

Видеопрезентация на тему:
«Мошенничество с банковскими картами с
использованием сотовой связи.
Как вычислить мошенника, обезопасить себя и своих
близких.»

- Выполнили: ученики 9.6 класса МБОУ БСОШ
- Лукьянов Г.И., Сабитов Н.С.
- Руководитель проекта: Попова Г.А.
- Видеоролик является продуктом проекта.

Как обезопасить себя и своих близких от телефонного мошенничества.

По данным МВД телефонные мошенники похитили у россиян около 39 миллиардов рублей за первое полугодие 2022 года.

Злоумышленники постоянно придумывают разные схемы обмана для того, чтобы выманить у своих жертв деньги или конфиденциальные данные для доступа к банковским счетам. Я расскажу о 7 признаках, по которым можно вычислить мошенников, а также действия, которые помогут вам защититься от обмана. Изучите сами и поделитесь с теми, о ком заботитесь.

Звонки со скрытых номеров

Скрытый номер – первый признак того, что вам звонят мошенники или спамеры с разнообразными рекламными предложениями. Звонок из банка может поступить только с официальных номеров, указанных на сайте или на банковской карте. Если вам звонят из конкретного отделения банка, то номер будет федеральным или мобильным, но не скрытым.

Что делать?

Не берите трубку и сбросьте звонок. Даже если номер отображается как официальный телефон организации, это может быть маскировка мошенников. Если вы хотите уточнить информацию, например, в банке, то наберите нужный номер вручную.



Запрос данных банковской карты

Чаще всего у жертвы хотят узнать номер карты, коды для подтверждения платежных операций, три цифры с обратной стороны банковской карты (CVC/CVV), логины и пароли от личного кабинета на сайте банка или в мобильном приложении.

Что делать?

Не сообщайте никому логины и пароли от аккаунтов, платежные данные, одноразовые коды из СМС. Помните, что настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли, а номер карты и срок ее действия узнает из системы обслуживания клиентов. Единственная ситуация, при которой требуется назвать устно одноразовый код, – личное обслуживание в банке или в магазине. Когда нужно подтвердить операцию, например, выдачу банковской карты или списание бонусов программы лояльности.



Сообщение тревожной информации от злоумышленников

Чтобы вогнать свою жертву в панику и заставить действовать необдуманно, мошенники специально нагнетают ситуацию. Например, они могут представиться сотрудниками банка и сообщить, что по карте проведена подозрительная операция, а для ее отмены нужно назвать код из СМС. Преступники также могут представиться сотрудниками полиции, ФСБ, прокуратуры и запугать уголовным делом или сообщить о попавшем в беду родственнике. В состоянии растерянности и волнения человек может выполнить любые просьбы: поделиться с преступниками конфиденциальной информацией или перевести деньги на счет обманщиков.

Что делать?

Не паникуйте и ни в коем случае не переводите деньги. Прекратите разговор и перезвоните родственнику, о котором вам сообщили, в банк или в то ведомство, из которого вам якобы звонили. Проверьте полученную информацию в официальных источниках. Если вы успели сообщить мошеннику какие-либо данные карты, позвоните в свой банк и скажите об этом оператору. При необходимости он сможет заблокировать вашу карту или приостановить возможность проведения операций в интернет-банке.



Давление со стороны мошенников

Мошенники не только стремятся вызвать сильные эмоции, но и торопят с принятием решения, чтобы у человека не было времени обдумать ситуацию. В ходе разговора злоумышленники могут предостерегать от самостоятельных попыток разобраться с проблемой. Часто они звонят поздно вечером или рано утром в выходные дни, когда человек спит и не может быстро сориентироваться.

Что делать?

Никогда не принимайте поспешных решений, особенно если они касаются ваших денег. Всегда берите паузу, чтобы разобраться в том, что происходит. Скажите, что перезвоните в банк или организацию самостоятельно, и сразу завершите звонок. Иначе мошенники продолжат запугивать и давить на вас.

