Virus Protection

Our virus protection scans all inbound and outbound emails using a multi-stage process. The process is broken down into the following four stages:

- **Stage 1: Restricted Attachments**
  Here, emails are scanned for dangerous types of file attachments. 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: Normalisation**
  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.

- **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.

- **Stage 4: Virus Scan**
  After the above pre-processing is complete, a virus scanner is used to scan the email and all of its uncompressed attachments. Everything is scanned to ensure maximum protection against new virus threats. ClamAV (www.clamav.net) is the current scanner 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.