**Anleitung**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Seite** | **Kapitel** | **Aufgabe** |
| **GI** | Doku­ment |  | Anleitung (Seite 1) aus Mappe holen und das Dokument unter dem Namen ***Klasse\_Name\_Word.docx*** speichern |
| **GI** | 2 | Was ist ein … | Alle 3 Absätze mit Erstzeileneinzug 1 cm formatieren |
| **GI** | 2;3 | Kleine Virenkunde | Alle Nummerierungen entfernen und durch automatische Nummerierung mit römischen Ziffern (I – VIII) ersetzen |
| **GI** | 4 | Effektiver Schutz… | \* durch automatische Aufzählungszeichen ☞ ersetzen |
| **GI** | 5 | Wie erkenne ich… | \* durch automatische Aufzählungszeichen ▪ ersetzen |
| **EI** | 5 | *(Überschrift oben)* | Textmarke namens SCHERZ bei der Überschrift setzen |
| **GI** | 6 | Was mache ich… | Alle 8 Absätze mit "Schritt \_:" hängend 3 cm gestalten. Tabulatorzeichen nach "Schritt \_:"einfügen! |
| **GI** | 6 | Und eines noch: … | Absatzabstand 1½ Zeilen, Abstand vor 6pt, linker + rechter Einzug 1cm, Blocksatz. Doppelte farbige Rahmenlinie, Schattierung mit hellem Streifenmuster |
| **EI** | 7 | *(am Ende erste Zeile)* | **x** durch einen Querverweis auf die Seitenzahl der Textmarke SCHERZ ersetzen |
| **GI** | 8 | Sinnlose E-Petitionen… | \* durch die autom. Nummerierung (1), (2), (3) ersetzen |
| **GI** | 9 | Merke: … | *(alles wie oben [PINSEL])* Absatzabstand 1½ Zeilen, Abstand vor 6pt, linker + rechter Einzug 1cm, Blocksatz. Doppelte farbige Rahmenlinie, Schattierung mit hellem Streifenm. |
| **EI** | 9 | *(letzte Textzeile)* | Auf dem Text "Hoax Info Service" einen Hyperlink auf ***http://hoax-info.tubit.tu-berlin.de/hoax/*** einfügen. |
| **GI** | 1, 4, 6, 9 |  | Die Seitenumbrüche durch Abschnittswechsel (Nächste Seite) ersetzen |
| **GI** | Doku­ment |  | Fußzeile für gesamtes Dokument: links: *Dateiname + Pfad (Feld)*, Mitte: *Familienname*, rechts: *Seite / Seitenanzahl (Felder)*; einfache Rahmenlinie oben |
| **EI** | Doku­ment |  | Folgende Kopfzeilen rechtsbündig und kursiv gestalten:  ***Kapitel Viren*** für die Seiten 2 – 4  ***Kapitel Hoaxes*** für die Seiten 5 – 6  **Kapitel Kettenbriefe** für die Seiten 7 – 9 Anmerkung: Seite 1 und 10 besitzen keine Kopfzeile |
| **GI/EI** | Doku­ment | GI: Überschrift1 verwenden | Alle fünf zentrierten Überschriften (*Anleitung, Viren, …*) in Großbuchstaben, färbig, mit Unterstreichung und mit dem Zeichenabstand *Erweitert 2pt* formatieren. Für sie Formatvorlage ***Kapitelüberschrift*** definieren! |
| **GI/EI** | Doku­ment | GI: Überschrift 2 verwenden | Alle dreizehn fetten Unterüberschriften (*Was ist ein…, Kleine Virenkunde, …*) färbig, unterstrichen, in Kapitälchen und schattiert formatieren. Für sie Formatvorlage ***Detailüberschrift*** definieren! |
| **GI/EI** | 10 | GI: ohne Ebenen | Automatisches Inhaltsverzeichnis erstellen: Ebene 1: ***Kapitelüberschriften*** Ebene 2: ***Detailüberschriften*** Inhaltsverzeichnis in Arial, Schriftgröße 11 formatieren. |
| **GI** | 10 |  | Am Textende das Feld *PRINTDATE* einfügen. |
| **GI** | Doku­ment |  | In den Dokumenteigenschaften als Autor *Vorname Nachname* eintragen. Das Dokument speichern und Word beenden. |
| **GI** | Dokument |  | Abspeichern als PDF UND Word-Format hochladen |

