Die Seminarunterlagen des Dettmer-Verlags für Internet Explorer 8 können Sie nach Ihren individuellen Wünschen verändern, da sie in digitaler Form geliefert werden

Aus technischen Gründen wurde in dieser Musterunterlage dieses Deckblatt zusätzlich eingefügt, und anders als im Original-Worddokument haben wir das Inhaltsverzeichnis am Ende platziert.

Dettmer Seminarunterlagen

Seminarunterlagen-Verlag Helmut Dettmer
Neuer Schafweg 12, D-76889 Kapellen
Telefon +49(0)6343 939 047
www.dettmer-verlag.de

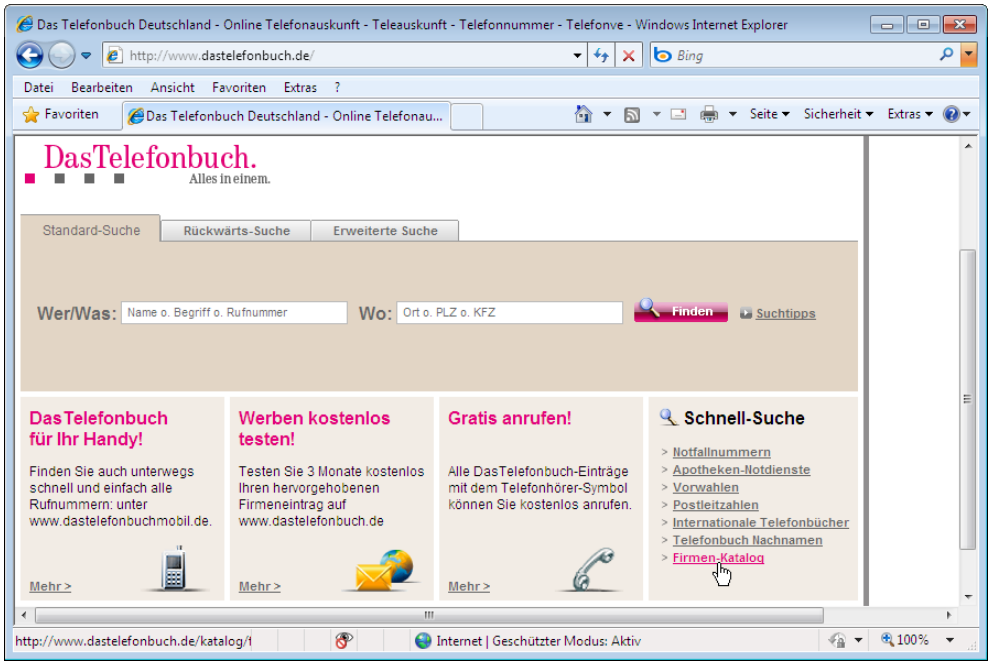
4 Surfen im Internet

Vielleicht fragen Sie sich, woher Sie eine Internet-Adresse erhalten? Dazu gibt es unterschiedliche Möglichkeiten. In fast allen Medien (Fernsehen, Radio, Zeitungen, Zeitschriften) werden immer wieder sehr interessante Adressen bekannt gemacht. Aber Vorsicht: manchmal heißt es nur "ZDF de". In die Adressleiste müssen Sie aber eingeben: www.zdf.de. Andere Adressen werden durch Freunde und Bekannte weitergegeben, und auf einige Adressen werden Sie vielleicht beim Surfen durch das Web ganz alleine stoßen. Nachdem das Internet inzwischen in das tägliche Leben Eingang gefunden hat, finden Sie viele Adressen auch "auf Verdacht", indem Sie einfach die Namen berühmter Firmen in eine URL-gerechte Form bringen, beispielsweise www.siemens.de. Zusätzlich gibt es auch noch entsprechende Suchdienste, die später vorgestellt werden.

