Приложение № 1

Памятка

«Виды мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий. Рекомендации по защите от действий мошенников»

Сегодня в повседневной жизни используется множество разнообразных высокотехнологичных устройств - пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний. Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Проанализировав все случаи такого мошенничества, предлагаем Вам понятную и полезную памятку. Рекомендации этой брошюры защитят Вас от действий мошенников и сберегут Ваши средства.

СПОСОБЫ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ

1) Обман по телефону: требование выкупа.

КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, **а** далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег. После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму - это мошенник.

Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

2) СМС-просьба о помощи

СМС-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Следует разъяснить, что на СМС с незнакомых номеров реагировать нельзя, это могут быть мошенники.

3) Телефонный номер-грабитель.

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит СМС с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь - **и** оказывается, что с Вашего счёта списаны крупные суммы.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует **о** том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Настоятельно советуем не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

4) Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло СМС-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с Вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.

Не следует звонить по номеру, с которого отправлен СМС - вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Существует множество вариантов подробно описанных мошенничеств.

5) Выигрыш в лотерее

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей. «Вы победили, сообщите код карты экспресс-оплаты».

Карточки экспресс-оплаты упростили процедуру зачисления денежных средств на счёт, но одновременно и открыли новые возможности для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором

мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры:

- просит представиться и назвать год рождения;
- грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.);
- спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);
- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер, куда надо перезвонить;
- поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа купить экспресс-карту, то все равно должен позвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора - сообщить свои коды. Якобы оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего присваивает ему персональный номер, с которым «победитель» должен ехать за призом.

Но если Вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из ситовой компании, то это объявят нарушением правил рекламой акции.

6) «Вы выиграли машину, нужны деньги для её оформления»

Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон - как правило, в ночное время - приходит СМС-сообщение. в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль.
Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров.

Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного телефона 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Предупреждаем: если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

7) Простой код от оператора связи

КАК ЭТО ОРГАНИЗОВАНО:

Вам поступает звонок либо приходит СМС-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или СМС могут быть самыми разными:

- предложение подключить новую эксклюзивную услугу;
- для перерегистрации во избежание отключения связи из-за технического сооя;
- для улучшения качества связи;
- для защиты от СПАМ-рассылки;
- предложение принять участие в акции от вашего сотового оператора.

Вам предлагается набрать под диктовку код или сообщение ЗМЗ, которое подключит новую услугу, улучшит качество связи и т.п.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Код, который Вам предложат отправить, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только вы его наберёте, Ваш счёт будет опустошён. Никакая услуга не будет подключена.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Обращаем Ваше внимание, что любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать своему мобильному оператору для уточнения условий.

СМС-сообщения могут быть самыми разными. Советуем Вам критически относиться к таким сообщениям и не спешить выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке СМС или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти СМС и заблокирует его аккаунт.

8) Штрафные санкции и угроза отключения номера

КАК ЭТО ОРГАНИЗОВАНО:

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что произошло нарушение условий договора:

- абонент сменил тарифный план, не оповестив оператора;
- не внес своевременно оплату;
- воспользовался услугами роуминга без предупреждения и так далее.
- Чтобы предотвратить отключение номера, Вам предлагается:
- купить карты экспресс-оплаты и сообщить их коды;
- перевести на свой номер сумму штрафа и набрать код;
- перевести средства на указанный номер.

После этого Вы якобы сможете доказать свою невиновность и при этом сохраните свой номер.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Пользуясь тем, что телефон Вам нужен постоянно и потеря номера может стать для Вас критической, мошенник запугивает Вас. В результате он получает возможность присвоить себе Ваши средства - с карт экспресс-оплаты либо напрямую со счёта телефона.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Рекомендуем перезванивать своему мобильному оператору для уточнения условий.

Помните, что у Вас, как у потребителя услуг связи, есть права, которые защищаются законом. Никакой оператор связи не может требовать выплачивать ему штрафы до тех пор, пока Ваша вина не будет доказана.

9) Ошибочный перевод средств

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит СМС-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.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Советуем Вам не 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.

10) Доступ к СМС и звонкам

Многие люди хотя бы раз в жизни испытывали любопытство по отношению к частной жизни своих родственников и знакомых. Мобильная связь, фиксируя СМС и звонки, даёт ложное ощущение, что каждый может стать шпионом. И мошенники пользуются этим.

КАК ЭТО ОРГАНИЗОВАНО:

В Интернете или прессе публикуется объявление, в котором Вам предлагается изучить содержание СМС-сообщений и список входящих и исходящих звонков интересующего Вас абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

После того как Вы отправите СМС, с Вашего счета спишется сумма намного больше той, что была указана мошенниками - до 500 рублей. Разумеется, интересующая Вас информация так и не поступает.

При этом большинство пострадавших не обращаются в полицию, не желая признаваться в желании шпионить за другими людьми. В результате мошенники остаются безнаказанными.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Предупреждаем: предложение о предоставлении данной услуги является мошенничеством, так как такая услуга может оказываться исключительно операторами сотовой связи и в установленном законом порядке!

11) Мошенничества с банковскими картами

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Предупреждаем: не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ РЕКОМЕНДУЕМ.

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Рекомендуем всем владельцам пластиковых карт следовать правилам безопасности:

ПИН-КОД - КЛЮЧ К ВАШИМ ДЕНЬГАМ

- Никогда и никому не сообщайте ПИН-код Вашей карты.
- Лучше всего его запомнить.
- Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.
- Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё - в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ВАША КАРТА - ТОЛЬКО ВАША

Не позволяйте никому использовать Вашу пластиковую карту - это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне - это Ваша ответственность и обязанность.

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.

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.

Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

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.

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.

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.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком - он обязан предоставить консультационные услуги по работе с картой.

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.