

**Director of Finance
and Administration**
Dr. Martin Mehrrens

Bibliothekstraße
VWG, room 2140
28359 Bremen

Phone (0421) 218-60100
Fax (0421) 218-60235
www www.uni-bremen.de/en/

Office:
Bettina Döring
Phone (0421) 218-60101
Fax (0421) 218-98-60101
Email sekrkanz@uni-bremen.de

Your correspondence dated: Our reference: Date: February 13, 2020

Blocking of potentially dangerous file types

To whom it may concern,

There is generally the risk when receiving emails that attachments from the sender may contain executable program code.

Upon clicking on such attachments, it may be the case that the contained program code is executed and that the malicious function subsequently becomes active on individual computers or within whole data networks.

Some of the file types that can contain such executable program code (in this case so-called macro viruses) are the well-known Microsoft Office formats, of which the document names end with the following filename extensions: doc, xls, ppt, etc.

For security reasons, the ZfN and the university administration will block the sending and receiving of email attachments that contain executable program code from February 17, 2020!

If an email with an attachment that should be blocked is received by the one of the stated email servers, the sender will automatically receive corresponding notification and the information that the email was not able to be delivered. Such emails with attachments will be automatically deleted.

Alongside the above-stated Microsoft Office file types, there are also others that can contain executable code. These file types, or rather their filename extensions, will be blocked by the email servers in the future. Please find a list of the filename extensions of such file types attached.

Please take note of the following when working with Microsoft office:

The Microsoft Office programs (Word, Excel, PowerPoint, etc.) have supported new file types, which do not contain executable code, for a long time now.

These file types can be recognized by their filename extensions – for example, docx, xlsx, pptx.

Since 2015, only versions of Microsoft Office that enable the saving of the new documents types without executable program code have been installed at the university.

Only these file types may be used from now on for security reasons!

Please check whether documents, for example templates or forms that are available as downloads on the university website, fulfil the new requirements.

The following filename extensions will not be delivered (will be blocked):

Office:

*.doc, *.docm, *.dot, *.dotm; *.xla, *.xlam, *.xls, *.xlsb, *.xlsm, *.xlt, *.xltm, *.xlw;
*.pot, *.potm, *.ppa, *.ppam, *.pps, *.ppsm, *.ppt, *.pptm

Further filename extensions that are not permitted for delivery:

*.exe, *.com, *.bat, *.ps1, *.cmd, *.hta, *.pif, *.scr, *.scf, *.psc1, *.vbs, *.inf, *.acm,
*.ax, *.cpl, *.dll, *.drv, *.efi, *.mui, *.mht, *.mhtml, *.ocx, *.sys, *.tsp, *.sct, *.vb,
*.vbe, *.ws, *.wsf, *.paf, *.msi, *.jse, *.msp, *.mst, *.msc'

The following filename extensions are permitted for email correspondence:

*.docx, *.dotx; *.xlsx, *.xltx; *.potx, *.ppsx, *.pptx

I ask for your understanding regarding the measures necessary for ensuring the security of the IT operations at the university and expect your full support in realizing these vital measures.

Kind regards,

Signed Dr. Martin Mehrtens