Осторожно, СПАМ!

Выполнила: студентка
Ф-та информатики, 53 гр.
Григорьева Ольга

Что такое Спам?

Что можно приравнять к Спаму?

- Массовая рассылка почтовых сообщений пользователям, не выразившим желание получать подобную корреспонденцию, причем нет разницы, коммерческая ли это реклама или просто полезная по мнению отправителя информация.
- Индивидуальные сообщения, тематика которых не имеет к адресату прямого отношения.
- Подписка человека на список рассылки без его ведома или желания.
- Помещение в конференцию, USNET, дискуссионный лист, гостевую книгу сообщений, не имеющих отношения к заданной тематике (off-topic) или сообщений являющих собой прямую рекламу (если это не разрешено установленными там правилами).

Лучше не использовать ни одно действие из пяти приведенных Выше пунктов в качестве инструментов интернет-маркетинга, так как:

- это нарушает сетевую этику;
- это может вызвать шквал негативной критики, почтовые бомбы в Ваш адрес, жалобы Вашему провайдеру с требованием закрытия Вашего аккаунта и т.д. ;
- Вы заработаете плохую репутацию;
- Ваш адрес попадет в черный список провайдеров и потом даже обычное Ваше письмо может не дойти до адресата;
- и, наконец, подобная реклама обладает низкой эффективностью, а часто просто наносит вред рекламодателю. Давно установлено, что негативная реакция на рекламу с легкостью может перейти и непосредственно на рекламируемый продукт.

Если Вам самим докучает назойливый спам (как правило, это совершенно не нужные Вам коммерческие пирамиды", реклама порносайтов и прочий хлам), несколько советов о том, как с ним бороться:

1. Спаммеры, как правило, собирают e-mail адреса с помощью специального робота или вручную (достаточно редко) из следующих мест:
- веб-страницы;
- конференции Usenet;
- списки рассылок;
- электронные доски объявлений;
- гостевые книги;
- чаты.

Собранные таким образом адреса либо непосредственно используются самими собирателями, либо продаются третьей стороне. Любая Ваша активность в сети рано или поздно приведет к тому, что вы станете очередной жертвой спаммеров.

2. Первую линию обороны, как правило, держит Ваш провайдер. Существуют "black lists" куда провайдеры заносят спаммеров, их сообщения уничтожаются автоматически до поступления в Ваш почтовый ящик на сервере.
3. Существует целый ряд программ позволяющих выявлять и автоматически удалять подобные сообщения, список некоторых из них Вы можете изучить по адресу: http://www.chat.ru/~admirall/article/SPAM/antispamprag.htm
4. Вы можете настроить непосредственно Ваш почтовый клиент, например, Outlook Express для уничтожения сообщений с заданным адресом отправителя или полем subj.
5. Вы можете написать письмо с жалобой провайдеру спаммера. Если Вы, например получите Спам от spammer@aha.ru, направьте жалобу на postmaster@aha.ru. Виновного в рассылке спама могут серьезно предупредить, либо вообще закрыть его аккаунт. Это не всегда срабатывает, т.к. искушенные спаммеры пытаются замаскировать свой почтовый адрес. Есть программа Spam Hater, позволяющая определить настоящего автора письма и связаться с его провайдером

Автоматизированные антиспам-системы.

Некоторое время назад существовало всего несколько систем предотвращения рассылок не запрошенных писем - спама. Системы эти работали очень стабильно, и каждая из них имела четкую направленность. Можно сказать, что все было "стройно", понятно и любой администратор почтового сервера знал, что если он хочет добиться вот этого, он должен использовать такую-то систему, а если вот этого - такую-то. Де-факто, существовал некий стандарт и все пользовались довольно стабильными системами, от которых известно было чего ждать. Стоит отметить три из них:

- **MAPS RBL - Realtime Blackhole List.**
- **MAPS DUL - Dial-up User List.**
- **ORBS - Open Relay Behaviour-Modification System.**

MAPS RBL - Realtime Blackhole List

Эта система была создана компанией MAPS (Mail Abuse Prevention System LLC), которая принадлежит ветерану интернета Полу Викси (Paul Vixie). Он известен как автор многих интернет-стандартов, со-автор сервера имен bind (named) и многим другим. Система предназначена для фильтрации по ее базе данных IP адресов, которые активно используются для рассылки спама и администраторы, ответственные за поддержку этих IP адресов или целых сетей, не принимают мер, не смотря на жалобы пострадавших от спама. Видимо, изначально система создавалась на голом энтузиазме, но на каком-то этапе было принято решение о ее коммерциализации. Доступ к информации из базы данных RBL стал ограничен и возможен только за плату. Как следствие - RBL перестало использовать очень большое число администраторов почтовых серверов и есть даже реплики о том, что коммерциализация явилась началом конца RBL. Необходимо признать - это была самая лучшая система, которая не позволяла вносить в свою базу данных хосты, которые могли быть настроены их администраторами, и острой необходимости именно в фильтрации этих хостов по всему миру объективно не было. Попасть в RBL можно было только за злостное игнорирование жалоб пользователей интернет на рассылаемый через конкретную систему спам.

