Основные схемы обмана граждан телефонными мошенниками, и как не попасться на их уловки

Правила поведения в случае мошеннических атак:

Ни в коем случае нельзя сообщать звонящему никакую информацию: ни личные данные, ни данные о банковских карточках, вкладах.

Нельзя переходить по предлагаемым ссылкам.

Нельзя вводить, сообщать коды из смс.

Нельзя переводить деньги на неизвестные счета «для сохранения» или в качестве «отступных».

Не смотря на то, что тема с телефонными мошенниками постоянно освещается в интернете и СМИ, люди довольно часто попадаются на удочку мошенников и этот вид криминального бизнеса процветает.

Виды мошенничества:

1. **Короткий вызов и сброс**

Самый частый и относительно самый безобидный с точки зрения потенциальных убытков сценарий. Мошенники регистрируют свой номер как платный, звонят потенциальной жертве и сразу сбрасывают вызов, ожидая, что абонент им перезвонит. И многие перезванивают. И если абонент перезванивает, то с его мобильного счета списывается некая сумма за звонок на платный номер. Размер суммы зависит от тарифа, который установлен мошенниками за входящие звонки на платный номер при его регистрации.

Таким образом, не надо перезванивать на номера, с которых идет вызов с быстрым сбросом звонка.

2. **Звонок о попавшем в беду родственнике**

Одна из самых старых, но до сих пор работающих схем . Такие звонки осуществляются мошенниками обычно поздним вечером, ночью или под утро. Полусонной потенциальной жертве сообщается, что с родственниками (или друзьями произошла беда. Какая это беда – зависит от фантазии мошенников. Сбил за рулем автомобиля пешехода, замешан в криминальной истории, попал в полицию, проиграл в карты, катастрофа, авария и т.д. В любом из сценариев необходимо срочно перевести или передать крупную сумму денег, чтобы не возбуждалось уголовное дело, заплатить врачам в больнице, оплатить транспортировку человека в тяжелом состоянии вертолетом, расплатиться с карточным долгом и т.д. Иногда первым общается

с абонентом якобы его родственник или друг попавший в беду, истерическим тоном и с фоновыми шумами, криками, а затем трубка передается тому, кто проблему может решить. Он-то и называет сумму и способ передачи денег.

В случае подобного звонка необходимо первым делом перезвонить самому родственнику или другу, от чьего имени звонят мошенники. С вероятностью 99,9% с ними все в порядке и никаких денег никому переводить и передавать надобности нет.

3. Звонок из банка или государственных органов

Абоненту могут звонить от имени менеджера банка, могут от имени службы безопасности банка. Могут звонить как с обычного мобильного номера,
так и с поддельного короткого номера банка. Могут назвать реальные фамилию,
имя и отчество абонента (практически любые базы данных без проблем покупаются в интернете). Задачи звонящего могут быть тоже разными, но цель одна – ваши накопления. Существуют следующие схемы:

попытка выяснить номер банковской карты, CVV-код и другие данные. Причинами могут назвать сбой программного обеспечения банка, попытка проведения подозрительной транзакции, восстановление счета, возврат денег, просьба подтверждения перевода денег или заполнение протокола безопасности

заставить перевести накопления на «защищенный» счет для предотвращения потери денег. Озвучиваемая причина – мошенническая попытка снять деньги со счета абонента (на самом деле деньги будут переведены на счет мошенников) или восстановление счета после компьютерного сбоя.

попытка выяснить банковскую информацию (секретный код из настоящего сообщения от банка) для отключения платных услуг, которые были подключены клиенту банка «по ошибке».

В таких случаях необходимо сбросить текущий звонок и перезвонить самому в банк по номеру, указанному на банковской карте или на сайте банка.

4. Звонок об ошибочном переводе денег

Звонок или сообщение поступает от человека, который «по ошибке» перевел деньги на счет мобильного телефона абонента или на его карту (счет), с просьбой вернуть ему деньги. При этом деньги действительно могут поступить. Порядочный человек тут же постарается вернуть чужие деньги.

