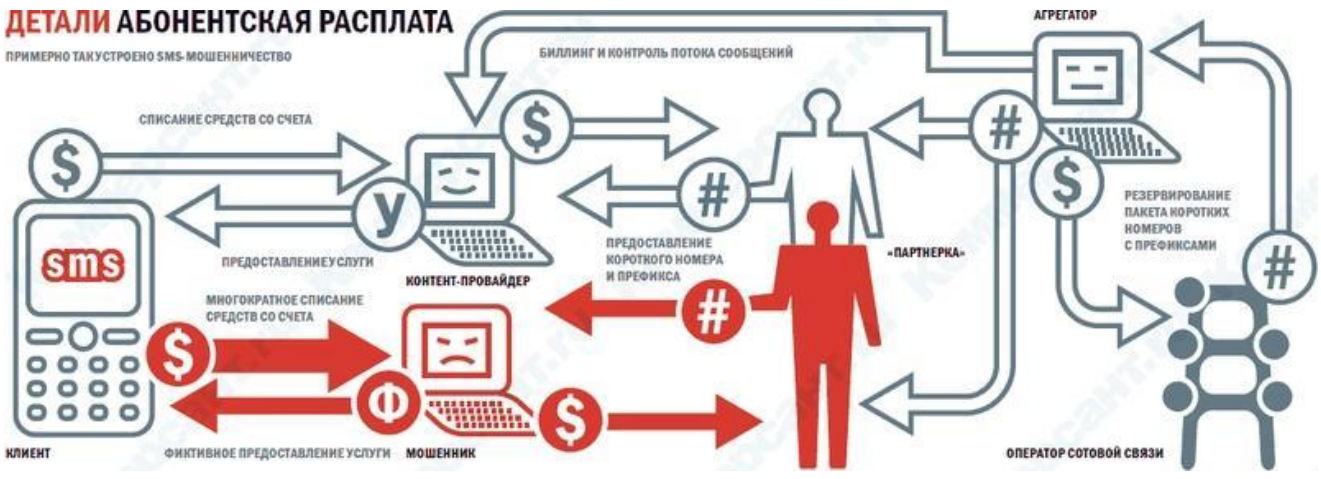
Как работают SMS мошенники и сколько они зарабатывают. Схемы.



Не проходит недели, чтобы в поле общественного внимания не возник вопрос о мошеннических схемах при пользовании услугами SMS-сообщений. "Огонек" попытался разобраться, как работают эти схемы и почему мошенники непобедимы.

Прежде это было экзотикой, теперь даже такие мощные структуры, как Сбербанк России, вынуждены обращаться к клиентам с призывом "быть бдительными" и не поддаваться на закинутые через мобильные телефонные сети приманки аферистов. Какой бы соблазнительной и (или) безобидной ни была просьба в поступившем на мобильник сообщении перезвонить на короткий номер или отправить на него SMS, не откликайтесь. Кто клюнет — тот поплатится. Причем в самом прямом смысле этого слова. Расплата неминуема, жертву стерегут наглые и прожорливые хищники. Кто они?

Как все работает

Предположим, гражданину Пупкину (вымышленному, конечно) захотелось рентабельного бизнеса, а стартового капитала, увы, у него не имеется. Стало быть, прямая дорога ему в контент-провайдеры. Так называются продавцы всякой неосязаемой всячины в коммуникационных сетях. Можно торговать мелодиями для телефонов, играми, гороскопами, диетами, датами будущей смерти — всем чем угодно.

Все, что нужно для старта бизнеса,— получить в аренду, причем в счет будущих прибылей, короткий телефонный номер и префикс (в виде цифр или букв, подлежащих размещению в теле будущих SMS-сообщений). На одном и том же номере может располагаться множество самых различных продавцов с различными сервисами (совсем как у фирм-однодневок, зарегистрированных пачками по одному юридическому адресу), идентификация конкретного продавца производится по префиксу.

Крупные операторы сетей (МТС, "Билайн", "Мегафон" и т. п.) с контент-провайдерами никак не связаны, для этого есть особый эшелон — агрегаторы. Именно агрегатор резервирует у десятков крупных и мелких сотовых операторов номера (не только в России — на всем постсоветском пространстве), на которые и садится потом условный Пупкин с выданным ему префиксом по условленному тарифу. Агрегатор отслеживает потоки SMS-сообщений, сортирует их по префиксам и биллингует, то есть начисляет вознаграждение инициаторам трафика — тем самым контент-провайдерам.

