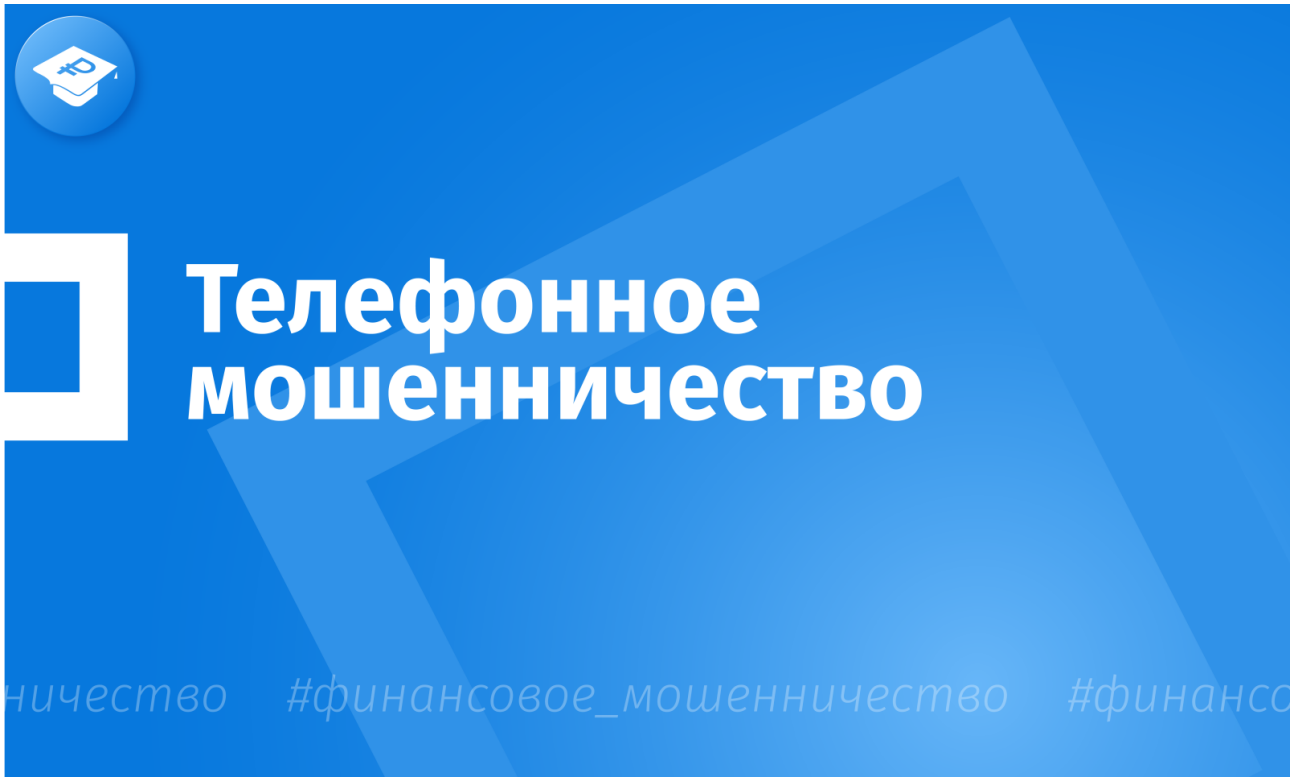
3 АВГУСТА, СРЕДА

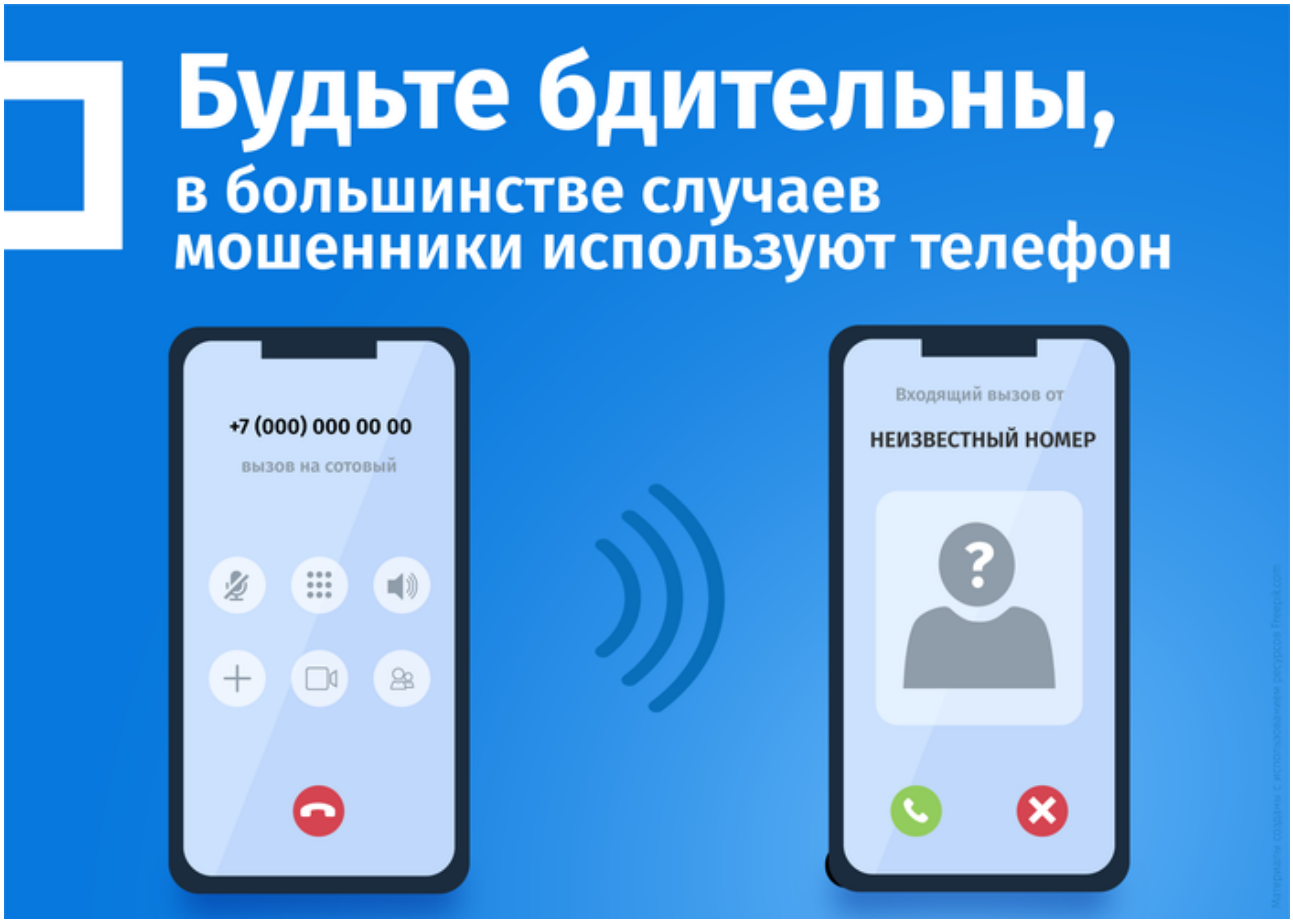
Открытый бюджет города Москвы

Как не стать жертвой мошенников?