Вполне возможно, что если деньги поступили на счет по номеру мобильного, то мошенники от имени абонента, указав его номер, выставили несуществующий товар на интернет-сервисе для размещения объявлений (например, Авито). Добросовестный покупатель оплатил товар, а мошенники попросят перевести якобы ошибочный перевод на их номер. В результате претензии за оплаченный, но не предоставленный товар будут предъявлены именно абоненту, на номер которого скинул деньги покупатель. Если «ошибочные деньги» пришли на карточку или банковский счет, то вполне возможно, что мошенники пытаются провести легализацию денег и запутывание следов украденных денег с банковских карт через карту или счет абонента. В таком случае, если вам поступили чужие средства (по ошибке отправителя или от мошенников), то необходимо обратиться в банк и произвести возврат средств, а не перечислять деньги по реквизитам, которые указывает звонящий.

5. Звонок или сообщение о выигрыше в лотерее

Звонок или сообщение поступает якобы от организаторов лотереи с радостной новостью о том, что вы счастливчик и вам полагается выигрыш (денежная сумма, бытовая техника и т.д.). Далее следует требование перевести мошенникам небольшую сумму для покрытия издержек на организацию лотереи или для оплаты налога с выигрыша.

Необходимо знать, что по закону все расходы на проведение лотереи ложатся на организаторов лотерей. А оплата налога на выигрыш осуществляется либо организаторами (выигравший получает сумму за вычетом налога), или победитель оплачивает налог самостоятельно, но после получения выигрыша.

6. Сообщение о необходимости подключения выбранной услуги

В интернете или через рассылку рекламируется какая-либо услуга, которая может заинтересовать абонента и имеет очень привлекательные условия. Для активации услуги заинтересованному абоненту отправляется сообщение о том, что для активации услуги необходимо отправить сообщением на указанный короткий номер подтверждение на согласие подключения услуги. Как правило данный короткий номер является подменным, зарегистрирован как платный (о чем, естественно, в сообщении информации нет). При отправке сообщения на данный номер со счета абонента списываются деньги.

При получении сообщения о необходимости подтверждения подключения услуги, путем отправки сообщения на короткий номер, следует насторожиться, так как существует очень большая вероятность, что со счета

за отправку сообщения будут списаны деньги, а рекламируемая услуга подключена не будет.

7. Звонок о возникшей проблеме на стороне сотового оператора

Звонящий представляется сотрудником сотового оператора, который обслуживает абонента. Сообщает о проблемах со связью, которые были на стороне оператора. Чтобы в дальнейшем исключить повторение сбоев абоненту предлагается произвести необходимые настройки на его стороне и для этого ввести на смартфоне комбинацию цифр, которые сейчас ему продиктует звонящий сотрудник. В противном случае сотовый оператор не только не гарантирует устойчивую связь, но и при определенных обстоятельствах СИМ-карта абонента может быть заблокирована оператором. Как правило данная ситуация говорит о том, что мошенникам известны все необходимые данные карты или счета абонента и для подтверждения финансовой транзакции (перевода денег со счетов абонента, т.е. банальной кражи) абоненту предлагается ввести код для подтверждения перевода средств.

В данном случае необходимо просто закончить разговор с мошенниками и ни в коем случае не вводить на смартфоне озвучиваемую лже-сотрудником комбинацию цифр.

8. Звонок или видео звонок «проверка связи», реклама услуги, опрос

В данной схеме обмана вариантов для причины звонка у мошенников великое множество. Это может быть звонок якобы от оператора сотовой связи, который проверяет качество связи. Может быть предложение услуги или товара. Может быть мнимый социологический опрос. Абоненту задают вопросы – он на них отвечает. Задача мошенников заполучить запись голоса абонента с ключевым словом «ДА». Так как некоторые банки уже ввели биометрическую идентификацию клиентов при совершении финансовых операций, то мошенникам для кражи средств со счетов абонента необходимо лицо и голос абонента. Сказанное абонентом и записанное мошенниками «ДА» (или другие необходимые им фразы) может при биометрической идентификации стать якобы согласием абонента на списание средств.

Необходимо быть осторожным при звонках с неизвестных номеров. Стараться не произносить «ключевые фразы», которые теоретически могут стать голосовым подтверждением списания средств. А лучше сразу же завершить такой разговор и ничего не говорить даже с целью потратить время мошенников.

