Профилактика преступлений, совершаемых дистанционным способом с помощью информационно-телекоммуникационных технологий. Как не стать жертвой телефонных мошенников

«Мобильное мошенничество» – один из самых распространенных методов, используемых злоумышленниками для незаконного заработка. Избежать незавидной роли пострадавшего поможет знание методов, с помощью которых представители криминального мира пытаются обмануть граждан.

Чаще всего жертвами телефонных мошенников становятся пожилые люди старше 60 лет: они более доверчивы в силу своего воспитания. Но бывает, что на уловки мошенников попадаются и клиенты банков в возрасте от 20 до 40 лет. Причина этого кроется в беспечности людей и невысоком уровне финансовой грамотности.

Кроме того, в разговоре с владельцами банковских карт мошенники используют приемы социальной инженерии – незаконного метода получения информации, при котором человек сам предоставляет все конфиденциальные сведения о карте. Если раньше большинство преступлений в этой сфере совершали одиночки из мест лишения свободы, то сегодня орудуют хорошо организованные преступные группы. И они прекрасно разбираются в человеческой психологии и методах воздействия на нее. Так, потенциальным жертвам звонят молодые девушки и мужчины с хорошо поставленным голосом и прекрасной дикцией. А на заднем фоне во время разговора слышен гул контактного центра - мошенники имитируют и его. Номера телефонов и пластиковых карт мошенники находят в банковских базах данных, которые сами и взламывают или получают от нечестные сотрудники финансовых учреждений.

Сообщение о блокировке банковской карты

Вершину телефонных мошенничеств возглавляет афера с отправкой SMS-сообщений с текстом, что ваша платежная карта банка заблокирована. И тут же в конце сообщения указывается номер, на который необходимо позвонить для ее мгновенной разблокировки.

После того как вы совершите звонок, оператор объясняет, что действительно произошел сбой системы и теперь нужно полностью назвать номер карты и ПИН-код для перерегистрации в базе данных. Люди, попавшись на уловку, по неосторожности называют всю информацию и сразу же лишаются всех денежных средств, которые были на счету.

ЗАПОМНИТЕ: ПИН-КОД И НОМЕР КАРТЫ НЕ ДОЛЖНЫ БЫТЬ ИЗВЕСТНЫ НИКОМУ, КРОМЕ ВАС.

Звонок о совершенном ДТП

Несколько лет уже процветает схема, по которой злоумышленники, совершив звонок, сообщают, что близкий родственник виноват в аварии, повлекшей жертвы, а для снятия ответственности требуют заплатить большую сумму денег сотрудникам правоохранительных органов через курьера.

Родители, родственники, услышав, что их ребенок или родственник попал в беду, готовы мгновенно отдать все ценности, лишь бы избежать наказания. Вскоре мошенники совершают второй звонок семье, чтобы уточнить время встречи с курьером. Большинство таких схем заканчивается тем, что родители (родственники), будучи в состоянии аффекта, передают большую сумму денег, аферистам.

Запомните: если поступил звонок с неизвестного номера и сообщают о происшествии, случившемся с близким родственником, то не спешите верить. Сразу же набирайте номер члена семьи, о ком идет речь, и уточняйте лично информацию. Затем звоните в правоохранительные органы и сообщайте о телефонном мошенничестве.

Звонок о хулиганстве близкого родственника

Схема, похожая с предыдущим вариантом, но немного видоизменена. Мошенники действуют по похожему сценарию, звоня семье и сообщая, что их ребенок виноват в краже или разбойном нападении на магазин и т.д.

Также встречается вариант, когда звонок происходит якобы от охраны супермаркета, где их ребенок разбил дорогостоящую витрину.

Родители, услышав такое, сразу готовы отдать необходимую сумму, чтобы решить проблему, без привлечения полиции.

Запомните: сразу звоните члену семьи и выясняйте, что произошло на самом деле. Если он отрицает подобное, то следующий звонок должен быть в правоохранительные органы.