Главная цель телефонных мошенников – заставить вас передать им конфиденциальную информацию. Наибольший интерес представляют данные банковских карт, коды доступа к личным кабинетам и аккаунтам, пароли. Набор инструментов для обмана граждан очень широкий. Наиболее часто от мошенников поступают предложения:

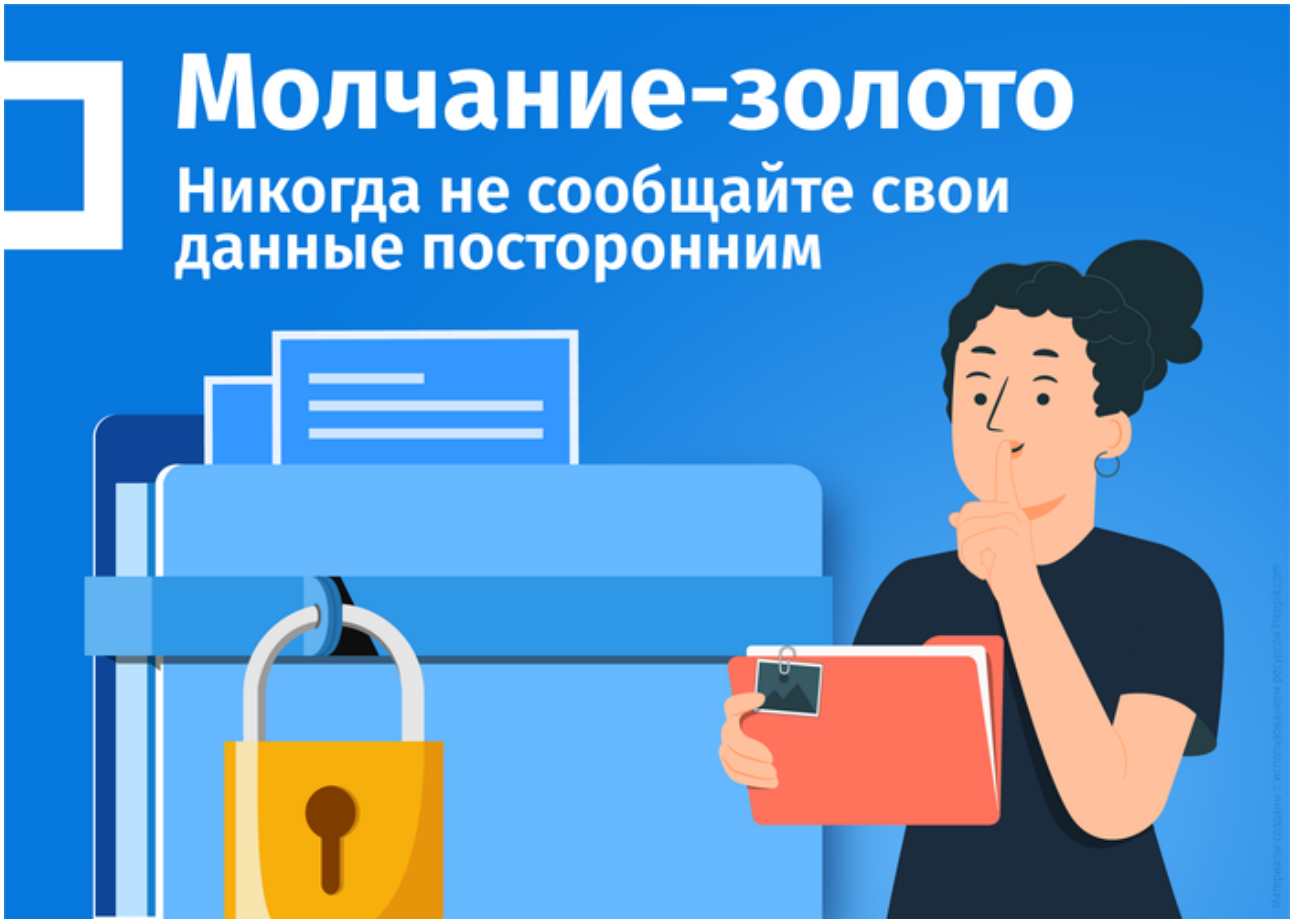
- спасти кого-то (родственника, знакомого, редкое животное), направив деньги по предлагаемым номерам телефонов или банковской карты;
- защитить ваши деньги, которые кто-то пытается похитить, разместив их на «безопасном счете»;
- получить деньги (призы, возврат налогов, социальные выплаты), сообщив свои персональные данные, реквизиты банковской карты или код подтверждения из смс-сообщения;
- помочь правоохранительным органам поймать преступников.



