ulm university universität uulm

To be secure ...

1. Avoid clicking on links in e-mails and opening attachments from senders whose identity is not certain. To do this, please attend the sender‘s e-mail address.

2. As a rule, captured e-mail content - i.e. with real subject and e-mail text - is used to pretend to continue an existing correspondence. The recipients are then asked to download important documents, for example. However, behind the corresponding link there is hidden malware.

3. Pay attention to the e-mail address of the sender. Incoming mails show both a name and an e-mail address. Both, the name and the e-mail address can be forged at will.

4. Pay attention to the appearance of links. If a link starts with „http“ instead of „https“, it refers to a foreign country (country code behind the „dot“; e.g. „.de“ stands for Germany) or it looks cryptic, this may be an indication of malware.

5. If an e-mail is already marked as SPAM by the university‘s mail server in the subject line, special caution is required. In case of doubt please contact the helpdesk of the kiz (helpdesk(at)uni-ulm.de) before opening the e-mail.

6. Special care must be taken with **Office file extensions**, such as „.doc“ or „.xls“, as they can contain malicious code with executable or active content. Do not enable macros (executable content) for Office files that you receive by e-mail. Even when sending files, use less critical formats such as PDF.

If you need support in the assessment of a suspicious e-mail or if you have general questions on the subject please contact the helpdesk of the kiz (helpdesk(at)uni-ulm.de).

Information is also available on the web pages of the kiz.