Информационно профилактические материалы на тему:

Функциональные возможности приложений для мобильных телефонов, ограничивающих поступающие спам-звонки и сообщения мошеннического характера.

Спам любого вида — это навязчивая реклама, которая как минимум отнимает драгоценное время, максимум — способна навредить и с финансовой точки зрения. При этом стандартный определитель номера, который по умолчанию вмонтирован в мобильное устройство, как правило, бесполезен.

Спам сообщения условно подразделяются на четыре группы:

- рассылки полезные – извещения о законченном ремонте ноутбука, необходимости внесения абонентской платы и другие;
- условно полезные – смс-ки, звонки о предстоящих скидках на товар, доставке необходимого товара в магазин;
- бесполезные – сообщения рекламирующие услуги банков, микро кредитных организаций, и многого другого;
- вредоносные – способные навредить, похитить личные данные, создать кредит без вашего ведома.

Последние действуют крайне хитрым способом. При поступившем звонке ваши ответы, обычно односложные (да, нет), записываются вредоносной программой. Имея образец вашего голоса, личные данные (номер, серия

паспорта, номер телефона) мошенники могут пройти аудио индефикацию с целью получения услуги или даже кредита. Доказать в дальнейшем через суд непричастность к данному заказу практически невозможно.

Естественный вопрос, который возникает у каждого подвергшегося спам – атаке, а откуда у злоумышленников номер телефона? Подавляющее большинство данных мошенникам, спамерам предоставляют сами граждане, будущие жертвы рассылок. Стоит только заказать онлайн товар через магазин, где попросят внести номер телефона, пройти аутентификацию аккаунта игры, и ваши персональные данные могут стать общедоступными. Причем все на законных основаниях, ведь пользователь, не вдаваясь в подробности лицензионного соглашения, подписанного договора при покупке товара, добровольно передаст свои данные. Да и где купить базу данных физических лиц — сейчас не проблема. Более того, чем опасны определители, спам звонков неизвестных разработчиков, так это все тем же сбором личной информации без гарантированного соблюдения конфиденциальности. Но обойтись без таких приложений все же нельзя, так как стандартный блэклист телефона забанит любые поступившие звонки с незнакомых номеров включая полезные, например, о необходимости погашения задолженности по кредиту.

Как обезопасить себя от спама и мошенничества?

Прежде всего, следует помнить, что любая борьба начинается с профилактики, поэтому при оформлении заказа в интернет-магазине, проведении акции через социальные сети внимательно читайте договор оферты. При поступившем звонке с целью уточнения ваших данных, обязательно уточните, с какой целью звонили и из какой фирмы? Лучше всего будет совершить проверочный звонок по адресату, если речь идет о банке, либо подъехать лично к его офису. Ни в коем случае не сообщайте личную информацию даже хорошо проверенному или знакомому абоненту. Если же вас уже атаковали мошенники, то выходов из сложившей ситуации всего два. Либо поменять номер, или же поставив приложение, начать борьбу со спамерами написав на них жалобу. Для последнего варианта есть пошаговая инструкция:

Прежде всего на девайс устанавливается программа выявления спам – звонков и приложение записи разговоров. Деинсталляция последней после отправки жалобы проста, а само приложение не занимает много места.

После поступившего звонка необходимо включить запись беседы, во время самого разговора спросить у звонившего наименование организации, ее точное наименование (ООО, МП и т.д), юридический адрес, электронную почту. Причем всю информацию звонивший должен сказать четко, если спамер произносит ее нечленораздельно, попросите его все повторить.

Затем обращаетесь к сотовому оператору с целью получения детализации звонков, чтобы иметь на руках полное доказательство звонка именно вам.

На электронный адрес пишется жалоба, где указывается, кто звонил, когда, с какой целью. Письмо должно содержать ссылку на статью 14 федерального закона №152-ФЗ. По этой статье вы имеете право получить информацию об

обработке этой компанией ваших личных данных. Так же к письму прикладывают запись разговора, скриншот детализации звонка, скан договора. Если, к примеру, речь идет о магазине, через который вы совершали покупку, то следует прикрепить скан той страницы, где вы соглашаетесь на использовании ваших данных. Укажите даже в тексте жалобы что по закону вы имеете право обратиться в ФАС. Главное получить подтверждающее письмо от компании, что ваши требования получены, и идет их дальнейшее рассмотрение. Обычно уже на этой стадии телефонные звонки прекращаются.

Если звонки не прекратились зайдите на страницу ФАС, Роспотребнадзор, Роскомнадзор где даны советы как запустить процедуру отправки жалобы в эти организации.

Все эти меры довольно эффективны, в России за последнее время было несколько случаев, когда таким образом крупные финансовые организации были оштрафованы, а истец получал материальную компенсацию. К примеру, если он во время звонков находился за границей. Однако если рекламный звонок поступил от частного лица принять какие – либо меры довольно трудно, тут вся надежда на приложение анти – спам для смартфона.

Еще один немаловажный фактор соблюдения конфиденциальности, регулярная проверка мобильных устройств, носителей на вредоносные вирусы которые могут «сливать» личные данные, пароли, адреса, номера телефонов, пользователей. Лучшим выходом будет установка платного антивирусника. Только такой тип антивирусного ПО с функцией поиска фишинговых сайтов способен полностью обеспечить сохранность ваших данных, уберечь вас от рук мошенников. Конечно, сразу возникает вопрос, какой лучше купить антивирус? По мнению покупателей, лучшим вариантом является Касперский, антивирус, заслуживший самые хорошие рекомендации специалистов. Некоторым подспорьем будет дополнительный, бесплатный сервис поисковой системы Яндекс, который вместе с голосовым помощником «Алиса» на ОС Android имеет функцию фильтрации звонков. Среди бесплатных антивирусов лидирует ESETMobile Security лучшие производители носимой электроники рекомендуют именно его к установке.

На что обратить внимание при выборе приложения?

Прежде всего, определитесь, будете ли вы пользоваться данной программой постоянно или же вам она потребуется однократно. Первый случай может потребовать софта, чей функционал более широкий, такие, как правило, ставятся платно. Во всех остальных случаях подойдут обычные, утилиты, устанавливаемые бесплатно через Google Play или App Store. Надо сказать сразу, ставить софт на гаджет следует только из этих магазинов. Затем конечно следует определиться с тем, какая у вас операционная система на телефоне. Как известно,