Как распознать мошенника?

Злоумышленники стремятся к тому, чтобы граждане добровольно передавали конфиденциальную информацию, включая данные для доступа к банковским счетам и картам. Мошенника легко распознать, если запомнить несколько признаков его поведения:

- Первым связывается с потенциальной жертвой. Звонок или смс-сообщение с незнакомого номера, электронное письмо или ссылка в мессенджере. Зачастую они содержат выгодное предложение, информацию о неожиданном выигрыше в лотерею или угрозе потери средств. Мошенник может представиться сотрудником банка, государственных и правоохранительных органов.
- Просит сообщить личные данные. Чаще всего злоумышленников интересуют код для подтверждения оплаты из смс, ПИН-код (4 цифры, необходимые для совершения покупки или снятия денег в банкомате), номер и срок действия карты или код безопасности (3 цифры на её оборотной стороне).



- Говорит о ваших личных финансах. Злоумышленник сообщает о попытке мошенников взломать личный кабинет онлайн-банка или взять на ваше имя кредит, предлагает перевести деньги на безопасный счет, выгодно инвестировать в новый высокодоходный проект или срочно оплатить штраф или госпошлину.
- Пытается вызвать у вас сильные эмоции. Мошенник старается воздействовать на вас при помощи приемов социальной инженерии (психологических манипуляций). Злоумышленник с помощью эмоций (страха или радости) пытается вывести вас из равновесия, заставить потерять бдительность.
- Торопит с принятием решений. Чем меньше времени предоставляется на принятие решения, тем выше вероятность ошибки. Этим правилом пользуются мошенники, требуя незамедлительно продиктовать личные данные во избежание блокировки карты или хищения денежных средств. Так человек не успевает распознать мошенника.
- Акцентирует внимание на актуальной новостной повестке. Например, в период пандемии мошенники требовали оплатить штрафы за нарушение карантина или самоизоляции, сдать анализ на платной основе, приобрести дорогостоящие лекарственные средства, сообщить данные для предоставления государственной поддержки пострадавшим.
- Предлагает помощь. Злоумышленник обещает перевести деньги на «защищенный» счет, оформить банковскую карту в зарубежных банках, осуществить международный перевод или выгодно обменять иностранную валюту. Получив деньги, исчезает.

Как не стать жертвой телефонных мошенников?

