The Fulcrum Group, Inc.
(817) 337-0300

Antivirus Tips For Small Businesses

This White Paper is brought to you by your friends at The Fulcrum Group, Inc.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Phone: 817.337.0300 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

How sure are you that your business systems can stand up to malware and viruses?

Our January newsletter (go to ***http://www.fulcrum.pro/newsletter/january-2016-newsletter-2/#6*** *) featured some basic tips for ensuring your business computer network antivirus program is on-point.*

This month's white paper provides ***solid tips and discussion points you'll want to talk about with your network provider*** *to safeguard your organization against today's tireless threat environment.*

Tip #1 - Always choose a centrally managed antivirus solution.

At The Fulcrum Group, the antivirus solutions we design and implement take into consideration your business size, usage, and other network needs.

- Symantec Endpoint Protection Cloud - Recommended for small businesses under 25 users, businesses without a server, or larger businesses with a distributed workforce (lots of remote workers)
- Symantec Endpoint Protection Small Business Edition - Recommended for medium-sized businesses with 25 or more users and at least 1 Windows server
- Symantec Endpoint Protection Enterprise Edition - Recommended for larger-sized businesses with more advanced and granular security needs

Tip #2 - Make sure your initial setup includes configuring exclusions for major network applications, line of business applications, as well as setting up logging and notifications.

Major network applications such as Exchange, SQL, IIS, and SharePoint have recommended antivirus exclusions that should be configured. Contact your line of business application software vendors for their recommendations on antivirus exclusions.

Be sure that antivirus logging and notifications are configured so that you can be notified should any of your computers are attacked by malware or viruses.

Tip #3 - Stay current on software versions, antivirus engines, and signature files.

Your antivirus software should automatically update signature files, but do remember that it may not automatically update software or engine versions. These may need to be completed manually on a regular basis.

Tip #4 - Review your computer inventory monthly to ensure all machines have antivirus software.

Check all PCs, laptops, and servers to make sure *active* antivirus and malware protection are in place. Just one computer without antivirus software can cause major malware infections on your network.

Tip #5 - Perform a full scan monthly on every computer on your network.

Light scans can be performed daily or even weekly, but a full scan is recommended at least monthly on all computers, including servers. These typically can be configured through the management console.

Tip #6 - If you have virtual servers on your network, make sure full scans are scheduled to run in non-overlapping schedule.

Having all VMs (ie., machines running VMware and Microsoft Hyper-V) on a virtual server host running a scheduled full scan can bring that virtual server host to its knees, and severely degrade network performance. Be sure to network scans are scheduled appropriately.

Tip #7 - Non-corporate owned computers should NOT be connected to the private network.

Employee devices and other personal devices accessing your network are very likely not to have active anti-virus enabled. Also, keep in mind the likelihood of these kinds of devices to lack patching and updates. All of these devices, along with non-corporate owned cell phones should be connected to a public network that IS NOT connected to the private LAN.

THE FULCRUM GROUP
One Technology Solution: Yours

Tip #8 - Don’t forget Windows patching and updates.

Many viruses and malware focus on attacking computers with missing Windows patches and updates. Use a Windows patching tool or service to ensure Windows updates are applied regularly.

Tip #9 - Tune your antivirus policies for any specific compliance needs.

If you need to comply with healthcare, financial, or other governmental compliance rules, additional tuning of antivirus policies may be required.

If you’d like to speak with any of our IT engineers or consultants further on this topic, or would be interested in a FREE IT Security Assessment, feel free to reach out to us by phone at 817.337.0300 or email – and visit our website at www.fulcrum.pro today to find out more about the solutions we recommend.

We always welcome the opportunity to speak with you – someone’s always here and glad to offer a word of advice!