***17 Grundinhalte / 7 Erweiterte Inhalte  
mind. 12 Grundinhalte für positive Beurteilung***

**Viren**

Computerviren gehören inzwischen zu den größten Bedrohungen für Rechner, Netzwerke und gar für das Internet selbst. Sie beschädigen Datenbestände und sorgen durch ihre teilweise extrem aggressive Verbreitung für eine nicht unerhebliche Datenlast.

**Was ist ein Computervirus?**

Ein Computervirus ist ein Programm, das auf einem Rechner weitgehend unkontrolliert Schabernack, aber auch richtig massive Schäden an Soft- und Hardware anrichten kann. Der Begriff "Virus" gilt jedoch nicht nur für das Schädigungspotential, sondern auch für die massenhafte Verbreitung. Viren können sich als vermeidlich nützliche Software tarnen, sie können sich Server-Dienste ermächtigen oder sie können auf entsprechenden Systemen gar selbst Server installieren und für ihre unbemerkte Weiterverbreitung sorgen.

Der Vergleich eines Computervirus mit einem echten Virus ist dabei durchaus statthaft. Ein Computervirus kann sich nicht allein vervielfältigen und seine Schadenskraft ausüben, sondern benötigt immer einen Wirt, im Falle des Computervirus einen Computer mit der entsprechenden Anwendung oder Systemplattform, für das es geschrieben ist.

Computerviren gibt es praktisch auf allen gängigen Betriebssystemplattformen. Mit weitem Abstand führt jedoch die Windows-Plattform mit weit über 40.000 bekannten Viren, von denen freilich die meisten Viren teilweise Jahrzehnte alt sind und einfach anderen Viren nachprogrammiert wurden. Die Vorliebe der Virenprogrammierer, ihre Viren vornehmlich für Windows-Betriebssysteme zu schreiben, erklärt sich durch die starke Verbreitung der Microsoft-Betriebssysteme und den meist wenig erfahrenen Anwendern.

**Kleine Virenkunde**

Bei Computerviren unterscheidet man zwischen verschiedenen Kategorien, die sich größtenteils durch ihre Verbreitungsart unterscheiden:

1. Boot-Viren  
Boot-Viren nutzen als Übertragungsmedium die Bootsektoren von Datenträgern. Sobald ein Computer auf einen Datenträger zugreift, wird zunächst der Bootsektor gelesen und dadurch der Virus geladen. Durch den begrenzten Speicherplatz der Bootsektoren sind Boot-Viren meist sehr klein und effizient programmiert. Da sie oft so programmiert sind, auch bei einem Warmstart im Arbeitsspeicher zu verbleiben, verbreiten sie sich gern mit jedem neu eingelegten Datenträger. Boot-Viren spielen heutzutage keine sehr große Rolle mehr, waren jedoch in den frühen Jahren der Heimcomputer eine sehr große Plage, gerade in Kreisen, in denen Software per Diskette getauscht wurde.

2. Programmviren  
Programmviren nutzen den "klassischen" Weg über ausführbare Programme, an die sie sich anhängen oder in dessen Namen sie sich ablegen und starten lassen. Werden diese Programme gestartet, wird so auch der Programmvirus aktiviert. Gern benutzen Programmviren Möglichkeiten, sich gegen wichtige Dienstprogramme der Zielplattform auszutauschen oder sich automatisch bei Systemstart starten zu lassen.

3. Hybridviren  
Hybridviren stellen die Mischform zwischen Boot- und Programmviren dar. Meist kommen Sie als Programmviren daher und installieren sich nach dem Aufruf der entsprechenden Datei als Boot-Virus in einen Bootsektor, von dort aus können sie bei jedem Datenträgerzugriff geladen werden. Höher entwickelte Viren installieren sich gleich als eigenständige Dienste, deaktivieren bekannte Anti-Virensoftware und benutzen Internet-Zugänge für die Weiterverbreitung per E-Mail oder anderen Diensten.

