많은 공공 데이터베이스의 운용경험을 보면 IP 주소(Insert Number)가 오픈릴레이 메일서버(또는 오픈 프록시 서버)로 이용될 수 있다는 점을 시사하고 있습니다. 우리는 귀 기관이 IP 주소를 사용하는 서버를 운용하고 있는 것으로 알고 있습니다. 본 메일에는 귀 기관의 온라인 활동에 영향을 미칠 수 있는 중요 정보를 포함하고 있습니다.

본 e-메일은 원치 않는 광고성 e-메일 확산을 방지하기 위해 미국 FTC 와 전세계 정부기관이 합동으로 참여하고 있는 "서버안전조치" (Operation Secure Your Server)프로젝트의 일환으로 보냅니다. 우리는 당신이 귀 기관의 서버를 안전하게 유지하여 귀 기관의 서버가 스팸에 악용되는 것을 방지하는 방법을 배우기를 원합니다. 먼저 우리는 귀하의 오픈 릴레이 서버 (또는 오픈 프록시 서버) 기능을 폐쇄할 것을 제안합니다.

오픈 릴레이(또는 오픈 프록시) 서버는 e-메일이 발송자로부터 최종 수신자에게 연결되는 과정에서 경로를 제공해 주는 역할을 하는 서버를 말합니다. 이러한 오픈 릴레이(또는 오픈 프록시)서버는 흔히 불법 스팸 메일 사업자가 대량의 스팸메일을 발송하는데 이용됩니다. 이러한 남용 행위는 전세계 소비자뿐만 아니라 법집행기관 및 귀 기관에도 많은 문제를 일으킵니다. 예컨대, 스팸을 받는 사람들은 귀 기관이 스팸 메일을 발송한 것으로 생각할 수 있습니다. 익명의 제 3 자가 귀하의 허락 없이 귀 기관의 서버와 인터넷 서비스를 이용할 수도 있습니다. 서버의 대량 스팸 전송으로 인해 귀 기관의 네트워크 접속에 장애가 발생할 수 있으며, 서버 운용비용이 늘어날 수 있습니다. 최악의 경우 인터넷서비스공급자(ISP)가 귀하의 인터넷 서비스를 중단시킬 수도 있습니다. 귀 기관의 서버를 안전하게 조정함으로써 귀 기관의 정보시스템이 스팸 메일에 악용되는 것을 방지할 수 있습니다.

우리는 오픈 릴레이(또는 오픈 프록시)와 관련된 추가적인 정보, 안전이 확보되지 않은 다른 서버로부터 피해를 당하지 않도록 하는 방법, 그리고 안전이 확보되지 않은 다른 서버와의 연결을 차단하는 방법 등을 제공하고 있습니다.

미국 FTC 의 관련 웹 페이지 및 이 프로젝트에 협력하는 각국 정부기관을 보시려면 www.ftc.gov/secureyourserver 를 클릭하십시오.
귀 기관의 오픈 릴레이 (오픈프록시)서버 기능을 폐쇄하는 방법은 www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.htm 을 클릭 하시기 바랍니다.
기타 문의사항은 secureyourserver@ftc.gov 로 연락하시기 바랍니다.

이 메세지는 “서버안전조치” 프로젝트에 참여하는 대한민국 공정거래위원회로 부터 당신에게 보내지는 것입니다.