

INBOX

Полное руководство по доставляемости
ваших писем



МАКСИМ ТИМОЩЕНКО

Максим Тимощенко

**INBOX. Полное руководство
по доставляемости ваших писем**

«Издательские решения»

Тимощенко М.

INBOX. Полное руководство по доставляемости ваших писем /
М. Тимощенко — «Издательские решения»,

ISBN 978-5-44-967897-3

Книга предлагает читателям глубокое погружение в тонкости и стратегии, которые помогут вам повысить показатели доставляемости, открытия и кликабельности ваших электронных писем. От основ доставки до продвинутых методов преодоления спам-фильтров, данное руководство подробно рассматривает все аспекты успешной доставки email-писем и помогает разобраться в сложных нюансах этой отрасли.

ISBN 978-5-44-967897-3

© Тимощенко М.
© Издательские решения

Содержание

ПРИВЕТСТВЕННОЕ СЛОВО	6
Смысл доставляемости	7
Технические требования к рассылкам	10
Конец ознакомительного фрагмента.	12

INBOX. Полное руководство по доставляемости ваших писем

Максим Тимошенко

© Максим Тимошенко, 2023

ISBN 978-5-4496-7897-3

Создано в интеллектуальной издательской системе Ridero

ПРИВЕТСТВЕННОЕ СЛОВО

Всем привет, меня зовут Тимошенко Максим, я являюсь руководителем направления e-mail-маркетинга в Газпром Медиа Холдинг. В этой книге я хочу рассказать о доставляемости в email-маркетинге, ориентируясь как на базовый уровень, так и на тех людей, которые уже хоть немного, но что-то делают в email-маркетинге или, может быть, даже работают с крупными базами, поэтому мы пойдем не только по верхам!

Я начну с глобального блока – доставляемости писем, который мучает многих клиентов: «А что же делать? А как же быть?». И могу сказать, что у многих крупных брендов не настроен до сих пор даже параметр DMARC, которого требуют многие email-провайдеры.

В рамках книги я буду раскрывать по большей части технические моменты доставляемости и автоматизации. Что такое доставляемость, зачем она нам нужна, каковы технические требования к рассылкам, что нужно обязательно сделать, какие существуют качественные показатели, что относится к маркетологу, а не к техническому специалисту. В общем, рассмотрим, как решать проблемы, на примерах конкретных почтовых провайдеров.

Некоторые части книги будут полезны руководителям отделов маркетинга, некоторые моменты из книги будут полезны вашим системным администраторам, разработчикам, некоторые непосредственно email-маркетологам, так как им необходимо будет настраивать техническую составляющую. Есть вещи, которые интересны на ESP (email server provider) – платформах. Их техническая часть, как правило, реализована самой платформой, но всегда стоит помнить, что качественные показатели относятся напрямую к маркетологу, к тому, кто будет отправлять письма.

Смысл доставляемости

Давайте подумаем, что такое спам. Спам – это массовая рассылка коммерческих писем тем, кто не выразил яркого желания их получать. Когда вы шлете тем людям, которые не ждут ваших писем, вам нужно получать явное согласие, чтобы не слать спам, причем оно должно быть выражено не ранее, чем за 12 месяцев. Практика показывает, что люди, подписавшиеся более 12 месяцев назад, могут забыть про вас. Важно постоянно чистить базу. Год – это долгий срок. Вы можете поставить себя на место таких людей и подумать: если год назад вы подписались на какой-либо сервис, вспомните ли вы его сейчас, если вы в течение года с ним не контактировали? Думаю, ответ очевиден.

Второй момент: когда вы получаете данные в рамках офлайн-конференций, обязательно надо предупреждать, что будете отправлять письма. В свое время я пересекался с «Инфобизнесменом» на какой-то из конференций, мы обменялись визитками, после этого мне пришла рассылка. Иначе говоря, я был удивлен, каким образом мой рабочий email попал в рассылку от него? На мой взгляд, это было не очень корректно.

При этом, даже если у вас есть согласие на получение рассылок, контент должен обязательно соответствовать ожиданиям подписчика, то есть, если человек подписывается на туризм, нельзя ему отправлять рассылки о инфобизнесе. Если человек подписывается на маркетинг, не надо ему отправлять письма про игрушки. Это вызывает негатив, и подписчики с большой долей вероятностью нажмут «ЭТО СПАМ».

Еще один важный момент: обязательно должна быть возможность отказаться от полученных рассылок как в рамках всей коммуникации, так и в сам момент подписки. И при начале пользования сервисом вы должны дать возможность не подписываться, а просто зарегистрироваться в нем.

Нельзя отправлять письма, если нет явного согласия: скрытые пункты, вписанные в политику обработки персональных данных или в политику пользования сервисом, – это не очень корректные моменты, из-за которых вы получите больше негатива, чем релевантных клиентов.

