

# **ПАМЯТКА**

## **«КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ»**

### **1. СМС сообщения о выигрыше в лотерее**

Вы получили электронное сообщение о том, что вы выиграли автомобиль (ноутбук, телевизор и т.д.) и Вас просят перевести деньги для получения приза!

**НИКОГДА не отправляйте деньги незнакомым лицам**

### **2. СМС сообщения с просьбой о помощи**

Вы получили с незнакомого номера сообщение «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «твой сын» или подобные.

**НИКОГДА не оплачивайте телефонные номера незнакомым лицам**

### **3. СМС сообщения о том, что банковская карта заблокирована**

С номеров, которые похожи на сервисный номер Сбербанка (900), например «900» (используются буквы «О»), 9 0 0 (используются пробелы между цифрами), поступает СМС с текстом, что банковская карта заблокирована. После чего мошенники пытаются узнать реквизиты карты и пароли доступа в личный кабинет.

**НИКОГДА не сообщайте по телефону реквизиты карты и пароль доступа в личный кабинет. Если есть сомнения, перезвоните в службу поддержки банка, телефон которой указан на Вашей банковской карте**

### **4. Звонки мошенников под видом родственников.**

Под видом близких родственников мошенники звонят гражданам по домашнему (городскому) телефону и сообщают, что задержаны за совершение какого-либо преступление или дорожно-транспортное происшествие с жертвами. Для освобождения от уголовной ответственности просят перечислить денежные средства через банкомат или передать курьеру.

**Основные схемы телефонного мошенничества**

**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. Цена вопроса составляет от одной до тридцати тысяч долларов США.

## **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.

## **5. SMS-просьба о помощи**

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростиившиеся 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:**

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

## **КАК ЭТО ОРГАНИЗОВАНО:**

Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помочь 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:**

Не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

## **6. 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.

### **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 позвониться 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.); объясняет, что в течение часа необходимо оплатить налог на получение приза, предлагает это сделать в ближайшее время, иначе приз отдадут другому участнику.

## **7. Простой код от оператора связи**

### **КАК ЭТО ОРГАНИЗОВАНО:**

Вам поступает звонок либо приходит SMS-сообщение 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 из-за технического сбоя;

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 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:**

Любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать своему мобильному оператору для уточнения условий

### **8. Ошибочный перевод средств**

## **КАК ЭТО ОРГАНИЗОВАНО:**

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.

### **9. 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:**

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**

Как защититься от мошенников

### **ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ**

Никогда и никому не сообщайте ПИН-код Вашей карты.

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.

### **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 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.

### **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.