы инсайдерскую информацию.

МВД по Республике Башкортостан

!!! **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;

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.

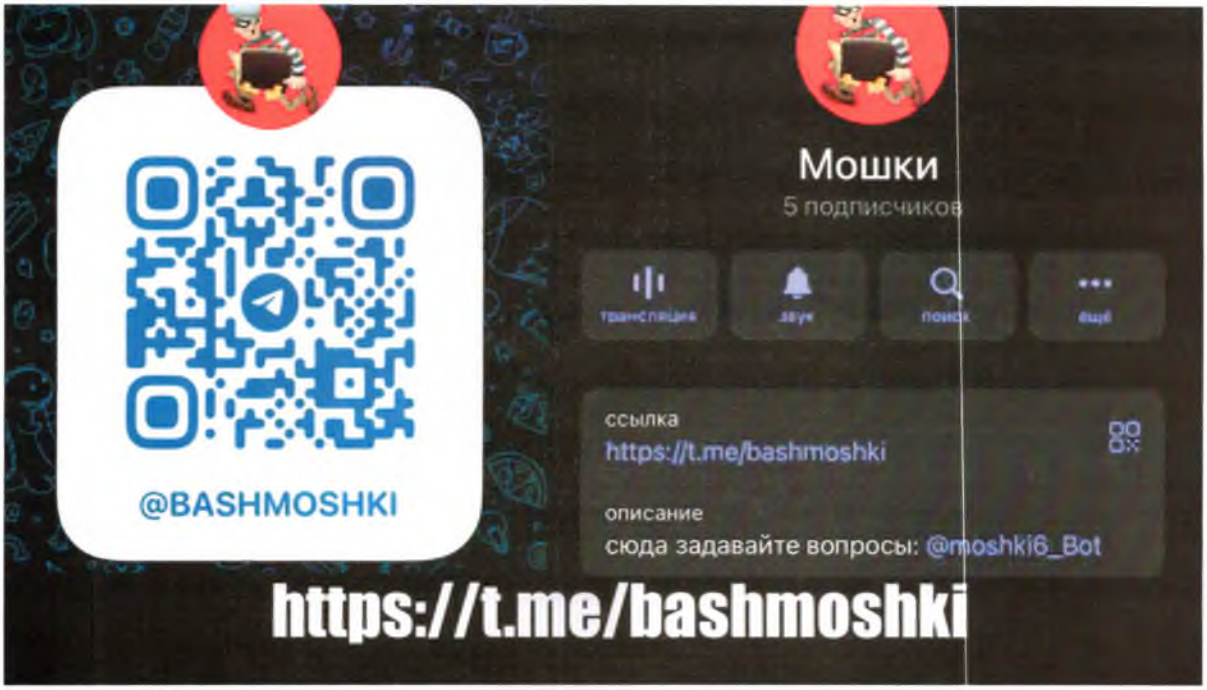
«Идут следственные действия, помогите задержать мошенников и не разглашайте информацию»
Работники правоохранительных органов **не проводят** процессуальные действия по телефону, **не запрашивают** финансовые данные и **не предлагают** поучаствовать в задержании мошенников.

«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


Мошки
5 подписчиков
трансляция
звук
поиск
ещё
ссылка
https://t.me/bashmoshki
описание
сюда задавайте вопросы: @moshki6_Bot
@BASHMOSHKI
https://t.me/bashmoshki