Wie bereits erwähnt, sind Hyperlinks bestimmte Worte, Wortfolgen eines Textes, Bilder oder Symbole die meist besonders optisch hervorgehoben werden. Außerdem verändert sich der Mauspfeil zu einer Hand, sobald Sie mit ihm über einen Link gleiten. Werden solche Worte oder Bilder angeklickt, so gelangen Sie automatisch zu einer anderen Webadresse oder zu einer anderen Textstelle im aktuellen Dokument.

Auf den meisten Webseiten finden Sie solche Verweise zu weiteren Informationsquellen. Wenn Sie diesen Links folgen, surfen Sie im Web:

1. Geben Sie oben in die Adressleiste ein: www.telefonbuch.de
2. Schließen Sie die Eingabe der ↵ Return-Taste ab.
3. Zeigen Sie auf einen Link. Oft handelt es sich bei den Verweisen um unterstrichene, farblich hervorgehobene Wörter. Aber es werden auch Grafiken zum Anklicken verwendet.



Die Maus zeigt auf einen Link

4. Der Mauszeiger verwandelt sich in eine Hand. Der Verweis kann sich auf eine andere Textstelle innerhalb der Seite, auf eine andere Seite auf dem gleichen Webserver oder auch auf eine Webseite irgendwo auf der Welt beziehen.

5. Achten Sie unten links auf die Statuszeile Ihres Explorer-Fensters. Dort unten sehen Sie den zugehörigen URL. Auf diese Weise können Sie schon vorher den Zielort erkennen.

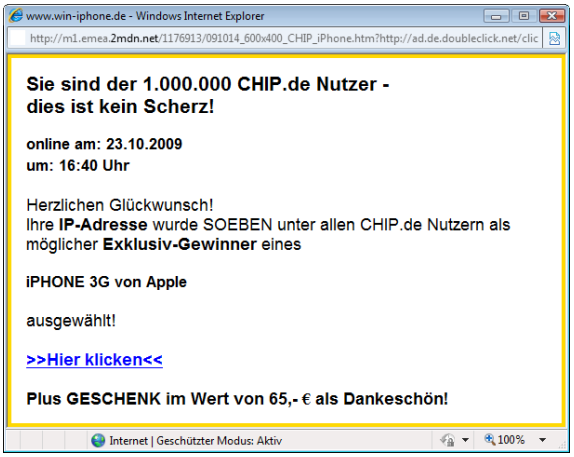
6. Führen Sie einen Klick mit der linken Maustaste aus. Der Explorer wechselt zu dem verknüpften Webdokument.

Für den Fall, dass Sie sich im Web verirren sollten: Die Startseite Ihres Explorers können Sie jederzeit wieder aufrufen, indem Sie auf das Haus in der Symbolleiste klicken. Auf der Seite 80 ist beschrieben, wie Sie die Startseiten-Adresse ändern.

4.1 Sicherheitswarnungen

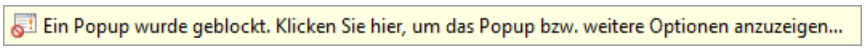
Popupblocker

Auf der Seite 8 wurden die Popups schon einmal angesprochen. Viele Internetseiten werden durch Werbung finanziert. Manchmal erscheinen zusätzliche kleine Werbefenster, die so genannten Popups. Ein typisches Beispiel sehen Sie im rechts stehenden Bild, bei dem man meinen könnte, man hätte das große Los gezogen. Dem ist aber nicht so.