4. Stealth – Viren  
Stealth - Viren besitzen einprogrammierte Mechanismen, um einer Erkennung durch ein Anti-Virenprogramm zu entgehen. Dazu gibt es verschiedene Ansätze mit unterschiedlichem Erfolg: Eine sehr einfache Variante ist, dass ein Stealth - Virus sich als eine vorhandene Datei tarnt und genau die gleiche Dateigröße vorgaukelt. Andere Ansätze gehen tiefer in die Betriebssysteminterna und versuchen, interne Systemaufrufe derart umzubiegen, dass Anti-Virenprogramme diese Viren erst gar nicht finden soll.

5. Polymorphe Viren  
Polymorphe Viren sind heimtückische Viren, die ihr Aussehen bei jeder Infektion verändern und zwar in der Form, dass der eigentliche Programmcode des Virus derart verändert wird, dass die Inkarnationen von Anti-Virenprogrammen nur sehr schwer oder teilweise auch überhaupt nicht gefunden werden können. Da deshalb ein Anti-Virenprogramm nicht einfach nach einer Sequenz des Virencodes suchen kann, ist es notwendig, dass die Programmlogik eines Polymorphen Virus vollständig analysiert werden muss, um auch ein Programm zu entwickeln, dass nach so einem Virus zuverlässig suchen kann.

6. Makroviren  
Makroviren nutzen die teilweise sehr umfangreichen Makrosprachen von hoch entwickelten Anwendungsprogrammen, beispielsweise modernen Textverarbeitungen. Im Gegensatz zu allen anderen Virenarten können Makroviren auch andere Betriebssysteme in Mitleidenschaft ziehen, wenn für diese die Anwendung mit der entsprechenden Makrosprache ebenfalls implementiert ist und der Befehlssatz identisch ist beziehungsweise der Makrovirus Eigenschaften der Makrosprache auf der anderen Plattform ausnutzt.

7. Trojanische Pferde  
Trojanische Pferde sind genau genommen keine Computerviren, da sie sich nicht von allein reproduzieren und verbreiten. Ihre Aufgabe besteht darin, geheime Funktionen auf einen Computer zu installieren. Dies wiederum wird mit einem augenscheinlich harmlosen Programm vorgenommen, welches meist als angeblich wichtiges Reparaturprogramm oder ähnliches getarnt wird. Geht nun der Nutzer eines so befallenen Systems ins Internet, meldet sich das Trojanische Pferd auf dem Rechner des Verbreiters und dieser kann dann entsprechende Funktionen über das Trojanische Pferd auf dem betroffenen Rechner ferngesteuert ausführen.

8. Würmer  
Würmer sind sozusagen "Kinder der Vernetzung" und haben ihren Hauptverbreitungsweg durch Netzwerke und durch das Internet. Sie nutzen oftmals Schwachstellen in Netzwerkschnittstellen von Betriebssystemen und Netzwerk-Hardware aus, um sich als eigenständige Dienste zu installieren. Das Hauptziel dieser Dienste ist die Weiterverbreitung auf denselben Wegen. Besonders perfide an Würmern ist ihre Aggressivität; ein ausgesetzter Wurm, der eine bis dato nicht oder kaum bekannte Schwachstelle einer Systemplattform ausnutzt, kann innerhalb weniger Stunden massive und im Internet deutlich spürbare und nachweisbare Datenlast erzeugen.

**Virengefahr durch das Internet**

Das Internet stellt für Virenprogrammierer einen neue, erheblich schnellere Verbreitungsplattform für ihre geschriebenen Schädlinge dar. Dennoch "spazieren" Viren nicht einfach so auf Ihren Rechner und befallen ihn, sondern bemächtigen sich den "offiziellen" Wegen, auf denen Daten auf Ihren Rechner kommen. Viren aus dem Internet werden entweder als ausführbare Programme eingeschleppt, die dann auf dem Rechner ausgeführt werden und zur Infizierung führen oder sie bemächtigen sich Schwachstellen von Programmen oder Betriebssystemen. Während ersteres durch eine entsprechende Disziplin des Nutzers steuerbar ist, ist letzteres eine Frage der Administration und Pflege des Rechners, die an den Nutzer des Rechners und den Hersteller der betreffenden Software gestellt ist.

