**Спам. Что это такое простыми словами?**

Хотя это не называлось спамом до начала 1990–х годов - сам термин происходит от ныне легендарного эскиза Монти Пайтона 1970 года "Летающий цирк". Действие происходит в небольшом кафе, где толпа (довольно раздражающих) викингов заглушает остальную часть разговора, распевая все громче и громче припевы “СПАМ, СПАМ, СПАМ...”, несколько менее популярного консервированного мяса.

Оглядываясь назад, неудивительно, что слово "спам" в конечном итоге будет принято для обозначения потока нежелательных коммерческих сообщений, которые часто воспринимаются как глушители нормальных коммуникаций.

**История.**

Самые первые нежелательные электронные сообщения были переданы по телеграфу еще в 1864 году. Эти сообщения были довольно сомнительными инвестиционными предложениями от богатых американцев.

Первый спам по электронной почте был отправлен человеком по имени Гэри Терк 3 мая 1978 года. Туерк, который в то время работал в Digital Computer Corp., отправил электронное письмо с предложением провести день открытых дверей, чтобы продемонстрировать новый компьютер VAX компании. Он был разослан примерно 400 из 2600 человек, у которых были учетные записи электронной почты в ARPANET (военная компьютерная сеть, предшествовавшая Интернету).

Туэрк утверждал, что его электронная почта принесла около 12 миллионов долларов новых продаж. Однако многие люди, получившие его электронное письмо, были сильно раздражены и пожаловались в Министерство обороны США, которое управляло ARPANET.

1993 год.

Термин “спам” действительно войдет в обиход только в 1993 году. Он был применен к публикации в сети. USENET была группой новостей, предшественницей Интернета, которая была (и остается) всемирной распределенной дискуссионной системой. Ее, в основном, можно рассматривать как гибрид электронной почты и веб-форумов.

В попытке внедрить систему модерации, которая позволяла удалять сообщения после их публикации, Ричард Депью случайно допустил ошибку. Из-за нее было опубликовано более 200 сообщений в дискуссионной группе news.admin.policy.

Позже, когда члены группы шутили по поводу инцидента, кто-то назвал его “рассылкой спама”. Так и была написана история.

**Что такое спам сейчас?**

Спам определяется как нерелевантные или нежелательные сообщения, отправляемые большому числу пользователей Интернета. Чаще всего отправителем является ботнет, который представляет собой сеть компьютеров (ботов или спам-ботов), зараженных вредоносными программами и контролируемых одной атакующей стороной (бот-пастухом).

**Где его можно встретить?**

Спам был проблемой во многих различных средствах массовой информации и неизменно возникает всякий раз, когда средство позволяет людям отправлять много сообщений без взимания платы за них.

В Интернете спам затронул электронную почту, мобильные сообщения, комментарии в блогах, а также социальные сети и мессенджеры, включая инстаграм, ватсап, телеграм и гугл. Он также появился в виде нежелательных факсов, VoIP-телефонии, Apple iMessage и СМС (текстовые сообщения на телефон).

**Для чего им занимаются?**

Спам - это хороший инструмент для мгновенного продвижения продукта или услуги тысячам интернет пользователей. Это самый дешевый способ коммерческого маркетинга.

К наиболее популярным темам относятся:

1. фармацевтические препараты
2. контент для взрослых
3. финансовые услуги
4. онлайн-дипломыме
5. работа на дому
6. онлайн-азартные игры
7. криптовалюты

Спамеры делают ложные заявления и обманывают получателей, заставляя их верить в то, что не соответствует в действительности.

Спам также используется для распространения нелегальной рекламы и отправки вредоносных файлов.

Кроме этого существует и такой вид спама как фишинг. Он часто выдает себя за рассылку от банков, интернет провайдеров или почтовых провайдеров, предлагая жертвам подтвердить или обновить свои учетные записи. Ссылки в фишинге ведут на веб-сайт, похожий на страницу входа в реальную организацию, поэтому жертва вводит свои учетные данные, которые затем отправляются фишеру.