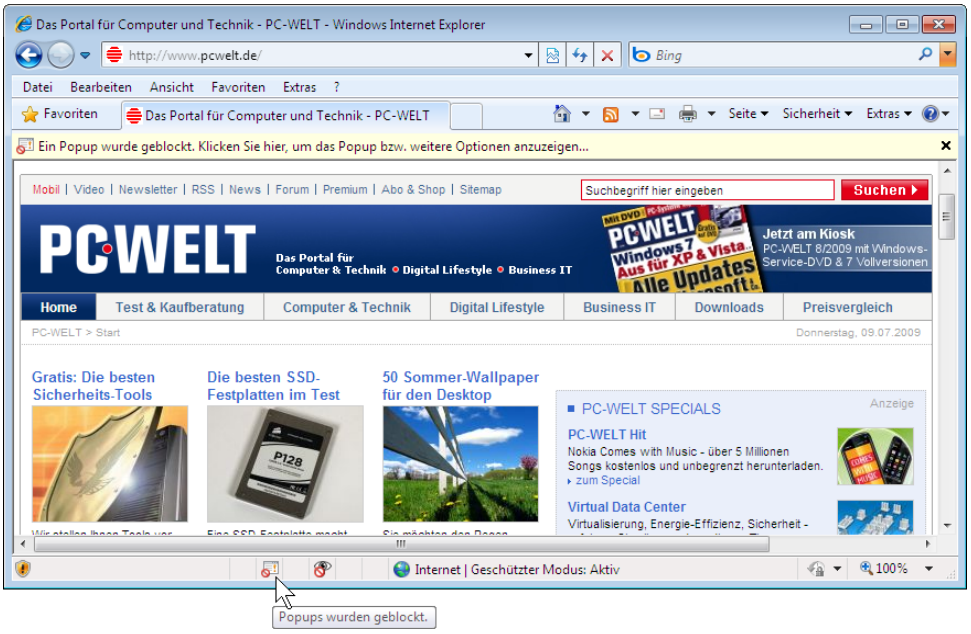
Ein typisches Popupfenster

Im Internet Explorer können die meisten Popupfenster gesperrt werden. Wenn Sie eine Website aufrufen, erhalten Sie bei geblockten Popups einen Hinweis in einer zusätzlichen Informationsleiste:



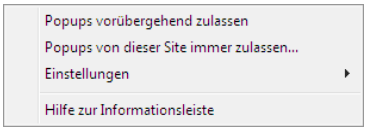
Die Informationsleiste

Darüber hinaus weist auch unten in der Statuszeile ein Symbol auf die geblockten Popups hin:



Internet Explorer mit der Informationsleiste oben und dem Blockiersymbol unten in der Statuszeile

Manchmal ist es aber einfach notwendig die Popups von einer Website zuzulassen, um weitere Informationen zu bekommen oder um ein Formular auszufüllen. Dazu klicken Sie auf die Informationsleiste oder unten auf das Symbol und wählen in dem dann erscheinenden Menü einen Befehl aus:



Popup-Menü

- **Popups vorübergehend zulassen**: Die Zusatzfenster werden jetzt und nur von dieser Website geöffnet.
- **Popups von dieser Site immer zulassen**: Die Zusatzfenster von dieser Website werden jetzt und in der Zukunft immer geöffnet. Dazu trägt dieser Befehl automatisch in den Popupblockereinstellungen die Internetadresse (URL) des Website-Betreibers ein, z.B. www.pcwelt.de.

Das Einstellen und Verwalten der Popupblockierung wird ab der Seite 87 erläutert.

Phishingwarnung (SmartScreen-Filter)

Phishing, die Computerfreaks lieben ja solche Kunstwörter, bedeutet **Passwörter fischen**. Beim Phishing sollen Sie dazu verleitet werden, persönliche oder finanzielle vertrauliche Informationen preiszugeben. Meistens bekommen Sie gefälschte, aber echt wirkende E-Mails einer Bank zugesandt, in denen Sie aufgefordert werden, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen oder Daten von Kreditkarten zurückzuschicken, oder Sie werden auf eine betrügerische Webseite geleitet, um dort diese Informationen einzugeben. Innerhalb von wenigen Minuten wird dann von den Trick-Betrügern Ihr Bankkonto über das Internet geplündert!!! Meistens geht es also darum, Ihnen Ihr Geld zu stehlen. Sollten Sie doch einmal Ihre Daten preisgegeben haben, verständigen Sie sofort Ihr Bankinstitut und lassen Sie das Konto sperren!!!

☞ Banken und andere Institute fragen niemals nach Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per E-Mail, per SMS oder telefonisch!

