

Good Net Neighbor Service Participation Form

In an effort to proactively reduce the number of security incidents caused by viruses and scanning, MOREnet will offer a Good Net Neighbor Service to MOREnet customers. This is a low-risk, volunteer-based, no-cost service.

Level One of the Good Net Neighbor Service will implement access control lists to block Windows Networking ports (TCP/UDP ports 135, 137, 138, 139 and 445). These ports are sometimes used by worms and viruses to scan, discover and infect other computers through the Internet.

NOTE: Customers should be aware that this service is not a substitute for patching/updating machines or using anti-virus protection.

Blocking these ports may affect:

- Access to Microsoft Exchange servers over the Internet using MS Outlook (blocking these ports will not affect using MS Outlook over the local area network).
- File/print sharing over the Internet.
- Other programs or applications that are configured to use ports 135, 137, 138, 139 or 445 to communicate over the Internet.

See the following links for more information on ports used by Windows servers and services.

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;832017>
- http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/cnet/cnfc_por_SIMW.asp
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;150543>

If you would like to participate in this service, and you understand the potential risks that are involved in blocking these ports, please complete and return this permission form by fax (573) 884-7699 or by mail to MOREnet Security Operations, 3212 LeMone Industrial Blvd., Columbia, MO 65201. Once MOREnet Security Operations receives your completed permission form, configuration changes will be completed and you will be contacted to verify that you have not experienced any unforeseen network problems.

If you have questions, contact MOREnet Security by phone at (800) 509-6673 or by e-mail at security@more.net.

Customer Information

Organization: _____ Phone Number: _____

Address: _____

I understand the potential risks involved in blocking TCP/UDP ports 135, 137, 138, 139 and 445.

Security Contact Signature: _____

Lead Network Technician Signature: _____