Агрегаторы, кстати, ворочают миллиардами и напрямую с Пупкиным тоже не связаны. Для этого у них есть партнеры помладше. Они так и называются — партнерские программы, или партнерки. Деньги, списанные с баланса телефона за отправку короткого

сообщения на платный номер, распределяются в следующих пропорциях: крупные операторы берут себе 30-50 процентов, агрегаторы — 7-10, партнерки чуть больше, остальное идет в карман непосредственному продавцу, подвигнувшему абонента тряхнуть кошельком. Цепочка выстроена совершенно законно — в самой пирамиде "мобильной ответственности" мошеннический компонент не заложен. Где же и как он возникает?

Контент-провайдеры, предоставляющие легальные сервисы, олицетворяют силы добра. Это, например, радиостанции с их платными SMS-сообщениями, опросами и голосованиями; газеты и интернет-ресурсы, получающие таким способом оплату рекламы и объявлений VIP-статуса; файлообменники; онлайн-консультанты; продавцы веб-контента (книг, музыки, видео, скачиваемых казуальных игр, программного обеспечения); системы электронных платежей — WebMoney, Yandex; провайдеры SMS-чатов, игр, викторин, сетей Wi-Fi.

Иное дело "силы зла". Это мошенники (предпочитают называть себя международным термином "фродеры"), заманивающие людей несуществующими услугами и не соответствующими действительности тарифами. Обещают пустить к вожделенному сайту за, предположим, 15 рублей, а на самом деле с баланса вашего телефона списывается несколько раз по 300 рублей — сначала за собственно код, потом за подтверждение, за активацию и так далее. Более того, в итоге клиент получает шиш вместо заветной услуги.

Липовый контент по содержанию может быть самым различным, но первенство держат популярные у народонаселения фальшивки: SMS-перехватчики (чтоб следить за деловыми партнерами), мобильные рентгены (чтоб смотреть через видоискатель встроенного в телефон фотоаппарата на одетую женщину, а видеть ее раздетой), мобильные локаторы (чтоб знать, где ошивается любвеобильный супруг), сетевые поисковики паспортных данных.

[["Ведомости", 29.03.2010, " Рискованные sms": GSM-локаторы распространены до сих пор: недавно корреспондент «Ведомостей» обнаружил такой сервис даже в магазине Appstore (продает программы для iPhone). Если внимательно вчитаться в условия сервиса, становится понятно, что это вовсе не реальная возможность обнаружить местоположение человека, а… игра. Но страничка рецензий полна комментариев невнимательных пользователей, обвиняющих авторов «локатора» в мошенничестве.
К концу прошлого года родился еще один способ вымогательства денег при помощи sms — так называемые «блокираторы». Это вирусы, блокирующие работу компьютера и предлагающие разблокировать его с помощью платного sms. Волна этих мошенничеств прошла в декабре — январе, они вызвали большой резонанс в СМИ и привлекли внимание сотовых операторов, получивших поток жалоб от абонентов. — Врезка К.ру]

[otdel-k.info, "Управление К предупреждает": Первые модификации вирусов-блокираторов, по данным антивирусных компаний, появились около 3-х лет назад. Как отмечают специалисты, сначала блокираторы не представляли серьезной угрозы: не запускались в Безопасном режиме Windows, легко удалялись с компьютера либо автоматически удалялись через несколько часов после установки, стоимость одного SMS-сообщения, которые требовали отправить авторы вредоносного кода, была не столь высокой, как сейчас.
В ноябре 2009 года произошел всплеск подобного рода мошенничества. Новые модификации вредоносных программ, блокирующих работу ЭВМ и вымогающих денежные средства появляются фактически еженедельно. Аппетиты злоумышленников выросли: если год-два назад стоимость одного сообщения с кодом разблокировки составляла 10-15 рублей, то сегодня — 250-700 рублей.