Также негатив возникает, когда вы пытаетесь спрятать то, что письма приходят от вас, то есть изменяете имя отправителя или домен. Это все не очень правильно. В США, Европе, Канаде есть законодательно закрепленные штрафы за спам-рассылку, и в законе четко указано, что в каждом письме должны быть физические контакты отправителя, чтобы имелась возможность выйти с отправителями на связь.

Что такое вообще доставляемость? О чем мы говорим и зачем нам это нужно? Доставляемость очень важна с точки зрения получения прибыли с email-рассылок потому, что, если письма в спаме, их никто не видит, соответственно, никто не открывает и не переходит на сайт, а вы не получаете целевые действия, которые вам нужны, и не зарабатываете нужные деньги.

При этом доставляемость делится на два типа: техническая и качественная, они различаются кардинально.

Техническая – это, то сколько сообщений вообще попало в почтовые ящики пользователей – без разницы, в какую из папок. Показатель технической доставляемости ESP сообщают в графе «Доставлено писем», и, как правило, он составляет 99,95%.

Качественная доставляемость – это то, сколько писем попало в inbox, то есть не было отфильтровано в спам. И это то, чего мы пытаемся добиться в email-маркетинге.

Влиять на доставляемость можно двумя вариантами: как я говорил, технически, с помощью настроек, сложных аббревиатур и так далее, и качественно: через репутацию, лояльность, привлечение подписчиков в рассылки, коммуникации.

Техническая часть больше относится к IT-специалистам, инфраструктуре, которая используется для отправки сообщений, и не всегда зависит от email-маркетолога. Качественные же показатели имеют отношение непосредственно к тем, кто создает контент и стратегию.

Также нужно четко понимать то, что технические составляющие – это первичная база, которая обязательно должна быть. То есть, если у вас будет отличная стратегия, ее будут любить ваши пользователи, но, если у вас нет попросту настроенных параметров, ваши письма никто не увидит. Таким образом, базовые параметры SPF, DKIM, политику DMARC нужно настраивать изначально.

Соответственно, если не настроить техническую часть, вероятнее всего, вы будете в спаме, потому что в данный момент почтовые провайдеры очень четко проверяют все эти нюансы. Если их нет, они рассматривают рассылки как спам, потому что для спамера нормально не заморачиваться, а купить разовый сервер, сделать рассылку и выбросить его.

Качественные отправители, хорошие email-маркетологи и крупные бренды настраиваются на длительную коммуникацию с пользователями, поэтому следят за такими вещами и стараются выстраивать долгосрочные отношения.

Немного подробнее поговорим про выделенные IP-адреса: сначала о разделении отправляющих IP-адресов, а затем о том, как происходит отправка писем. Предположим, у вас есть почтовый сервер (SMTP Server), который, как правило, привязан к вашей форме рассылок, то есть форма подписки у вас, получается, не привязана к платформе, потому что вы сами настраивали почтовый сервер. У почтового сервера есть параметры отправки: домен отправителя и IP-адреса, с которых уходит почта. Это то, что находится на вашей стороне, и вы их контролируете, вы можете их менять. Почему это важно? Например, возьмем сервис GetResponse – это платформа, ориентированная на средних и мелких клиентов. Соответственно, выделять под каждого клиента пул IP-адресов не имеет смысла, это неоправданное использование ресурсов со стороны платформы. Поэтому GetResponse, так же как «Юнисендер», MailChimp и другие ESP – все платформы такого уровня, используют общие IP-адреса для большого количества своих клиентов, это означает, что репутация IP-адресов распределяется по каждому из отправителей и формируется также суммарно из репутации каждого отправителя.

К чему это может привести? К тому, что платформа в какой-то момент упустит момент понижения репутации за счет одного из отправителей. Например кто-то загрузил огромную купленную базу, сделал по ней рассылку, и на нее пожаловались, репутация IP упала, и уже ваши хорошие рассылки, которые используют те же самые IP-адреса, идут в спам. Такие ситуации случаются часто, и это тот риск, который несут общие IP.

Не все платформы предоставляют выделенные IP, но у тех, кто нацелен на хороший уровень работы, они есть. И не всегда выделенные IP даются бесплатно. Так что выделенные IP-адреса, с одной стороны, – хорошо, потому что вы сами формируете репутацию, с другой стороны – это проблема, потому что, если у вас случайно пошел какой-то плохой трафик, то вы сами себя топите. Соответственно, с выделенными IP все зависит от вас с точки зрения репутации.

Давайте поговорим, почему имеет смысл разделять новостные и транзакционные письма с разных IP-адресов и с разных доменов.

