Viren	Beschreibung
Bootsektor-viren	Beim Starten des Rechners (Booten) von der Festplatte oder von einem Wechseldatenträger wird das Virus aktiviert. Die Original-Bootsektoren werden überschrieben, das Gerät muss neu konfiguriert werden.
Dateiviren	Hängen sich an Programmdateien an und löschen oder manipulieren Daten.
Makro- und Scriptviren	Sind in Makrosprachen von Programmen, z. B. OFFICE, geschrieben und können u. a. Dateien löschen oder manipulieren.
Trojanische Pferde	Sind als harmloses Programm getarnt (z. B. als Bildschirmschoner oder Update), das jedoch versteckt Anweisungen enthält, mit denen sich der Virenautor Zugriff auf die Daten verschaffen kann, die auf dem befallenen Computer gespeichert sind. Aktiviert werden sie, indem Nutzer/innen das infizierte Programm starten.
Backdoors (Hintertüren)	Lassen eine Fernsteuerung des Rechners zu. Damit können Angreifer/innen von außen über das Netzwerk Daten manipulieren oder ausspionieren.
Würmer	Können sich selbst vervielfältigen und verbreiten sich über Netzwerke oder über Wechselmedien wie USB-Sticks. Beispielsweise kann ein Wurm Kopien von sich selbst an alle Kontakte aus dem E-Mail-Adressbuch senden und sich dann wiederum auf alle Kontakte in deren Adressbüchern ausbreiten. Beispiele für Computerwürmer sind: Sasser, Blaster, Conficker.
Exploits	Gelangen unter Ausnutzung von Sicherheitslücken im Betriebssystem oder durch Anwendungsprogramme in den Computer und können ihn teilweise oder ganz lahmlegen.

Folgende Maßnahmen schützen vor Computerviren:

- Regelmäßiges (mindestens wöchentliches) Anfertigen von **Sicherheitskopien** der wichtigsten Daten.
- Installation einer **Antivirensoftware.**
- Keine Attachments öffnen, deren **Ursprung nicht zweifelsfrei seriös** ist.
- **Attachments** von einer Antivirensoftware **prüfen lassen.**
- Durch **Voreinstellungen in WINDOWS und OUTLOOK** lässt sich die Gefahr von Viren ebenfalls stark einschränken.
- Auch Original-CD-ROMs und -datenträger können Viren enthalten.
- Im BIOS-Setup sollten Sie die Boot-Reihenfolge auf „C, A" oder „C only" einstellen, damit nicht versehentlich von einem infizierten Wechselmedium gebootet wird.

Die zentralen **Gefahrenquellen** für einen Virenbefall sind E-Mail-Anhänge, WWW-Downloads, FTP-Downloads, IRC (Internet Relay Chat), Newsgroups sowie OFFICE-Dokumente und Multimedia-Dateien.

Zur Erinnerung! Zentrale Gefahrenquellen für einen Virenbefall sind:

- E-Mail-Anhänge
- WWW-Downloads
- FTP-Downloads
- IRC (Internet Relay Chat)
- Newsgroups
- OFFICE-Dokumente
- Multimedia-Dateien

Computerviren verursachen mittlerweile jährlich Schäden in Billionenhöhe mit steigender Tendenz.

1.2.2 Spams

Bei Spams handelt es sich **nicht** um Viren, weil sich ein Spam nicht selbstständig verbreitet. Spams sind Werbemails, die unverlangt in großen Massen verschickt werden. Sie sind lästig, jedoch nicht schädlich.

In Österreich ist das Zusenden elektronischer Post als Massensendung zu Werbezwecken nur mit Zustimmung des Adressaten erlaubt.

Die Absender der E-Mails sind in der Regel nicht zu ermitteln, da sie sich gefälschter Absenderadressen bedienen oder die Adresse sofort nach Sendung löschen. Zurückmailen, um das Spam abzubestellen, ist nutzlos – im Gegenteil: Es dient den Spammern als Bestätigung, dass die angeschriebene Adresse tatsächlich abgerufen worden ist.

Auswirkungen von Spams

Spams füllen nicht nur auf lästige Art und Weise den Posteingang, sie ...

- ... verursachen **Kosten durch Downloadzeiten** und **Speicherplatz.**
- ... beanspruchen die **Bandbreite** (besonders beim Versand von Bildern oder Multimediadateien).
- ... sind vom Standpunkt des Datenschutzes **bedenklich.** Nicht selten findet man die E-Mail-Adressen aller Empfänger im Cc-Feld des E-Mails.
- ... können zum **Ausfall eines Mailservers** führen.

Spams werden unverlangt und in großen Massen verschickt.

Es gibt verschiedene technische Hilfsmittel, um sich zur Wehr zu setzen. Dazu zählen z. B. Spamfilter (spezielle Software), die auf bestimmte Reizwörter in der Betreffzeile („Subject": z. B. money, cash) oder im Text bzw. auf Namen oder Mailadressen im Absenderfeld („From") reagieren.

Die E-Mails können Sie direkt am Mailserver überprüfen und auf Wunsch löschen. Bestimmte Absender können im Vorhinein gesperrt werden. In E-Mail-Programmen (z. B. OUTLOOK) können Sie individuelle E-Mail-Filter einrichten. Die Schwierigkeit bei all diesen Maßnahmen ist jedoch, dass möglicherweise auch legitime bzw. erwünschte E-Mails automatisch gesperrt werden.

