

DUAL SCANNING VIRUS PROTECTION

Our virus scanning solution scans all inbound and outbound emails using a multi-stage, dual scanner process.

Stage 1: Restricted Attachments

First, emails are searched for dangerous types of file attachments. Dangerous files are those that contain executable code, which can be used by malicious persons to spread viruses or do harm to your computer. Restricted file types include, but are not limited to program files (.exe, .com), script modules and files (.bas, .vbs, .js), Internet links (.url, .ins), and shortcuts to files (.lnk, .pif). When an email is sent or received that contains a restricted file attachment, the email is rejected and the sender receives a “bounced” email notification informing them of the restriction.

Stage 2: Normalization

This stage searches for email formatting vulnerabilities that can be used by viruses to hide from virus scanners. If any vulnerability is found, our system corrects the formatting of the message so that it can be thoroughly scanned for viruses. This is called “normalizing” the message, and most notably this process protects against all known Microsoft Outlook security threats.

Stage 3: Decompression

Next, if the email contains any compressed attachments such as zip files, the compressed attachments are temporarily unzipped so that the contents can be scanned for viruses. Many of today’s viruses use compression as a way to sneak their way past virus scanners. This elevates that risk. If the attachment cannot be decompressed, such as the case with password protected zip files, the original file is scanned for virus signatures that occur in compressed attachments.

Stage 4: The Dual Virus Scan

After the above preprocessing is complete, two separate virus scanners are used to scan the email and all of its uncompressed attachments. Everything is scanned twice to ensure maximum protection against new virus threats. ClamAV (www.clamav.net) and F-Prot (www.f-prot.com) are the current scanners of choice, although our system was designed to be able to plug-in any virus scanner on the market, should the need to do so arise.

Both anti-virus vendors employ engineers around the clock who respond to new and emerging virus threats. Updated virus definitions are automatically pushed to our system directly from the vendors. This gives our customers protection from new viruses within minutes.

Virus Notifications

When a virus is detected, the email is quarantined within our network. Since all of today’s viruses forge the From address on their emails, our system does not automatically bounce a notification back to the forged sender. Doing so would create a nuisance by sending bogus virus alerts to innocent people, and we discourage other email providers from sending these alerts as well.

A virus notification is bounced back to the sender if a customer sends a virus while using webmail or SMTP Authentication. This is the only case where a notice is sent to the sender because it is the only case where the From address is guaranteed not to be a forgery.

Approximately 2% of all incoming email messages are viruses. With this volume, “virus blocked” notices can be as annoying as spam, and serve no purpose. Therefore our system does not send “virus blocked” notices to the intended recipient of a virus. Instead, our administrative control panel shows details regarding the number of viruses blocked.

Zero Added Points of Failure

Redundancy and failover support are built into every aspect of the email hosting system. Should any portion of the virus scanning process fail, safeguards are in place to ensure that the remaining stages execute and email traffic continues without interruption. Additionally, if either of the two virus scanners encounters an error, there are additional scanners that automatically step in to rescan the email.

Effectiveness

As of October 2005, over 100,000 virus-infected emails are blocked by our email hosting system each day. This number can spike to over 1 million during new virus outbreaks. The virus scanning system has been designed to handle these extreme spikes for extended periods of time with ease, without mail delivery delays, and without missing a single virus.