

# E-mail security (spam and virus protection)

The university computing centre uses Sophos Central Email Security to defend against spam, phishing and virus emails.

## Report spam and phishing emails

A small number of spam e-mails could still possibly get into your mailbox. If you want to report such e-mails, send them as an attachment to the address „[is-spam@labs.sophos.com](mailto:is-spam@labs.sophos.com)“. It is easy to send the e-mail as an attachment with most e-mail programs by starting a new e-mail and then dragging and dropping the spam e-mail into the window with the new e-mail. You should then see an attachment with the extension .eml.

A description of the procedure can be found in the Sophos Knowledge Base:

<https://community.sophos.com/kb/en-us/23113>

## Central quarantine

Sophos Central Email Security holds back recognized spam/phishing emails in the quarantine area. You will receive a daily „digest message“ by email to keep you informed. If a filtered email has been detected incorrectly, you can release it via the Sophos Self Service Portal at <https://central.sophos.com/manage/self-service> if necessary. \*\*Please proceed with the necessary caution.

Instructions and further information on the Sophos Self Service Portal can be found at:

<https://docs.sophos.com/central/SelfService/help/de-de/index.ht>

## Undelivered emails

Depending on the current threat situation, certain attachments may not be delivered to your mailbox. These include password-protected zip files. You will receive the email without the attachment and, if necessary and after careful checking, you can unlock the complete email via the Sophos Self Service Portal.

## Protection against dangerous links

Manipulated links in emails pose a major threat. To provide you with the best possible protection, we use Sophos „Time of Click Protection“, which checks at the time of clicking on a link whether it is malicious. The original link is converted for this purpose. The URL then reads, for e.g.

[https://eu-central-1.protection.sophos.com/?d=typo3.org  
&u=aHR0cHM6Ly90eXBvMy5vcmcvc2VjdXJpdHkvYWR2aXNvcnkvdHlwczMtZXh0LXNhLTlwMjMtMDA0](https://eu-central-1.protection.sophos.com/?d=typo3.org&u=aHR0cHM6Ly90eXBvMy5vcmcvc2VjdXJpdHkvYWR2aXNvcnkvdHlwczMtZXh0LXNhLTlwMjMtMDA0)

&i=NjMxMDUzN2Y3YTZIMTAxMDc5YjI0OGVk  
&t=d3d2WmFjVWtuZEpHRIRaeVAvaklaajlmaG15K2RNRE11L3BQKzdpN0ZEYz0=  
&h=57e969f343344d3986686abcf79e0dc1 &s=AVNPUEhUT0NFTkNSWVBUSVZ9U3b4-DQ5Jakn4-A04o-HYCPRTRfAX8vtJppV3Ly2nljsax-adUQ1nuEnKhO8zss

The first parameter after the „?“ contains the name of the destination server for you to check.

the server is: <https://eu-central-1.protection.sophos.com> and receives the following parameters:

d=typo3.org

u=aHR0cHM6Ly90eXBvMy5vcmcvc2VjdXJpdHkvYWR2aXNvcnkvdHlwczMtZXh0LXNhLTIwMjMMDA0 -  
base64 encoded URL

The original URL can be determined again in cleartext at any time using a base64 decoder (here as an example: <https://www.base64decode.org/>)

For the technically interested: The server eu-central-1.protection.sophos.com compares the original URL with entries in the Sophos SXL database. If it is a dangerous URL, a warning appears, otherwise the user is redirected to the original destination.

## Permitted file attachments

The receipt of files that may contain executable program code may be rejected. In particular, outdated Microsoft Office documents such as \*.doc and \*.xls are not permitted. Please use the current file formats, i.e. \*.docx or \*.xlsx.

From:

<https://hrz-wiki.jade-hs.de/> - **HRZ-Wiki**

Permanent link:

<https://hrz-wiki.jade-hs.de/en/tp/email/protection>

Last update: **2025/01/21 13:50**

