

Yes! I would like to volunteer at *Highland Fest 2007!*

July 20 – 22

Welcome!

We really appreciate your desire to help the *Highland Business Association* serve our community by volunteering during Highland Fest. To help us as we fill in the three day schedule, please complete the following questionnaire:

Personal Information

Please Print Clearly!

Volunteer Name: _____

Company Name: _____

Address: _____

City: _____

State: _____ Zip Code: _____

E-mail: _____

Home Phone: _____

Work Phone: _____

Mobile Phone: _____

Please indicate the best number to use when contacting you.

Schedule Information: Festival Hours

Friday

2:00 pm – 11:00 pm

Saturday

10:00 am – 11:00 pm

Sunday

11:00 am – 5:00 pm

Friday

Saturday

Sunday

Check In & Set Up
8:45 am – 2:00 pm

First Shift
9:45 am – 2:00 pm

First Shift
10:45 am – 2:00 pm

First Shift
1:45 pm – 6:00 pm

Second Shift
1:45 am – 6:00 pm

Second Shift
1:45 pm – 5:00 pm

Night Shift
5:45 pm – 10:00 pm

Night Shift
5:45 pm – 10:00 pm

Street Closing
4:45 pm – 7:00 pm

Please indicate which shift(s) you are available to volunteer.

**FAX THIS BACK to 651-699-0245, or MAIL to
HBA, 790 Cleveland Ave. S., Suite 219, St. Paul, MN 55116.
Call Brian Haws at 651-336-0248 with questions!**

Ten Steps to a Secure Small Business Network, by *Brian Haws, Highland Support*

It's not as complicated as it may seem. Don't wait for lightning to strike.

1. Awareness.

Perhaps one of the most important ingredients of a secure network is awareness. Familiarize yourself with various security threats.

2. Security Policy.

A security policy should consist of various rules and behaviors, such as a password policy requiring users to have passwords that cannot be easily guessed or broken and firewall rules permitting specific traffic in and out of the network. It should also include scheduled virus and spyware scans, scheduled backups and applying automated updates to all computers.

The following three resources are a must for any single computer or network connected to the Internet.

3. Firewall

A firewall acts as the security guard between your network and the Internet. Software firewalls that are installed directly on the computer are required in cases where the machine leaves the office, or where it is the only computer in the business. Hardware firewalls installed on firewall-dedicated machines are required in networks comprised of a number of computers. Firewalls differ from one another: some provide in-depth firewall protection and additional security services, while others offer only very basic protection. The main purpose of a firewall is to keep out unwanted traffic, such as a computer worm attempting to infect computers. Note that some firewalls can also be used to block specified outgoing traffic, such as file sharing programs, and to block specified incoming traffic. Many hardware firewalls offer additional services such as email antivirus and antispam filtering, content filtering, and secure wireless connection.

4. Antivirus.

Antivirus (AV) software is used to scan and protect files on the computer on which it is installed, files that are downloaded to the computer, and of course email. It is crucial to keep the antivirus software updated at all times, as new viruses are found almost everyday. Do not forget that simply having the software is not enough. Always schedule an automatic scan that runs either daily or weekly.

5. Patches and Updates.

Microsoft and other software vendors provide updates that are meant to fix bugs and patch potential security holes in their software. Make sure you regularly check for updates. You can even decide on a specific day (once a week is usually enough). The recommended way to check for updates is to let the Operating System (Windows XP for example) automatically check for itself. Microsoft generally releases important updates Tuesday nights, which would be a good time to schedule the updates.

6. Backup.

Always backup information. The more important the information is, the more copies of it you should have available. Make sure not to leave it lying around or misplace it. Create a backup policy to back the data up regularly. If possible, encrypt sensitive information and always keep a copy of the files in a safe location off site. It is also recommended to back up firewall, email, and Internet configuration settings to enable quick access to these settings in case of a failure.

7. ISP and/or Gateway Failover.

For businesses that are dependent on Internet connectivity, it is crucial to have a backup Internet connection and a backup firewall/gateway to preserve connectivity and production in the event that your primary Internet connection goes offline or the main firewall/gateway malfunctions. Several firewall gateways offer smooth and automated failover and ISP backup options. If temporary connectivity loss means potential business interruption, you can configure a failover Internet connection.

8. Antispam and Antispyware.

Spam filtering can be implemented on the mail server, on the firewall/gateway, or on the machine receiving the messages. Most antispam software uses various filters and blacklists to attempt to eliminate spam without deleting legitimate emails. In small networks with few mailboxes, you may consider locally set antispam software, but in larger networks with more users, you may want to use spam scanning on the firewall/gateway.

9. Blocking Specific Sites, IM Clients, and File Sharing Programs.

The best way to deal with questionable sites online, IM conversations during work hours, and bandwidth-wasting file sharing is to enforce their exclusion on the gateway. Some firewalls allow you to select specific services to which access should be blocked and to filter Web sites by address and/or by category.

Improving Productivity Safely

10. Remote Access VPN and Site-to-Site VPN.

Virtual private network (VPN) technology allows you to connect two or more remote networks in a private connection, creating a tunnel of encrypted data between the two points providing privacy and encryption for the data as it is transferred over the Internet. This is especially useful if you have two or more branches in your business or would like to access your office network remotely. For example, your sales representative does not have to carry confidential information on his laptop when visiting abroad. All he has to do is connect to the Internet and access the data in the office through a secure connection. There are numerous options that offer VPN server and connection support.