Рассылаемые злоумышленниками программы сегодня не удаляются автоматически из системы по прошествии некоторого времени, как отмечают специалисты, приобретают дополнительные функции. В частности, по информации крупного производителя антивирусного ПО российской компании «Dr. WEB», вредоносные программы-блокираторы препятствуют запуску некоторых программ в зараженной системе (файловых менеджеров, антируткитов, утилит сбора информации, которая может помочь в лечении системы).
Только за два месяца 2010 года число пострадавших в России от блокировщиков Windows составило несколько миллионов пользователей. С учетом того, что средняя стоимость SMS-сообщения — 300-600 рублей, предположительные потери россиян от этого вида вредоносного ПО только в первом месяце 2010 года составили сотни миллионов рублей. — Врезка К.ру]

["РБК daily", 26.03.2010, "Востребованная услуга": Федеральная налоговая служба проинформировала на своем сайте о выявлении случаев мошенничества с использованием символики ФНС. Аферисты от имени налоговой предлагали гражданам узнать, имеется ли у них задолженность. В листовке, копию которой ФНС также повесила на сайте, предлагается отправить SMS на короткий номер с номером ИНН налогоплательщика. Листовки распространялись в Петербурге в начале марта. Стоимость одного сообщения указывалась в размере 3 руб. Однако при отправке у заинтересовавшихся должников списывалось 110 руб. При этом никаких ответных сообщений на «запрос» так и не поступало. «ФНС не имеет отношения к данным мошенническим действиям и призывает граждан к бдительности», — говорится в сообщении ведомства.
Услуга по SMS-информированию сегодня действительно предоставляется в ряде регионов — в Петербурге, Кировской, Кемеровской, Нижегородской, Пензенской областях, Алтайском крае, Чувашии, ХМАО. При этом цена такого запроса не превышает стоимости обычного сообщения оператора мобильной связи. Ответное сообщение является бесплатным. Узнать легальный номер для отправки сообщений ФНС предлагает в местных СМИ и на сайтах территориальных налоговых управлений. — Врезка К.ру]

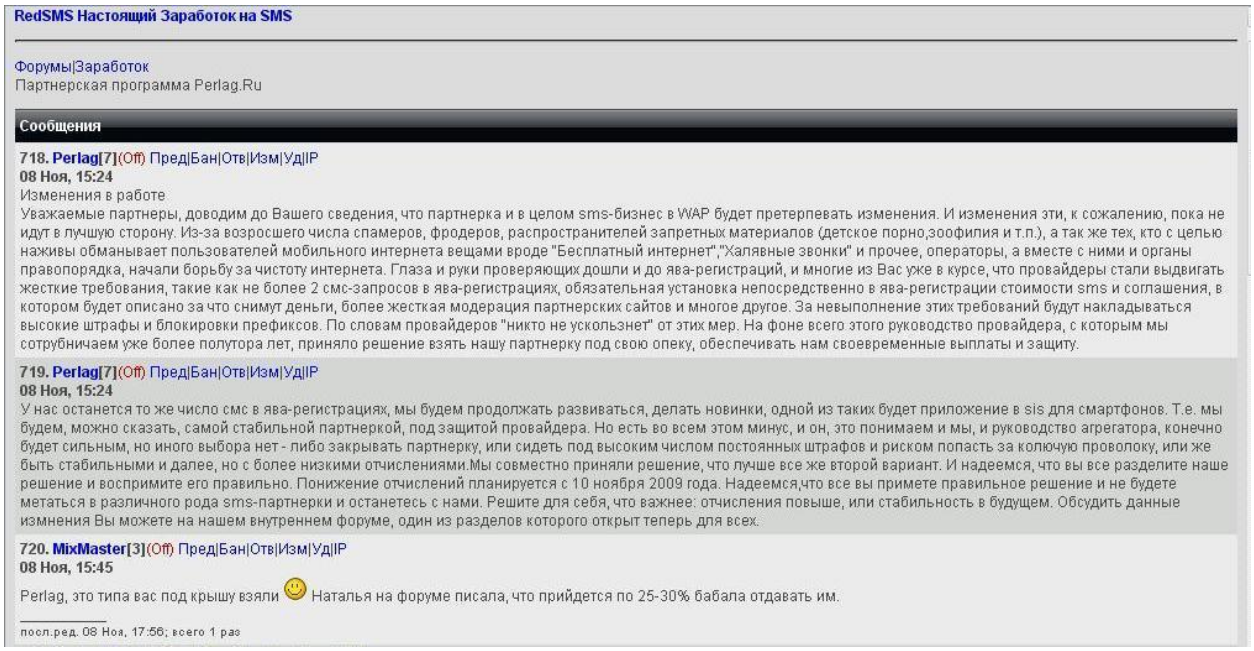
Наиболее продвинутые пираты распространяют так называемые SMS-алармы, то есть с виду безобидные программы (например, игра для мобильника, "новейшая" версия браузера и т. п.), инфицированные вирусом. Стоит закачать их в телефон, как эти программы без ведома владельца начинают отправлять SMS-сообщения на платные номера — итог тот же: прощайте денежки.

