# Security

**Das Wichtigste: Sichern Sie Ihre Daten !!!!**



## 1. Viren: = zerstörerischer Programmcode

- Verwenden Sie **aktuelle** Virenschutzsoftware eines bekannten Herstellers und aktualisieren Sie **täglich** !
- Aktuelle Viren verbreiten sich über das Adressbuch, eine Virenwarnung bedeutet **nicht** automatisch, dass Ihr PC infiziert ist, sollten Sie trotzdem Bedenken haben, überprüfen Sie die Festplatten mit der **aktualisierten** Virensoftware
- Sollten Sie einen Virus nicht entfernen können, verwenden Sie das gegen den Virus speziell geschriebene Entfernungsprogramm (im Downloadbereich unter "**Virus Remover**")
- Seien Sie kritisch gegenüber empfangener Emails, **LÖSCHEN** Sie E-Mails unbekannter Absender, öffnen Sie **NIEMALS** deren Attachments
- Microsoft versendet **NIEMALS** Virenwarnungen oder Sicherheitsupdates, diese Mails sind **IMMER** der Virus selbst --> Mails löschen

## 2. Malware: = Dialer, Trojaner, Adware (Werbesoftware, Cookies)

- Verwenden Sie z.B.: Ad-Aware zum Schutz gegen Malware (das kostenlose "Ad-Aware" findet und entfernt Malware, das kostenpflichtige "Ad-Aware Pro" schützt zusätzlich vorab das Betriebsystem mittels "Ad-Watch" gegenüber eindringende Malware)
- **Adaware Pro:** Aktualisieren Sie **täglich** automatisch und starten Sie Adwatch automatisch bei Systemstart !
- **Adaware:** Führen Sie das Programm immer bei **veränderten** Systemverhalten aus (PC wird langsamer / instabil / braucht für die Internetverbindung länger,....)
- **Dialer:** Wählen Sie nicht automatisch aus einem Programm (Internet Explorer, Outlook Express,...) sondern wählen Sie die DFÜ-Verbindung zu Ihren Provider händisch !

## 3. Pop-up Fenster: = automatisch öffnende Fenster des Browsers

- Verwenden Sie z.B.: Google Toolbar

## 4. Browser Hijacker: = entführen den Browser auf ungewünschte Webseiten

- Verwenden Sie z.B.: cwshredder

## 5. Sicherheitslücken des Betriebssystems: = Angriffsmöglichkeiten für Viren und Hacker

- Verwenden Sie das Windows Update bei Microsoft Betriebssystemen
- Installieren Sie **alle** "Wichtigen Updates und Servicepacks", die für Sie **relevanten** "Windows Updates" und bei **Bedarf** "Treiberupdates"
- Alternativ verwenden Sie **"Automatische Updates"** (in der Systemsteuerung)

## 6. Firewall: = Schutz vor Eindringlingen

- Verwenden Sie z.B.: Outpost, Sygate Personal Firewall oder Tiny Personal Firewall
- **LESEN** Sie **auftretende Meldungen genau** durch und **entscheiden** Sie sich **durch logisches Verständnis !**
- Bei **Breitbandzugängen** verwenden Sie unbedingt einen **Router mit integrierter Firewall** und lassen Sie diesen von einem **Fachmann** einrichten !
- Sollten Sie **Wireless Lan Geräte** verwenden, **aktivieren** Sie **ALLE möglichen Sicherheitsfunktionen** der Hardware (verwenden Sie kryptische Passwörter, Security auf MAC-Ebene, Firewall, Verschlüsselung,...)

## 7. Passwörter:

- Verwenden Sie **verschiedene Passwörter** für unterschiedliche Anwendungen
- Verwenden Sie **sichere Passwörter** (KEIN Name von Familienmitgliedern / Tieren / Hobbies / Geburtstage und dergleichen !)
- Passwörter sollten **lange, kryptisch sein und Sonderzeichen beinhalten und nicht notiert werden** !
- Passwörter sind auch kryptisch durch **Eselsbrücken** leicht merkbar z.B. "wer will schon für 2$ die stunde und weniger am wochennende arbeiten?" = wws42$dh+<awa?
- **Ändern** Sie Ihre Passwörter öfters !

## 8. Eingriff in die Privatsphäre: = Senden persönlicher Daten an den Software Hersteller

- Verwenden Sie z.B.: xp-Antispy, um die Privatsphäre vor Microsoft zu schützen
- auch andere Hersteller "lesen" mit, verwenden Sie nur **Original-Software** !

## 9. Hoax: = Kettenmails mit erfunden Inhalt (zum Weitersenden bestimmt)

- Vertrauen Sie **KEINEN** Mails über Gratisangebote, vermeintlichen Organhandel, obskuren Virenwarnungen großer Konzerne, Mails aus Nigeria, usw !
- Sollten Sie eine Mail für glaubwürdig halten, **überprüfen** Sie die tatsächlichen Wahrheitsgehalt **VOR (!) Weitersenden** an andere Kontakte unter der **Hoaxliste** --> dort geben Sie einfach ein markantes Wort aus der Kettenmail ein (z.B.: Nigeria), Sie werden sich wundern wie wenige Kettenmails "echt" sind

## 10. Spam: = Massenmails an Alle

- Verwenden Sie z.B.: **Spamihilator** oder ähnliches (Mozilla, Outlook 2003, GMX-Account,.....)
- Verwenden Sie **Nachrichtenregeln** und einen Spamordner in Ihrem E-Mailprogramm (wenn Wort "x" im Betreff, dann verschiebe Mail in Ordner "Spam")
- Verwenden Sie **verschiedene E-Mail** Adressen für verschiedene Zwecke (z.B.: GMX-Account für nicht vertrauenswürdige Kontake aus dem Internet und eine eigene für persönliche Kontakte)
- Geben Sie ihre **Haupt E-Mail Adresse nicht auf Ihrer Webseite** an, nehmen Sie eine allgemeine leicht änderbare Adresse (nicht im Klartext, sondern als Link oder Script)
- Verwenden Sie bei Ihrer E-Mail Adresse einen **langen Namen** vor dem "@", z.B.: wolfgang.tatzreiter@domäne.com, Spammails werden oft automatisch nur bis maximal 8 stellen vor dem "@" generiert.

## 11. Internet Tauschbörsen: = Dateientausch zwischen Internetnutzern

- Download Copyright geschützter Inhalte (Musik, Software, Filme, Bilder,...) ohne Zustimmung des Copyrightbesitzers ist **ILLEGAL !**
- Tauschbörsen wie **Kazaa** werden mit Werbung finanziert und schmuggeln unbemerkt **Werbesoftware** auf Ihren PC, der PC wird oft merkbar langsamer
- Viele Dateien aus Tauschbörsen sind mit **Viren, Dialern und Trojanern** infiziert, wozu das Risiko eingehen ?
- Verwenden Sie legale Downloadangebote wie z.B.: **iTunes** für Musik,
- Unterstützen Sie den Handel und Sie erhalten dadurch Arbeitsplätze, kaufen Sie Musik-CDs, Software, Bücher und gehen Sie ins Kino ;-)