Сообщение о выигрыше

Мошенники отправляют сообщения на телефон с текстом о вашем выигрыше большой суммы денег или автомобиля. Но чтобы получить вознаграждение, необходимо всего лишь заплатить налоговый сбор через банковский перевод или пополнение абонентского номера. Человек, обрадовавшись новости, готов заплатить нужную сумму, лишь бы получить выигрыш.

Запомните: если вы не принимали участие в лотереях, то внезапных побед тоже быть не может.

Продажи через интернет

С развитием современных технологий теперь можно совершить продажу любой ненужной вещи, поместив рекламу на торговой площадке в интернете. Воспользоваться услугой способен каждый пользователь, оставив под объявлением свой телефон. Не только потенциальные покупатели просматривают рекламу, но и мошенники.

Аферисты, позвонив по указанному ваши телефону, сообщают о готовности купить вещь. А для того чтобы они смогли совершить денежный перевод, необходимо назвать ваш номер банковской карты. Вы, будучи рады быстрому покупателю, называете номер, не чувствуя подвоха.

Затем через некоторое время снова звонит тот же аферист, объясняя, что перевод не получается совершить. Для этого нужно назвать еще три цифры, но расположенные на обороте. Получив такую информацию, мошенник без труда завладеет вашими средствами.

Запомните: не сообщайте никому трехзначный номер, указанный на обратной стороне карты.

Звонок от мобильного оператора о призе, либо о необходимости подключить новый тарифный план

Телефонные мошенники уверенны, что представившись оператором мобильной связи, смогут войти в доверие абонента. Схема выглядит следующим образом: поступает звонок, где оператор радостно сообщает, что ваш номер попал в тройку лидеров на выигрыш дорогого телефона.

Чтобы стать окончательным победителем вам предлагают перевести небольшую сумму денег на счет организатора конкурса.

Запомните: операторы никогда не требуют пополнять банковские карты. Сразу звоните в полицию и сообщайте про мошенников.

В другом случае мошенник в ходе телефонного разговора с абонентом сообщает, что тарифный план более поддерживается оператором и необходимо произвести подключение к новому тарифному плану, путем набора на телефоне комбинации цифр. В этом случае жертва также лишается денежных средств.

Запомните: никогда не набирайте на телефоне сомнительные коды, в предназначении которых не уверены.

Выгодное предложение работы

Злоумышленники размещают в газетах или в интернете объявления о невероятной вакансии с зарплатой в 2000$ и бесплатной комнатой в общежитии. При этом отсутствует адрес и конкретные обязанности.

А для того чтобы записаться на собеседование необходимо отправить сообщение на короткий номер. В результате после отправки, ваш баланс на телефоне обнуляется.

Запомните: если в объявлении о вакансии не указана полная информация о работе, а для связи предоставлен короткий номер телефона, то перед вами мошенническая организация.

Просьба перечислить деньги больному ребенку

Мошенники рассылают сообщения на любые номера, с текстом о тяжелобольном ребенке. В сообщении также указывается номер банковской карты.

Запомните: не зная полной информации об этой ситуации, вы рискуете перевести свои средства мошенникам.

Звонок родителям

Эта схема основана на использовании вашего телефона злоумышленниками. На улице к вам подходит порядочно одетая женщина, которая слезно просит дать ваш телефон, чтобы позвонить ее больным родителям. Аргументирует это тем, что ее телефон разрядился.

Стараясь помочь человеку, вы сразу даете согласие на звонок. Женщина набирает телефон, но после этого ваш счет полностью обнуляется. Аферисты обычно звонят на платные номера, которые снимают все ваши деньги.

Запомните: чтобы не стать жертвой обманщиков, не передавайте свой телефон в чужие руки.

Сообщение о списании средств с банковской карты

Злоумышленники отправляют сообщения с текстом, полностью идентичным банковскому уведомлению о списании средств за совершенную покупку. Ниже указывают номер, по которому можно узнать подробную информацию.