Памятка начинающему контент-провайдеру состоит из перечня кар за мошенничество: от невыплаты вознаграждения за созданный трафик до казенного дома. Казалось бы, сам смысл мошенничать как-то теряется. Но потом выясняется, что на самом деле все не так уж строго. В лихие игры не играют многие серьезные контент-провайдеры, но на связи у агрегаторов (даже у самых крупных) имеется совсем небрезгливый эшелон — те самые партнерки.

Большинство из них от новых клиентов не требует предъявлять документы — достаточно заполнить онлайн-формуляр (у партнеров, знаете ли, все на доверии). И все там поэтому под псевдонимами. Деньги за трафик перечисляют на всевозможные веб-кошельки, где тоже все на доверии. Ну вот, собственно, и вся схема — в такой мутной водице что хочешь может водиться. И, собственно, исправно водится.

Разговор в узком кругу

В распоряжении "Огонька" оказались некоторые документы, связанные с партнеркой под названием PerLag. Речь, в частности, идет об онлайн-конференции, на которой поднимался вроде не имеющий отношения к мобильным сетям, но весьма занятный вопрос: "Платить ментам или не платить?" А если платить, то какие гарантии, что за "не совсем честный трафик" не посадят? Это была повестка дня закрытого партнерского форума, бурлившего после анонса, сделанного одним из владельцев, выступающим под ником Кисеночек (в миру Наташа.— "О").



RedSMS Настоящий Заработок на SMS

Форумы|Заработок
Партнерская программа Perlag.Ru

Сообщения

718. Perlag[7](Off) Пред|Бан|Отв|Изм|Уд|IP
08 Ноя, 15:24
Изменения в работе
Уважаемые партнеры, доводим до Вашего сведения, что партнерка и в целом sms-бизнес в WAP будет претерпевать изменения. И изменения эти, к сожалению, пока не идут в лучшую сторону. Из-за возросшего числа спамеров, фродеров, распространителей запретных материалов (детское порно,зоофилия и т.п.), а так же тех, кто с целью наживы обманывает пользователей мобильного интернета вещами вроде "Бесплатный интернет","Халявные звонки" и прочее, операторы, а вместе с ними и органы правопорядка, начали борьбу за чистоту интернета. Глаза и руки проверяющих дошли и до ява-регистраций, и многие из Вас уже в курсе, что провайдеры стали выдвигать жесткие требования, такие как не более 2 смс-запросов в ява-регистрациях, обязательная установка непосредственно в ява-регистрации стоимости sms и соглашения, в котором будет описано за что снимут деньги, более жесткая модерация партнерских сайтов и многое другое. За невыполнение этих требований будут накладываться высокие штрафы и блокировки префиксов. По словам провайдеров "никто не ускользнет" от этих мер. На фоне всего этого руководство провайдера, с которым мы сотрудничаем уже более полутора лет, приняло решение взять нашу партнерку под свою опеку, обеспечивать нам своевременные выплаты и защиту.

719. Perlag[7](Off) Пред|Бан|Отв|Изм|Уд|IP
08 Ноя, 15:24
У нас останется то же число смс в ява-регистрациях, мы будем продолжать развиваться, делать новинки, одной из таких будет приложение в sis для смартфонов. Т.е. мы будем, можно сказать, самой стабильной партнеркой, под защитой провайдера. Но есть во всем этом минус, и он, это понимаем и мы, и руководство агрегатора, конечно будет сильным, но иного выбора нет - либо закрывать партнерку, или сидеть под высоким числом постоянных штрафов и риском попасть за колючую проволоку, или же быть стабильными и далее, но с более низкими отчислениями.Мы совместно приняли решение, что лучше все же второй вариант. И надеемся, что вы все разделите наше решение и воспримите его правильно. Понижение отчислений планируется с 10 ноября 2009 года. Надеемся,что все вы примете правильное решение и не будете метаться в различного рода sms-партнерки и останетесь с нами. Решите для себя, что важнее: отчисления повыше, или стабильность в будущем. Обсудить данные измнения Вы можете на нашем внутреннем форуме, один из разделов которого открыт теперь для всех.