**Effektiver Schutz vor Viren**

Mit einigen Grundregeln lässt sich die Virengefahr von Systemen nachhaltig senken und nahezu gänzlich eliminieren:

\* Schaffen Sie sich ein Anti-Virenprogramm an!  
Arbeiten Sie mit einem Betriebssystem, für das Computerviren existieren und laden Sie oft Dateien aus dem Internet, sollten Sie die Anschaffung eines Anti-Virenprogramms anvisieren. Anti-Virenprogramme können im Zweifel Auskunft über einen möglichen Virenbefall des Systems oder einzelner Dateien geben. Zweifellos kostet ein Anti-Virenprogramm Geld, dennoch sollten Sie die Anschaffung wie eine Versicherung sehen.

\* Halten Sie Ihr Anti-Virenprogramm aktuell!  
Das beste Anti-Virenprogramm kann nur wenig schützen, wenn es nicht auf dem aktuellen Stand ist und auch aktuelle Viren kennt. Für die Aktualisierung ihrer Virendatenbank haben gängige Anti-Virenprogramme deshalb eine Aktualisierungsfunktion, mit der sie von ihrem Hersteller regelmäßig Datenbankaktualisierungen herunterladen. Deaktivieren Sie diese Funktionen nicht.

\* Niemals aus dem Internet heruntergeladene Dateien direkt ausführen!  
Dateien, die aus dem Internet heruntergeladen wurden, müssen grundsätzlich als bedenklich eingestuft werden und dürfen nicht direkt ausgeführt werden. Dies gilt für alle Dateien, die entweder direkt ausgeführt werden oder Makros enthalten können, beispielsweise Word-Dokumente. So heruntergeladene Dateien sollten Sie mit einem Anti-Virenprogramm prüfen, bevor Sie sie nutzen.

\* Achten Sie auf Ihr E-Mail-Programm!  
E-Mail-Programme gehören zu den Haupteinfallstoren für Viren, deshalb muss hier besonders darauf geachtet werden, eventuell zugesandte Dateien besonders kritisch zu prüfen, auch bei Dateien, die vermeintlich von Ihnen bekannten Absender stammen. Absenderangaben können in E-Mails gefälscht sein und diverse Würmer können auf dem Rechner Ihres Bekannten zu Werke sein und, unbemerkt von ihm, Viren versenden. Achten Sie auch auf die Anzeigeeinstellungen für E-Mails. HTML-Mails können Befehle enthalten, bestimmte Dateien automatisch zu starten. Grundsätzlich ist es ratsam, in der Grundeinstellung Mails nur in Klartext anzeigen zu lassen.

\* Pflegen Sie Ihr Betriebssystem und ihre Internet-Software!  
Achten Sie darauf, möglichst aktuelle Versionen von Internet-Software zu nutzen und sich regelmäßig über Aktualisierungen zu informieren. Für das Betriebssystem Windows XP existiert beispielsweise die Funktion "Automatische Updates", die sich in der Systemsteuerung konfigurieren lässt und standardmäßig so eingestellt ist, dass Updates des Betriebssystems automatisch herunter geladen und installiert werden können.

**Hoaxes**

**Die Situation**

Seit Jahren kursieren Warnungen vor (angeblichen) Viren, die sich per E-Mail verbreiten sollen. Diese "Warnungen" werden meist von gutgläubigen Menschen verbreitet, die diese per E-Mail von ihresgleichen erhalten haben. Sie zeigen dabei oft sogar ein Engagement, das man sich sonst nur wünschen könnte, im Glauben, sie täten den Adressaten einen Gefallen, in dem sie sie vor gefährlichen Viren warnen. Die Empfänger werden aufgefordert, E-Mails, die im Betreff (subject) einen der weiter unten genannten Begriffe enthalten, nicht zu lesen sondern sofort zu löschen. Andernfalls würde ein Virus furchtbare Dinge mit dem Rechner des Empfängers anrichten.

