ulm university universität ulm

Zu Ihrer eigenen IT-Sicherheit ...

1. Vermeiden Sie es unbedingt, Links in E-Mails anzuklicken und Anlagen von Absendern zu öffnen, deren Identität nicht zweifelsfrei feststeht. Achten Sie dazu bitte bei Absendern unbedingt auf die angezeigte E-Mail-Adresse des Absenders.

2. In der Regel wird mit Hilfe von erbeuteten E-Mail-Inhalten – also mit echtem Betreff und E-Mail-Text – vorgetäuscht, eine bestehende Korrespondenz fortzuführen. Darin werden die Empfänger dann z. B. zum Download wichtiger Dokumente aufgefordert. Hinter dem entsprechenden Link verbirgt sich jedoch eine Schadsoftware.

3. Achten Sie auf die E-Mail-Adresse des Absenders. Eingehende E-Mails zeigen sowohl einen Namen als auch eine E-Mail-Adresse an. Der Name und die E-Mail-Adresse sind beliebig fälschbar.

4. Achten Sie auf das Aussehen von Links. Beginnt ein Link mit „http“ anstelle von „https“, verweist er auf ein fremdes Land (Länderkennung hinter dem „Punkt“; z. B. steht „.de“ für Deutschland) oder sieht er kryptisch aus, so kann dies ein Indiz für eine Schadsoftware sein.

5. Ist eine E-Mail im Betreff bereits vom Mailserver der Universität als SPAM gekennzeichnet, ist besondere Vorsicht geboten. Im Zweifelsfall kontaktieren Sie vor dem Öffnen der Mail den Helpdesk des kiz (helpdesk(at)uni-ulm.de).

6. Besondere Vorsicht gilt bei **Office-Dateiendungen**, wie beispielsweise „.doc“ oder „.xls“, da diese Schadcode mit ausführbarem bzw. aktivem Inhalt enthalten können. Aktivieren Sie bei Office-Dateien, die Sie per E-Mail erhalten, keinesfalls die Makros (ausführbarer Inhalt). Verwenden Sie selbst beim Dateiversand möglichst unkritischere Formate wie PDF.

Wenn Sie bei der Beurteilung einer verdächtigen E-Mail Unterstützung benötigen oder wenn Sie generell Fragen zum Thema haben, dann wenden Sie sich bitte an den Helpdesk des kiz (helpdesk(at)uni-ulm.de).

Informationen erhalten Sie auch auf den Webseiten des kiz.