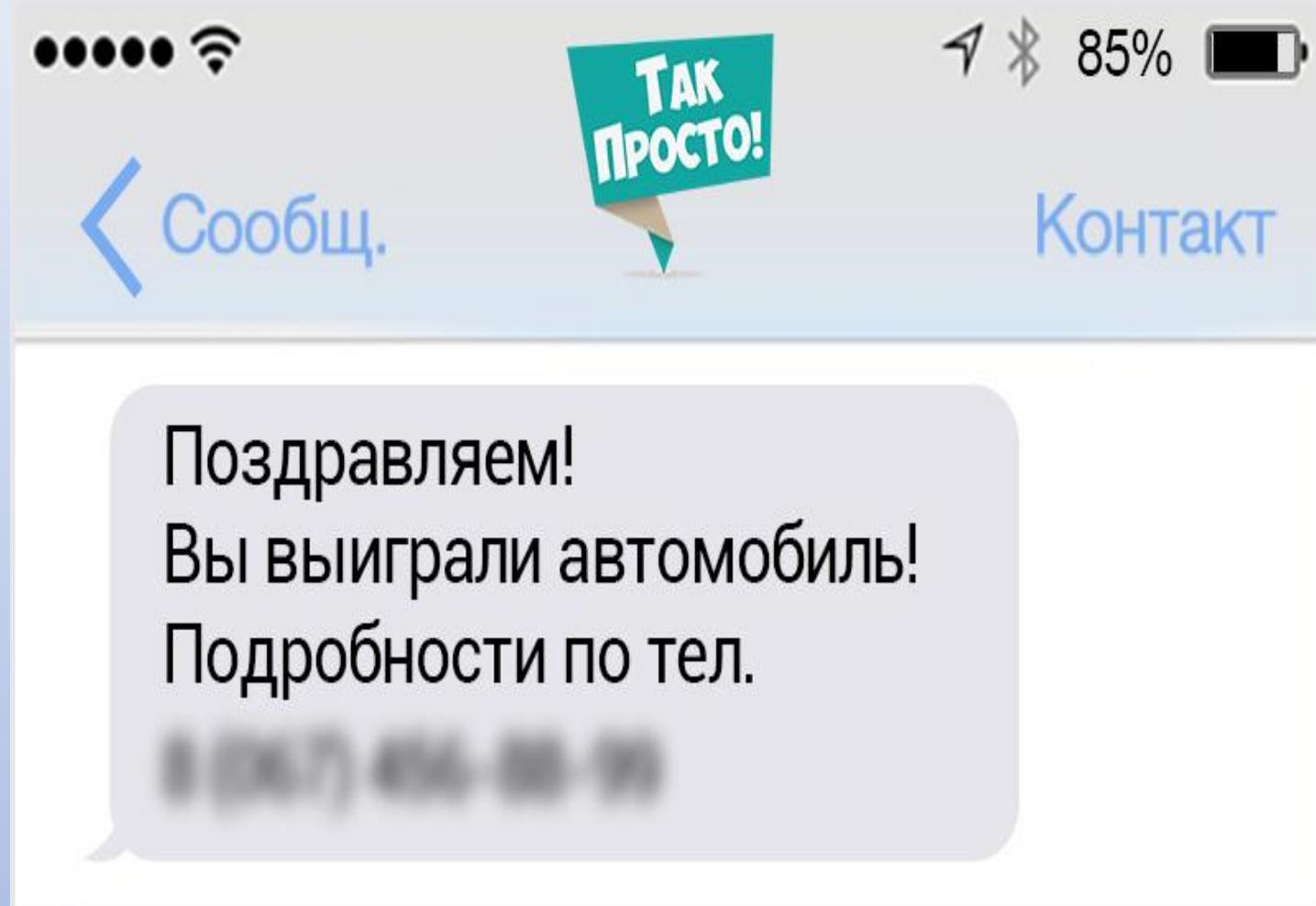


Сообщение о внезапном выигрыше

Вам могут сообщить о внезапном выигрыше в лотерею, предложить прибыльную работу или участие в беспроигрышном конкурсе. Взамен могут попросить перейти по ссылке, оплатить небольшой взнос или сообщить данные карты для перечисления вам «выигрыша».

Что делать?

Если вы действительно участвовали в лотерее, перезвоните на официальный номер компании, чтобы уточнить информацию о выигрыше. Не переходите по неизвестным ссылкам и не сообщайте реквизиты карты.



Просьба от мошенников о переходе по ссылке из SMS-сообщения

Во время разговора мошенники сообщают, что вам пришла ссылка в СМС, и настойчиво уговаривают ее открыть. Так злоумышленники хотят, чтобы под видом антивируса, банковского приложения или другого полезного сервиса вы установили вредоносную программу. Это позволит получить доступ к вашему смартфону и похитить данные или деньги, воспользовавшись мобильным банком, или подписать вас на платные рассылки.

Что делать?

Не переходите по ссылкам, которые присылают во время звонка, и не устанавливайте навязываемые приложения. Всю необходимую информацию ищите на официальных сайтах банков, а безопасные программы – в магазинах приложений.