**Fakt ist...**

... dass alle diese Warnungen keinen ernstzunehmenden Hintergrund haben (was die Gefährlichkeit der vermeintlichen Viren angeht). Es handelt sich wohl mehr um ein soziologisches Phänomen. Es gibt die E-Mails, vor denen gewarnt wird, meist gar nicht. Diese Warnungen werden Hoaxes genannt (engl. hoax, altengl. hocus: Scherz, Falschmeldung). Vielmehr stellen diese "Warnungen" die eigentlichen Viren dar, denn sie richten erheblichen Schaden an, in dem sie Menschen verunsichern und Arbeitszeit binden (z.B. auch meine gerade). Außerdem belasten sie durch ihre nicht geringe Zahl das Internet durch nutzlosen Datenverkehr (zugegeben, da gibt es noch mehr Dinge, auf die das zutrifft). Generell werden nie echte Virus-Warnungen auf diese Weise in die weite Welt geschickt! Sehr wohl können aber Viren in Dateianhängen (Attachments) von E-Mails enthalten sein.

**Welche Hoaxes sind bekannt?**

Die Zahl der Hoaxes ist nicht gering, die meisten sind letztlich nur Nachahmungen ("copycats") des ersten dokumentierten Hoax "GoodTimes". Eine vollständige Liste kann hier leider nicht wiedergegeben werden. Sie wäre ziemlich lang. Es stellt sich zudem die Frage, welche dieser Hoaxes wirklich in Deutschland kursieren, diese kann jedoch nicht abschließend beantwortet werden. Wenn Sie eine verdächtige E-Mail erhalten, die hier nicht aufgeführt ist, schauen Sie erstmal bei Rob Rosenberger rein (nur bei Virenwarnungen). Wenn Sie unsicher sind, was von einer E-Mail zu halten ist, schicken Sie sie an diese Adresse.

**Wie erkenne ich einen Hoax?**

\* Der Adressat wird aufgefordert, die "Warnung" an möglichst viele Menschen weiterzuleiten.

\* Das Subject (Betreff) enthält oft den Begriff "Virus Warnung" oder sinnverwandtes.

\* Die Wirkung des Virus wird sehr drastisch dargestellt und beinhaltet Dinge, die ein Computer-Virus gar nicht kann (z.B. Hardware beschädigen).

\* Häufig wird als Quelle eine namhafte Firma oder Organisation genannt, um die Glaubwürdigkeit zu verbessern (a.k.a. False Authority Syndrome). Bei diesen Firmen finden sich jedoch keine Hinweise auf eine solche Warnung.

\* Oft finden sich Aktualitätsangaben wie "gestern" oder "am Freitag", die keinen Bezug zu einem bestimmten Datum haben können. Wenn ein Kettenbrief schon ein paar Tage, Wochen oder Monate unterwegs ist - wann war dann "gestern"?!

Keine der genannten Firmen hat tatsächlich jemals Warnungen dieser Art publiziert. Es werden generell nie echte, offizielle Virus-Warnungen als Kettenbriefe geschickt, das sind alles Hoaxes!

**Was mache ich, wenn ich eine solche Mail erhalte?**

1. Sie erhalten eine E-Mail mit einer Warnung vor diesem oder jenem Virus

Schritt 1: Leiten Sie sie auf keinen Fall weiter! Falls die Warnung ausnahmsweise ernst zu nehmen sein sollte, werden Sie von mir hören. Schreiben Sie an diese Adresse, wenn Sie Fragen haben. Melden Sie den Hoax, wenn alles klar ist, hier.

Schritt 2: Informieren Sie den Absender, dass er einer Falschmeldung aufgesessen ist. Geben Sie hoax-info.de als Referenz an, wenn Sie mögen. [Standard-Antworttext]

Schritt 3: Löschen Sie sie dann.

Schritt 4: Löschen Sie niemals eine Datei auf Ihrem PC wegen einer solchen E-Mail!

Schritt 5: Vergessen Sie dann die ganze Sache - verschwenden Sie keine wertvolle Zeit damit!