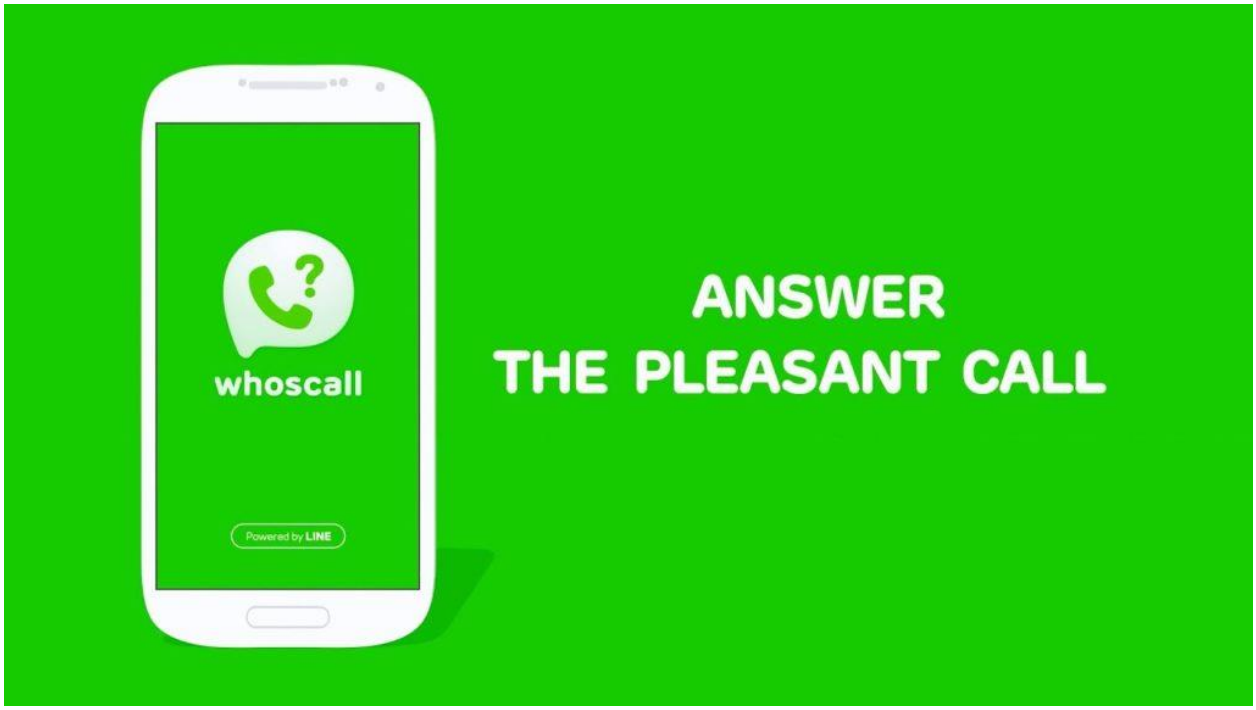
основные ОС — это Android и iOS, однако сейчас набирает популярность операционка HarmonyOS. Она разрабатывается компанией Huawei.

Общедоступные приложения защищающие от нежелательных звонков:

- 2ГИС
- Kaspersky Who Calls.
- Phone by Google («Телефон Google»)
- Truecaller.
- «Не бери трубку»
- «Сбербанк Онлайн»
- «Яндекс»
- Заключение

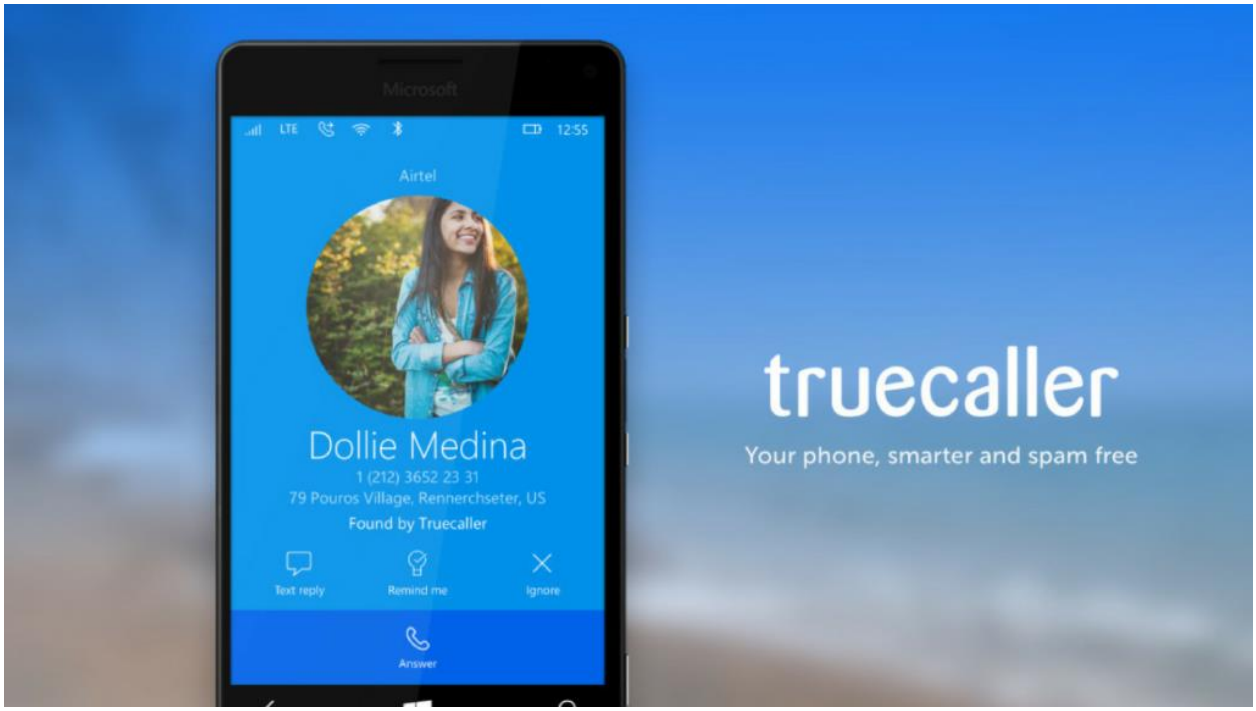
Приложений для борьбы со спамом, определители номеров для смартфонов.

Whoscall.



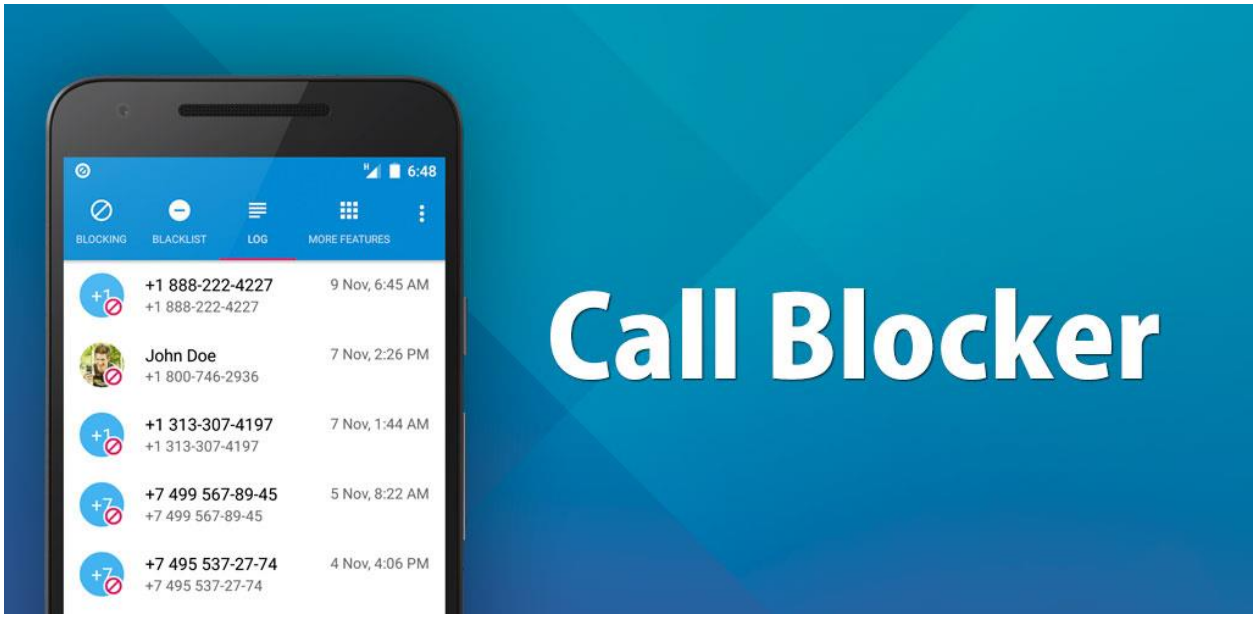
Софт – определитель благодаря простому, читаемому интерфейсу, хорошему функционалу, имеющим хорошую совместимость с устройствами. Немаловажно и то, что инсталляция, настройка производится довольно легко. Кроме борьбы с нежелательными звонками программа поможет фильтровать SMS-, MMS-сообщения.

