

# SMS-спам атакует

Можно ли избавиться от рекламных рассылок на сотовый телефон?

**Получаете ли вы рекламные SMS на свой телефон от службы такси или доставки еды, ночных клубов, магазинов косметики или одежды, спортклубов, юристов?.. Если нет – проверьте, включён ли ваш телефон или не забыли ли вы взять его с собой.**

**В** России рекламные рассылки теперь приходят на сотовые телефоны едва ли не чаще, чем на электронные ящики, что, кстати, раздражает гораздо больше! В отличие от компьютера, телефон мы практически не выключаем, он сигнализирует о получении сообщений, а SMS-спамеры не церемонятся и отправляют послания в любое время дня и ночи. К тому же в электронной почте особенно навязчивых спамеров можно внести в «чёрный список», а на телефоне это сделать сложнее. Но всё-таки бороться с SMS-спамом можно и нужно!

**Пожалуйста, прекратите!**

Если вы сами подписались на рассылку, то у вас должна быть возможность добровольно от неё отписаться. Это относится к многочисленным сетевым

магазинам, фирмам, где вы когда-либо что-то покупали или заказывали, получили дисконтную карту и заполнили анкету. Обычно в анкете мелким шрифтом есть строка, поясняющая, что вы соглашаетесь на получение информации через SMS. Однако любая приличная компания по первому требованию клиента прекратит рассылку. Условия отказа должны быть указаны в полученных вами сообщениях или на сайте компании.

Если отписаться не получается или вы получаете рассылки, на которые не подписывались, — внимательно изучите функции вашего телефона. Многие модели предлагают возможность занесения номера в «чёрный список». Если же раздражают информационные сообщения самого оператора, то и их можно отключить через меню телефона.

К примеру, цепочка действий для отключения подписок оператора «Ростелеком»

такова: меню — раздел U-меню, далее — U-life, настройки — вещание — выключить. Затем телефон нужно перезагрузить. Либо можно позвонить по телефону 11802 — в клиентскую службу «Ростелекома», и оператор исключит ваш номер из рассылки. Однако это не значит, что на ваш телефон отныне не будет приходить спам «такси — адвокаты — грузчики». Оператор может лишь избавить вас от собственной информационной или развлекательной рассылки.

## Наказание по закону

Наказать спамеров и избавиться от ненужной рекламы в телефоне можно с помощью Управления Федеральной антимонопольной службы (УФАС) России по Пермскому краю, которая осуществляет надзор и контроль соблюдения законодательства о рекламе. Ваша жалоба не может быть анонимной — в ней придётся указать фамилию, имя, отчество, адрес и номер телефона, приложить фотографию SMS, детализацию и копию договора с оператором связи

и, также разрешение на обработку ваших персональных данных.

«При заключении договора на обслуживание с оператором связи надо быть внимательным, — полагает заместитель начальника УФАС по Пермскому краю Марина Кудрявцева. — Как правило, там есть пункт о том, что вы согласны получать подобные сообщения. Но вы можете отказаться от них в письменном виде в офисе вашего оператора. Однако к нам ежедневно обращаются многие пермяки, которые уже написали заявления своему оператору мобильной связи с претензией. Но оператор отвечает, что он лишь доставляет SMS от отправителя до адресата и не отслеживает, личное это сообщение или оно носит рекламный характер, — закон запрещает вскрывать сообщения при пересылке. А источник спама может крыться за длинной цепью посредников. Чаще всего мы прослеживаем цепочку из 5-6 звеньев, которые зарегистрированы в разных городах страны, чтобы выйти на то лицо или организацию, которое непосредственно за-

нимается рассылкой спама. В частности, потребовалось четыре месяца, чтобы выйти на одного из таких спамеров — ООО «Сияние», которому сейчас грозит штраф в 100 тыс. руб. за нарушение закона «О рекламе».

## Не надо SMS!

Не так давно стартовал интернет-проект «SMS не надо!», который также обещает избавить вас от навязчивых рассылок. Нужно лишь оставить заявку: указать свой номер телефона, имя отправителя SMS и текст спам-сообщения на сайте smsnenado.ru.

**PR-менеджер сайта smsnenado.ru Анна Лютенко:**

— Если мы уже работаем с этой компанией, то отписываем автоматически или высылаем пользователю инструкцию по отписке. Если мы точно знаем, что SMS пришло от компании-спамера, то человек получает инструкцию по подаче жалобы в УФАС. Наши операторы звонят в компанию, о которых мы ещё ничего не знаем, и выясняют, как можно отписаться от рассылок. Боль-

шинство людей, получающих рассылки, не знают, куда и каким образом жаловаться. И действительно, процедура не очень простая и даже может быть разной в отдельных регионах. Одна из наших целей — консультировать граждан, как правильно отстаивать свои права — куда жаловаться, как правильно составить текст, какие документы приложить.

Абсолютным лидером по подаче заявок на сайт smsnenado.ru сегодня является Санкт-Петербург, на втором месте — Москва, на третьем — Пермский край. Примечательно, что 88% абонентов не давали своего согласия на рассылки. Поэтому большинство жалоб — именно на незаконные рассылки.

