**Email Bombing/Spamming**

**Description 1**

Email bombing is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message (such as vacation(1)) that is setup incorrectly. Email bombing/spamming may be combined with email spoofing (which alters the identity of the account sending the email), making it more difficult to determine who actually sent the email. [1] [2] [3]

**Note: all three references use the same description**

**Reference**

**[1]** [**https://www.cert.org/historical/tech\_tips/email\_bombing\_spamming.cfm**](https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm)**?**

**[2]** [**http://resources.sei.cmu.edu/asset\_files/WhitePaper/2002\_019\_001\_496605.pdf**](http://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_496605.pdf)

**[3]http://www.windowsecurity.com/whitepapers/misc/Email\_Bombing\_and\_Spamming\_.html**