**«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 рекомендации, которые защитят Вас от действий мошенников и сберегут Ваши средства.

**СПОСОБЫ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ**

***1) Обман по телефону: требование выкупа.***

КАК ЭТО ОРГАНИЗОВАНО:

Совершается звонок 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 кому­то 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) SMS­просьба о помощи***

SMS­сообщения 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 SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

***3) Телефонные вирусы***

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-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 какой­либо 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 SMS – вполне возможно, что в

этом случае с Вашего телефона будет автоматически снята крупная сумма.

***4) Простой код от оператора связи***

КАК ЭТО ОРГАНИЗОВАНО:

Поступает звонок либо приходит SMS­сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или

SMS могут быть самыми разными:

• предложение подключить новую эксклюзивную услугу;

• для перерегистрации во избежание отключения связи из­за технического сбоя;

• для улучшения качества связи;

• для защиты от СПАМ­рассылки;

• предложение принять участие в акции от вашего сотового оператора.

Вам предлагается набрать под диктовку код или сообщение SMS, 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.

SMS­сообщения могут быть самыми разными. Необходимо 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 SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

***5) 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:

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 ПИН­код для ее перерегистрации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН­код. 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 ПИН­код! 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:

ПИН­КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ

• Никогда и никому не сообщайте ПИН­код Вашей карты.

• Лучше всего его запомнить.

• Относитесь к ПИН­коду как к ключу от сейфа с вашими средствами.

• Нельзя хранить ПИН­код рядом с картой и тем более записывать ПИН­код 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 ПИН­КОД

Если Вам позвонили из какой­либо 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 сайты­двойники. Помните: хранение реквизитов и ПИН­кода 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 ЗАЩИЩЁННЫМИ 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 ПИН­код, 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 какими­либо 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

Материал предоставлен следственным отделом

Отдела МВД России по Черепановскому району