Телефонное мошенничество

Сегодня мошенники не вытаскивают деньги из кармана и не взламывает квартиры. Жертвы сами переводят деньги злоумышленникам или передают им конфиденциальные данные — так работает социальная инженерия

Как работают телефонные мошенники

- Около 30% мошеннических атак в России происходит через телефонные звонки. В большинстве случаев злоумышленники используют приемы социальной инженерии, которые позволяют выманить доступ к личным данным или заставить человека добровольно совершить какое-то действие, например снять деньги со счета.
- Это выглядит так: мошенник звонит человеку и представляется сотрудником банка, госструктур или мобильного оператора. Для связи обычно используют мессенджеры — так сложнее отследить звонок, а еще не нужно тратить деньги на звонки в другие города.

- Злоумышленник делает все, чтобы заставить человека нервничать: говорит, что взломали его банковский счет, аккаунт на Госуслугах или что на него завели уголовное дело. При этом сильно торопит собеседника, якобы на счету каждая минута.
- Мошенники рассчитывают на то, что в стрессе и спешке человек может поддаться на уловки — даже если раньше слышал, что звонки от службы безопасности банка или из отделения полиции не стоит воспринимать всерьез. В результате жертва сама переводит деньги мошенникам или сообщает информацию для доступа к счету или смартфону: код из SMS, номер карты, логины и пароли.
- Рассказываем о самых распространенных схемах обмана и о том, как не стать их жертвой.

Если вы столкнулись с конкретной схемой обмана, можете сразу перейти по одной из ссылок ниже.

Мошенники представляются сотрудниками полиции

Мошенники могут представляться специалистами разных госслужб, но чаще всего выдают себя за сотрудников правоохранительных органов. Они говорят человеку, что тот стал фигурантом уголовного дела, и выдумывают разные причины, например: «На ваше имя пытались взять кредит. Мы предотвратили эту попытку, но нам нужна ваша помощь, чтобы поймать преступника» или «Ваш счет использовался в преступных схемах. Мы завели дело о мошенничестве, и вы должны поучаствовать в расследовании».

Мошенники называют жертву по имени и отчеству и сообщают другую личную информацию, используют банковские термины, ссылаются на статьи уголовного кодекса. Иногда они работают группами: переключают с одного «представителя силовых структур» на другого, могут прислать документы с печатями, якобы переводят звонок на сотрудников других ведомств, например ФСБ и ЦБ.

При этом мошенники постоянно торопят жертву, подчеркивают, насколько важно то, о чем они говорят, призывают не вешать трубку и стараются как можно дольше удерживать человека на линии, чтобы он не мог в спокойной обстановке посоветоваться с близкими или юристом. Также злоумышленники убеждают собеседника в том, что информацию, которую он только что услышал, нельзя никому сообщать, иначе человеку грозит уголовное преследование.

Мошенник может попытаться что-то узнать о жертве: сталкивалась ли она раньше с обманом, картами какого банка пользуется, сколько денег лежит на счете. А потом начнет требовать, чтобы жертва назвала данные карты или перевела деньги. За отказ от сотрудничества мошенники угрожают уголовным делом.

Что делать. Помните, что 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. И тем более не соглашайтесь привозить наличные по определенному адресу или передавать их лично в руки какому-либо человеку.

Возьмите паузу и положите трубку: не бывает ситуаций, когда решения нужно принимать моментально.

Говорят, что звонят из службы безопасности банка

В такой схеме мошенник представляется сотрудником службы безопасности банка и сообщает человеку, что деньгам на его счете что-то угрожает. Злоумышленник просит ответить на контрольный вопрос или назвать банковские данные, например ПИН-код, номер карты или CVC-код.

При этом мошенник может попросить перевести деньги с карты на якобы безопасный счет, который на самом деле принадлежит ему или его сообщникам.

Как не попасться. Реальные сотрудники банка никогда не требуют информацию для доступа к счету или приложению.

Они также не просят сделать что-то со счетом, поскольку могут сами отменить операцию, заблокировать карту или доступ в личный кабинет, если заметят подозрительную активность. А значит, им незачем торопить клиента и просить его срочно принять какое-то решение.

Специалисты банка говорят с клиентом спокойно, не давят. А если вы захотите сбросить звонок и перезвонить в банк, поддержат это решение.

Уверяют, что произошла внутрибанковская утечка

Есть еще одна, менее известная схема мошенничества, когда жертве говорят, что произошла утечка данных и кто-то из сотрудников решил украсть деньги. Так человека пытаются настроить против настоящих специалистов службы безопасности. При этом злоумышленник предупреждает собеседника о возможном звонке специалистов из реальной службы безопасности и уверяет, что верить им нельзя, даже если они будут рассказывать о мошеннических схемах.

Цель мошенника — убедить жертву, что доверять можно только ему.

Также злоумышленники могут сказать собеседнику, что кто-то скомпрометировал его личный кабинет и, чтобы поймать сотрудника-мошенника, нужно якобы имитировать перевод. Для этого человека убеждают, что личный кабинет, который он видит на своем экране, — фейк, который поможет банку отследить недобросовестного работника, а значит, клиент отправляет деньги как бы понарошку, они никуда не уйдут. Хотя на самом деле человек видит настоящий интерфейс и переводит деньги прямо на счет мошенников.