Truecaller.



Программа антиспам, ведущая собственную базу данных. Борьба с рекламщиками происходит путем синхронизации приложения с базой данных, которая меняется в зависимости от местоположения пользователя. То есть при переезде владельца смартфона его черный список нежелательных звонков, например, от служб вызова такси, автоматически обновится. Подобная схема исключает ошибки при выборе номера, который нужно «забанить» или на какой звонок следует ответить. При этом когда вы неоднократно отмечаете номер как нежелательный другие пользователи так же получат информацию о нем, как о нежелательном. Плюсом программы является полное замещение операционной «звонилки», хотя кого-то это может и смутить.

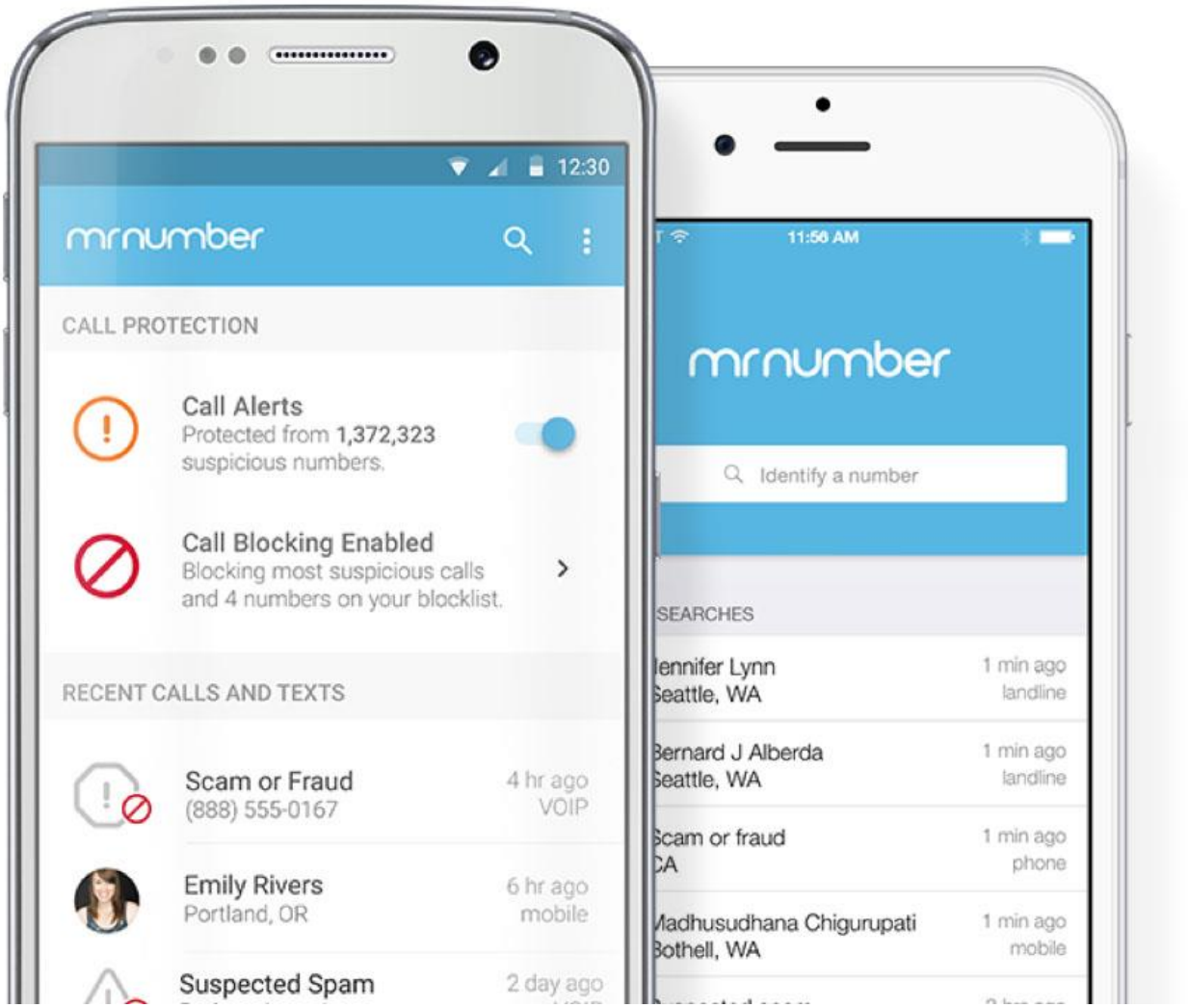
Callblock.



Назвать Callblock программой для борьбы с нежелательными звонками довольно трудно, скорее, это небольшое приложение. При поступившем вызове оно не может, как вышеуказанные системы распознать звонившего, определить его, но эффективно заблокирует его. Плюсом является пополняемая база данных, содержащая номера самых злостных спамеров из 100 стран. Эффективность утилиты будет тем выше, чем больше на ваш номер поступает вредоносных сообщений.

Доступны только 30 дней бесплатного использования, затем придется ее арендовать по цене 1,99 доллар за месяц.

Мистер Номер.



Еще одно приложение, работающее со внутренней базой спамеров, и их определением (телемаркет, микрокредиты, вымогатели). Причем включение Мистера Номера происходит автоматически, без согласия или уведомления владельца телефона. Вредоносный, потенциально опасный вызов блокируется автоматически, остальные сортируются самим владельцем. Управление программой осуществляется, в том числе через голосовую почту. Если ваши критерии выбора максимум эффективности при элементарности использования сервиса, обратите внимание на Мистера Номера.