Получив такое сообщение, человек находится в недоумении о случившемся, и сразу набирает указанный номер. После совершенного звонка, можно обнаружить отсутствие денег на счету телефона.

Запомните: получив такое уведомление, проверьте сначала баланс карты и совершенные платежи. Звоните только в справочную службу банка, который вас обслуживает.

Звонок от службы безопасности банка

Аферисты разработали новую схему, при которой звонят на номера, и представляются представителями службы безопасности банка. При этом они утверждают, что ваша банковская карта сегодня подвергалась несанкционированному взлому.

Чтобы обезопасить свой счет, необходимо провести идентификацию данных, назвав полностью фамилию, имя, отчество, номер карты и пароль.

Запомните: при звонке с банка попросите уточнить, кому они звонят. Обычно злоумышленники, набирают номера наугад, не зная информации про вас. Кроме того, никогда не передавайте данные о банковской карте и ее пароле.

Просьба пополнить телефон

Распространения получила схема, при которой на телефон приходит SMS-сообщение с текстом «Мама, срочно переведи деньги на счет. Потом перезвоню!»

Этот вид мошенничества также тщательно планируется, подбирая телефонные номера семьи со старшеклассниками. Заботливые родители, стараются помочь своему чаду и пересылают некоторую сумму денег на номер, с которого пришло уведомление.

Запомните: при подобном сообщении сразу звоните своему ребенку и выясняйте подробности.

Вирусное ММС-сообщение

Опытные мошенники стараются получить доступ к вашим банковским счетам через рассылку вирусных сообщений. Приходит сначала обычное SMS-сообщение, в котором указана информация, что вам поступило ММС, но чтобы его получить перейдите по указанной ссылке.

Если пользователь телефона отреагирует и перейдет на указанный сайт, то телефон автоматически подвергается вирусной атаке. Вы ничего, не заподозрив,

станете жертвой очередной аферы, при которой все ваши секретные пароли будут изъяты мошенниками.

Запомните: не поддавайтесь на подобные сообщения, игнорируйте призывы посетить какой-либо сайт через телефон.

Вирусное приложение

Жертвой хитрых мошеннических схем может стать каждый. Обладателям телефонов с операционной системой Android необходимо быть наиболее внимательными. Злоумышленники создают мобильные игры, приложения, которые при установке выдают сообщение «Критический сбой системы Android» или «Android software update».

Пользователь телефона, нажимая на сообщение, сразу попадает на сторонний сайт. Те, кто стал жертвой подобной схемы, утверждают, что приложение автоматически начало отправлять смс-сообщения на платные номера до полного обнуления баланса.

Запомните: качественный антивирус сохранит ваш телефон от действий злоумышленников. Также не используйте сомнительный контент.

Вирусная блокировка компьютера

Неопытные пользователи компьютера могут стать жертвой мошенничества, который основан на всплывающей рекламе и оповещающем о вирусном заражении системы.

Чтобы обезопасить систему, необходимо отправить смс-сообщение на короткий номер. По неопытности пользователи могут выполнить просьбу мошенников, что приведет к исчезновению денег на счету телефона.

Запомните: не обращайте внимания на рекламные оповещения в интернете. Полностью игнорируйте подобные сообщения. Если сообщение вызывает сомнение, то проконсультируйтесь у более опытного пользователя.

Сообщение от оператора связи

Мошенники рассылают SMS-сообщения от имени мобильных операторов с текстом о предоставлении вам нового эксклюзивного тарифного плана или денежного бонуса в качестве компенсации за кратковременный сбой в сети.

Далее следует информация, что для вашего согласия, отправьте пустое смс-сообщение на этот же номер. После этого аферисты получают всю денежную сумму с вашего телефонного счета.

Запомните: удостоверьтесь у мобильного оператора в телефонном режиме об этой акции. Если подобного не подтвердят, то это должно стать для вас веским аргументом проигнорировать смс-сообщение.