Aber es kann auch noch andere Gründe geben: Es möchte jemand Daten *auf* Ihrem Computer stehlen oder *über* Ihren Computer in das Netz eines Unternehmens oder einer Behörde eindringen. Die staatlichen Organe, wie Polizei und Verfassungsschutz, finden aber immer einen Weg, um an die Daten in Ihrem Computer zu gelangen.

Übrigens, da wir gerade bei dem Thema Spionage sind: Wenn Sie mit dem Notebook ins Ausland reisen, auch ins befreundete, sollten auf dem Computer nur die Daten gespeichert sein, die Sie für diese Reise unbedingt benötigen. Manchmal werden bei der Grenzkontrolle alle Informationen vom Notebook kopiert, um sie entsprechend auszuwerten. Passwörter und Daten-Verschlüsselungen stellen für die Dienste meistens kein Problem dar.

Bei eingeschaltetem Phishingfilter versucht der Internet Explorer, Sie in der Sicherheitsstatusleiste im rechten Teil der Adressleiste vor Phishing-Websites zu warnen.

Sicherheitsstatusleiste
im rechten Teil der Adressleiste

Wenn bei Microsoft bekannt ist, dass es sich bei der aktuellen Webadresse um eine Phishing-Website handelt, sehen Sie das rote Abwehrschild-Symbol .

Bekannte Phishing-Website

Sollte die Webadresse bei Microsoft noch nicht bekannt sein, aber einige Merkmale deuten wohl mutmaßlich auf eine Phishing-Website hin, erscheint das gelbe Abwehrschild-Symbol

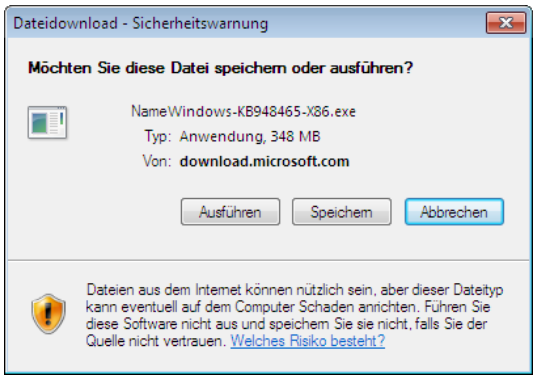
Mutmaßliche Phishing-Website

.

Auf der Seite 89 wird das Ein- und Ausschalten des Phishingfilters und ab der Seite 45 werden weitere Informationen zur Sicherheitsstatusleiste beschrieben.

Weitere Sicherheitswarnungen

Teilweise werden weitere Sicherheitshinweise vom Internet Explorer eingeblendet. Wenn diese Hinweise beim Versenden nicht vertraulicher Daten auftreten, oder wenn Daten von einer vertrauenswürdigen Quelle geladen werden sollen (etwa ein Update von einer Softwarefirma), so können Sie solche Hinweise einfach mit einem Klick auf die Schaltfläche [Ausführen] übergehen. Manchmal soll auch ein neues Zusatzprogramm (Add-On, Add-In) für den Browser installiert werden.