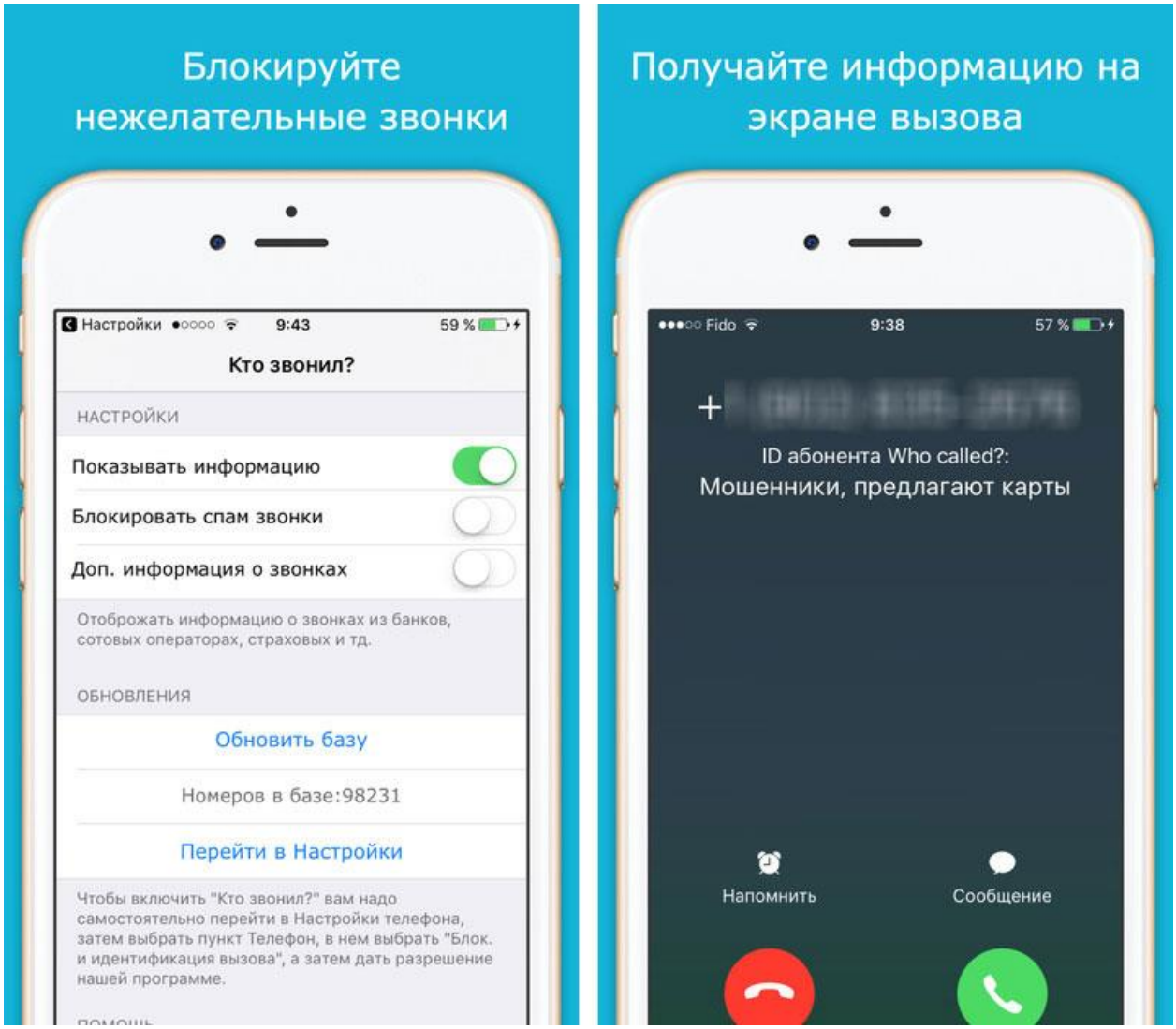
Showcaller.

Главное преимущество этой проги — небольшой, чуть более 4 мегабайт, размер файла. Это позволяет ставить «Шоуколлер» на недорогие, бюджетные смартфоны с малым объемом оперативной памяти. Более того, часто популярные модели смартфонов не имеют слота под SD карту, а стало быть, их физическая память ограничена. В таких случаях «Шоуколлер» будет просто незаменим. Программа бережет энергию аккумулятора, продлевая тем самым автономное время работы планшета или смартфона. На высоте функциональные возможности «Шоуколлера», при поступившем вызове показывается номер, иконка звонившего с наименованием рода деятельности.

RoboKiller.

Очень мощное средство борьбы, способное «отвадить» практически 100% всех нежелательных рекламщиков. Не какие новинки на рынке систем борьбы со злостными рекламщиками, жуликами не сравнятся с Робокиллером. Его «сердце» — аналитическая система, способная расшифровать поступивший звонок, определяя уровень шума, речь, количество времени между словами. После чего абонент либо блокируется, звонок сбрасывается, и номер попадает в базу данных. Алгоритм сервиса таким образом распределяет абонентов, сортируя их по направленности, записывая разговор что просто бесценно при дальнейшей подачи жалобы. Поэтому при использовании сервиса большая часть вопросов, как включить антиспам, записать беседу, отпадает сама по себе. У системы богатый функционал описание которого может занять не одну страницу

Кто звонил?



Быстро формирующая блэклист по вашему усмотрению, дополняя тем самым свою базу данных. Последняя имеет семилетнюю историю, охватывая огромный диапазон жуликов всех мастей. Часть функций системы платная, прежде всего, имена абонентов, как они зарегистрированы у других жертв рекламного «террора». Беспокоится о том, сколько стоит полный доступ к утилите не стоит. Ведь пользователю ежедневно даются монетки, которые позволяют разблокировать часть платных функций. Полезна утилита будет организациям, беспокоящимся о своем имидже, так как она четко показывает, как респонденты реагируют на их опросы, рекламные акции.

KnownCalls («ноун-колс» от англ. *known calls — понятные звонки*) — это новое, полностью бесплатное приложение для борьбы с нежелательными звонками, разработанное под платформу Android. Ключевой особенностью приложения является полная безопасность Ваших

персональных данных: приложение не производит сбор, хранение, обмен или какую-либо передачу Ваших данных и контактов, а также не работает с внешними базами. Вся работа происходит полностью на Вашем устройстве с Вашей телефонной книгой, доступ в Интернет не требуется.

Принцип работы приложения KnownCalls прост: приложение отклоняет все звонки, поступающие с номеров, не входящих в список контактов на Вашем устройстве. Это не только сэкономит Ваше время, которое вы ранее тратили на ответ неизвестному номеру, но и сделает Ваш номер непривлекательной целью для массовых обзвонов, что выгодно отличает приложение от решений, которые просто не показывают спам-звонки.

Большинство колл-центров использует для массовых обзвонов случайные, каждый раз новые номера, поэтому блокировать их по одному зачастую не имеет смысла: следующий звонок может поступить с другого номера. Недостаток других приложений для блокировки звонков в том, что они работают с задержкой: сохраняют звонки в общую базу, пока не соберется критическая масса для установления факта массового обзвона номером. Таким образом, другие приложения могут пропускать нежелательные звонки, если вы окажетесь в числе первых получателей звонка с нового номера. Такой способ блокировки неэффективен. В отличие от подобных приложений, KnownCalls — это надежная блокировка. Любой номер, не значащийся в телефонной книге устройства, будет заблокирован. При этом приложение не передает звонки и номера звонивших Вам людей в какие-либо базы.

Преимущества приложения для блокировки звонков **KnownCalls**:

- безопасность персональных данных: приложение не собирает и не пересылает Ваши персональные данные;

- для работы не требуется подключение к сети Интернет;

- полностью отсутствует реклама;

- простая настройка в 1 клик.