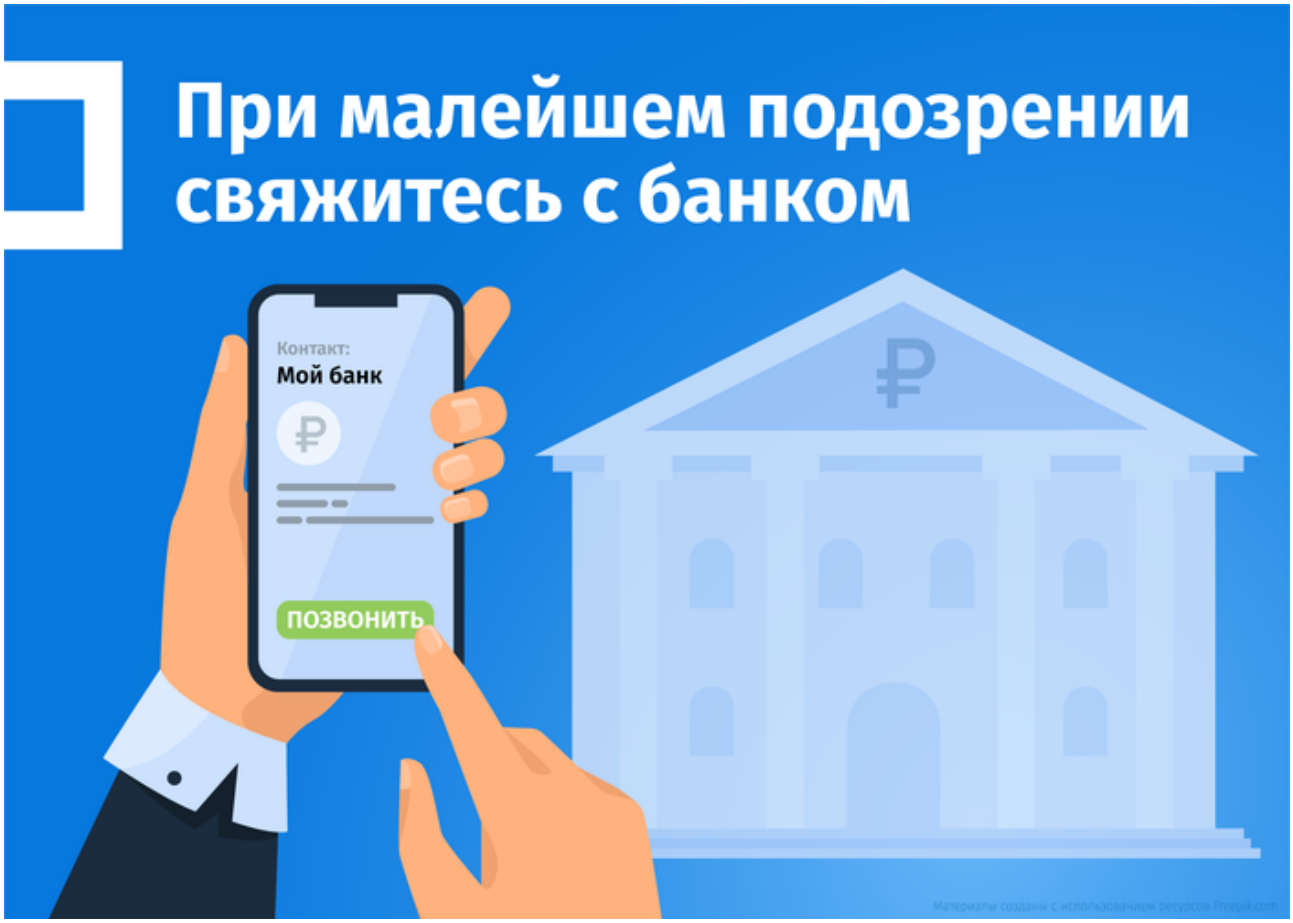
- Не принимайте необдуманных решений. Звонящие часто пугают, утверждая, что деньги уже уходят с вашего счета. Лучшее решение в такой ситуации – немедленно

прекратить телефонный разговор, заблокировать номер звонившего. Если есть сомнения – звоните в свой банк, его номер размещен на оборотной стороне вашей карты.

- Не сообщайте в телефонном разговоре данные: фамилию, имя, отчество, паспортные данные, номер и срок действия банковской карты, ее ПИН-код и три цифры с оборотной стороны карты, коды из СМС и push-уведомлений. Опять же: есть сомнения – звоните в банк сами, набрав номер вручную.
- Не публикуйте в открытом доступе свои персональные данные. С их помощью злоумышленникам проще расположить вас к себе, обращаясь по имени и представляясь сотрудниками банков, иных организаций.

В случае, если ваши персональные данные все же появились в открытом доступе, проявляйте особую бдительность. Смените пароль для доступа к личному кабинету в банке и на сайте государственных услуг. Держите номер горячей линии банка под рукой.

- Используйте свое право об отзыве согласия на обработку персональных данных. Пишите соответствующие заявления, если больше не планируете пользоваться услугами компании или обеспокоены сохранностью конфиденциальной информации.
- Сообщите в банк о том, что вам звонили мошенники и предоставьте их номера телефонов. Обязательно заблокируйте эти номера на своем телефоне во избежание повторных звонков.



По материалам портала Правительства Москвы "Открытый бюджет города Москвы": https://budget.mos.ru/