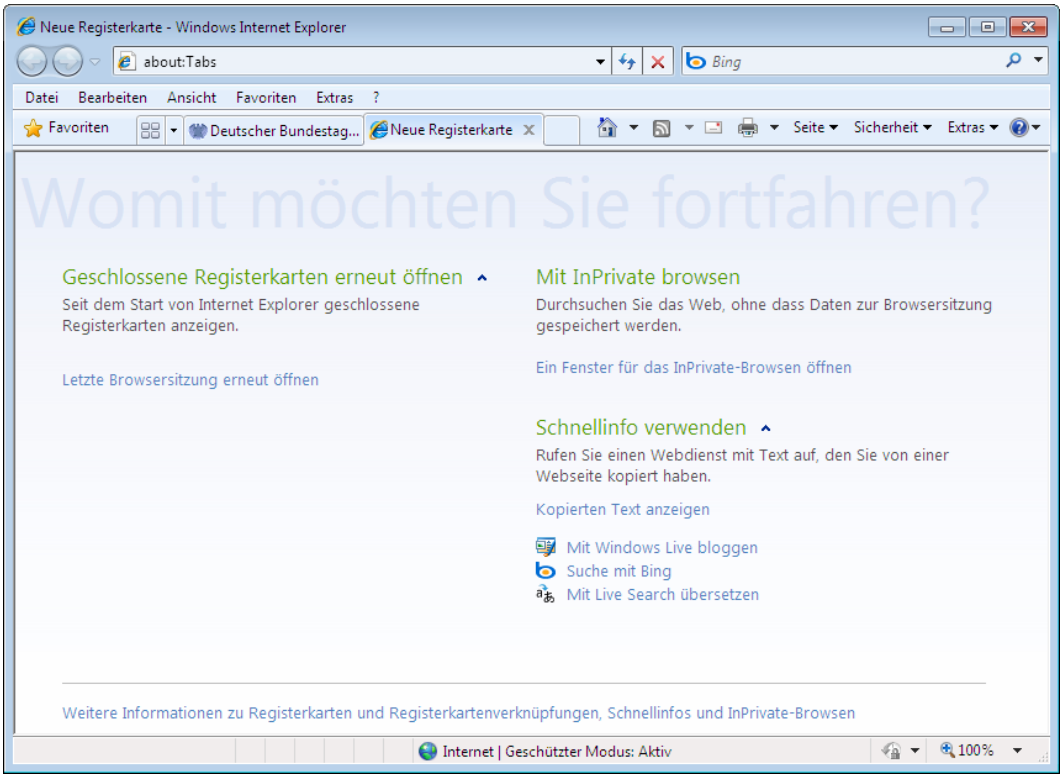


Eine Warnung

Von unbekannten Webseiten sollten Sie jedoch niemals Daten herunterladen, nachdem Sie vom Internet Explorer davor gewarnt wurden! Die verschieden Sicherheitsstufen können Sie in den **Internetoptionen** (Seite 80) einstellen.

4.2 InPrivate-Browsen – Surfen ohne Spuren

Auf der Seite 28 wurde die Schaltfläche **neue Registerkarte** bereits vorgestellt: Der Internet Explorer öffnet eine weitere Karte mit interessanten Informationen und Verknüpfungen:



Neue Registerkarte

Im linken Bereich **Geschlossene Registerkarten erneut öffnen** können Sie mit einem Klick auf die Verknüpfung (Link) **Letzte Browsersitzung erneut öffnen** wieder alle Webseiten auf Ihren Bildschirm holen, die beim letzten Schließen des Internet Explorers noch geöffnet waren.

Der Browser merkt sich also, welche Webseiten Sie besuchen und darüberhinaus noch viele weitere Informationen. Aber vielleicht ist Ihnen das ja garnicht recht? Wenn Sie beispielsweise für Ihre Partnerin, Ihren Partner gestern ein Geburtstagsgeschenk über das Internet gekauft haben und heute kann sie/er im Internet Explorer nachträglich herausfinden, was es denn für ein Geschenk sein wird, geht die Überraschung verloren. Und das ist sicherlich noch eine harmlose Form der Datenüberwachung.

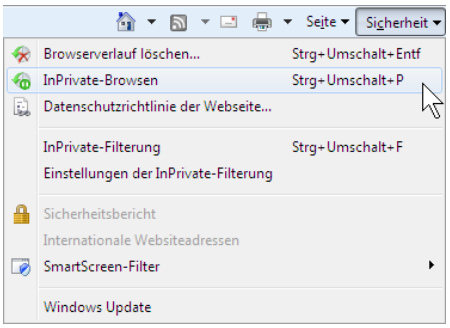
Wenn nun auf einer neuen Webseite der Internet Explorer diese ganzen Informationen nicht festhalten soll, klicken Sie im rechten Bereich auf den Link **Ein Fenster für das InPrivate-Browsen öffnen**. Es erscheint ein neues Fenster:

InPrivate-Browsen in einem neuen Fenster

Sie können ein **InPrivate**-Fenster aber auch über die Schaltfläche [Sicherheit] in der Symbolleiste (Bild rechts) oder mit der Tastenkombination

[Strg]+[⇧]+[P] öffnen.