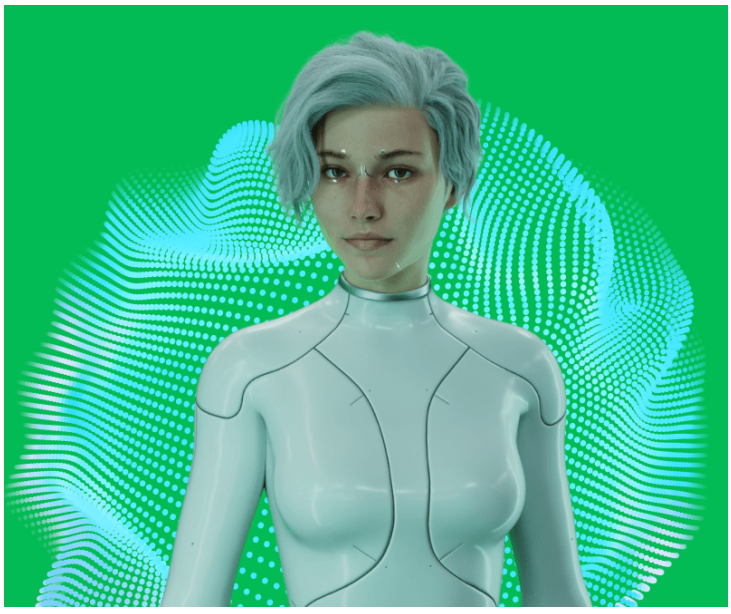
Безопасность от сотовых операторов.

Кроме того у каждого сотового оператора имеются свои способы блокировки спам-звонков и смс. Имеются как платные так и бесплатные контенты. Для подключения указанной услуги, достаточно получить информацию по горячей линии своего сотового опе

Услуга называется «SMS-контроль» и она бесплатная. Набрав на телефоне команду *903# (вызов) абоненты могут отписаться от любых SMS-подписок и добавить их в черный список оператора. Это позволит исключить появление спама в будущем.

Агент Ева

Бесплатный виртуальный секретарь и личный помощник. Блокирует спам, отвечает на звонки, защищает в интернете



Услуга «Чёрный список».

Поступил звонок от нежелательного абонента? Добавьте его в «чёрный список», чтобы в дальнейшем спамер не смог дозвониться или отправить сообщение на ваш номер. При этом настраивать блокировку можно достаточно гибко.

Так, после подключения услуги пользователь может отключить источник спама на постоянной основе. Если вы более лояльны к рекламе, установите время действия запрета, например, в рабочие часы. Не обязательно полностью отсекать тот или иной номер — некоторые звонки можно переводить на голосовую почту и прослушивать сообщения в удобное время. Или не прослушивать.

Услуга «Чёрный список» для детей.

Для детей в МТС предусмотрена специальная модификация предыдущей услуги. По сути, она объединяет в себе возможности родительского контроля, блокировки звонков и антиспама для SMS.

Для использования услуги в личном кабинете необходимо подключить связку «родитель — ребёнок». Связка может быть установлена как на один расчётный счёт, так и на разные. Далее папа или мама настраивают правила работы услуги:

1. Запретить все звонки и SMS со всех номеров или выбранных из адресного списка.
2. Установить запрет по дням, часам или постоянно.
3. Запретить SMS со всех номеров.
4. Настроить уведомления для родителей о спам-сообщениях на номер ребёнка.

Суммарное количество правил, которые можно настроить, может достигать 300.

Значительная часть спама приходится на рекламу по SMS, подчас непрошеную. У абонентов МТС есть возможность заблокировать такие сообщения, подключив одну или две бесплатных услуги, каждая из которых нацелена на разные категории SMS.

«Защитник».

Благодаря этому сервису вы можете передать общение с нежелательными номерами искусственному интеллекту МТС. «Защитник», сверяясь с постоянно обновляемой спам-базой, без вашего участия ответит на такие звонки, задаст уточняющие вопросы, расшифрует разговоры и сохранит их в текстовом виде —

просмотрите их позже в приложении Мой МТС, когда вам будет удобно. Или никогда.

Услуга «Антиспам».

Этот сервис предназначен для блокировки рекламных рассылок в SMS. Если вы получили спам-объявление, в течение 24 часов отправьте SMS с номером отправителя рекламы на короткий номер 6333 — это ничего не стоит, если вы находитесь в зоне действия сети МТС. В течение суток служба поддержки МТС пришлёт уведомление о регистрации жалоб и даст рекомендации по блокировке ненужной рассылки.

Услуга «Супер АОН».

Наверняка вы пользуетесь услугой автоматического определения номера. Однако она не позволит распознать так называемый скрытый номер — при звонках людей, подключивших себе услугу «АнтиАОН». Для распознавания скрытых номеров нужно тяжёлое вооружение — сервис «Супер АОН». Важно учесть, что эта услуга дополняет обычный АОН, а не заменяет его.

Приложение МТС Кто звонит.

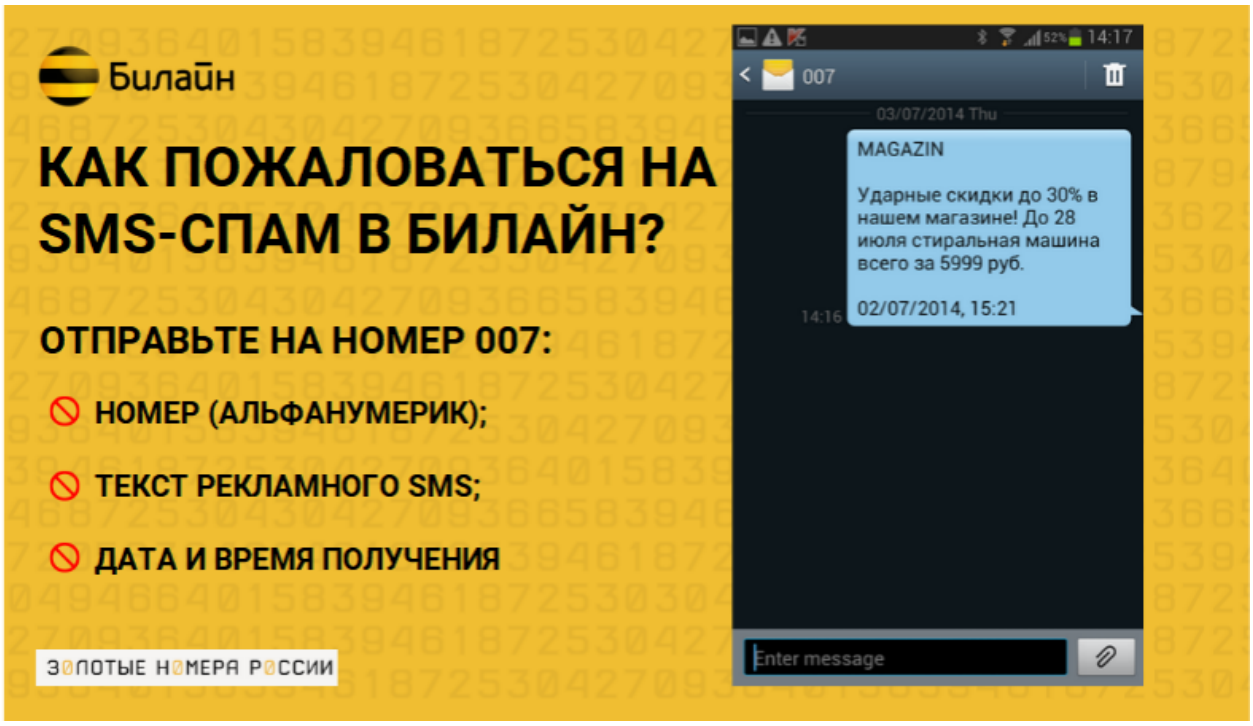
МТС Кто звонит — это, по сути, ещё одна разновидность определителя номера. Но если стандартный АОН распознаёт только те номера, которые пользователь занёс в телефонную книгу, то это приложение сверяется по базе тысяч организаций по всей России. Если звонит спамер, приложение об этом сообщит, при этом иногда будет понятно, какого рода услуги собираются вам навязать. Если звонит организация, незамеченная в спаме, вы сможете увидеть ее название, если данные о номере есть в базе.

