CLAIMS

1. A method of detecting malicious electronic messages (100) transmitted from at least one message sending device (110, 120, 130) to at least one message receiving device (210, 220, 230), the method being carried out by a messaging server (1000) and comprising the steps of:
   a) generating, by the messaging server (1000), at least one signature for an electronic message (100) to be transmitted from the at least one message sending device (110, 120, 130) to the at least one message receiving device (210, 220, 230);
   b) storing, by the messaging server (1000), the generated at least one signature in a data storage unit (1050);
   c) determining, by the messaging server (1000), whether the electronic message (100) is malicious;
   d) if the electronic message (100) is determined to be malicious, determining, by the messaging server (1000), on the basis of the at least one signature generated for the determined malicious message, whether electronic messages (100) comparable to the determined malicious message (100) were classified as non-malicious and transmitted to the at least one message receiving device (210, 220, 230) in the past, wherein the determining step comprises comparing the at least one signature of the determined malicious message with signatures in the data storage unit (1050) which are associated with previously transmitted electronic messages (100); and
   e) if it is determined that electronic messages (100) comparable to the determined malicious message (100) were classified as non-malicious and transmitted to the at least one message receiving device (210, 220, 230) in the past, notifying, by the messaging server (1000), the at least one message receiving device (210, 220, 230) about a potential threat.

2. The method according to claim 1, wherein at least the steps (a) to (c) are repeated, by the messaging server (1000), for each new message to be transmitted from the at least

one message sending device (110, 120, 130) to the at least one message receiving device (210, 220, 230).

3. The method according to anyone of the preceding claims, wherein step (a) and step (b) further comprise: generating, by the messaging server (1000), a message identifier (ID) for the electronic message (100) and storing, by the messaging server (1000), the generated message ID together with the generated at least one signature in the data storage unit (1050).

4. The method according to anyone of the preceding claims, wherein step (a) further comprises: generating, by the messaging server (1000), for the electronic message (100) to be transmitted, specific message information suitable for classifying the transmitted message later on.

5. The method according to claim 4, wherein step (b) further comprises: storing, by the messaging server (1000), the generated specific message information together with the generated at least one signature in the data storage unit (1050).

6. The method according to claim 4 or 5, wherein the specific message information comprises at least one of the following information:
   - transmission time of the message;
   - message sender information;
   - message destination information; and
   - information about message attachments.

7. The method according to anyone of the preceding claims, wherein the signature is generated, by the messaging server (1000), on the basis of at least one of the following elements:
   - at least one message attachment property; and
   - URL information associated with the message sending device (110, 120, 130) which the message stems from.

8. The method according to anyone of the preceding claims, wherein the step (c) further comprises:
   - comparing, by the messaging server (1000), the electronic message (100) with known virus signatures; and
   - classifying, by the messaging server (1000), the electronic message (100) as malicious, if the message (100) sufficiently matches one of the known virus signatures.

9. The method according to anyone of the preceding claims, further comprising at least one of the following steps:
   - transmitting, by the messaging server (1000), the electronic message (100) to the at least one message receiving device (210, 220, 230), if the message (100) has been classified as non-malicious; and
   - blocking, by the messaging server (1000), the electronic message (100), if the message (100) has been classified as malicious.

10. The method according to anyone of the preceding claims, wherein step (e) further comprises: providing, by the messaging server (1000), information to the at least one message receiving device (110, 120, 130) which indicates that a specific message transmitted in the past may be malicious.

11. A computer program product with program code portions for carrying out the method according to at least one of the preceding claims 1-10, when the computer program product is executed on a computer device.

12. The computer program product according to claim 11, which is stored on a computer-readable recording medium.

13. A messaging server (1000) which is configured to transmit electronic messages (100) received from at least one message sending device (110, 120, 130) to at least one message receiving device (210, 220, 230), wherein the messaging server (1000) is designed to detect malicious electronic messages (100) and comprises:

- a generating unit (1010) configured to generate at least one signature for an electronic message (100) to be transmitted from the at least one message sending device (110, 120, 130) to the at least one message receiving device (210, 220, 230);
- a data storage unit (1050) configured to store the generated at least one signature;
- an antivirus unit (1020) configured to determine whether the electronic message (100) is malicious or not;
- a determining unit (1030) configured to determine in the case of a determined malicious message and based on at least one signature generated for the determined malicious message, whether electronic messages (100) comparable to the determined malicious message (100) were classified as non-malicious and transmitted to the at least one message receiving device (210, 220, 230) in the past, by comparing the at least one signature of the determined malicious message with signatures in the data storage unit (1050) which are associated with previously transmitted electronic messages (100); and
- a signalling unit (1040) configured to signal a potential threat to the at least one message receiving device (210, 220, 230), if it is determined that electronic messages (100) comparable to the determined malicious message (100) were classified as non-malicious and transmitted to the at least one message receiving device (210, 220, 230) in the past.

14. A messaging system (1) comprising:
    - at least one message sending device (110, 120, 130);
    - at least one message receiving device (210, 220, 230); and
    - the messaging server (1000) according to claim 13, wherein the messaging server (1000) is in communication with the at least one message sending device (110, 120, 130) and the at least one message receiving device (210, 220, 230).