**Почему он вреден?**

Около 90% электронной почты занимают спам сообщения. Это приводит к потере пропускной способности, влияет на производительность сервера и потребляет много места на жестком диске.

Они влияют на производительность труда сотрудников, поскольку побуждает их постоянно проверять почтовый ящик.

Спам-письма могут быть опасными, потому что открытие, переход по любым ссылкам или загрузка вложений могут заразить устройство вирусами.

**Основные виды.**

Ниже приведены некоторые из наиболее распространенных видов спама, используемых в настоящее время.

1. **Email spam.**

По-прежнему одним из наиболее распространенных видов спама является нежелательная массовая электронная почта (UBE) или нежелательная коммерческая электронная почта (UCE).

1. **Маскировка.**

Этот тип спама обычно используется для повышения рейтинга веб-сайта. Он вводит поисковые системы в заблуждение, заставляя их думать, что контент более релевантен для поиска, чем есть на самом деле.

1. **Скрытый текст.**

Скрытый текст часто помещается за изображениями, тем самым становясь вне поля зрения посетителей. Эти виды спама легко обнаруживаются провайдерами. Однако, не следует путать его с поисковой оптимизацией или SEO.

1. **Взломанные веб-сайты и вредоносные программы.**

Часто спам возникает, когда веб-сайты взламываются третьими лицами с целью показа рекламных ссылок или контента. Вредоносное программное обеспечение, или "вредоносное ПО", - это форма нарушения работы компьютера, выполняемая хакерами для сбора личной информации или получения доступа к ней. Этот тип рассылки создает угрозы, которые могут нанести вред компьютерам пользователей и их данным, делая их уязвимыми для вирусов.

1. **Неестественные ссылки на сайт или с сайта.**

Это обманчивые ссылки, которые перенаправляют пользователя на другую ссылку.

1. **Телефонный спам.**

Что такое спам в телефоне? В него входят спам-звонки и сообщения на смартфон. Нежелательные сообщения могут приходить, как и в качестве оповещений в социальных сетях (instagram, whatsapp, telegram), так и обычных смс.

А что такое спам звонок на мобильный телефон? Это тип спама, который происходит, когда человек или компания звонит большому количеству людей одновременно.

**Email спам.**

Обычный пользователь электронной почты может получать пару спам-писем в день, и это, как правило, неизбежно. Но если ты получаешь значительно больше, чем несколько нежелательных рекламных писем в день, на это есть причина.

**Причина номер один:**

В 95% случаев ты предоставил свой адрес электронной почты кому-то, кто связался напрямую или продал твою информацию другой стороне (или и то, и другое).

Вот некоторые ситуации, в которых ты, возможно, указал свой адрес электронной почты:

**1.Подписка на бесплатные продукты.** Ничто никогда не бывает полностью бесплатно, без каких-либо условий. Эти компании зарабатывают деньги, используя (или продавая) твою контактную информацию в рекламных целях.

**2.Попытка загрузить программы без дополнительной платы.**

**3.Всплывающие окна “Вы выиграли!”.** Как бы нам всем ни хотелось, чтобы любое из этих уведомлений о победителях призов или розыгрышей было правдой, суровая реальность такова, что они на 100% ложны.

**4. Создание учетной записи на веб–сайте.** Почти все веб-сайты в настоящее время требуют, чтобы ты зарегистрировал учетную запись, чтобы ими пользоваться.

**5. Покупка товара у онлайн–компании.** Покупка у любой компании, занимающейся онлайн-заказами или заказами по почте, обычно предполагает предоставление адреса электронной почты, даже если тебе не требуется создавать учетную запись.