1.2.3 Hoaxes und Kettenbriefe

Hoax = engl. für Falschmeldung, Jux, Scherz.

Als Hoaxes bezeichnet man **Falschmeldungen, z. B. über nicht existierende Viren.** Derartige Informationen werden in der Regel per E-Mail übermittelt. In diesen Meldungen wird vor einem Virus gewarnt, das es in Wirklichkeit gar nicht gibt.

Woran erkennen Sie einen Hoax?

Hoaxes erkennen Sie an folgenden Merkmalen:

- Sie werden z. B. vor **Viren oder trojanischen Pferden,** die mit E-Mail über das Internet versandt werden, **gewarnt.**
- Der Betreff enthält Schlagwörter wie OMG, Warnung, Skandal, Unglaublich ...
- Üblicherweise stammt das E-Mail von **einer Person,** manchmal von **einem Unternehmen.**
- Im Verlauf der Nachricht werden Sie mehrmals aufgefordert, jede Person im **Bekanntenkreis per E-Mail zu warnen.**
- Die **Wirkung** des Virus bzw. der „Bedrohung" wird **sehr drastisch dargestellt** und beschreibt Schäden, die ein Computervirus gar nicht verursachen kann, z. B. die Hardware beschädigen.
- Häufig wird als **Quelle** eine **namhafte Firma oder Organisation** genannt, um die Glaubwürdigkeit zu verbessern.
- Die gesamte Nachricht ist in einem **technischen Jargon** verfasst.

Viele tauchen zunächst nur in englischer Sprache auf und werden später von einer Person ins Deutsche übersetzt und weitergeleitet. Das Gleiche gilt auch für Kettenbriefe. Ziel ist es, technisch nicht versierte Computernutzer/innen zu verunsichern, zu einer bestimmten Reaktion zu bewegen oder gar in Panik zu versetzen. Hoaxes und Kettenbriefe fallen in die Kategorie der Spams.

Erkennen Sie eine Nachricht als Hoax, führen Sie folgende Schritte durch:

1. **Leiten Sie die Nachricht nicht weiter,** um an dieser Stelle die Wanderschaft des Hoax zu unterbrechen.
2. **Informieren Sie die Senderin/den Sender** der Nachricht, dass es sich um eine Falschmeldung gehandelt hat.
3. Wenn Sie nicht sicher sind, ob eine Nachricht ein Hoax ist, **recherchieren Sie in Datenbanken von Antivirusunternehmen** oder über anerkannte Institutionen oder in der Fachliteratur, ob das Virus dort bekannt ist oder bereits als Hoax registriert wurde (**www.hoax-info.de**).
4. **Löschen Sie keine Datei** auf dem PC wegen eines derartigen E-Mails.

Beispiele: Kettenbrief

```
SEHR WICHTIG !!!!!!!!!

An einer Tankstelle, tankte eine Frau ihr Auto,da wurde Sie von einem
Mann als Maler bekleidet,angesprochen,ob Er ihr helfen könne.
Sie verneinte... Er bot ihr seine Visitenkarte an,falls Sie einen Maler
brÄuchte. Nach einem hinundher, ....um ihn loszuwerden nahm Sie die
Visitenkarte an und der dubiose Herr stieg in einem Auto ein das von
einem zweiten Mann gelenkt wurde, und Sie fuhren davon. Nachdem Sie
losfuhr fühlte Sie sich immer berauschter und hatte mühe zu atmen. Sie
Öffnete das Fenster und bemerkte gleichzeitig das dieser komische Geruch
von Ihrer Hand stammt, mit der Sie die Visitenkarte entgegen nahm !!
Die 2 Männer verfolgten Sie.  Da es ihr sichtlich immer schlechter ging
fuhr sie auf den nächsten Parkplatz,stoppte, begann wie wild zu Huppen
und schrie um Hilfe. Die 2 verfolger fluchteten,ihr ging es aber immer
schlechter.
DIE VISITENKARTE WURDE IN EINE FLÜSSIGKEIT DROGE GETRÄNKT, die BURUNDANGA
HEISST,sie wird von Kriminellen verwendet um Leute zu Berauben oder
Vergewaltigen !!!

Diese flüssige Droge kann über verschiedensten Arten von Papieren an jeden
übertragen werden und somit diese Person ausser gefecht setzen.
Diese Substanz ist viel viel schädlicher und wirksamer als jegliche
ursprüngliche Droge oder Schlafmittel.
Also,nehmt keine Visitenkarten oder Ähnliches von wildfremden an !!!!
Ähnliche Masche, Sie werfen eine Visitenkarte in den Briefkasten und
warten im Auto bis jemand reintappt und dann schlagen Sie zu !!!
Andere Möglichkeit sind die Typen die einen angeblich das Auto für den
Export abkaufen wollen und einem die VK bei der Scheibe der Fahrerseite
befestigen !!!

SEID VORSICHTIG und warnt soviel Leute wie möglich.
```

Originaltext

Aufgrund eines Hoax müssen keine Dateien von Ihrem PC gelöscht werden!

Hoaxes sind Falschmeldungen. Man kann sie mit der sogenannten Zeitungsente (Falschmeldung in Zeitungen) vergleichen.

Haben Sie auch schon einmal einen Kettenbrief per E-Mail erhalten? Wie haben Sie darauf reagiert? Wie hätten Sie im Nachhinein betrachtet darauf reagieren sollen?

Nähere Informationen zu Hoaxes finden Sie unter www.hoax-info.de