ОСТОРОЖНО!!!
ТЕЛЕФОННЫЕ МОШЕННИКИ!!!
КАК НЕ ДАТЬ СЕБЯ ОБМАНУТЬ.

Что делать, если звонят мошенники? Основные правила, которым нужно следовать при телефонном мошенничестве.

Любой внезапный телефонный звонок может исходить от мошенников. Неожиданность — одна из главных причин, почему люди так часто попадаются на обман. Поэтому важно всегда быть готовым к тому, что на том конце провода окажутся злоумышленники. Предугадать это невозможно, поэтому остается следовать простым правилам.

Сохранять спокойствие

Обычно мошенники давят на два чувства — страх и корысть. В первом случае злоумышленники пугают жертву, что ее деньги или кто-то из ее близких находится в опасности. Во втором случае — "радуют" якобы внезапным выигрышем, выплатой и другими призами, от которых трудно отказаться.

Самое важное в этой ситуации — оставаться спокойным и не идти на поводу у эмоций. Именно необдуманных и импульсивных решений от жертвы и ждут злоумышленники.

Не сообщать свои личные данные

Даже если звонящий знает имя, фамилию и отчество жертвы, он может оказаться мошенником. Эти данные пользователи часто оставляют при регистрации на сайтах, поэтому найти их не составляет труда. Но более конфиденциальную информацию (данные паспорта, страховки, адрес и т.д.) мошенники не знают и обязательно попытаются вытянуть. Разглашать их нельзя.

Не сообщать коды, пароли и логины

Мошенники не могут получить доступ к деньгам жертвы, пока не получат пароль, полные данные банковской карты, CVV/CVC-код или секретный код для

подтверждения операции. Именно эти данные они и просят назвать в первую очередь, когда представляются, например, сотрудниками банка.

Эти данные нельзя передавать никому. Настоящие банковские сотрудники НИКОГДА не просят эту информацию, так как не имеют права получать к ней доступ — она полностью конфиденциальная.

Не выполнять то, о чем просят мошенники

На эмоциях жертвы могут выполнить все, о чем попросят злоумышленники: перевести деньги на "безопасный" счет, пройти к ближайшему банкомату, сменить пароль и т.д. Все эти действия направлены на то, чтобы украсть деньги жертвы, поэтому выполнять их нельзя. Любые проблемы настоящий сотрудник банка попросит решить в отделении банка, а не по телефону.

Не переводить деньги

Очевидно, что любые просьбы перевести деньги на "безопасный" счет, заплатить комиссию, чтобы забрать "выигрыш в лотерею" или получить подарок — самые простые способы обмануть жертву и украсть ее деньги.

Не переходить по ссылкам

Мошенники, которые представляются сотрудниками государственных организаций, часто могут попросить перейти по ссылке в SMS, чтобы заполнить бланк или анкету. Такие ссылки ведут на фишинговые сайты злоумышленников, которые выглядят как настоящие (обычно это Сбербанк, Авито и Госуслуги).

Не скачивать приложения

Еще один способ получить доступ к деньгам жертвы — заставить ее скачать и установить стороннее ПО. Мошенники могут назвать его "новой версией банковского приложения" или "безопасной версией", но верить этому нельзя. Любые программы, скачанные по ссылкам неизвестных людей, могут навредить телефону и передать личные данные пользователя злоумышленникам.

Сбрасывать вызов и перезванивать самостоятельно

Если звонок вдруг стал подозрительным, единственный верный выбор — сбросить вызов и перезвонить самостоятельно в ту компанию, от имени которой звонили мошенники: банк, налоговая, полиция и т.д. Если звонок и правда был совершен оттуда, сотрудники по официальному номеру это подтвердят.

Мошенники представляются сотрудниками полиции — как их быстро вычислить?

Телефонные мошенники все чаще представляются сотрудниками силовых структур РФ (Полиция, Росгвардия, ФСБ, МВД), ведь так вероятность напугать и запутать жертву намного выше.

Как работает схема?

Жертва получает звонок якобы от сотрудника полиции, ФСБ или МВД. Во многих случаях мошенники работают в команде: звонят от имени представителей разных структур и подтверждают слова друг друга, чтобы повысить уровень доверия. Основная задача мошенников — заполучить деньги жертвы, но делать они это могут разными способами.