Продажа поддельных и нелицензированных биологически активных добавок (БАДов)

В недобросовестной рекламе, попадающей даже в телевизионные средства массовой информации, БАДы позиционируются как высокоэффективные средства для лечения практически всех заболеваний. Естественно, любая торговля «панацеей» - это преступный обман. К тому же БАДы, как правило, стоят немалых денег, а попадаются на эту удочку обычно малообеспеченные граждане, пенсионеры и инвалиды. Некоторые средства, продаваемые таким образом, могут быть не только бесполезны, но и вредны для здоровья.

Опознать недобросовестных «лекарей» несложно. Обычно БАДы распространяют нелегальные торговцы, выдающие себя за медработников. Эти люди обзванивают или обходят квартиры и даже организации, навязывая свои услуги по диагностике и лечению любых болезней.

Запомните: покупать биологически активную добавку к пище можно только в аптеках, аптечных магазинах, аптечных киосках, специализированных магазинах по продаже диетических продуктов или специальных отделах магазинов.

Ошибочный перевод средств

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

На самом деле происходит следующее: чтобы во второй раз списать сумму с Вашего счёта, злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. То есть первый раз Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

Не следует поддаваться на обман. Если Вас просят перевести якобы ошибочно переведённую сумму, напомните, что для этого используется чек.

Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник.

Итак, основные способы и меры защиты от телефонного мошенничества:

1. Если вам прислали СМС, в котором предупреждают о блокировке вашей карты, ни в коем случае не отвечайте и не перезванивайте по этому номеру. Если сомневаетесь в правдивости поступившей информации, позвоните в службу поддержки или задайте вопрос в официальных сообществах вашего банка в социальных сетях.

2. Если мошенники вам звонят, представляясь сотрудником службы безопасности банка, не вступайте с ними в диалог, а сразу завершайте разговор. Помните: сотрудник банка никогда не будет просить у вас номер карты и тем более ПИН-код.

3. Сообщать пароли и данные своей банковской карты нельзя никому. Не поддавайтесь на провокации, лучше сразу свяжитесь с вашим банком по номеру телефона, указанному на карте, и уточните всю информацию.

4. Получив звонок или сообщение, постарайтесь успокоиться и не принимать решение сразу. Лучше сказать звонящему, что вам необходимо время, чтобы всё обдумать.

5. Никогда и ни при каких обстоятельствах не сообщайте никому своих персональных данных или конфиденциальной информации: пин-код банковской карты, номер счета, логин и пароль от страниц в социальных сетях. Задавайте вопросы. Если звонящий представляется как сотрудник полиции, банка, доктор поликлиники, страховой агент, первое, что нужно сделать, попытайтесь узнать информацию о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации и прочее настоящего сотрудника не смутят, а мошенников заставят занервничать.

6. Прежде чем реагировать на сообщения или звонки от «родственников» или «друзей», попытайтесь дозвониться человеку, от имени которого пришло сообщение, кому-то из его близких, с которыми он в настоящее время может находиться.

7. Лучший способ обезопасить себя - игнорировать подозрительные звонки или сообщения. Если все же вы попались на удочку мошенников, немедленно сообщите в полицию или обратитесь с заявлением о совершенном мошенничестве. В нем подробно опишите все обстоятельства: когда, и с какого номера телефона пришло сообщение (сделан звонок), кто звонил, каким именем,

фамилией, должностью представился, подробности разговора или сообщения, информация, которую требовалось сообщить.

8. Немедленно блокируйте карту при ее утере. Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

9. Пользуйтесь защищенными банкоматами. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

10. Опасайтесь посторонних. Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

11. Банкомат должен быть «чистым». Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

12. Банкомат должен быть полностью исправным. В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

13. Не доверяйте карту официантам и продавцам. В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

КМУ ГСУ ГУ МВД России по Свердловской области