720. MixMaster[3](Off) Пред|Бан|Отв|Изм|Уд|IP
08 Ноя, 15:45
Perlag, это типа вас под крышу взяли Наталья на форуме писала, что прийдется по 25-30% бабала отдавать им.

посл.ред. 08 Ноя, 17:56; всего 1 раз

Волноваться было из-за чего — денег на "крышу" просили ни много ни мало полтора миллиона рублей в неделю. Это четверть доходов PerLag. Агрегатор у перлаговцев — "Первый Альтернативный" — мощная структура, входящая в холдинг, где кроме SMS-бизнеса есть свое телевидение, банк и т.д. Он-то и стал взимать с PerLag 25 процентов, якобы на крышевание. Месячный доход партнерки, как нетрудно посчитать, составляет 25 млн рублей. Таких партнерок у агрегатора не один десяток, а у оператора соответственно не один десяток таких агрегаторов. (Тексты в полном объеме размещены на сайте www.antisud.com.)

Выяснив из "разговора в узком кругу" (его запись в редакции имеется) координаты курирующего PerLag представителя "Первого Альтернативного" по имени Роман, мы написали ему письмо. Ответа не получили. Как, впрочем, и сообщения почтового робота о несуществующем адресе. Секретаршу "Первого Альтернативного" — милую, отзывчивую девушку — просьба соединить с Романом нисколько не удивила. Мужской голос ответил, что Роман еще не пришел и что в последнее время он работает в основном из дома.

Пришлось снова набрать секретаршу и, раскрывшись, спросить, может ли кто-нибудь рассказать "Огоньку" об SMS-мошенничестве. "Да, конечно,— ответила секретарша.— Соединяю с менеджером проектов". После пяти музыкальных минут девушку как подменили — менеджер не в курсе проблемы, начальник службы безопасности отъехал очень надолго и, кстати, никакой Роман у нас не работает, извините...

По странному стечению обстоятельств, буквально на следующий день агрегатор объявил о разрыве отношений с PerLag. А еще через день PerLag самоликвидировался. Под каким

именем всплывет теперь ?Кисеночек с шайкой преданных флибустьеров — пока неизвестно.

Испытано на себе

Неудача с "Первым Альтернативным" вынудила искать подходы к другому лидеру на этом рынке — к агрегатору "ИнкорМедиа".

Поиск оказался не труден. Сайт vichesli.net бойко торговал телефонными справочниками всех регионов. Стоимость 18 рублей. SMS-номер 7122 — зарезервирован агрегатором "ИнкорМедиа".

В ответ на посланное SMS пришел код доступа, помещение которого в соответствующую графу на сайте вызвало сообщение о технической ошибке. Телефон службы поддержки оказался фальшивым. Баланс между тем облегчился не на 18, а на 300 рублей. После этого, понятное дело,— звонок в службу поддержки "Билайна" (с сим-карты которого было послано SMS).

Сотрудник колл-центра претензии не удивился — буднично перевел стрелки на "ИнкорМедиа", а те без лишнего шума вернули кровные 300 рублей. И... поблагодарили за бдительность.

Через неделю мы попытку повторили. Сайт по продаже телефонных книг по-прежнему торговал. Только номер сменил на 3354 (тоже числящийся за "ИнкорМедиа"). Процедура (включая списание 300 рублей со счета) повторилась один в один, впрочем, как и звонок оператору с последующим отсылом к агрегатору и благодарностью за бдительность в конце. Еще через неделю мошеннический сайт переехал на номер "Первого Альтернативного", а так и неудовлетворенное любопытство отправилось на Петровку, оттуда в святая святых — отдел "К", к старшему оперуполномоченному Сергею Макаренко.

— Законодательство таково, что даже если на мошенника жалуются сотни обманутых, по 300 рублей каждый, мы не можем возбудить уголовного дела. При ущербе до 1000 рублей возможна только административная ответственность,— рассказал он.— Найти злоумышленника — тут особой сложности нет, потому что технически движение денежных средств легко документируется. Есть телефон, есть статистика, есть биллинг, по которому все видно. Несмотря на то что мошенник может быть зарегистрирован в партнерке под вымышленным именем или через липовую фирму-однодневку, деньги из виртуального кошелька он все же выводит на конкретное лицо с паспортом. Так что доказательная база очень хорошая. Но лазейка имеется, и ею пользуются.