2. Sie erhalten eine E-Mail, vor der Sie jemand gewarnt hat

Schritt 1: lautet das subject "Returned or undeliverable mail" oder "(no subject)" oder so ähnlich, kann es sich um eine normale Mail oder Fehlermeldung handeln, die Sie lesen sollten. Es kann jedoch auch ein E-Mail-Wurm sein, der sich mit derartig betitelten Mails selbst versendet! Z.B. W32/Netsky.q

Schritt 2: enthält das Betreff dagegen einen der o.g. Begriffe, erlaubt sich wahrscheinlich jemand einen schlechten Scherz mit Ihnen, da die Mails, vor denen gewarnt wird, eigentlich gar nicht existieren.

Schritt 3: Löschen und vergessen! Lassen Sie sich nicht zu unangemessenen Reaktionen hinreißen – das ist reine Zeitverschwendung. Weisen Sie den Absender allenfalls höflich aber bestimmt darauf hin, dass Sie solche "Scherze" nicht lustig finden.

Und eines noch: Viren können sehr wohl per E-Mail verbreitet werden. Sie können nämlich im Anhang (Attachment) als Teil eines ausführbaren Programms verschickt werden. Hier sei auch auf Macro - Viren (z.B. Melissa) hingewiesen (speziell Microsoft Word ab Version 6.0, \*.doc; aber auch andere), sowie auf VBS-Viren (z.B. VBS/Loveletter) und E-Mail-Würmer (wie Hybris oder MTX).

Es gibt nur einen wirksamen Schutz gegen Hoaxes: Information!

**Warum soll ich das glauben, was hier steht …**

… und nicht den Warnungen in Kettenbriefen? Eine gute Frage. Vielleicht, weil Sie meinen, der Inhalt dieser Seiten sei von Fachleuten zusammengestellt worden. Das trifft zumindest für die meisten der angegebenen Quellen zu, für mich selbst nehme ich dieses Prädikat nicht in Anspruch. Allerdings betreibe ich diese Informationsseiten immerhin schon seit 1997.

Schauen Sie auch unter nach unter Weitere Informationen nach, dort finden Sie seriöse Quellen, aus denen auch ich oft meine Informationen zu diesem Themengebiet beziehe. Sie sind leider meist auf Englisch, wie so vieles im Internet.

Bevor Sie sich fragen, warum Sie mir glauben sollten, sollten Sie sich allerdings zunächst fragen, warum Sie den Behauptungen in Kettenbriefen Glauben schenken sollten, die durch keinerlei Nachweise oder Quellenangaben erhärtet werden.

**Kettenbriefe**

Auch Kettenbriefe zählen zu den Hoaxes (engl. für Falschmeldung, Jux, Scherz – siehe Seite **x**), denn auch hier existiert kein realer Hintergrund, der eine Weiterleitung an andere rechtfertigen könnte. Darüber hinaus fallen sie auch in die gleiche Kategorie wie Werbe-Mails: Sie sind unverlangte Massen-Mails (Spam, UBE).

**Varianten:**

1. Pyramiden - Systeme (Schneeball - Systeme, 'Make Money Fast')

Hier werden die Empfänger aufgefordert einen bestimmten Betrag an den Absender zu zahlen. Sie sollen dafür Informationen bekommen, wie sie das selbst auch mit anderen machen können. Meist sollen dazu 5 bis 7 (wertlose) Textdokumente verkauft werden, die auch als Rourke-Reports bekannt sind. Oft werden diese Systeme z.B. als Die Perle im Internet tituliert. Durch die lawinenartige Verbreitung soll man in ein paar Tagen hunderte oder gar tausende von Dollar / EURO verdienen und dann immer weiter. Dass das nicht funktionieren kann, wird schnell klar, wenn man sich mal vor Augen hält, welche Teilnehmerzahlen erforderlich werden, wenn man als zehnter in einer solchen Kette noch etwas verdienen soll.

Angenommen, man verschickt in jeder Ebene 10 Mails, deren Empfänger auch wieder 10 Mails verschicken und so fort (unvermeidliche 99% Blindgänger also nicht mitgerechnet), dann ergibt das in Ebene 10 bereits 1010 (10.000.000.000 also 10 Milliarden) Mails! Es wird aber derzeit von nur ca. 600 Mio Internet-Nutzern weltweit ausgegangen (diese Zahl mag je nach Quelle variieren, die Größenordnung ist entscheidend) - und es leben weniger als 7 Mrd. Menschen auf diesem Planeten. Die einzigen, die evtl. profitieren, sitzen in den ersten 3 - 5 Ebenen. Da diese Aktionen schon ein paar Jahre laufen, können Sie kaum erwarten, zu diesen zu gehören (Sie erfahren das aber ohnehin nicht). Den Absender können Sie übrigens sehr leicht ausfindig machen: Er steht mit Namen und Postadresse an der Stelle, wo man 'Report Nr. 1' bestellen soll...