9. Звонок из налоговой службы

Звонящий представляется инспектором налоговой службы. Озвучивается любая версия якобы проблемы абонента с налогами. Задаются уточняющие вопросы, цель которых узнать, как можно больше личных сведений и данных об абоненте. Абонент обычно готов предоставить звонящему любые личные сведения и данные, чтобы бы не иметь проблем с налоговой службой. Обычно разговор заканчивается тем, что инспектор вроде как понял, что «ошибочка вышла» и претензий у налоговой к абоненту нет. Абонент рад тому, что проблема разрешилась. На самом деле для абонента проблемы могут только начинаться, так как полученные таким путем данные об абоненте могут (и будут) использоваться мошенниками в других схемах.

10. Сообщение о неиспользованных бонусах

Абоненту приходит сообщение о том, что на его счету скопились бонусы или скидочные баллы на довольно приличную сумму, но срок возможности их использования истекает. Абонент теряется в догадках где это он заработал столько бонусов. Далее «случайно выясняется», что абонент не активировал свой аккаунт в этом магазине. Чтобы воспользоваться бонусами, ему дают ссылку для регистрации аккаунта в известном интернет-магазине. На самом деле перейдя по ссылке абонент попадает на фейковый сайт, который является точной копией реального интернет магазина. На радостях абонент совершает покупки, частично оплачивает их бонусами, а для оплаты остальной суммы должен ввести данные своей карты (эти данные и используют мошенники, опустошая карточный счет абонента).

Не следует доверять таким сообщениям, особенно если вы не понимаете каким образом и за что были начислены бонусы. По ссылке переходить тоже не следует, но если уж перешли, то необходимо в адресной строке внимательно посмотреть адрес сайта, на котором вы оказались. Адрес мошеннического сайта может быть очень похож на адрес настоящего интернет-магазина и отличаться от последнего всего одной буквой. А уж вводить данные своей карты в такой ситуации – это значит заранее попрощаться со своими деньгами.

11. Заманчивое сообщение со ссылкой

Абоненту приходит сообщение, в котором описаны «скидки, подарки, распродажи, «секретная» информация и т.д. (все зависит от фантазии мошенников). Чтобы получить обещанное предлагается перейти по ссылке, которая имеется в сообщении. Не важно, от ожидания выгоды,

халявы или простого любопытства, но если абонент переходит по ссылке, то на смартфон устанавливается вирусное приложение, которое дает мошенникам доступ к данным мобильного приложения банка абонента. Не трудно догадаться, что очень быстро мошенниками будут украдены все деньги с карт абонента.

Ни в коем случае нельзя переходить по ссылкам, которые находятся в сообщениях, пришедших с неизвестных номеров телефонов и электронных адресов.

12. Сообщение с просьбой спасти животных

Абоненту приходит жалостливое сообщение о том, что где-либо (в приюте для животных, зоопарке, на ферме) собираются усыпить животных (кошек, собак, лошадей, попугайчиков и т.д.). Чтобы спасти животных необходимо позвонить по указанному номеру и договориться о том, чтобы забрать бедное животное к себе и тем самым спасти его. Если нет возможности забрать животное к себе, то абоненту рекомендуется переслать данное сообщение друзьям и знакомым, которые возможно смогут взять животное к себе (тем самым повышается доверие к сообщению, ведь придет оно вам от друга или родственника). Сердобольные абоненты, готовые предоставить кров бедному животному, перезванивают по указанному номеру. В результате, с баланса перезвонившего списывается кругленькая сумма, так как номер оказывается платным.

При получении жалостливых сообщений с такими историями не следует перезванивать на указанный номер телефона и пересылать эти сообщения другим абонентам.

Чтобы не попасться на удочку мошенников:

не паникуйте, успокойтесь и постарайтесь трезво мыслить в стрессовой ситуации, которую пытаются создать для Вас мошенники

не перезванивайте на незнакомые номера

если в разговоре с Вами человек представляется работником банка, государственных органов, представителем фирмы и т.д. – лучше найти на сайте организации официальный номер и перезвонить на него самому

не сообщайте в разговоре личные данные, данные счетов, пластиковых карт и т.д.

не переходите по ссылкам из сообщений

не реагируйте на звонки или сообщения о выигрыше в лотереях или розыгрышах, в которых Вы не участвовали

если Вам предлагают выгодные услуги, скидки и т.д., прекратите разговор

не перечисляйте деньги по реквизитам, указанным в сообщении или озвученным мошенниками

В памятке рассказано лишь об основных схемах, которые используют телефонные мошенники для кражи денег и персональных данных у доверчивых граждан. У каждой из этих схем есть множество вариаций, используемых предлогов и причин.