В то время как намеренная выдача адреса электронной почты, безусловно, является наиболее распространенным способом запуска спам-сообщений, поступающих в почтовый ящик, есть несколько других, которые не так хорошо контролируемы:

1. **Продажа списков рассылки.** Все предыдущие способы несут в себе один дополнительный риск. Если какая-либо из этих компаний не пользуется достаточной репутацией, они могут фактически заниматься (в первую очередь или во вторую очередь) продажей твоей контактной информации. После того, как информация была продана, восстановить твою конфиденциальность практически невозможно.
2. **Скомпрометированные базы данных электронной почты.** Возможно, ты читал новости компаний, которые стали целями (и жертвами) хакеров. Эти кибер-злоумышленники получают доступ к частным базам данных компаний, содержащим контактную информацию клиентов. Это досадный риск, о котором мы все должны знать при использовании Интернета. Проявлять осторожность в отношении того, с какими компаниями ты делишься своим адресом электронной почты, - лучший способ снизить риск. Если ты хочешь узнать, был ли раскрыт твой адрес электронной почты, сайт haveibeenpnwned.com это отличное место для проверки. Если тебя скомпрометировали, рекомендуется сменить пароли, особенно если ты используешь один и тот же пароль на нескольких веб—сайтах (не рекомендуем).

**Цели.**

Спам по электронной почте приходит во многих формах, в зависимости от цели спамера, включая следующие:

1. **Маркетинговые сообщения.** Этот тип спама распространяет нежелательные или незаконные товары, или услуги.
2. **Сообщения о вредоносных программах.** Некоторые спам-письма содержат вредоносные программы, которые могут обманом заставить пользователей разглашать личную информацию, платить деньги или предпринимать какие-либо действия, которые они обычно не совершают.
3. **Мошенничества и аферы.** Афера с авансовым взносом - хорошо известный пример мошенничества по электронной почте. Пользователь получает электронное письмо с предложением, которое якобы приводит к вознаграждению, если он внесет предоплату или небольшой депозит. Как только они произведут платеж, мошенник придумает дополнительные сборы или просто перестанет отвечать.
4. **Предупреждения антивируса**. Эти сообщения "предупреждают" пользователя о вирусе и предлагают "решение" для его устранения. Если пользователь клюнет на приманку и нажмет на ссылку в электронном письме, хакер может получить доступ к его данным. Электронное письмо также может загрузить вредоносный файл на устройство.
5. **Победители лотереи.** Спамеры рассылают электронные сообщения, утверждая, что получатель выиграл лотерею или приз. Чтобы получить приз, получатель должен нажать на ссылку. Она используется для кражи личной информации пользователя.

**Как бороться?**

Фильтры нежелательной почты, которые могут быть частью системы безопасности или надстройки системы электронной почты, могут улавливать нежелательные сообщения и помещать их в папку "Спам", а не в "Входящие". Однако полностью избавиться от спама невозможно.

Тем не менее, пользователи могут снизить свою уязвимость к спаму с помощью следующих способов:

1. Сообщать, блокировать и удалять любые подозрительные сообщения.
2. Добавление стороннего фильтра защиты от спама.
3. Настройка фильтра для блокировки сообщений, содержащих определенные слова или фразы.
4. Создание списка разрешенных адресов электронной почты с IP-адресами или доменами, которым пользователь доверяет.
5. Использование одноразовой учетной записи или скрытого адреса почты на форумах или в социальных сетях.
6. Не переходить по ссылкам и не открывать вложения от неизвестных отправителей.
7. Никогда не отвечай на эти сообщения. Если электронное письмо является "спамом", оно, как правило, приходит с учетных записей "без ответа" (которые не могут получать сообщения), и, если это "фишинг", вы подтверждаете, что информация, которую они получили незаконно, верна, и они могут продолжать ее использовать.

**Как предотвратить попадание моих рассылок в спам?**

Отправители могут избежать ошибочного определения их электронных писем как спама, выполнив следующие действия:

1. Поддерживать свою репутацию.
2. Использовать инструменты аутентификации.
3. Удалять слова, которые могут быть помечены фильтрами защиты и привести к тому, что электронное письмо отправиться в папку “спам”;
4. Создать релевантный, приятный для пользователя контент.
5. Просить пользователей зарегистрироваться, чтобы убедиться, что они вовлечены. Так, они с меньшей вероятностью отметят электронное письмо как спам;
6. Использовать надежную службу массовой рассылки электронной почты.