Еще один вариант: мошенники звонят жертве от имени полиции и говорят, что деньги украли не со счета в их банке, а с единого межбанковского счета ЦБ, доступ к которому якобы есть только у сотрудников банка, где обслуживается жертва. Дальше человека переводят на работника Центробанка, который предлагает застраховать деньги жертвы на едином межбанковском счете ЦБ, а для этого перевести деньги на специальный счет. На самом деле никакого единого счета ЦБ не существует — человек просто переводит деньги мошенникам.

Как не попасться. Злоумышленники могут подделать номер банка, и на телефоне высветится знакомый набор цифр. Поэтому лучше убедиться,

что звонок был из банка, — для этого позвоните по официальному номеру, который указан на его сайте или позвоните по номеру 8 (843) 231-72-87. Если из банка не звонили и вы сообщили мошенникам данные карты, ее заблокируют, перевыпустят и передадут информацию настоящей службе информационной безопасности.

Представляются сотрудниками мобильного оператора

Мошенники звонят от лица сотового оператора под разными предлогами. Чаще всего они говорят, что:

- у абонента заканчивается срок действия сим-карты и нужно продлить договор;
- от него поступила заявка на смену номера;
- из-за технического сбоя его перевели на тариф подороже.

Еще злоумышленники предлагают бесплатно подключить 5G.

Чтобы подключить новую услугу или отменить ошибочную операцию, мошенники просят назвать код из SMS. На самом деле код нужен, чтобы взломать личный кабинет жертвы на сайте мобильного оператора и настроить переадресацию сообщений на свой номер. Этого достаточно, чтобы взломать аккаунт на Госуслугах или банковский счет и вывести сбережения.

Как не попасться. Никому не называйте код из SMS. Сотрудникам мобильного оператора такая информация ни к чему: чтобы подключить новую услугу или отменить операцию, они просят назвать клиента персональные данные, например серию и номер паспорта.

Если чувствуете подвох, положите трубку и перезвоните в поддержку по официальному номеру:

- Т-Мобайл — 8 800 555-49-29;
- МТС — 0890;
- Билайн — 0611;
- Мегафон — 0500;
- Теле2 — 611.

Этого достаточно, чтобы проверить, действительно ли с сим-картой есть проблемы.

Пугают взломом Госуслуг

Злоумышленники представляются сотрудниками поддержки Госуслуг и говорят, что из-за утечки все данные попали к преступникам и прямо сейчас они взламывают аккаунт.

Другой сценарий — профиль на Госуслугах уже взломали и прямо сейчас мошенники пытаются оформить через него кредит. Чтобы им помешать, нужно сменить пароль от аккаунта — для этого достаточно назвать код из SMS.

Если жертва назовет цифры, мошенники взломают аккаунт — и теперь уже действительно смогут взять кредит на чужое имя, получить налоговый вычет или продать данные на черном рынке.

Как не попасться. Служба поддержки Госуслуг никогда не запрашивает персональные данные, логины, пароли и секретные слова. Если слышите подобное, положите трубку и сообщите о произошедшем команде портала по номеру 8 800 100-70-10 или 115 с мобильного.

Включите оповещение о входе: если мошенник войдет в ваш личный кабинет, вы сразу об этом узнаете. Для этого откройте свой профиль на Госуслугах → «Безопасность» → «Вход в систему» → выберите «Оповещение после входа» и перетащите ползунок вправо.

Просят установить фальшивое приложение

От лица сотрудников госслужб или банка мошенники просят установить антивирус, новую версию банковского приложения, сервис для диагностики телефона или уплаты налогов.

На самом деле это программа удаленного доступа. С ее помощью преступники видят все, что происходит на телефоне другого человека, и могут им управлять, например смотреть, какие пароли вводят, и читать SMS.

Как не попасться. Скачивать приложения только по ссылкам с официальных сайтов. Смотреть на рейтинг приложения, количество загрузок, проверять отзывы и использовать антивирус.

Как понять, что звонят мошенники

Если вам позвонили с незнакомого номера и требуют что-то сделать, задайте себе один из вопросов ниже. Если хотя бы один из пунктов совпадает, это повод насторожиться. Положите трубку и спокойно обдумайте ситуацию, если

нужно, позвоните родственникам или сами перезвоните в банк по одному из номеров, указанных на официальном сайте.

Кто звонит?

- Сотрудник колл-центра.
- Сотрудник службы безопасности банка.
- Сотрудник правоохранительных органов, например полиции или ФСБ.
- Сотрудник Центробанка или других госструктур.
- Сотрудник мобильного оператора.
- Телефонный бот.

Что говорит?

- «С вашего счета пытаются списать средства».
- «На вас оформили кредит».
- «Ваш родственник в опасности, и ему срочно нужны деньги».
- «Ведется расследование, нужна ваша помощь».
- «Заканчивается срок действия сим-карты».
- «Мошенники взломали Госуслуги».

Что просит сделать?

- Сообщить персональные данные: кодовое слово, код из Push-сообщения или SMS, реквизиты карты, логин и пароль от аккаунта на Госуслугах.
- Перевести средства на безопасный счет или открыть новый счет, а старый закрыть, так как он был скомпрометирован.
- Снять деньги в банкомате.
- Оформить кредит.
- Сформировать QR-код в приложении банка и прислать его.
- Установить специальное приложение.