Уголовные дела, впрочем, все же возбуждаются — если абонент послал несколько SMS подряд, а также, если имело место применение вируса или взлом, здесь, по словам Макаренко, есть основания для дела независимо от суммы ущерба. Например, если злоумышленник взломал ваш аккаунт на "Одноклассниках", чтобы от вашего имени разослать вашим друзьям приглашение прислать SMS на такой-то номер, тут сразу возникает уголовная ответственность по статье 272 УК РФ.

В этих разъяснениях все выглядело логично, но вопросы оставались: "Кто виноват?" и "Что делать?".

— Мы действуем в рамках существующего закона, работаем от заявления,— разъяснял

старший оперуполномоченный.— Если граждане будут подавать заявления в милицию и отслеживать ход привлечения к ответственности, мошенничество существенно снизится. По месту совершения правонарушения сотрудники территориального ОВД обязаны принять заявление. Надо обязательно брать квиток. Потом к нам с "земли" (из ОВД.— "О") приходят запросы, и мы проверяем в полном объеме. Пусть наши граждане научатся отстаивать свои права, а не машут рукой. Ошибочно, кстати, считается, что люди, пострадавшие при посещении порноресурсов, стесняются жаловаться. Много жалоб именно оттуда. Наверное, потому что там основной вал обмана...

Порочный круг

Насчет вала обмана у представителей "племени агрегаторов" свои представления. Анатолий Жупанов, исполнительный директор агрегатора "Премиум Мобайл", поделился ими с "Огоньком":

— Мошенники регистрируют у провайдера "белый" сервис, а потом вдруг начинает идти "черный" трафик. Бороться с этим можно. Политика нашей компании, например, такова: мы постоянно мониторим сервисы и при малейших нарушениях блокируем. Никакого вознаграждения мошенники от нас не получат. А нет экономической почвы — нет и мошенничества.

Если бы агрегаторы дружили между собой, то однажды вечером они все собрались бы, попили кофе и сказали: "А давайте прекращать это все!" Но такого произойти по определению не может.

Выходит, полная безнадега — порочный круг, из которого не вырваться. Но не все так считают.

— Мошенники, операторы и агрегаторы находятся в сговоре,— уверен контент-провайдер Федор Соколов.— Я знаю, как с жалобами поступают: никак. Иногда возвращают деньги, но чаще просто отправляют запрос контент-провайдеру, а тот пишет, что жалоба не подтвердилась. Если не проявить настойчивости, даже заявку не примут. Покупатель материальной продукции имеет право вернуть непонравившийся товар в течение 14 дней. А продавцы контента делают ставку на импульс, боятся дать покупателю подумать хотя бы секунду, иначе у них доходность снизится. Они неплохие психологи...

На своем сайте в разделе "Зло" Федор разместил описание видов SMS-мошенничеств, а в

разделе "Добро" — способы борьбы с ним, советы о том, куда обращаться, если с вас сняли деньги. По собственной инициативе он тестирует на вирусы продаваемые в сети программы, сообщает в службы безопасности операторов об интернет-ресурсах мошенников, но от него чаще всего отмахиваются. Несколько раз ему мстили, избирая его сайт мишенью для ddos-атак.

— Операторов волнует только объем привлеченного трафика, больше они ни во что не вникают,— рассказывает Федор Соколов.— В итоге сложилась ситуация, когда доля мошенничества достигает 50-60 процентов всего SMS-рынка. Рассуждения о борьбе с мошенничеством на таком фоне — профанация. Операторы же видят префиксы. Все SMS, которые получены мошенническим путем, очень несложно определить и вернуть деньги всем пострадавшим, а не только тем, кто обратился...

С такой категоричностью не согласны представители крупных операторов, они убеждены, что и так делают все, что могут. "По сравнению с 2008 годом более чем в три раза увеличилось количество жалоб на мошенничество,— сообщила "Огоньку" Евгения Чистова, менеджер проектов "Билайна",— поэтому мы ввели штрафы размером в 10 процентов с выручки от короткого номера или минимум 150 тысяч рублей по жалобе. Но эти меры не всегда срабатывают, потому что штрафы уже заложены нечистоплотными провайдерами в стоимость. Мы одно время специально сажали человека мониторить Сеть на предмет выявления сайтов, предлагающих незаконные сервисы, например продажу SMS-локаторов. Их было так много, что работу оператора на клавиатуре можно было сравнить с игрой на пианино. Он выключал номера, а они кочевали от одного партнера к другому. Тем не менее совместно с МВД и другими операторами мы практически вытеснили "локаторы" из Сети. Правда, мошенники постоянно совершенствуются. Новая волна — подписки на сервисы от псевдооператоров. Злоумышленники встраивают код авторизации в текст сообщения, и, кликая по ссылке, абонент тем самым его активирует. Абонент даже не поймет, за что у него списываются деньги..."