”Антиспам-защита” для СМС.

Одним из первых операторов, реализовавших автоматическое определение спама в сообщениях, стал Билайн. Данная платформа работает бесплатно, и по отзывам абонентов справляется со своими задачами исправно.

Оператор не только определяет в автоматическом режиме массовые рассылки сообщений, но и контролирует партнеров, использующих услугу рассылок по SMS своим клиентам.

Важно! Ни один оператор не вправе блокировать рекламные сообщения, если пользователь выразил согласие на их получение. Поэтому, если вам поступает реклама от определенной компании или магазина, и не хотите ее получать в дальнейшем, необходимо обратиться в поддержку, чтобы отозвать свое согласие.



А вот если вы не подписывались на рассылку, но вам поступило рекламное сообщение, и система защиты Билайна его также не заблокировала, направляйте жалобу провайдеру связи. Необходимо отправить сообщение бесплатно, указав в тексте следующее:

- Альфанумерик/номер телефона;
- Полный текст полученного СМС;
- Точные дата/время доставки.

После отправки такой жалобы на номер 007р, оператор проводит проверку, и блокирует данного отправителя в своей сети, если она выполняется незаконно.

”Кто звонит” — умный АОН.

Предоставляемая оператором услуга рекомендована тем, кто часто получает звонки с незнакомых номеров. Благодаря данному сервису, можно принять правильное решение — отвечать или нет на такие звонки.

Для пользователей смартфонов доступно множество приложений, отлично справляющихся с такой задачей. Однако стоит учитывать, что для использования необходимо установить приложение, предоставить ему разрешение, и использовать функцию, чаще всего, это доступно только при активном подключении к интернету.

А вот услуга Билайна работает без интернета, и не требуется установка приложение. Определение номера звонящего происходит на стороне системы оператора, и уже в момент звонка можно увидеть на экране своего телефона предупреждение о спаме, опросах, мошеннических звонках. Пользоваться сервисом доступно практически на любом телефоне.

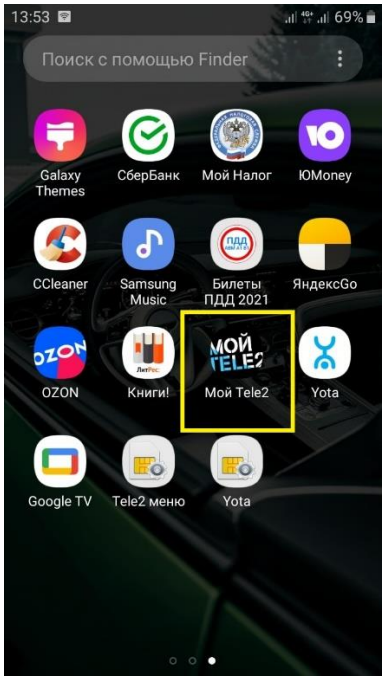
Три рубля в сутки — плата за пользование, и она начисляется независимо от того, сколько звонков поступило, или их в текущих сутках не было вовсе.

Для активации используйте:

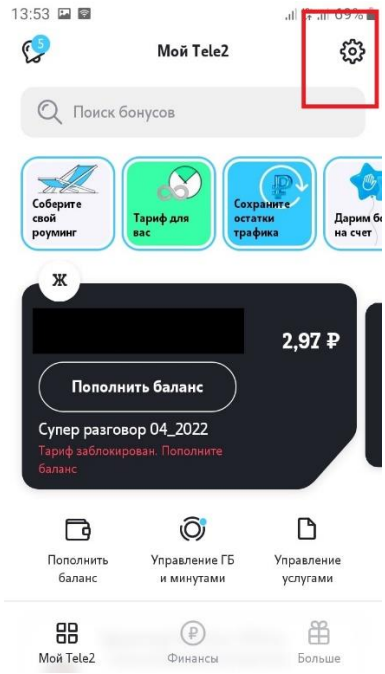
- Позвоните на 09977р;
- Напишите **СТАРТ** в SMS на номер 1260;
- Воспользуйтесь ЛК на сайте.

Однако учитывайте, что ограничения на использование “Кто звонит”. Так, для использования умного определения спама у вас не должно быть активного запрета на информационно развлекательные сервисы, а также услуга VoLTE.

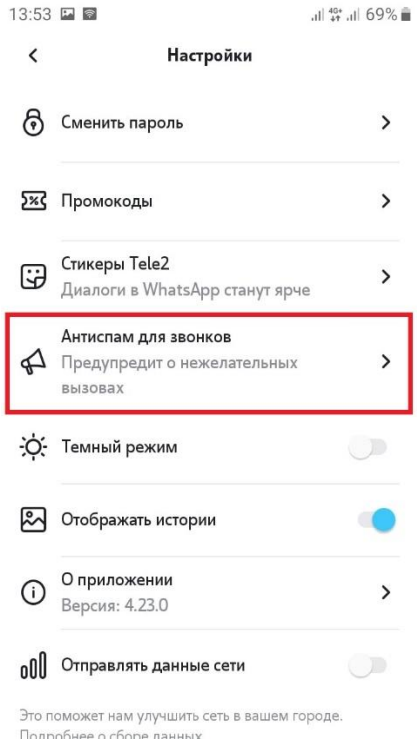
Откройте приложение Мой Tele2, нажав на значок на главном экране смартфона.



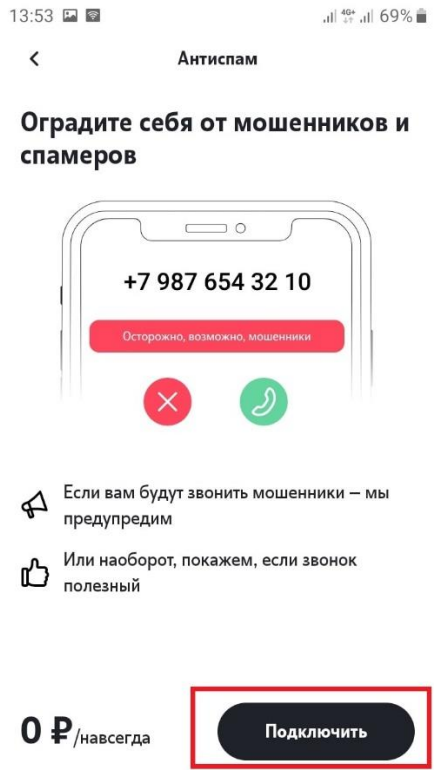
На главной странице, вверху справа нажмите на значок Настройки.