Примеры SMS-сообщений мошенников

Ваша банковская карта заблокирована! По вопросам снятия блокировки обращайтесь по т. 8 (800) 555-17-94
Технический отдел

МАМ!кинь УТРОМ 500р.на89654064181(Билайн)Проблемы.Потом все объясню

Платеж 200,00 р зачислен 07.11 в 11:59 через QIWI(qiwi.www.ru)

07.11.2011 11:18

Извините клал жене 200 руб.ошибочно положил вам.жене положил ещё раз,верните дочке на ном.89108050497 это МТС.Она в больнице.Спасибо!

priz.europapluz.ru
Pozdravlaem! Vy vyigrali noutbuk `Asus VX-2`.
Podrobno po telefonu: [+7-912-144-78-67](tel:+7-912-144-78-67).
Europa+

Абонент Ира оставил Вам сообщение.
Открыть: tr.im/4jz7f

На ваше резюме поступила вакансия Зп до 77880 руб Сайт Zarplata.msk.ru

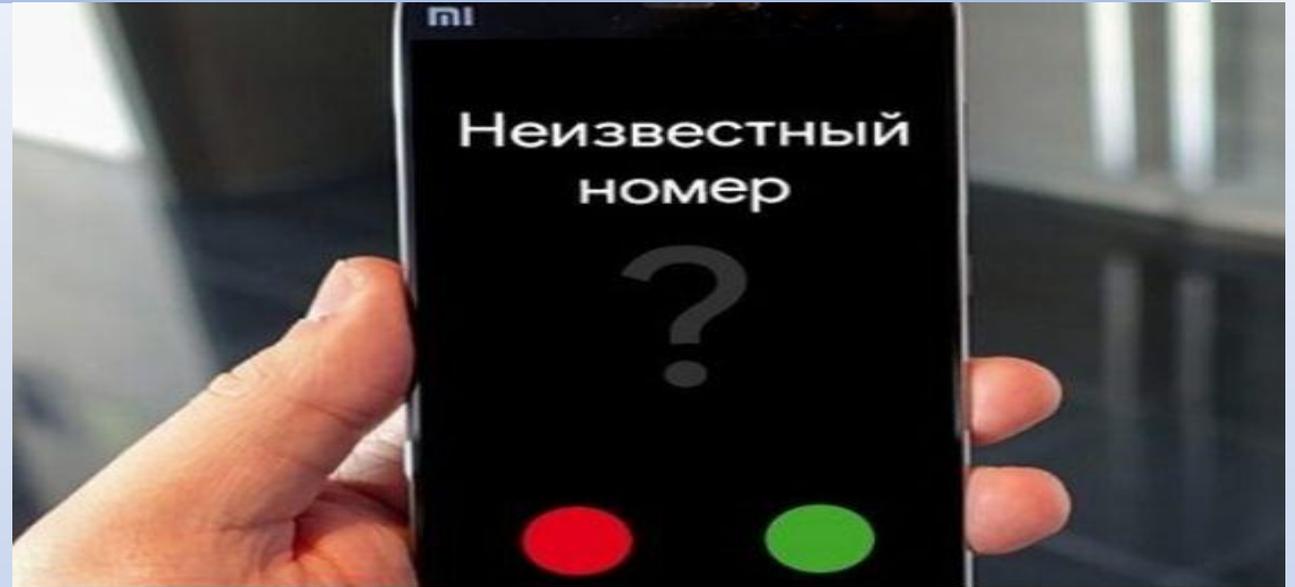
с ТОБОЙ хотят познакомиться.Для получения СПИСКА отправь: МУР на 5556

Сбрасывание звонков

Звонят с неизвестного номера и сбрасывают звонок? Скорее всего, это мошенники. Так они пытаются вынудить вас из любопытства перезвонить на этот номер, однако обратный звонок чаще всего оказывается платным. Иногда мошенники оставляют сообщение в голосовой почте – это повышает шанс, что вы решите перезвонить.

Что делать?

Не перезванивайте, если номер вам неизвестен. Установите программу или подключите сервис определения номеров мошенников. Эти сервисы распознают и блокируют звонки спамеров, в том числе замаскированные под официальные номера банков и ведомств. Номер проверяется в базе, и во время звонка высвечивается информация о том, кто вам звонит. Однако помните, что базы операторов не всегда обновляются автоматически, поэтому регулярно обновляйте их вручную и не теряйте бдительности.



**ЗАЧЕМ
ВАМ ЗВОНЯТ
С НЕИЗВЕСТНОГО
НОМЕРА
И СБРАСЫВАЮТ?**

Подведение итогов

Простые правила, которые помогут вам обеспечить свою безопасность и не стать жертвой телефонных мошенников.

1. Не паникуйте. Просто скажите «я вам перезвоню» и завершите разговор. Возьмите паузу и не принимайте поспешных решений.
2. Не сообщайте никому реквизиты карты, CVC/CVV-код на обратной стороне карты, коды из смс и ПИН-коды.
3. Не переводите деньги на счета незнакомых вам людей.
4. Не устанавливайте на смартфон приложения из непонятных источников.
5. Чтобы прояснить ситуацию, самостоятельно перезванивайте на горячую линию банка или государственного ведомства по телефонам, указанным на его официальном сайте.
6. Установите программу, которая проверяет звонки и умеет блокировать спам-вызовы.
7. Проверяйте информацию в официальных источниках.