Пресс-секретарь МТС Ирина Осадчая с коллегой из "Билайна" согласна: "Мошенничество на 100 процентов не победить. Хотя система штрафования у нас очень серьезная — МТС штрафует на 90 процентов от дохода по номеру, а не на 10, как другие операторы. За последние месяцы наказаны такие крупнейшие агрегаторы, как "Первый Альтернативный", "ИнкорМедиа", "Нева Лайн", "РМ-Инвест", суммы существенные. Подвижки, правда, есть: внедрение системы штрафов и активное информирование абонентов помогли снизить количество жалоб практически в 2,5 раза. Очень действенной мерой мы считаем сервис "Инфоконтент" — проверку стоимости контентной услуги. Это когда абонент может послать бесплатное SMS-сообщение на короткий номер со знаком "?" и через несколько секунд получить в ответ сообщение с указанием провайдера данной услуги и ее реальной стоимости".

"Огонек" послал "?" на первый попавшийся короткий номер. В ответ получил афоризм на тему употребления алкоголя. С баланса списалось 3,5 рубля (спасибо, что не 300!). Оказалось, что услуга информирования о стоимости работает только с симок МТС, а "Огонек" отправил запрос с симки другого оператора...

SMS-мошенники зарабатывают более 160 млн долларов в год

[…] Микроплатежи с помощью SMS плотно вошли в нашу жизнь. С их помощью пользователи скачивают фильмы и музыку, рингтоны и заставки для мобильных телефонов, оплачивают книги в электронных библиотеках, повышают свой рейтинг в службах знакомств и.т.д. Эти «микроплатежи» с точки зрения законодательства РФ работают на грани фола, но, тем не менее, честно выглядят с точки зрения потребителя, который получает услугу в обмен на деньги, списанные с его мобильного счета. Как правило, подобная схема прозрачна, а стоимость таких SMS не превышает 1-2 долларов США.

Гораздо хуже дело обстоит у «независимых» сервисов, которые эксплуатируют более зависимые ипостаси человеческой души. Это «секретные диеты для похудания», «поиск местонахождения абонента по номеру мобильного телефона», «расчет точной даты смерти абонента», «проверка коэффициента интеллекта», «скачивания цифровых наркотиков» и прочие вкусности.

Что ж, любопытство в данном случае и оказывается тем тайным пороком, который играет на руку мошенникам, а, будучи обманутым, немногие стремятся признать свою глупость, и рассказать о ней коллегам по цеху. Сотрудники МВД утверждают, что практически не получают жалоб от жертв SMS-мошенников, что позволяет последним неделями и месяцами «пахать тучную поляну» без боязни разоблачения. В кулуарах те же сотрудники утверждают, что в России жертвами SMS мошенничества становится каждый пятый.

Рассмотрим простой пример. Вам предлагается узнать местонахождение абонента сотовой связи, для чего вы должны получить некий код доступа, стоимостью якобы в 8 рублей. Ничтоже сумняшеся, вы шлете SMS на короткий номер. Тогда вам приходит предложение послать еще SMS с неким кодом на этот же номер, для подтверждения того, что вам исполнилось 18 лет. Выполнив действие повторно, вы с удивлением обнаруживаете новое сообщение, например, о том, что сайт содержит информацию для взрослых, и вы должны в третий раз послать запрос, что согласны с просмотром «информации для взрослых». «Ну что ж, 8 рублей умноженные на три — не такая астрономическая сумма», — рассуждаете вы, и третье SMS летит мошенникам. Проблема заключается в том, что на «номерах-лохотронах» тарификация подобных запросов стоит 250-350 рублей, а вовсе не 8 на которые вы рассчитывали. При этом особый цинизм заключается в том, что вам предлагают скачать программу типа SMS-локатор, которая именно на вашем компьютере отказывается работать.

В России такая информация частным лицам не предоставляется в целях безопасности самих абонентов. Это возможно только с предварительного согласия самого владельца. Тем не менее, следует ради справедливости заметить, что ваше местоположение сотовому оператору отлично известно, но эта точность в лучшем случае измеряется сотнями метров, и никаким третьим лицам ими не передается.

