Computer-Sicherheit und der richtige Umgang mit E-Mails

E-Mails sind quasi das Tor für viele Gefahren - insbesondere Computer-Viren - die ihrem Computer Schäden zufügen können.
Der richtige Umgang mit E-Mails minimiert das Risiko!

Umgang mit E-Mail-Anhängen (Attachments)

Öffnen Sie grundsätzlich keine Dateianhänge von E-Mails, wenn Sie sich unsicher sind, was dieser Dateianhang enthält; bspw. bei Mails von unbekannten Absendern oder wenn im E-Mail Text nichts über die angehängte Datei erwähnt wird. Notfalls beim Absender nachfragen!!
Umgekehrt gilt: Sie sollten beim Versand von Anhängen im eMail-Text dem Empfänger mitteilen, um welche Datei es sich handelt.

Hinweis:
Die Endungen bekannter Dateien sind bei Windows standardmäßig ausgeblendet / unsichtbar.

Empfehlung:
Dateiendungen einblenden

1. Windows-Explorer starten (Windowstaste + e)
2. Extras -> Ordneroptionen -> Ansicht
3. Häkchen entfernen bei Option „Erweiterungen bei bekannten Dateitypen ausblenden“

Anlagen die folgende Endungen enthalten, sind sehr suspekt:

- com
- exe
- bat
- vbs
- pif
- scr
- zip (gepackte Dateien, die wiederum Programme enthalten können)

Eher ungefährlich sind Anlagen mit den Endungen:

- doc (Word-Dateien)
- rtf (Textdateien - Word)
- pdf (Adobe-Acrobat-Reader-Dateien)
- xls (Excel-Dateien, Tabellenkalkulation)
- txt (reine Textdateien)
- jpg (Bilddateien)
- gif (Bilddateien)
- tif (Bilddateien)
- ppt (Powerpoint-Dateien)

Anm.: Aber auch Word- und Excel-Dateien können sog. Makro-Viren enthalten.

Achtung: Dateinamen werden oft "getarnt". So kann eine Datei, die eine scheinbar ungefährliche Endung hat in Kombination mit unsicheren Endungen gefährlich sein.

Beispiel:
textdatei.doc.exe
textdatei.rtf.com
o.ä.

Tipp:
Anlagen zunächst abspeichern und nicht direkt aus dem E-Mail-Programm öffnen. Dann mit Hilfe eines Antivirenprogramms die gespeicherten Dateien überprüfen.