Wenn Sie eine derartige Mail erhalten, senden Sie eine Beschwerde an den Provider des Absenders. Etliche Provider (etwa FreeMailer wie GMX) betrachten die Teilnahme an solchen Schneeballsystemen als Missbrauch ihrer Dienste und Verstoß gegen die Nutzungsbedingungen. Sie sperren dann den Account des Versenders oder sprechen zumindest eine Verwarnung aus.

Ebenfalls in diese Kategorie fallen die (meist nicht per E-Mail betriebenen) so genannten Herzkreise, Schenkkreise und Männerkreise. Hierbei geht es um weitaus höhere Summen, meist mehrere 1000 Euro. Auch das in den 1980er Jahren bekannt gewordene Pilotenspiel war nichts anderes.

2. Gewinnspiele und Artverwandtes

Bill Gates schenkt jedem $1000,- oder eine Windows98-CD, Nike verschenkt Sportartikel, Disney World zahlt jedem $5000,- oder eine Alles - Inklusive - Reise nach Disney World und so weiter und so weiter...

Mit ein bisschen gesundem Menschenverstand merkt man gleich, dass das Quatsch ist. Aber, da wird ja (z.B.) gesagt, Microsoft habe ein System entwickelt, das jede weitergeleitete Mail registrieren könne (das 'Microsoft E-Mail Trecking System'), das würde man gerade testen und als Belohnung fürs Mitmachen ... so. Das ist natürlich nicht richtig, ein solches System existiert nicht.

Glücksbriefe

Diese an sich harmlos erscheinenden Kettenbriefe stellen durch ihre Zahl und Häufigkeit doch eine Belastung der Netz-Ressourcen und eine Belästigung der meisten Empfänger dar. Es wird wohl kein vernünftiger Mensch ernsthaft annehmen, dass diese Briefe (die es seit Jahrhunderten auch in handschriftlicher Form gibt), irgendeine andere Wirkung als die eben genannte haben. Viele finden es einfach lustig oder meinen, sie würden jemandem damit zumindest eine Freude machen. Tenor: "Schaden kann's ja nicht!"

Einige dieser Glücksbriefe drohen jedoch auch mit ernsten Konsequenzen für den Fall, dass sie nicht weitergeleitet werden. Dies kann abergläubische Menschen durchaus verunsichern; sie leiten sie dann lieber weiter, womit das Ziel wieder einmal erreicht wäre.

3. Tränendrüsen-Briefe

Da sitzt in Florida (oder New York, England, Australien, ...) ein kleines Kind, das bald an Krebs (oder einer anderen Krankheit) sterben wird und sein letzter Wunsch ist es, dass dieser Kettenbrief um die Welt gehen möge (oder es mögen ihm/ihr alle schreiben). Nun macht mal alle schön mit, es ist doch für einen guten Zweck, außerdem bekommt die jeweilige Klinik (oder wer auch immer) von irgendeiner Stiftung (oder sonst woher) soundsoviel Dollar (oder Cents) für jede Weiterleitung. [ Beispiel... ]

Wieder stellt sich die Frage, wer die Mails eigentlich zählt, wenn sie nicht alle an eine bestimmte Adresse geschickt werden. Wer da an wen Geld zahlt, ist auch nicht immer gesagt und ob das dann auch passiert, weiß man ohnehin nicht. Wer ohnehin die Absicht und das Geld hat, einem kranken Menschen zu helfen, wird diese Hilfe nicht davon abhängig machen, dass ein Kettenbrief oft genug weitergeleitet wird, damit rechnerisch der nötige Betrag zusammenkommt.

