Люди отдали сотни тысяч рублей за телефонные разговоры с насильником

Автор: Илья ТРЮМОВ + gzt.ru
23.04.2010 00:18

*****Банду телефонных мошенников, обманувших более ста владельцев сотовых телефонов, обезвредили сотрудники управления «К» МВД России. Во главе преступной группы стоял осужденный за изнасилование и грабеж молодой человек.**
*****Группа состояла из пяти человек и действовала на протяжение года. Основную роль 25-летний заключенный исполнял сам, а главной помощницей была его сестра.**
*****По словам представителя управления «К» Ирины Зубаревой, аферист прямо из колонии звонил на мобильные телефоны москвичей, назывался любым именем и начинал беседу на общие темы. Некоторые признавали в нем кого-то из своих знакомых и поддерживали разговор.**
*****Тогда злоумышленник рассказывал, что у него серьезные проблемы с милицией и просил взаймы, обещая вернуть через неделю. Объясняя, что находится в отъезде, он просил перевести ему деньги через электронную платежную систему в один из подмосковных банков.**
*****Деньги получали сообщники и передавали сестре организатора группы, а она тут же клала их на свою сберкнижку. Время от времени девушка переводила деньги брату в колонию.**

Здесь - оперативная съемка

Подозреваемый в телефонном мошенничестве уже отбывает срок за грабеж и изнасилование

*****В день преступник делал десятки звонков и, как правило, всегда находил доверчивых слушателей. На сегодняшний день уже установлены около сотни потерпевших, но, возможно, их было гораздо больше. Кто-то перевел аферисту 10 тысяч, кто-то 20, но рекорд поставила одна москвичка – она облагодетельствовали мошенников сразу на 200 тысяч.**
*****По словам Зубаревой, сейчас все участники группы задержаны. Было изъято 580 тыс. рублей, полученных преступным путем. Возбуждено уголовное дело по ст. 159 УК РФ (мошенничество). На допросе организатор банды частично признал свою вину.**

Мошенники — затейники

*****Зубарева отметила, что подавляющее большинство таких преступлений**

Автор: Илья ТРЮМОВ + gzt.ru
23.04.2010 00:18

совершают лица, находящиеся в исправительных колониях, которые имеют одного или нескольких сообщников на свободе.
*****«Используя мобильный телефон, злоумышленник просто подряд перебирает номера по возрастанию либо убыванию последней цифры,— пояснила она GZT.RU.— Если раньше звонки осуществлялись на мобильные телефоны с прямым абонентским номером, то в настоящее время это и прямые, и федеральные, и городские номера».**

Добычей мошенников стали сотни тысяч рублей

*****По ее словам, мошенники постоянно видоизменяют схемы, позволяющие заполучить деньги у граждан. Так, уже хорошо известная схема «мама-папа, я попал в беду» в последнее время чаще выглядит как «одолжи денег другу через платежную систему».**

Самые популярные схемы «развода» абонентов

1. «Случай с родственниками»
*****Мошенник представляется родственником, другом или сослуживцем близкого вам человека и сообщает, что с ним приключилась беда (попал в аварию, сбил человека). У пострадавшего во время ЧП якобы сломался телефон и приходится звонить с чужого. Предстоит еще много звонков, поэтому необходимо пополнить человеку баланс. Далее следует просьба купить карточку и продиктовать по телефону ее код.**
2. «Ложный приз»
*****На мобильный телефон абонента звонит лжеведущий известной музыкальной радиостанции и поздравляет с выигрышем ценного приза. Однако для его получения нужно в течение 30 минут купить карту пополнения счета и сообщить ее данные диджею. Заплатив деньги и придя через несколько дней за подарком, обманутый абонент узнает, что на радиостанции никто подобного конкурса не проводил.**
3. SMS-просьба
*****В последнее время абоненты сотовых операторов стали получать SMS-ки просьбой «позвони по…номеру, если номер не отвечает, положи на него …рублей и перезвони». Некоторые абоненты, особенно люди пенсионного возраста, пополняют счет мошенников, думая, что пишет кто-то из близких людей.**
4. «Платный код»
*****Вам звонит человек, представляющийся сотрудником службы технической поддержки (центра поддержки клиентов) сотового оператора с предложением подключить новую эксклюзивную услугу (варианты: для перерегистрации во**

избежание отключения связи из-за технического сбоя, для улучшения качества связи). Для этого предлагается набрать под диктовку лжесотрудника код, который является комбинацией для осуществления перевода средств со счета абонента на счет мошенников.
5. «Штрафные санкции» оператора
*****Мошенник представляется сотрудником службы технической поддержки оператора сотовой связи и сообщает, что при замене тарифного плана вы не оповестили оператора и нужно оплатить штраф, отправив номера карт оплаты на некий номер (то есть мошенникам).**
6. «Акции» оператора
*****Абонент получает сообщение об акции, проводимой его оператором. По ее условиям до конца недели (месяца, года, жизни) человек получает возможность осуществлять бесплатные звонки по стране. Для этого ему необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагались) «оператора» коды нескольких карт оплаты.**
7. «Ошибочный перевод средств»
*****Человек получает SMS-ку, оповещающую о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу же после ему звонит мошенник, который утверждает, что только что перевел деньги на его номер ошибочно и просит вернуть деньги обратно тем же «Мобильным переводом».**

*****«Мошенничество в мобильной связи появилось вместе с самой мобильной связью,— рассказал GZT.RU начальник Департамента по гарантированию доходов и управлению фродом ОАО „МегаФон“ Сергей Хренов.— Мошенники используют множество уловок и хитростей для обогащения за счет других абонентов и постоянно их совершенствуют. С появлением новых возможностей в мобильной связи мошенники стремятся использовать и их».**
*****Так, современные аферисты могут внедрить на телефон вредоносное программное обеспечение (вирусы, порнобаннеры, псевдоантивирусы, шифровальщики файлов), а потом вымогать деньги за его деактивацию. Используются так называемых «порнозвонилки» и SMS и MMS-отправители, которые без ведома абонента совершают звонки на международный номер сервиса «только для взрослых» или отправляют сообщения на premium номера и на телефоны из адресной книги жертвы для распространения «вредоноса».**

К такого рода сообщениям нужно относиться крайне осторожно.

*****В последнее время активизировалось продвижение мошеннических сайтов, предлагающих сервис, якобы основанный «на самых современных технология»: определение местоположения других абонентов, получение расшифровки чужих**

SMS-сообщений, сканеры тела и т.п. Нужно только отправить SMS на определенный номер. При этом стоимость SMS указана в разы ниже реальной, а «сервис» не предоставляется.
*****Популярны также звонки и SMS, используемые для получения информации о номере, сроке действия и PIN-коде банковской карты — в дальнейшем с их помощью происходит кража денежных средств.**

Операторы против мошенников

*****Из-за постоянно растущего количества телефонных мошенничеств сотовые операторы и сами подключились к борьбе с ними.**
*****По словам Хренова, сотрудниками «МегаФона» разработана и реализуется адекватная система превентивных мер, которые осуществляются в тесном взаимодействии с правоохранительными органами.**
«Сбор и анализ всей поступающей информации, связанной с мошенничеством, осуществляется оператором в режиме реального времени,— рассказал он.— В случае подтверждения данных о мошенничестве номера и префиксы (буквенно-цифровые идентификаторы, указываемые в sms), используемые для обмана абонентов, блокируются. В ряде случаев специалисты компании передают эту информацию в правоохранительные органы».
*****Также, по его словам, в апреле 2010 года «МегаФон» запустил функционал «Advice of Charge» (AoC), который заключается в информировании абонентов при попытке отправки SMS о стоимости и в получении подтверждения желания отправки. AoC устанавливается на premium номера, которые используются в мошеннических целях.**
*****«В разработке находятся и другие сервисы компании, направленные на защиту интересов абонентов»,— сказал Хренов.**

Что делать и чего не делать

*****К элементарным нормам безопасности можно отнести следующие действия.**
*****Если вы получили звонок или SMS от неизвестного лица и заподозрили, что имеете дело с мошенниками, прервите звонок и не перезванивайте. Также строго не рекомендуется отправлять на данный номер SMS-сообщения. В противном случае с вашего счета могут быть моментально списаны денежные средства.**
*****Сразу же звоните в абонентскую службу своего оператора связи и передайте ему всю информацию о произошедшем инциденте (номер звонившего, текст SMS и т.п.). Также следует поступить, если вы все же стали жертвой телефонных мошенников. По словам Хренова, в большинстве случаев при подтверждении факта мошенничества средства возвращаются на счет абонента в течение нескольких дней.**
*****Если вам поступило предложение от радиостанции активировать карточки экспресс-оплаты с целью получения приза, включите радиостанцию и**

прослушайте ее эфир. Радиостанциия не требует активировать карточки экспресс-оплаты при проведении лотереи.
*****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 выражается просьба передать взятку сотруднику правоохранительных органов, готовому урегулировать вопрос, следуйте следующим рекомендациям:**
*****— задайте своему родственнику наводящие вопросы, ответы на которые знаете вы оба, либо попросите его описать себя;**
*****— если вы разговариваете с якобы представителем правоохранительных органов, спросите, в какое отделение милиции доставлен родственник. Набрав 02 и узнав номер дежурной части данного отделения милиции, можно поинтересоваться, действительно ли родственник находится там и кто занимается этим делом;**
*****— если разговор закончен, а вы сомневаетесь в личности звонившего и в подлинности изложенных фактов, постарайтесь перезвонить на мобильный телефон звонившего. Если он отключен, очертите круг лиц, которые могут знать о его местонахождении (коллеги по работе, друзья, родственники), свяжитесь с ними для уточнения информации.**
*****Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счет карточкой экспресс-оплаты, но прежде потребует сообщить оператору личный PIN-код, перезвонив на определенный номер. Помните, что активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на карточке, а личный код никому никогда не сообщается.**
*****Если вы получили SMS-сообщение на мобильный телефон от якобы знакомых с просьбой положить на их счет деньги, перезвоните по указанному номеру и выясните личность отправившего SMS.**
На мобильный телефон может поступить SMS-сообщение с предложением оградить вас от СПАМ-рассылки либо принять участие в акции от вашего сотового оператора. В сообщении предлагается отправить «бесплатное» SMS, состоящее из набора цифр, на один из коротких номеров, а затем перейти по ссылке для удаления своего имени из списка. В результате этих манипуляций вы потеряете около 100–150 рублей, но СПАМ получать все равно будете.
*****SMS-сообщения могут быть весьма разнообразны, и в данном случае совет может быть один: критически относиться к таким сообщениям и не спешить выполнить то, о чем вас 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.**

Источник: www.gzt.ru. Добавил на портал Новодар Илья ТРЮМОВ.