E-Mail - Attachments

10.07.2025 13:36:50

FAQ-Artikel-Ausdruck

Kategorie:	Kommunikation & Kollaboration::E-Mail	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	13:54:03 - 31.03.2025

Schlüsselwörter

Attachments, Office E-Mail

Lösung (öffentlich)

Size The maximum permitted size of an email at TU Dresden is limited to 30 MB. This applies to sending and receiving.
This value was determined by the ZIH after reviewing the size specifications of the large mail providers, which usually allow up to 25 MB, as well as other universities, and confirmed by the responsible university committees. It does not make sense to increase this limit, as we would then not be able to deliver larger emails to providers with a lower limit. It therefore makes more sense to refuse emails that are too large as soon as our users attempt to send them.

Due to the technical coding required for the email medium, each attachment increases in size by approx. one third, so that a maximum of 21 MB (net file size) can be attached to the currently permitted maximum size of 30 MB.
Security

File attachments can contain malware, which is why special care must be taken before opening them. In principle, a file attachment should only be opened if the email comes from a trustworthy source. If an email you receive is signed and encrypted, you can at least be sure that the person has written to you.

Attachments that lead to emails being rejected All emails sent and received by TU Dresden and their attachments are checked and their sending or receipt is prevented where the security situation requires it. Attachments are unfortunately used extensively for phishing and to spread malware.
The following files are not accepted by our system as attachments to an unencrypted email for security reasons:
-

encrypted archives (e.g. password-protected files in .zip, .rar, .tar formats)

-

Microsoft Office files that contain macros

-

OneNote files (.one, .onepkg)

When sending such attachments, you will receive a non-delivery message.
For example, the message: "Remote Server returned '550 This message contains malware (Heuristics.OLE2.ContainsMacros)'".

Remedy:
Option 1: Store the file on [1]Datashare and send the link to the file.
Option 2: [2]Encrypt and sign the message with S/MIME.

Email Encryption Alternatively, [3]emails can be signed and encrypted and sent with the attachments mentioned above. According to the IT regulations of TU Dresden, the use of certificates for signing and encrypting emails is generally required (§ 17 para. 8).

Alternatives for Exchanging Files via Email

For larger amounts of data, we recommend using a more suitable medium. You will usually receive an access link via the service used, which you can send to the recipient by email together with a password. The recipient is then able to download the data at any time. At the same time, the storage space of the mailbox is saved. Available services for example are:

- [4]Datashare
- [5]SharePoint
- [6]Shared Storages

[1] https://faq.tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=651
[2] https://faq.tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQExplorer;CategoryID=77
[3] https://faq.tickets.tu-dresden.de/v/ItemID=1086
[4] https://tu-dresden.de/zih/dienste/service-katalog/zusammenarbeiten-und-forschen/datenaustausch#section-1
[5] https://tu-dresden.de/zih/dienste/service-katalog/zusammenarbeiten-und-forschen/groupware/sharepoint
[6] https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/datenspeicher/details