

Anti-Virus Tips

Anti-Virus Tips for Business Owners and Email Administrators

As businesses continue to adopt Internet-based communication and productivity tools, spammers and virus authors will continue to compromise those systems. Businesses need to be prepared for attacks by enforcing Internet-usage policies, educating employees on the dangers of violating those policies, and aligning themselves with the right vendors and partners.

Businesses should be aware of measures that can be taken to prevent their networks from being compromised by computer viruses and other attacks. We recommend the following:

- Install a firewall and block incoming and outgoing traffic that is not needed for business use. We recommend only opening specific ports critical to everyday operations.
- Do not allow employees to use peer-to-peer (P2P) file sharing websites and applications such as Kazaa. Many of the recent viruses can be transmitted through the use of these applications.
- Warn employees about the detrimental affects of downloading applications and offensive content from the Internet. Many Internet users do not realize that downloading "neat" applications or pornographic materials from un-trusted sites can install .spy-ware. on their computer and compromise office networks.
- Warn employees about opening attachments from unknown persons. When an employee receives an attachment that they are not expecting they should always confirm with the sender that the attachment is legitimate before opening it.
- Make sure that your IT administrator or email service provider specifically blocks executable attachments in order to block malicious programs and increase the chances of blocking viruses during the early stages of an outbreak. The following executable file types should be blocked by your mail server:

<http://office.microsoft.com/assistance/2000/Out2ksecFAQ.aspx>

- Make sure that your IT administrator or email service provider is blocking dangerously formatted emails, such as emails that take advantage of Microsoft Outlook vulnerabilities to hidden attachments. To test if your mail server is capable of blocking these dangerous emails, visit:

<http://www.webmail.us/testvirus>

- Install virus-scanning software on your mail servers or ensure that your email service provider is offering virus protection.
- Create and execute a policy in which your virus scanning definitions are updated hourly on all mail and file servers and automatically receive and install new virus definitions as they are released from anti-virus software vendors.
- Install virus-scanning software at the desktop level. Schedule the software to automatically update the virus definitions daily. We have found that many employees do not update the software themselves. Also, many people often turn their scanners off and forget to turn them back on.
- Keep operating systems and other software applications up-to-date. Vulnerabilities are discovered in most software applications over time and virus authors will take advantage of these vulnerabilities.

If and when a virus is detected, we recommend taking the following course of action:

- As soon as you realize that a specific computer is infected, take that computer off your network so that fixes can be installed without the risk of further spread. An infected computer behind a firewall can infect other computers behind that same firewall.
- Once you discover what type of virus has infected the computer, check with your anti-virus provider to see if they have any related removal instructions or tools available for download. Avoid connecting to the Internet to download the patches. Instead, download them on a separate computer and copy the files via floppy disk or writable CD. If you must connect to the Internet to download the patches, do so from an isolated Internet connection, such as dial-up, to prevent infecting other computers on your network.
- If you do not know what type of virus has infected your computer, download an up-to-date copy of your virus scanning definitions and run a scan on your computer. Follow similar download precautions mentioned above.
- Depending on the level of damage performed by the virus, an entire operating

system reinstall may be needed.

Here are some of our thoughts moving forward:

- Viruses will continue to take advantage of vulnerabilities in software applications, specifically bugs in popular Internet applications such as Microsoft Outlook, Outlook Express, and Internet Explorer. Your mail server virus scanner must be able to detect viruses that take advantage of the email vulnerabilities found in Microsoft Outlook.
- Email viruses will be more widespread and costly over the next 12 months and will affect businesses to a great extent. This is because business users are becoming more reliant on email and the Internet for daily business purposes. As businesses rely more on the web, it will be more costly when computers become compromised. Additionally, as more businesses gain access to high-speed Internet connections, viruses have greater opportunity to spread.
- Virus authors, like spam authors, are also getting smarter and using better techniques to fool email users and to bypass virus-scanning devices. They are designing emails to look like legitimate emails, such as order confirmations or undeliverable mail, which entice the recipient to open infected emails.
- Viruses will continue to be built with efficient mass mailing mechanisms to help them spread rapidly. Bulk mailer worms like SoBig.F and MyDoom, can bring down email systems because the traffic is so immense. Both of these viruses were so widespread that many email service providers had to turn off virus warning notifications to their users, because that too was creating a drain on mail servers and filling up users' mailboxes.
- Viruses will continue to forge the "From" address used to send the infected email. A large number of incorrectly configured mail filters today respond to these viruses by sending a virus alert email to the forged From address. This effectively doubles the amount of traffic caused by the virus and clutters the mailboxes of innocent, non-infected people. Anti-virus vendors and mail server administrators will have to become responsible and permanently disable these virus alerts