**Семь способов стать спамером по ошибке**

Пользователи Интернета любят отправлять в "Спам" все неугодные им письма, поэтому удобной корзиной для спама снабдили своих пользователей почти все Интернет-почтовики. К сожалению, наряду с нечестными сервисами от быстрого решения этого страдают за одно и множество легальных компаний.

Ваше письмо летит в спам, как правило, по глупой случайности. Но иногда причина все же в том, что ресурс не предает должной важности антиспамовой политике. "Если электронную корреспонденцию определенной компании ящик принимает за спам, в большинстве случаев это происходит из-за ошибки, которую совершает сама же компания", - говорит Ричи Дженнингз, главный специалист по анализу безопасности компании Ferris Research.

Для того, чтоб подобная участь не постигла и ваш сервис, мы приводим здесь семь наиболее часто встречаемых просчетов в этой сфере. Избегайте их – от этого зависит, получат ли клиент ваше сообщение.

**1. Игнорирование отмены подписки.**

Это и так просто как день, и ничего нового тут нет, но если не соблюдать простое правило не отправлять рассылку тем, кто уже от нее отказался, то очень скоро можно получить "сюрприз": раздраженный пользователь просто-напросто устанет от частых рассылок и ваши письма полетят прямиком в корзину его почтового ящика.

Посмотрите на это, как на грамотное управление. "Все основывается на менеджменте: знаете ли вы, кому отправляете письма, и нужна ли им эта почта?", - говорит Рос Фубини , старший директор по развитию в компании Symantec. "Как вы составили список этих людей или где его купили, и хотят ли эти люди вообще получать ваши письма?"

Дженнингз говорит, компании должны удостовериться в том, что их линки для отмены подписки действительно рабочие. "Если человек попадает на страницу с ошибкой 404, так как ссылка в его письме не работает, то считайте, что это ваш промах. Будьте готовы к скорой репутации спамера. Это, кстати, считается незаконными в США и других странах. Вы должны уважать желание тех, кто хочет отменить рассылку, это диктует закон".

Вместо того чтоб отписаться от рассылки, когда она им уже неинтересна, некоторые пользователи сначала ставят свое согласие, а потом передумывают. А для избавления от надоедливых писем используют корзину "Спам". И вот на имени вашей компании появляется пятно – в последствии спамовые фильтры могут внести вас в черный список и применять тот же ход и для всех остальных пользователей – ваши письма будут застревать при проверке. "В случае, если клиент пользуется AOL, Google`s Gmail или Hotmail, у вас возникает реальная проблема - там стоят "обучаемые" на спам фильтры", говорит он.

Где же выход? В AOL отправители писем попадающих в "Спам" могут зарегистрироваться для "обратной связи". "Таким образом, если подписчик помечаетваше письмо как спам, и отсылает его с такой пометкой в корзину, а вы при этом являетесь добропорядочной компанией, то на ваш ящик приходит сообщение о том, что вас посчитали спаммером", - говорит Дженнингз. С помощью этой услуги можно узнать, и кто именно пожаловался на вас, а потом удалить соответствующий адрес из базы подписчиков.

В Hotmail есть обе эти опции – "Спам" и "Отписаться от рассылки", и проблема решается еще проще. Вы должны оставлять вверху письма место, чтоб почтовик мог разместить там необходимые кнопки.

**2. Смена темы.**

Это, пожалуй, самая частая история. Пользователь подписывается на получение писем с рассылками или обновлениями одной тематики, но в итоге начинает получать почту от другого сервиса, рассылки которого он не заказывал.

Компания радостно объявляет: "У нас появилась новая рассылка, и мы подумали, что это могло бы заинтересовать вас". От нее, естественно, можно от оказаться, но восторга у пользователя это обычно не вызывает, а вот из-за этих действий у вас очень даже может появиться репутация спамера.