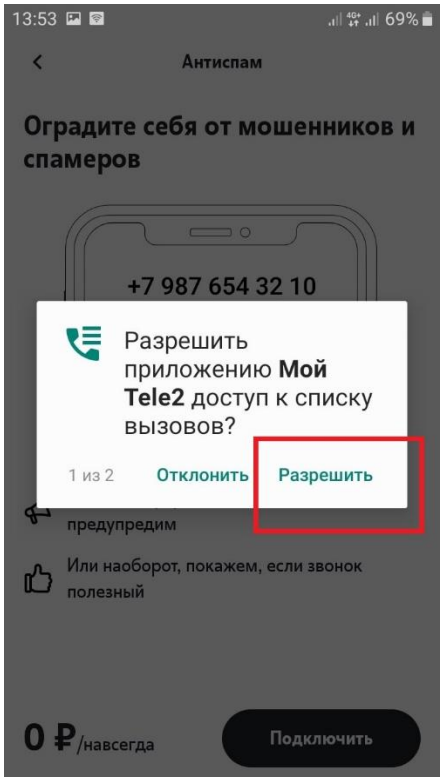
В открывшемся окне нажмите на вкладку Антиспам для звонков.



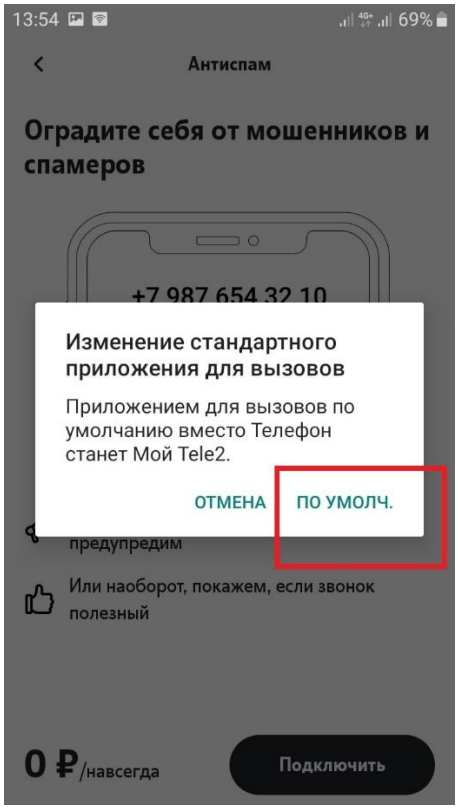
Внизу страницы нажмите на кнопку Подключить.



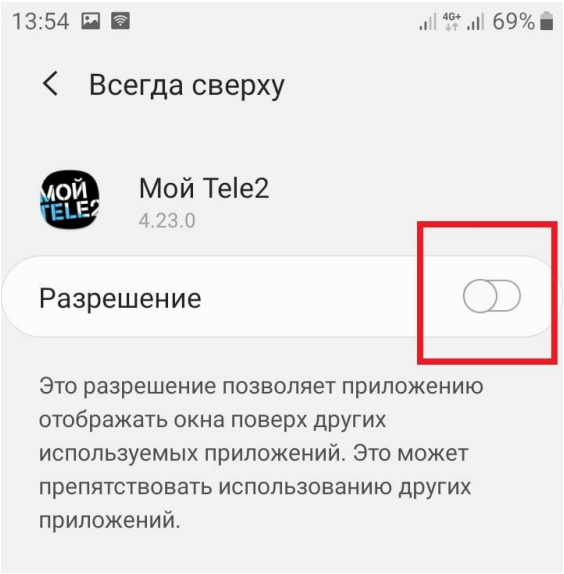
Разрешите приложению доступ к списку вызовов.



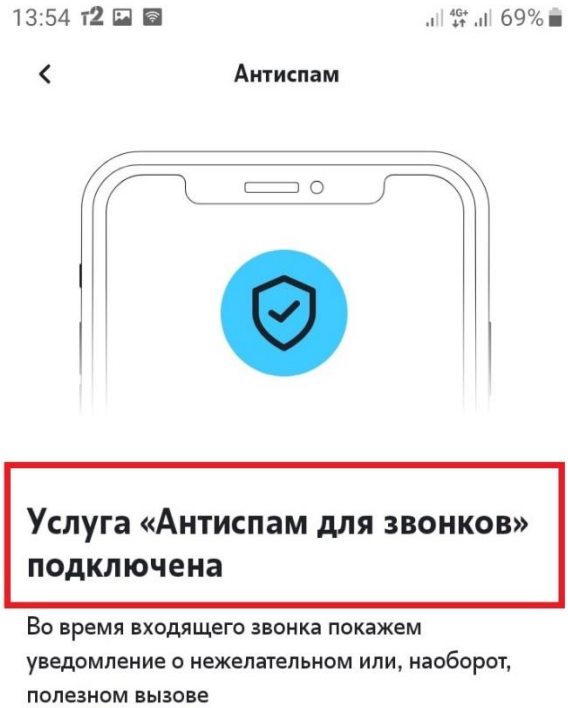
В открывшемся окне Изменение стандартного приложения для вызовов, нажмите на вкладку По умолчанию.



Разрешите приложению отображать окна по верх других используемых приложений.
Учтите, это может препятствовать работе других приложений. Если вы заметили какие-то проблемы, отключите данное разрешение.



Готово, вернитесь в приложение, услуга Антиспам для звонков будет подключена.



Отключается данная услуга через настройки телефона Разрешение приложений.

ТИНЬКОФФ

Тинькофф запустил новую платформу безопасности для клиентов Тинькофф Банка и Тинькофф Мобайла — она дает пользователям максимально возможную на рынке защиту от мошенничества и спама.

Это достигается за счет того, что платформа одновременно объединяет банковские алгоритмы защиты от социальной инженерии (Тинькофф Банка) и технологии собственного телеком-оператора в экосистеме Тинькофф (Мобайла).

По данным внутренних исследований, клиенты Тинькофф Банка, пользующиеся услугами Мобайла, в два раза лучше защищены от атак мошенников, чем просто клиента банка или телеком-оператора.

Это первая подобная интеграция в России защитных инструментов банка и мобильного оператора в одной платформе.

Один из ключевых сервисов платформы — технология «Нейрощит», которая на основе искусственного интеллекта выявляет и пресекает попытку мошенничества непосредственно во время телефонного звонка.

Усиленную защиту обеспечивает синергия всех инструментов в периметре экосистемы благодаря скорости обмена данными между банком и оператором и бесшовному процессу интеграции. Например, маркировка перевода как рискованного, если он совершается клиентом на номер телефона вне звонкового профиля абонента Мобайла. Проверка 98,5% операций проходит без дополнительного вовлечения клиента.