MAPS DUL - Dial-up User List

Еще одна антиспамерская система компании MAPS. Основной ее целью была борьба со спамом, который рассылался с dilaup-сетей интернет-провайдеров напрямую без использования промежуточных почтовых серверов прямо по MX-записям для целевых доменов. В первую очередь система предназначена для помещения в ее базу данных информации о тех IP-сетях провайдеров, которые используются для выделения из них IP адресов для пользователей, осуществляющих сеансовые подключения к интернет. То есть, для так называемых dialup-пользователей. Как правило, обычный пользователь, позвонивший своему провайдеру обычным модемом, отправляет почту через соответствующий SMTP-сервер своего провайдера, что является правильным. Однако, существуют люди, которые рассылают спам именно используя такие dialup-подключения, а также есть специальные программы, которые берут заранее подготовленный список email-адресов для рассылки и отправляют почту как правило не через сервер провайдера, а напрямую на сервера, которые ответственны за обработку почты для получателей писем. То есть, в данном случае, спама. Система DUL позволяла не принимать почту от таких пользователей. Конечно, бывают случаи отправки и не только спамерских писем описанным выше образом, но их мало и отправитель получал сообщение об ошибке, в котором давались рекомендации о том, как настроить свою почтовую программу так, чтобы почта все-таки могла отправляться. Система DUL тоже стала коммерческой и доступ к ней теперь платный. Это не позволяет использовать ее всем желающим. Попасть в DUL можно было двумя путями - сам провайдер мог внести туда свои dialup-сети или они могли туда попасть превентивно из-за имевшего место спама с dialup конкретного провайдера. Во втором случае можно было написать в MAPS и попросить удалить свою сеть из DUL если ее присутствие в базе данных казалось провайдеру нежелательным.

ORBS - Open Relay Behaviour-Modification System

В эту систему попадали так называемые "открытые релеи" (open relays) - почтовые серверы, которые позволяют посторонним лицам (спамерам) пересылать через себя почту от кого угодно в адрес кого угодно. То есть, сервера, которые использовались или могли быть использованы для рассылок незапрошенной рекламы. На веб-сервере системы ORBS существовала специальная форма, воспользовавшись которой любой желающий мог "попросить" специального робота проверить любой IP адрес на предмет наличия на нем открытого релея. Попасть в эту базу данных было очень просто, так как система не предусматривала процедуры, предшествующей попаданию в базу в отличие от RBL, например. ORBS могла проверять почтовые серверы и на так называемый multi-stage open relay. Например, если у клиента некоего провайдера был неправильно настроенный почтовый сервер, который пересылал любую почту и спам, в том числе на сервер провайдера, который занимался доставкой такой корреспонденции далее, то в базу данных попадали оба почтовых сервера - пользовательский и провайдерский. Все бы ничего, но в подавляющем большинстве случаев ни пользователь, ни провайдер не получали никаких уведомлений о факте внесения в базу данных по спамерам. Итог - другие пользователи провайдера не могли нормально получать и отправлять почту, так как сервер провайдера находился в базе данных ORBS, и некоторое количество почтовых систем в мире отказывались с ним работать. К сожалению, администраторы почтовых серверов, которые устанавливали у себя поддержку ORBS, не особо разбирались в том, что это такое. "Раз это антиспам-система", - думали они, "мы будем ее использовать, хуже не будет". А было как раз хуже, так как их почтовые сервера переставали принимать вполне нормальную почту, совсем не спам.

В заключение хочется пожелать тем, кто не любит спам и пытается бороться с этой чумой Интернета, относиться к выбору средств защиты более продуманно и не использовать системы, методы работы которых можно называть не иначе как варварскими. Не всегда виноватый в пересылке спама является злоумышленником, который спит и видит, как сделать Вам хуже. В большинстве случаев как раз наоборот. Не нужно рубить с плеча. Постарайтесь быть более человечными и не уподобляться тем, кто готов не оставить камня на камне ради мира во всем мире

Используемые источники

- http://www.rumail.us/
- http://www.rumail.us/history.htm
- http://www.rumail.us/antispam.htm