Auch die vor über 10 Jahren durch die Presse gegangene Postkarten-Aktion für ein todkrankes Kind in England ist übrigens bis heute nicht zu stoppen, dieses (damalige) Kind wird noch heute mit Unmengen an Post überhäuft, die es gar nicht haben will. Die Idee dazu kam nämlich von jemand anderem. [mehr darüber...]

Es gibt sicher viele tausend kranke Kinder überall auf der Welt, viele von ihnen zum Sterben verurteilt, und einige fänden es vielleicht sogar toll, viele E-Mails zu bekommen. Mit Sicherheit wissen die aber nichts von diesen Aktionen und werden es auch nie erfahren, geschweige denn, dass jemals auch nur ein Cent für ihre Behandlung dadurch aufgebracht würde.

4. Sinnlose E-Petitionen

In diese Kategorie fallen Kettenbriefaktionen, die dazu aufrufen, sich für oder gegen dies oder jenes einzusetzen. Das mag alles gut gemeint sein und die Ziele der Aktion mögen höchst ehrenwert sein, jedoch gilt hier ganz klar:

\* Kettenbriefe sind kein adäquates Medium, um seriöse Anliegen zu kommunizieren.

\* Kettenbriefe ändern nichts.

\* Niemand, der etwas ändern könnte, nimmt Kettenbriefe ernst oder auch nur zur Kenntnis.

Beispiele für solche Aktionen sind die Kettenbriefe "Taliban's War on Women" und "Filmboykott". Hinzu kommt, dass solche Aufrufe häufig aus USA stammen und dann -- wenn überhaupt! -- auch nur dort ein Zusammenhang zur Realität hergestellt werden könnte. Diese hier in Europa weiterzuleiten, hätte ohnehin keinen Sinn.

5. Urban Legends

Die weitaus größte Gruppe unter den im Internet verbreiteten Falschmeldungen sind die Urban Legends ('Großstadtmärchen', Wandersagen, Gerüchte). Hier wird auch der größte (und z. T. der amüsanteste) Unfug verzapft. Die Bandbreite der weiter erzählten Geschichten reicht von Gesundheitswarnungen aller Art (z.B. vor bestimmten, angeblich krebserregenden Lebensmitteln oder Kosmetika) über Warnungen vor bestimmten Tricks von Betrügern (die es in der Praxis nicht gibt) bis zu Horror-Geschichten darüber, was der Nichte des Friseurs des Bekannten einer entfernten Verwandten aus Dingsda 'selber passiert' sein soll...

**Ein paar Beispiele:**

\* angebliche Terror-Anschläge (falsche Warnungen)

\* Nokia, Ericsson u. Siemens verschenken [keine!] Handys

\* HIV-Infektion in der Disco (oder im Kino, Theater, ...)

\* Rattenurin auf Getränkedosen

\* Warnung vor Aspartam (Süßstoff)

\* Wurmeier in Kebab?

\* Kindesentführung im Einkaufszentrum

\* Asbest in Tampons

\* Brustkrebs durch Deo-Spray

**Merke**: Das Internet ist ein großartiges Informationsmedium -- aber Sie sollten nicht alles glauben, was Sie irgendwo im Internet lesen. Das Internet ist auch die Tummelwiese für Verschwörungstheoretiker, Weltuntergangsprediger und sonstige Personen mit Pseudo-Paranoia und/oder überzogenem Sendungsbewusstsein. Verbreiten Sie diesen Unfug bitte nicht weiter!

**Fazit: Finger weg von Kettenbriefen.**

Soweit sie nicht ohnehin in Deutschland illegal sind (Pyramidensysteme), handelt es sich meist bestenfalls um schlechte Scherze, die man nicht unterstützen sollte. Allgemein ist ein Kettenbrief auch kein geeignetes Mittel, um seriöse Hilferufe und andere wichtige Dinge zu verbreiten, denn dieses Medium ist bereits allzu sehr diskreditiert (eben weil damit überwiegend Unsinn verbreitet wird).

Kostenpflichtige Informations-Hotline: +49 (0)30 314 - 120144 (15 Cent pro Minute)

Weitere kostenfreie Infos auf den Webseiten von: Hoax Info Service

**Inhaltsverzeichnis**

Zuletzt gedruckt am: