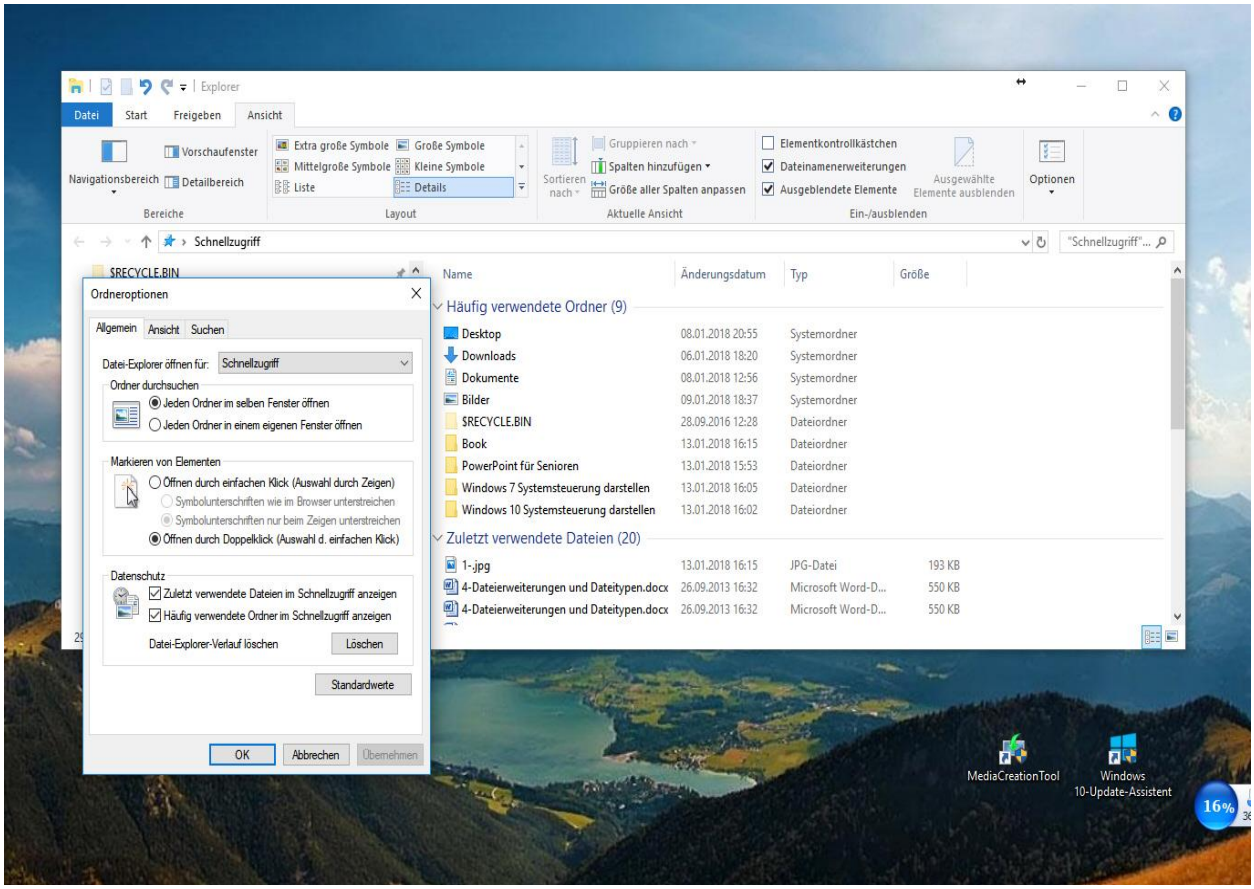
Seniorentreff Grafrath 2021



Dateierweiterungen und Dateitypen

Dateierweiterungen und Dateitypen

Dateien werden mit einem merkantilen Namen versehen. Außerdem folgt nach dem Namen eine sogenannte „Erweiterung“. Sie besteht aus **einem Punkt und nachfolgend aus drei oder vier Buchstaben**. Diese ermöglichen dem System, den Dateityp einem entsprechenden Programm zuzuordnen und die Datei damit zu öffnen.

Daher muss beim Umbenennen unbedingt die *Dateierweiterung* erhalten bleiben.

Bei der Speicherung aus fast allen Anwendungsprogrammen (z.B. Word, Excel, PowerPoint) wird empfohlen, beim Speichern einer selbsterstellten Datei **nur den Dateinamen**, also nicht die Erweiterung einzugeben. Die Programme hängen nämlich selbständig die entsprechende Dateinamen-Erweiterung an. Vielleicht haben Sie es auch schon bemerkt, dass die verschiedenen Dateitypen im Windows-Explorer je nach Anwendung neben ihrem Namen auch durch unterschiedliche **Icons** angezeigt werden.

Beispiele:

.doc, **.docx** Word-Dokument

.xls, **.xlsx** Excel-Arbeitsmappe

.ppt, **.pptx** PowerPoint-Präsentation

.mdb **.accdb** Access-Datenbank

.rtf Rich Text Datei (WordPad und viele andere Textverarbeitungsprogramme)

.txt nur Text-Dokument (Editor und alle Textverarbeitungsprogramme)

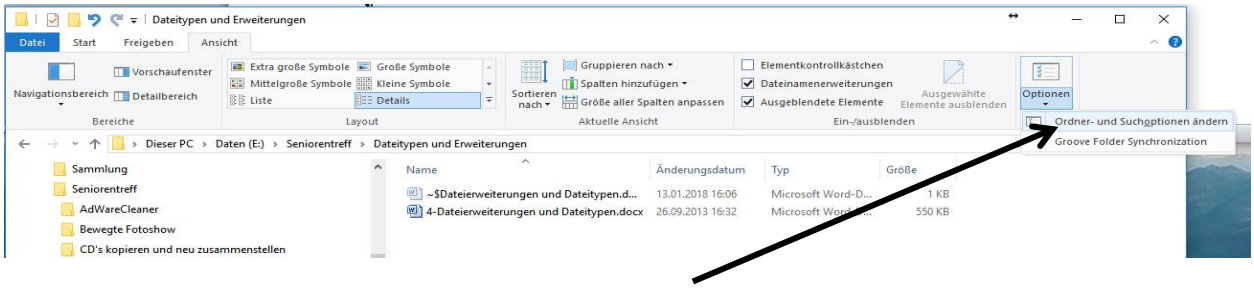
.htm, **.html** HTML-Dokumente (**H**yper**T**ext **M**arkup **L**anguage): Webseiten

Bei der Grundeinstellung Ihrer Windows-Installation werden diese Erweiterungen leider allgemein ausgeblendet. Was Microsoft sich dabei versprochen hat, steht in den Sternen.
Denn gerade bei der Unterdrückung dieser Erweiterung, können Sie nicht feststellen ob Sie z.B. im Begriff sind, ein verdächtiges Programm/Datei mit einem Vireninhalten zu öffnen oder sich wundern, dass die Datei sich nicht öffnen lässt, da Sie ein zugehöriges Programm nicht installiert haben .

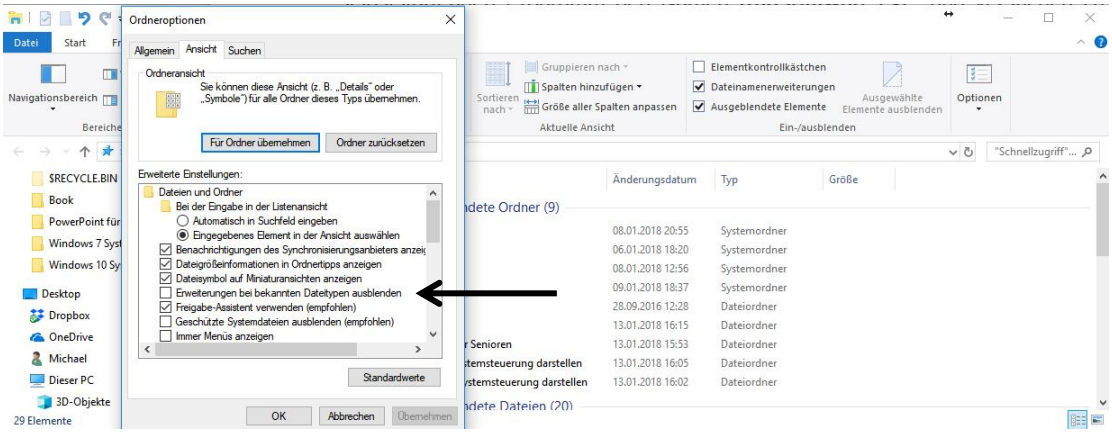
Das kann somit in einem unbedachten Moment zu einer Vireninfektion Ihres Rechners führen. Weiter unten werde ich Ihnen das einmal vorführen. Deshalb ist hier eine Änderung dieses Zustandes dringend erforderlich.

Nun zu der Änderung.
Sie haben ja schon festgestellt, dass Microsoft immer mehrere Möglichkeiten für eine Zustandsänderung oder einen Programmaufruf (z.B. Explorer) anbietet. So auch hier:

Rufen Sie die Ordneroptionen im Explorer über den Reiter **ANSICHT; OPTIONEN; ORDNER- UND SUCHOPTIONEN ÄNDERN** auf



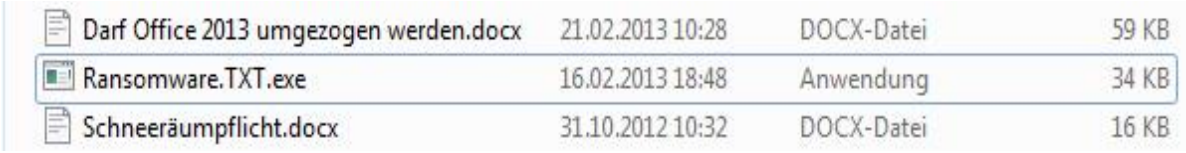
In dem sich öffnenden Ordneroptionsfenster klicken Sie wiederum den Reiter **ANSICHT** an und suchen dort nach dem Eintrag **ERWEITERUNG BEI BEKANNTEN DATEITY-PEN AUSBLENDEN**. Sofern Sie in dem zugehörigen Kästchen ein Häkchen finden, bitte **unbedingt** entfernen.



Stellen Sie sich vor, Sie seien ein „Böser Mensch" und erstellen Virenprogramme. Selbststartende Programme haben dabei die Dateierweiterung **.EXE**. Ich gebe nach Fertigstellung meinem selbststartenden Programm den Namen **Ransomware.exe.** und verberge dank Microsoft die Dateierweiterung. Das Programm mit Klick hierauf startet automatisch, da das Programm ja selbstausführend (**.EXE**) ist, trotz der Ausblendung der Dateierweiterung.

Da ich jein böser Mensch bin, füge ich in diese Datei nun aber noch eine Pseudo-Erweiterung mit dem Namen **.TXT** ein und speichere diese mit „beiden Erweiterungen", so dass meine Datei nach der Manipulation jetzt **RANSOMWARE.TXT.EXE** heißt. Dies ist unüblich, denn Microsoft geht grundsätzlich davon aus, dass nach dem eigentlichen Namen **ausschließlich ein PUNKT gefolgt von der ERWEITERUNG** folgt. Danach gehört **.TXT** ausschließlich **zum** Dateinamen Ransomware und dient nicht als Erweiterung. Die Datei könnte ja auch anders geschrieben Ransomware-Txt lauten, dann erst erschiene die Erweiterung **.EXE**

Die manipulierte Datei sieht also ohne dem besagten Häkchen wie folgt aus:



Nach Setzen des Häkchens aber so:

Darf Office 2013 umgezogen werden	21.02.2013 10:28	DOCX-Datei	59 KB
Ransomware.TXT	16.02.2013 18:48	Anwendung	34 KB
Schneeräumpflicht	31.10.2012 10:32	DOCX-Datei	16 KB

Sie gehen jetzt also davon aus, dass es sich bei der angezeigten Datei **nur** um eine Textdatei handelt und versuchen sie durch Anklicken zu öffnen. Eigenartigerweise kennt Microsoft plötzlich aber die „echte“ Erweiterung und die lautet **.EXE (verborgen).** Das Unheil nimmt nunmehr „Microsoft-gewollt“ seinen Lauf. **Virus willkommen!!**

Trojaner bleiben so getarnt

Windows-10-Einstellungen so nicht sicher

Windows 10 ist beim Umgang mit Dateinamenerweiterungen zu unvorsichtig.

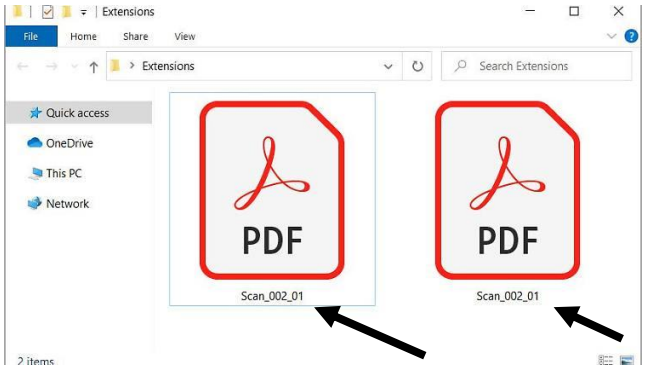
Wie oben dargestellt gibt es in Windows 10 auch diese Grundeinstellung, die es Trojanern bei Phishing-Angriffen ermöglicht, seine Tarnung aufrechtzuerhalten. Nutzer sollten deshalb diese Einstellung sofort ändern.

Viele erfolgreiche Hackerangriffe erfolgen nach ähnlichem Muster über E-Mail-Anhänge. Die Schad-Software wird dabei immer raffinierter, man kann Spam-Mails kaum noch von echten Nachrichten unterscheiden. Unter anderem verbreitet sich "Trojaner-König" Emotet über E-Mail-Anhänge, die arglose Nutzer öffnen, weil der Schädling unter anderem in der Lage ist, die Nachrichten-Inhalte inklusive Absenderadressen und Kontakt-Informationen auf dem Computer eines Opfers auszulesen. Das nutzt er aus, um täuschend echt aussehende Spam-Mails zu verschicken. Doch erst seit dem 27.01.21 - gibt es **Entwarnung**. Länderübergreifend wurde Emotet an diesem Tag inclusive Server „gekillt“. Windows 10 machte es den Angreifern dabei durch allzu lockere Grundeinstellungen auch zu einfach, die verseuchten Anhänge zu tarnen. Das lässt sich aber leicht ändern.

Zu kompliziert für Nutzer?

Das eigentliche Problem sind die Dateierweiterungen, genauer Dateinamenerweiterungen. Dabei handelt es sich um die Abkürzungen, die bei Dateinamen hinter dem Punkt stehen und den Dateityp definieren. Bei komprimierten Bildern ist das beispielsweise oft ***.jpg***, bei Videos ***.mpeg, mp4*** oder bei Musik ***.mp3***. Die Erweiterungen zeigen einem

Rechner, mit welcher Anwendung eine Datei erstellt wurde, welche Programme sie öffnen können und welches Symbol für die Datei verwendet werden soll.

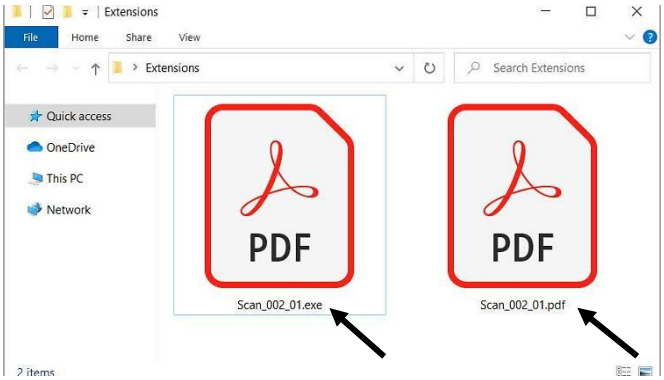


Wenn die Anzeige der Erweiterungen nicht aktiviert ist, sieht man den Unterschied zwischen echtem und falschem PDF nicht.

Der Dateiexplorer von Windows 10 zeigt die Endungen in der Grundeinstellung nicht an. Warum das so ist, ist nicht ganz klar. Laut "**BleepingComputer**" könnte es sein, dass Microsoft die Ansicht für Nutzer weniger verwirrend machen möchte. Möglicherweise soll die Darstellung auch einfach nur ordentlicher aussehen. Wie dem auch sei, Nutzer können so im Explorer nicht auf den ersten Blick erkennen, ob eine Datei auch das ist, was sie vorgibt zu sein.

Unsichtbar verpackt

Hängen Angreifer so eine gefälschte Datei in einer E-Mail direkt an, verraten sie sich allerdings schnell. Denn im Gegensatz zum Dateiexplorer zeigen Windows Mail, Thunderbird und andere Clients Erweiterungen gewöhnlich automatisch an. Angreifer verschicken gefälschte Dateien daher in einem Zip-Archiv verpackt, was auch bei harmlosen E-Mails oft der Fall ist. Im Beispiel von "**BleepingComputer"** handelt es sich angeblich um einen gescannten Vertrag. Wenn man das Archiv entpackt und auf dem PC speichert, zeigt der Explorer ein PDF an, das völlig ungefährlich aussieht, obwohl es sich um eine ausführbare Datei (.exe) handelt und nach einem Doppelklick Schad-Software installieren könnte.