Для того, чтоб не получить позорный ярлык спамера, предоставьте пользователю выбор, подписываться на новые рассылки или нет, вместо того, чтоб слать их без разрешения клиента. "Нужно предоставить пользователю возможность с самого начала подписываться на новые рассылки, а не подталкивать их к отказу, размещая у себя одну лишь кнопку для прекращения рассылки", - советует Фубини.

Передавать списки электронных адресов клиентов по своей маркетинговой сети, может, и удобно, но в итоге это может стать ножом в спину для вашей же компании. Это касается и передачи списков братским компаниям. "Такая практика почти тоже самое, что продавать почтовые списки, но вот только тут торговля идет внутри своей компании", - говорит он. "Ведь новая рассылка – это не то, на что изначально подписывался клиент".

Фубини говорит, что встречал ситуации, когда компании составляли почтовый список для одного вида продукции, а затем решали использовать его для других товаров, не имеющих отношения к первым, что и приводило к серьезным проблемам. Необходимо задать вопрос, а на самом ли деле подписчик хочет слышать об этом втором продукте.

"Если компания рассылает мне информацию о продаже ботинок для турпоходов, а потом начинает слать мне рекламу лыж другой марки, для меня это чистой воды спам", - говорит он.

"Такая ситуация оправдана и правомерна тогда, когда клиенты подписались на рекламу, скажем, всех рождественских новинок". Необходимо быть аккуратным в использовании списка почтовых адресов, которым вы владеете. Ведь компания отсылает письма тем, кто пока хочет их получать и соглашается слышать ее слышать…

3. Предоставлять нечеткие инструкции по регистрации и игнорирование запросов пользователей.

Это вопрос того, насколько вы уважаете мнение клиентов: "Будьте по-настоящему честными с людьми и дайте им возможность отказаться от рассылки, если они этого захотят", - говорит Фубини.

Если пользователю не предоставляется возможности проставить при заполнении флажок согласия на получение рассылок, это может показаться подозрительным, и вас запросто обвинят в непрофессионализме. По словам Дженнингза из Ferris Group ожидать от пользователя того, что он просто отпишется от получения ваших рассылок неправильно: "В Европе нужно давать письменное согласие. Если рассылки сами проставляют галочку по умолчанию, это не письменное согласие".

Если инструкции по отписке от рассылки нечеткие, это только отвернет от вас пользователей, и проблемы вам обеспечены. Подобная формулировка натолкнет на мысль о том, что что-то тут нечисто. Если они полагают, что уже отписались (следуя нечетким указаниям) и все еще продолжают получать от вас письма, вас могут посчитать спамером, говорит Дженнингз.

"Лучше вести честную политику и потерять всего нескольких пользователей, кто внимательно относится к своим почтовым ящикам, чем создать себе же проблемы и получить репутацию спамера от огромного количества пользователей", - говорит Фубини.

4. Не контролировать внутренние компьютеры и серверы, которые могут быть использованы против вас

Андрю Ли, главный исследователь компании Eset говорит, что недавно проводил проверку компании одного своего клиента, и обнаружил там зараженные вирусами машины под столами в хозяйственной комнате. Там сканировались тысячи IP-адресов каждую минуту. "Никто не знал, что данное оборудование стояло там, и почему оно там находилось также, но, судя по возрасту железа, длилось это уже долго", - говорит он. "Очень тяжело избавиться от клейма спамера или быть в "черном" списке IP. И очень тяжело потом вернуть все обратно".

Ли рекомендует плотно наблюдать за своими серверами и компьютерами, а также другими электронными ресурсами и программным обеспечением. "Просто поразительно, сколько компаний не следит за тем, сколько у них серверов и компьютеров, про которые им неизвестно… в свое время их подключили по делу, но потом за не надобностью забыли".

Необходимо удостовериться, что все компьютеры, на которых хранится база электронных адресов пользователей, не подвержена атакам вирусами. "Если пользователь от своего надежного отправителя загружает список подписчиков на свой компьютер, а эта база уже заражена Троянами или вирусами, вылавливающими на вашем жестком диске электронные адреса, чтоб затем рассылать по ним спам. Если это все же случилось, ждите неприятностей", - говорит Дженнингз.

5. Не обновлять базы данных и списки адресов.

Не достаточно всего лишь держать закрытыми базы данных на компьютерах и серверах. Необходимо быть крайне аккуратным, используя и старые почтовые списки.

В устаревших почтовых базах данных может не еще не содержаться информации об уже отменивших рассылку пользователях, говорит Фубини. Необходимо проверить, насколько процедура отказа от рассылки на данный момент реальна - подтвердить ее, подписавшись самому, а потом отказаться. Эти проверки необходимы, если вы заботитесь о качестве своих сервисов".

В случае слияния компаний вам в руки попадают новые базы данных, но на самом деле их передача новому хозяину может оказаться очень неправильным шагом. Покупатель, возможно, уже отписался от всех рассылок, но во его адрес еще остался в одной старой базе данных. Реакция покупателя – вы не реагируете на мой запрос не отсылать мне новых писем, значит, вы спамер.

И если о вашей компании заявили в Spamcop или какую-то другую компанию по спам-контролю, последующие шаги не заставят себя ждать.

"Немедленно реагируйте на них, отписывая пользователей [которые этого просят] и обновляя свой список", - говорит Дженнингз. "Спрашивайте: как так вышло, что мы вдруг начали получать жалобы по поводу наших рассылок… Почему люди говорят, что это спам? Это передача лишних заданий полномочий другим? Что мы сделали не так?"

Размещать на своем сайте уязвимые почтовые формы.

Ли отмечает, что если вы по старинке используете на своем сайте один протокол передачи для управления спамом (нераспространенная уже сегодня практика т.к. сейчас именно бот-сети выбрасывают большую часть спама), тогда спамер старой школы сможет ваши формы использовать для своей рассылки. "На сегодня эти сервисы уже вышли из употребления, хотя иногда и используется небольшими компаниями, когда у них нет большого опыта соответствующей работы"

Не позволяйте вашей базе клиентских адресов быть доступной через сеть. Индустриальный шпионаж зачастую начинается рассылкой домену потенциальной жертвы огромного количества сообщений под разными именами, чтоб узнать, какой будет реакция компании . "Это делается для того, чтоб спамеру было понятнее, какие адреса существуют внутри организации и взял на прицел отдельные элементы".

"Разумно создать базу небольшого количества адресов, которые выходят за пределы организации. Это может помочь уменьшить поток входящего спама, так как именно эти адреса можно выделить для фильтрования".

Если ваши электронные адреса доступны в сети, спамеры могут использовать их для своих дел, что прикрепит и к вашей организации липкий спамерский ярлык. "Избежать этого по большому счету невозможно, но ограничить себя несколькими адресами вполне реально".

7. Работать с третьей стороной в переписке, которая не обладает чистой репутацией. Будьте бдительными к тем, кому доверяете свою почту: некоторые провайдеры не могут похвастаться безупречной репутацией, говорит Дженнингз. Они вполне вероятно станут рассылать ваши рассылке пользователям, которые в них не заинтересованы, и вас могут забанить по прокси, говорит он. Смотрите в оба, с кем имеете дело

Можно только тогда с уверенностью сказать, что вы выбрали надежный сервис, когда вы знаете, что эти компании руководствуются аналогичными принципами, что и вы – проверяют базу электронных адресов и поддерживают ее "чистоту". "К сожалению, даже законные компании, у которых нет планов заниматься спамом, были замечены в том, что привлекали к своим рекламным компаниям более чем сомнительные фирмы".

Как обезопасить себя? "Если все вас устраивает и кажется идеальным, спросите у них, откуда они берут свои почтовые списки, а также попросите взглянуть на страницу отказа от рассылки"