Чаще всего развод связан с банком. Злоумышленники уведомляют жертву, что деньги на ее счету под угрозой по одной из нескольких причин:

1. Неизвестный пытался снять деньги жертвы или оформить на нее кредит.
2. Личные данные жертвы были «слиты» банковскими сотрудниками.
3. Независимо от выдуманной мошенниками причины, их цель заключается в том, чтобы заставить жертву снять деньги со своего счета и перевести их на «безопасный» счет, который на самом деле принадлежит злоумышленникам.
4. Реже встречается схема, где мошенники от имени сотрудника полиции вымогают деньги якобы за попавшего в беду родственника. Звонившие утверждают, что помочь

ему смогут, только после того, как жертва переведет определенную сумму денег (взятку) на указанный номер счета.

Как распознать обман?

Мошенники, представляющиеся сотрудниками силовых структур, работают примерно по одной и той же схеме. Именно по ее ключевым признакам и можно с уверенностью сказать, что на том конце провода находятся злоумышленники. Ниже перечислим, как мошенники себя выдают во время разговора:

1.Настаивают на том, что вся информация должна остаться в тайне. Используют такие фразы как «тайна следствия», «конфиденциальная информация», угрожают уголовной ответственностью в случае, если жертва попытается связаться и рассказать все членам семьи или друзьям.

Мошенникам не нужно, чтобы жертва консультировалась с другими людьми, которые могут распознать обман. И хотя закон о неразглашении данных предварительного расследования действительно существует, он действует только после того, как следователь получит соответствующую подписку. Если же звонившие упоминают о «неразглашении банковской тайны», то эта статья относится только к самим банкам и их сотрудникам.

2. Узнают о сумме, которая хранится на всех счетах жертвы. Мошенникам нужно знать, сколько денег они смогут получить, и как много жертва сможет снять в банкомате.

3. Спрашивают, в каких банках жертва хранит деньги, картами каких банков пользуется для оплаты покупок и получения заработной платы. Такая информация редко доступна злоумышленникам изначально. Чаще всего о жертве они знают лишь ее имя и номер телефона.

4. Вселяют недоверие к сотрудникам банка. Мошенники уверяют жертву, что украсть ее деньги хотят именно сотрудники банка, а значит доверять им и рассказывать о звонках «из полиции» нельзя. Так злоумышленники исключают для себя вероятность того, что жертва получит помощь извне и раскусит обман.

Неотъемлемой частью этой схемы является момент, когда жертва отправляется в банк, чтобы снять деньги. Так как речь чаще всего идет о крупной сумме, то получить ее без подтверждения своей личности у клиента вряд ли получится. Мошенники опасаются, что настоящие сотрудники банка смогут помочь жертве и отговорят ее снимать деньги. Поэтому во время всех действий с банкоматом они просят не контактировать с банковскими работники и не сообщать им настоящую причину снятия средств с карты.

5. Упоминают, что снятые жертвой деньги ей не принадлежат, а значит их обязательно нужно перевести на новый счет — уйти с ними домой просто так не позволят.

6. «Давят» банковскими терминами, законами и другой узкоспециализированной информацией. Задача мошенников — загрузить жертву информацией так, чтобы у нее не осталось времени на рассуждения.

7. Утверждают, что проблема решается по телефону. Мошенники будут всеми силами убеждать жертву в том, что ей не нужно приходить в отделение полиции или другой структуры, сотрудниками которой назвались неизвестные. Настоящие сотрудники вызывают свидетелей в отделение с помощью повестки, а не пытаются выяснить информацию по телефону.

Что делать, если по телефону представляются сотрудниками полиции, МВД или ФСБ?

Мошенники тщательно готовятся к звонкам жертвам, ведь убедить их становится все сложнее. Они могут называться именами реально существующих сотрудников структур и предлагать проверить эту информацию на официальных сайтах отделений.

Но самое убедительное для жертвы — это проверка официальных телефонных номеров. Если человек начинает сомневаться в словах мошенников, те используют последний козырь: предлагают жертве проверить номер отделения полиции или МВД на его официальном сайте, а затем перезванивают с этого номера. Для этого злоумышленники пользуются подменой номера, поэтому доверять любым номерам, с которых звонят «сотрудники» крайне не рекомендуется.