Amendments of the RZ Trier to the user rules

RZ HT RECHENZENTRUM
HOCHSCHULE TRIER I STUDIENORT TRIER

1. Treatment of unsolicited commercial E-Mails (SPAM)

The IT-department of the Trier University of Applied Sciences offers users of the E-Mail service at the Trier and Idar-Oberstein locations the possibility of filtering out unwanted advertising E-Mails ("SPAM E-Mails"). Incoming E-Mails are examined by an evaluation program according to several, constantly updated criteria for the presence of characteristics of unwanted E-Mail advertising. We use multiple practices to filter SPAM in the following order:

Blacklisting: If the E-Mail originates from a SPAM distributor generally known on the Internet, the acceptance is refused. If the sending mail server is configured correctly, the sender will be informed about the undeliverability. To identify such SPAM mailing lists, we check each incoming E-Mail to see if the sender is on one of several publicly available, regularly updated lists of known SPAM mailing lists.

Greylisting: We have implemented greylisting according to the RFC 6647 guideline (https://tools.ietf.org/html/rfc6647). Most SPAM mailing lists do not meet these requirements, so their E-Mails will not be accepted. Here, too, it depends on the configuration of the sending server whether the sender is informed about the undeliverability.

Rating system: Non-rejected E-Mails are rated according to a constantly updated procedure with regard to their spam probability. If an evaluation threshold specified in the system is exceeded, our mail server marks the respective E-Mail by prefixing the sequence "{ SPAM }" in the subject line. The E-Mails are delivered after the evaluation.

The recipient can use our **Spamblock** service (www.hochschule-trier.de/go/spamblock) to specify whether these E-Mails are to be stored in his regular mailbox or in a mailbox controlled by Spamblock. In the spam block mailbox, E-Mails are automatically deleted after a retention period of 9 days. Further information on the functionality of Spamblock can be found on the service's website.

Liability:

The rating programs are only an attempt at rating. Regardless of the reliability already achieved, there is always the possibility of error in individual cases. It is therefore expressly pointed out that the user himself is responsible for the further treatment of marked E-Mails. The university is not liable for the consequences of non-delivery.

Data protection:

The handling of E-Mails is fully automated. Except for the possible addition of the text sequence "{SPAM}" in the subject line, the content of the E-Mail is neither changed nor are E-Mails or parts thereof deleted by us. Data protection is therefore not compromised.

2. Treatment of potentially virus-infected E-Mails

General principles:

E-Mails infected with viruses and worms pose a major threat to the information infrastructure. To protect the infrastructure, an effective and at the same time user-friendly defense is required.

In order to prevent the internal and external spread of viruses via E-Mails, all E-Mail servers administered by the IT-department check **all incoming and outgoing** E-Mails. All virus scanners are equipped with an automated update function, so that as soon as new viruses and worms appear, the updated protection function takes effect as soon as the software manufacturer provides an appropriate update.

Procedure:

Virus-infested E-Mails are intercepted and **not forwarded!** Only if an analysis of the virus/worm shows that it does not falsify the sender address is the sender automatically informed that his E-Mail has not been delivered due to virus infection.

In addition, E-Mails with attachments of the type .exe, .vbs, .pif, .scr, .bat, .com are generally not forwarded due to the high risk potential. The sender will be informed. Such files must be packed in a .zip archive before sending.

Liability:

The analysis of E-Mails for viruses and worms is only as good as the database with recognition features available to the virus scanner. Although these are updated automatically, it cannot be ruled out that due to the unavoidable delay between the occurrence of a new virus/worm and the availability of an updated database, virus-infected E-Mails may pass through the virus scanner. The virus scan of the IT-department therefore does not release the user from his duty of care in handling E-Mails. He should therefore check each E-Mail to see whether the sender is known, whether a corresponding E-Mail (with attachment if necessary) is expected and whether the text part of the E-Mail is sensibly related to the sender. The university is not liable for the erroneous or unconscious delivery of E-Mails containing viruses.

Data protection:

The checking of E-Mails for viruses or worms is fully automated and therefore harmless under data protection law. The high risk potential, however, requires an intervention in such a way that under certain circumstances parts of E-Mails or entire E-Mails are not delivered. In this respect, it cannot be ruled out that important or time-critical information may be withheld from the recipient. However, this also cannot be ruled out due to general technical problems in E-Mail traffic. It is therefore advisable anyway to secure the transfer of important or time-critical information through multiple communication (request confirmation, queries, etc.).

Trier, 05.01.2015