Однако главной спасительной мерой в море спама мог бы стать закон, позволяющий операторам — и, более того, обязывающий их — фильтровать сообщения, поступающие на телефоны россиян. Такой законопроект уже есть, и он вполне может быть воплощён в жизнь. Тем более что технические способы фильтрации спама операторами существуют.

## • безопасность

# Мошенники на связи

Как не попасть на крючок аферистов и сохранить деньги на счёте мобильного телефона

**Сегодня в арсенале мобильных мошенников есть сотни захватывающих предложений, которые на первый взгляд кажутся безобидными, но в конечном итоге приводят к исчезновению денег с лицевого счёта. Казалось бы, в первую очередь внимание злоумышленников должны привлечь пользователи самых современных гаджетов, но на практике владельцы более простых моделей несут не меньше рисков. Одна из причин этого кроется в том, что действия мошенников рассчитаны, как правило, на доверчивых и недостаточно опытных пользователей мобильных телефонов. Чтобы абоненты сотовой связи всегда были начеку, эксперты МТС рассказали о наиболее распространённых вариантах уловок, к которым прибегают телефонные мошенники, и об основных способах борьбы с ними.**

## Ошибочный платёж

Одна из популярных недавно схем мошенничества через SMS вроде «Мама, я попал в аварию» уступает место новой уловке. На телефон абонента поступает сообщение о том, что на его счёт начислена определённая сумма. Следом второе SMS — уже с другого номера: «Извините, я ошибся и случайно отправил деньги на ваш счёт. Пожалуйста, верните их». Как правило, это мошенничество. Вопросами неправильно зачисленных платежей всегда занимается оператор, и денежных переводов от абонента в этом случае не требуется.

В подобной ситуации прежде всего проверьте свой баланс — действительно ли на счету появилась та самая сумма? Если платёж всё же поступил, и счесть не позволяет проигнорировать это SMS, вы можете порекомендовать отправителю сообщения обратиться к своему оператору связи.

## • Мнение эксперта



**Директор филиала МТС в Пермском крае Андрей Попов:**

— Проблема мобильного мошенничества в последние годы, действительно, является актуальной и находится в области нашего пристального внимания. В МТС действует комплексная программа, позволяющая бороться с различными видами мошенничества. Специалисты компании ежедневно анализируют поступающую информацию и пресекают новые варианты мошенничества, активно сотрудничая с правоохранительными органами.

Чтобы максимально оградить себя от действий мошенников, пользователям необходимо ответственно и внимательно относиться к информации, поступающей с неизвестных номеров. Также рекомендуем регулярно заходить в личный кабинет, чтобы контролировать свой счёт и оперативно следить за списком подключенных опций. Если, по вашему мнению, вы пострадали от телефонных мошенников или вас насторожили сомнительные звонки или SMS-сообщения, сразу обращайтесь в контактный центр вашего оператора связи. Абоненты МТС в подобных ситуациях могут позвонить по номеру 8-800-250-08-90 или написать о проблеме на горячую линию по адресу 911@mts.ru. Мы оперативно рассматриваем данные вопросы и в случае подтверждения информации принимаем меры против мошенников.

кий номер услуги, в ответ на которое поступит сообщение с полной информацией об интересующем сервисе, в том числе о действительной стоимости отправки сообщения на указанный номер. Чтобы отписаться от всех платных подписок, абонентам оператора достаточно

отправить бесплатный запрос, набрав на телефоне команду \*111\*919#.

## «Техподдержка» не дремлет

Чтобы завоевать доверие абонента, мошенники неред-

ко примеряют на себя самые разные роли, в том числе могут представиться техническим специалистом сотового оператора. Под видом сотрудника техподдержки мошенник связывается с абонентом и просит произвести ряд операций на мобильном телефоне для якобы дополнительной настройки SIM-карты или программного обеспечения. В итоге эти действия приводят к тому, что средства абонента переводятся на лицевой счёт мошенника.

При поступлении подобных звонков ни в коем случае не выполняйте указания неизвестного лица и не вводите под диктовку коды на своём телефоне. Сотовые операторы, как правило, производят любые перенастройки сети так, чтобы не беспокоить своих клиентов. Если вы сомневаетесь в достоверности информации, лучше сразу связаться со специалистами контактного центра оператора связи по номеру, указанному на официальном сайте компании, и перепроверить все данные. Абонентам

МТС в таких случаях рекомендуем обращаться по телефону 8-800-250-0890.

## Осторожно, спам!

Одной из излюбленных уловок мошенников также остаётся отправка различных спам-сообщений. Например, вам могут сообщить о выигрыше крупного приза и предложить ознакомиться с условиями его получения на сайте. Затем мошенники попросят вас положить на лицевой счёт крупную сумму и набрать определённую комбинацию цифр и символов, якобы для получения «кода регистрации». Как только вы совершиете указанные действия, деньги с вашего лицевого счёта попадут к мошенникам.

Не доверяйте таким сообщениям. Если о проведении лотереи вы узнали только тогда, когда «выиграли» приз, то, вероятнее всего, вас пытаются обмануть. Рекомендуем не следовать инструкциям злоумышленников и прекратить с ними общение.