Вот что входит в новую платформу защиты клиентов банка и Мобайла.
Инструменты, разработанные для Тинькофф Мобайла:
Нейрощит:
- анализ в момент операции;
- активный звонок, переадресация звонка, посещение подозрительных сайтов;
- выявление массового обзвона/рассылки;
- дерево контактов;
- блокировка СМС-спама.
Инструменты, разработанные для Тинькофф Банка:
- подтверждение подозрительных операций: селфи, звонок, видеозвонок, СМС, контрольный вопрос;
- самозащита: вход по лицу/отпечатку, уведомления, лимит по карте, обучение финансовой безопасности;
- определитель номера;
- защитник Олег;
Call Defender:
- анализ по черным спискам номеров, распознавание подмены номера банка;
- антивирус;
- сверка голоса;
- система фрод-мониторинга 24/7: Machine Learning & AI, нехарактерное поведение, платежные привычки, цифровой отпечаток, контроль клонирования и перевыпуска сим-карт.

Нейрощит — новая технология Тинькофф Мобайла для защиты абонентов от мошенников в режиме реального времени. Нейрощит анализирует и сопоставляет огромное количество технических характеристик входящего звонка.

Ключевое преимущество этой технологии — выявление мошенников через анализ технической информации, содержащейся в звуковой волне. Во время разговора звук преобразовывается в набор специфических данных. В режиме реального времени искусственный интеллект обрабатывает их и сравнивает с накопленными «эталонными» наборами данных мошеннических звонков. Если количество совпадений превышает допустимый порог, искусственный интеллект маркирует разговор как потенциально опасный и разрывает его. Сценарии мошенничества регулярно меняются, поэтому ИИ постоянно обучается на всех входящих данных.

Искусственный интеллект анализирует и другие характеристики входящего номера, среди которых история звонков, объемы и характер трафика, частотность и уникальность. Анализ технической информации звонка позволяет выявить мошеннический звонок практически со стопроцентной вероятностью.

Если номер включен в черный список.

Определитель номера Тинькофф маркирует входящий звонок как мошеннический, но абонент поднимает трубку, ассистент Олег предупреждает абонента о потенциальном мошенническом звонке в начале разговора. Далее пользователь самостоятельно принимает решение о продолжении разговора.

Тинькофф Мобайл анализирует номер входящего вызова и проверяет, используется ли номер мошенническими колл-центрами или участвует в спам-звонках. Если да, оператор сразу передаст информацию в банк для дополнительного мониторинга последующих банковских операций.

Дерево контактов.

По звонковому профилю абонента формируется список контактов, с которыми обычно взаимодействует клиент. Крупный перевод денег или несколько небольших подозрительных платежей на счет лица, которое не входит в дерево контактов, маркируются системой фрод-мониторинга и могут быть приостановлены.

Блокировка СМС-спама.

Если оператор зафиксирует факт массовой рассылки, номер будет заблокирован и абоненты Тинькофф Мобайла не получат спам-сообщение.

Подтверждение подозрительных операций.

Если клиент совершает нехарактерные для него операции или проводит их с нового устройства, система попросит подтвердить действие с помощью селфи, звонка, видеозвонка, СМС или контрольного вопроса. Формат проверки зависит от степени риска.

Самозащита клиентов.

Клиенты могут самостоятельно подключить инструменты, помогающие предотвратить мошенничество.

Доступ к приложению Тинькофф с помощью Face ID или отпечатка. Эти данные, в отличие от кода, нельзя подсмотреть, подобрать или скопировать.
СМС- и пуш-уведомления помогают клиенту следить за операциями и вовремя заблокировать карту, если он их не совершал.

Лимит по карте ограничивает возможные мошеннические списания, особенно если карта часто используется для онлайн-покупок или подписок и ее реквизитами могут завладеть в связи с утечкой из базы данных продавца.
Тинькофф также обучает навыкам финансовой безопасности с помощью сторис в приложении, пуш-уведомлений, образовательных курсов и других форматов.

Определитель номера.

Бесплатный определитель телефонных номеров помечает потенциально мошеннический звонок, предупреждает абонента и автоматически передает эту информацию в систему фрод-мониторинга Тинькофф.

Защитник Олег.

Защитник Олег — бесплатный телефонный секретарь, специально обученный защищать людей от нежелательных звонков спамеров и мошенников. Защитника Олега можно подключить к любому номеру сотовой связи, но для абонентов Тинькофф Мобайла доступна расширенная функциональность с возможностью кастомизации помощника.

Tinkoff Call Defender.

Первая банковская антифрод-платформа для защиты от телефонного мошенничества. Система автоматически проверяет, есть ли входящий номер в черном списке, и передает информацию службе безопасности банка для более внимательного изучения последующих действий со стороны клиента.

Мошенники могут также использовать номера Тинькофф Банка. Tinkoff Call Defender мгновенно выявляет и блокирует такие звонки.

Антивирус.

Во время запуска мобильного приложения банка смартфон автоматически проверяется на наличие вирусов, вредоносных приложений и программ удаленного доступа. Антивирус подает сигнал системе фрод-мониторинга, если обнаруживает подобные программы.

Сверка голоса и селфи.

Тинькофф использует собственные разработки по сверке голоса и селфи клиента, чтобы убедиться, что в банк с запросом обращается сам клиент, а также технологию liveness, которая анализирует, живой человек проходит аутентификацию или мошенник подставляет фото или видео клиента.

Система фрод-мониторинга 24/7.

Система фрод-мониторинга оценивает риски и защищает клиентов с помощью набора алгоритмов, усиленных машинным обучением и технологиями искусственного интеллекта. Система исследует поведение клиента, его платежные привычки, цифровой отпечаток используемого устройства и другие показатели, чтобы выявлять и предотвращать мошенничество. Кроме того, во время отправки банком СМС система сверяет уникальный для каждой сим-карты IMSI-код, чтобы контролировать клонирование и перевыпуск сим-карт мошенниками.

Безопасны ли блокираторы звонков?

Эксперты по информационной безопасности предупреждают, что не все приложения для блокировки звонков безопасны. Так, такие приложения могут собирать личные данные пользователя: историю звонков, список контактов, адреса электронной почты и другие. Состав информации зависит от доступа, который владелец устройства предоставляет приложению. Потом эти данные могут передаваться третьим лицам, например, они могут попасть в базы данных других приложений или их могут продать недобросовестным рекламодателям или мошенникам. Риски, связанные с предоставлением сомнительному приложению доступа к личным данным, выше, чем риск быть обманутым мошенником. Тем, кто всё же решится установить приложение, нужно проверить его через специальный сканер ImmuniWeb Mobile App Security Test, обязательно изучить пользовательское соглашение и не предоставлять ему доступ к личным данным. Приложения работают по принципу «проверить входящий номер в базе». База составляется самими пользователями, и туда могут попадать безобидные номера, если на них, например, пожалуются конкуренты. Также приложение может подключаться к базе крупного оператора связи или банка. Но это платная услуга, поэтому разработчики таких сервисов могут зарабатывать с помощью рекламы или на продаже данных пользователей. При этом даже самые

хорошие приложения не способны определить подмену номера — когда звонок осуществляется с одного номера телефона, а при входящем вызове пользователь видит другой, скажем, телефон своего банка.