Nachdem die Einstellungen geändert wurden, ist die bösartige Datei entlarvt.

Um sofort zu sehen, um welchen Dateitypen es sich tatsächlich handelt, genügen wenige Schritte. Zunächst öffnet man den Datei-Explorer. Wenn man keine Verknüpfung in der Taskleiste oder auf dem Desktop sieht, gibt man unten links ins Such-Fenster "Datei-Explorer" ein und klickt dann auf den obersten Treffer der Suchergebnisse. Im geöff-

neten Fenster wählt man dann oben *Ansicht* aus und setzt bei *Dateinamenerweiterungen* ein Häkchen.

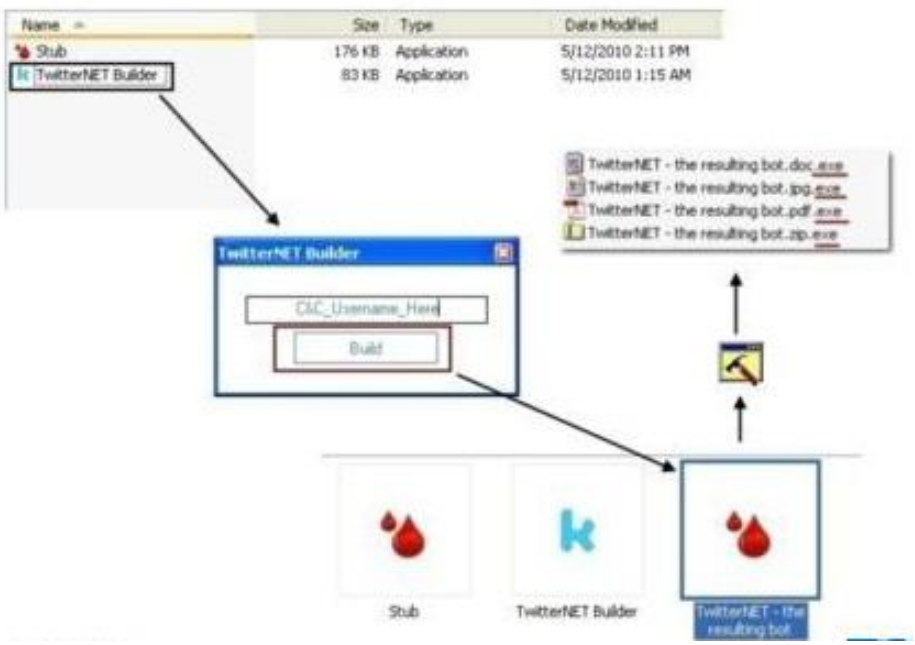
HTML deaktivieren

Wichtig: Auch wenn man die Anzeige der Erweiterungen aktiviert hat und jetzt gefährliche Anhänge leichter erkennen kann, ist man nicht sicher vor Schad-Software. Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) weist darauf hin, dass es bei E-Mails im HTML-Format schon genügen kann, sie zu öffnen, um schadhaften Code auszuführen. Das BSI rät daher, im E-Mail-Programm die Anzeige im HTML-Format zu deaktivieren, auch wenn dann manche Inhalte nicht richtig dargestellt werden.

In **Mozilla Thunderbird** geht man dazu oben in der Menü-Leiste zu *Ansicht* und klickt dann hinter *Nachrichteninhalt* auf *Reiner Text*.
In **Microsoft Outlook** klickt man erst auf die Registerkarte *Datei* und dann unter *Optionen* auf *Trust Center*. In den *Einstellungen für das Trust Center* aktiviert man im Anschluss unter *E-Mail-Sicherheit* bei *Als Nur-Text* lesen das Kontrollkästchen *Standardnachrichten im Nur-Text-Format lesen*.
In **Windows Mail** klickt man links unten auf das Zahnrad-Symbol und dann auf *Lesebereich*. Dort schiebt man beide Regler unter *Externer Inhalt* auf Aus.

Wie kommen z.B. die Bots (Malware) auf den PC?

So gelangt auch Bot-Software auf den gleichen Wegen in den PC - wie herkömmliche Malware. Sie werden unter allerlei Vorwänden als Mail-Anhänge verschickt, als vermeintlich nutzbringende Programme zum Download angeboten, stecken in infizierten Raubkopien legitimer Programme oder werden über Sicherheitslücken im Browser und dessen Erweiterungen (Plug-ins) eingeschleust indem die Erweiterung **.EXE** ausgeblendet wird.



Zur Abrundung des Themas **Dateierweiterung** als Anlage noch eine Zusammenstellung der gebräuchlichsten Erweiterungen und deren Bedeutung

Erweiterung	Beschreibung
.$$$	temporäre Datei, kann nach Programmbeendigung gelöscht werden
.arc	gepackte Archivdatei des ARC Packprogramms
.arj	gepackte Archivdatei des ARJ Packprogramms
.asc	Textdatei im ASCII-Standard (meist aber mit der Endung .txt)
.asd	Dateiendung für die automtische Sicherung von Word
.atm	Adobe Type Manager Datei (Schriftverwaltung)
.avi	Videodateien unter Windows (auch: Video for Windows)
.bak	Sicherheitskopie (Backup)
.bat	Textdatei zur Stapelverarbeitung
.bmp	Bitmap (Windows – Standardgrafikformat)
.cmd	OS/2 Stapelverarbeitungsdatei
.com	Programmdatei
.dat	Datendateien (z.B. Winmail.dat)
.dbf	dBase Datenbankdatei
.dll	Daten von Windows – Programmen- **d**ynamic **l**ink **l**ibrary
.docx	Microsoft Word Dokumente
.dotm	Microsoft Word Dokumentvorlage
.drv	Windows Treiberdatei (driver)
.exe	Programmdatei (executable – ausführbar)
.gif	Grafikformat (Graphik Interchange Format)
.hlp	Windows – Hilfedatei
.htm	HTML (Format der Internetseiten)
.html	HTML (Format der Internetseiten)
.ico	Windows Icondaten
.inf	Installations – Informationen
.ini	Initialisierungsdatei eines Programms
.jpeg	JPEG Grafikdatei
.jpg	JPEG Grafikdatei
.lha	LHA gepacktes Archiv
.lib	Bibliotheksdatei
.lnk	Verknüpfung unter Windows
.mid	MIDI Musikdatei

.mov	Quicktime Movie
.mp3	MP3 Musikdatei (MPEG 1 Layer 3)
mp4	MP4 Filmdatei incl. Sprachausgabe, Videodatei
.mpg	Videodatei
.old	Sicherungskopie von Dateien
.pdf	Adobe Acrobat Dokument
.pps	PowerPoint Datei (Präsentation)
.rar	gepacktes RAR – Archiv (Anleitung zum Öffnen)
.rtf	RTF Textformat (Rich Text Format)
.scr	Windows Bildschirmschoner
.sys	Windows Steuerungsdatei
.tif	TIFF Grafikformat (Tagged Image File Format)
.tiff	TIFF Grafikformat (Tagged Image File Format)
.tmp	Temporäre Datei
.txt	ASCII Textformat
.vbs	Visual Basic Scripte, eine ausführbare Scriptdatei.
.wav	Windows Sounddatei
.wps	MS Works Datei (Anleitung zum Öffnen)
.xlb	MS Excel – Datei
.xlc	MS Excel – Datei
.xlsx	MS Excel – Datei
.zip	gepacktes ZIP Archiv

Nur bestimmte Dateien lassen sich noch über eMail-Anhang versenden. Dateien mit der Erweiterung **.exe** oder **.com** oder **.ppsx** z.B. werden von ihrem eMail-Provider abgelehnt, da sie alleine nur mit **einmaligem** Anklicken bereits ausgeführt werden. Doch auch hier gab es einen Trick wenn Sie derartige Dateien trotzdem übertragen wollten. Sie änderten einfach die Dateierweiterung um und gaben ihr z.B. einen anderen Namen **.xyz .** Sie mussten jetzt lediglich Ihrem Partner die ursprüngliche Dateierweiterung mitteilen, damit er sie auf die ehemalige umbenennen konnte. Auch das geht heute nicht mehr.

Wenn Sie interessiert sind, was es alles für Dateierweiterungen gibt, dann schauen Sie einmal unter der Internetadresse nach:

https://de.wikipedia.org/wiki/Liste_von_Dateinamenserweiterungen/A