Транзакционные сообщения – это восстановление пароля, сопровождение заказа, подтверждение регистрации, это те письма, которые обязательно должны быть доставлены пользователям.

Маркетинговые сообщения – промо-акции, распродажи и т. д. – это письма, которые приносят вам прибыль, но, если они не придут, вы потеряете только прибыль.

Для подписчика не будет критичным то, что он не получит этого письма с распродажей. При этом, если он не получит письмо с восстановлением пароля, он вообще отстранится

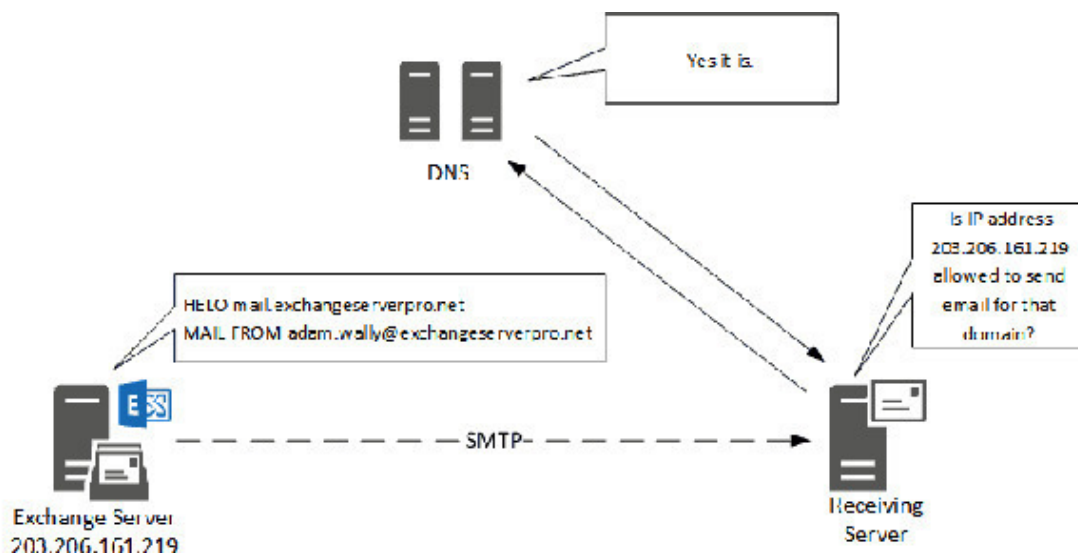
от пользования вашим сервисом. Поэтому есть тактика разделения доменов и IP по разным типам сообщений.

Как это делается? Для промо используется домен типа promo.<domain>.com, а для транзакций – order.<domain>.com. Соответственно, репутация разделяется по этим доменам, и в случае если ваши массовые рассылки попадут в спам, письма восстановления пароля все равно будут приходить.

Базовый принцип – это разделение вашего основного корпоративного домена и домена, использующегося в массовых рассылках. Аналогичная тактика применяется для разделения разных типов писем.

Может также использоваться замена доменов, смена IP в зависимости от страны, в которую вы отправляете, то есть, например, если вы шлете в Россию, Украину, Белоруссию, там можно использовать одни и те же IP. А если вы еще отправляете письма условно в Америку или Китай, тогда имеет смысл брать другие домены, другие IP-адреса. В отношении Китая – там все очень строго: нужно иметь сервер, который физически находится на территории КНР.

Технические требования к рассылкам SPF-запись



ru.wikipedia.org/wiki/Sender_Policy_Framework

SPF (sender policy framework) – это подпись, содержащая информацию о серверах, которые могут отправлять почту с вашего домена. Наличие SPF снижает вероятность попадания вашего письма в спам.

Важно помнить, что SPF-запись может быть только одна для одного домена. В рамках одной SPF может быть несколько записей (например, если письма отправляются с нескольких ESP – маловероятно, но все же чуть позже будет пример). Для поддоменов нужны свои записи.

Пример записи SPF

Название записи	Формат	Содержание
ваш_домен. (у некоторых хостингов вместо этого может подставляться @ или оставаться пустое поле. При написании названия «ваш_домен.» оно заменится автоматически)	TXT	v=spf1 +a +mx -all

SPF запись определяет, от имени каких IP-адресов вы можете отправлять письма, то есть это та запись, которую проверяет почтовый провайдер mail.ru, yandex.ru, gmail.ru и другие, они смотрят на соответствие IP-адреса, с которого фактически пришло письмо, и IP-адреса с которого вы разрешили отправлять. SPF-запись публикуется в открытом доступе в форме DNS. Вы можете посмотреть SPF-запись любого домена, просто воспользовавшись нужным сервисом.

Приведем пример Lamoda. У них запись выглядит следующим образом:

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.