Т.е с точки зрения абонента, это наиболее «обидная разводка», но пока существуют ревнивые мужья и жены, а также «подозрительные родители» мошенники чувствуют себя вольготно.

Что же касается «секретных диет», «коэффициента интеллекта», и цифровых наркотиков то здесь все зависит от степени жадности и изобретательности мошенников, и с вас либо в один прием снимут 250-350 рублей, либо опять же разведут на 2-3 SMS, в результате «заработав» такую же сумму. Правда, в этом случае, в отличие от SMS-локатора, вам взамен дадут несколько мелодий с невнятным шипением (цифровые наркотики), или «дату вашей смерти», приблизительно высосанную из пальца.

Еще одним, пожалуй, наиболее гнусным способом отъема денег является опять-таки SMS-рассылка с просьбой о помощи: абоненту приходит сообщение, что для спасения ребенка необходима редкая группа крови. В SMS указан номер, при звонке на который с абонента списываются деньги. При этом узнать, куда отправилась так называемая «помощь», естественно, не представляется возможным.

Ну и классика жанра. Самыми распространенными видами мошенничества с использованием мобильного телефона являются розыгрыши призов и вымогательство во спасение.

В первом случае все просто: расчет делается на то, что человек, обрадовавшись неожиданной удаче, с удовольствием совершит формальный платеж, чтобы потом забрать ценный приз. Чтобы получить неожиданный подарочек, участнику радиовикторины всего-то нужно приобрести карточку экспресс-оплаты сотовой связи и сообщить код «радиоведущему». Каков дальнейший сценарий развития событий, нетрудно догадаться.

Вторым классическим приемом «отъема денег» является вымогательство крупной суммы во имя спасения родственника жертвы, который якобы попал в беду. Этот вид мошенничества — столь же артистичный и замысловатый, как и первый «классический». Только к выбору жертвы подход здесь более осознанный: требуемые мошенниками суммы вырастают с 40 рублей до 15-20 тысяч долларов, так что платежеспособность абонента — основное условие. Примечательно, что в состоянии аффекта мало кто из жертв действительно задумывается над тем, почему необходимую сумму попросили предоставить в виде карт оплаты сотовой связи, а не, например, наличными.

[Вести.Ру, 30.03.2010, "СМС-мошенники пытаются нажиться на терактах в метро": Мошенники рассылают москвичам СМС-сообщения с просьбой перечислить деньги для пострадавших при терактах на станциях метро "Парк культуры" и "Лубянка". Как сообщили ИТАР-ТАСС в Управлении информации и общественных связей столичного ГУВД, "милиция расценивает все эти факты как телефонное мошенничество, и по ним будут проводиться соответствующие проверки".
Милиция обращается к москвичам с убедительной просьбой быть бдительными и не попадаться на уловки мошенников. "Информация о счетах, которые будут открыты для помощи жертвам терактов, будет сразу же официально распространяться по каналам СМИ", — сказал собеседник агентства. Это не первая попытка телефонных мошенников нажиться на чужом горе. После пожара в пермском ночном клубе "Хромая лошадь", который унес жизни 156 человек, мошенники также рассылали СМС-сообщения жителям Пермского края и других регионов с предложением перечислить деньги якобы для пострадавших. — Врезка К.ру]

«А что же операторы сотовой связи», — спросите вы? «А ничего», — отвечу вам. На словах «большая тройка» операторов внимательно рассматривает все немногочисленные жалобы на мошенников, и на словах борется с фродерством (SMS мошенничеством). На самом же деле все спускается на тормозах, ведь с каждого «микроплатежа» на короткие номера сотовые операторы получают 30%-40% дохода. Деньги не пахнут.

Согласно мировой статистке, уровень потерь операторов фиксированной и мобильной связи от различного рода телефонного мошенничества и мелкого вредительства составляет от 2 до 6% от общего объема трафика. Компании в своих оценках более категоричны: свои убытки они оценивают в 25%. Если эти проценты перевести в живые деньги, то получится 25 миллиардов долларов. Российские операторы от мировой

статистики не сильно отстают. Ущерб российских операторов, опрошенных «Россіей», эксперты оценивают в 150-160 миллионов долларов. И такие потери прирастают ежегодно еще в среднем на 5-6% в год. […]