

Согласно информации, содержащейся в различных базах данных, открытых для общего доступа, IP-адрес [insert number] может быть открытым почтовым сервером-ретранслятором или открытым прокси-сервером. Насколько мы понимаем, данный IP-адрес используется вашим сервером. В этом сообщении содержится важная информация, которая может повлиять на работу вашей компании в Интернете.

Данное сообщение было направлено вам в рамках программы «Операция: Защитите свой сервер», которая является совместным проектом Федеральной торговой комиссии США и других правительственных организаций по всему миру, обеспокоенных проблемами, связанными с распространением незапрашиваемой электронной почты рекламного характера (спама). Мы предлагаем вам узнать о том, как можно защитить свои серверы и не стать невольным источником спама. В качестве первого шага мы рекомендуем вам закрыть ваш открытый сервер-ретранслятор или открытый прокси-сервер.

Открытые серверы-ретрансляторы или открытые прокси-серверы представляют собой серверы, которые позволяют любому компьютеру в любой точке мира перенаправлять через них электронную почту на другие почтовые адреса в Интернете. Открытые серверы-ретрансляторы или открытые прокси-серверы часто используются лицами, которые наводняют Интернет спамом. Такое неправомерное использование сети создает проблемы для пользователей во всем мире, а также для органов охраны правопорядка и для вашей организации. Например, получатели могут решить, что источником спама является ваша система; неизвестные третьи лица могут использовать ваши серверы и ресурсы Интернет; ваши сетевые соединения могут оказаться перегруженными потоками данных; ваши административные издержки могут возрасти; а также ваш поставщик услуг Интернет может отключить ваш доступ к сети Интернет. Обеспечение безопасности вашего сервера поможет защитить вашу систему от ненадлежащего использования.

Мы предлагаем дополнительную информацию об открытых серверах-ретрансляторах или открытых прокси-серверах, а также о способах защиты вашей организации от рисков, связанных с такими незащищенными серверами, в том числе пошаговые инструкции по их закрытию. Перейдите по ссылке www.ftc.gov/secureyourserver, чтобы посетить специальную веб-страницу, на которой приводится список организаций, участвующих в данном проекте. Чтобы перейти непосредственно к инструкциям по закрытию вашего открытого сервера-ретранслятора или открытого прокси-сервера, нажмите на ссылку www.ftc.gov/bcp/online/pubs/buspubs/secureyourserver.htm.

Если у вас возникнут вопросы, касающиеся инструкций или этого письма, пожалуйста, напишите по адресу secureyourserver@ftc.gov.