An der Schaltfläche InPrivate in der Adressleiste und an dem Hinweis [**InPrivate**] in der Titelleiste erkennen Sie die neue Datenschutz-Vorkehrung.



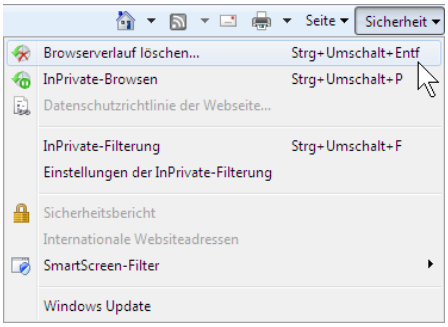
Ein InPrivate-Fenster öffnen

Damit wird verhindert, dass der Browserverlauf (Seite 76), temporäre Internetdateien (Seite 9), Formulardaten (Seite 45), Cookies (Seite 9) sowie Benutzernamen und Kennwörter vom Internet Explorer gespeichert werden, sodass es keine Anhaltspunkte zum Suchverhalten des Anwenders oder den Verlauf gibt.

Den Browserverlauf löschen

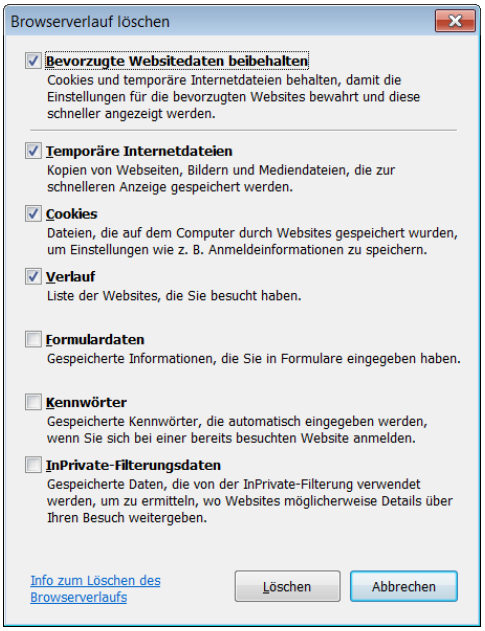
Die gespeicherten Daten, die gerade vorher genannt wurden, können Sie aber auch in einem Nicht-**InPrivate**-Fenster löschen. Dazu klicken Sie jederzeit auf die Schaltfläche [Sicherheit] in der Symbolleiste und wählen den im rechten Bild gezeigten Befehl, oder Sie drücken die Tastenkombination

[Strg]+[⇧]+[Entf].



Den Browserverlauf löschen

Es wird das nachfolgende Dialogfenster (Dialogfeld) geöffnet:



Kontrollkästchen aktivieren bzw. deaktivieren

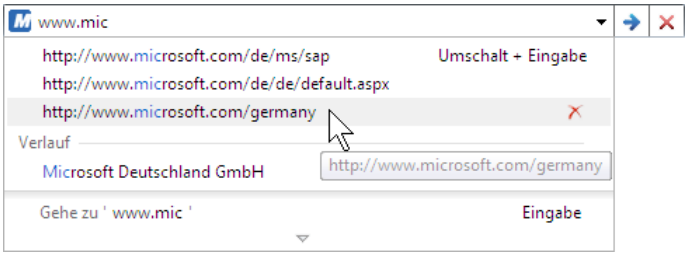
Aktivieren ☑ bzw. deaktivieren ☐ Sie die entsprechenden Kontrollkästchen, und klicken Sie dann auf die Schaltfläche [Löschen]. Danach ist es sehr zu empfehlen auch den Internet Explorer ☒ zu schließen! (auch Seite 14)

4.3 Eine weitere Internet-Tour

Am besten machen Sie sich mit dem Internet Explorer mit einer weiteren kleinen Web-Sitzung vertraut. Das folgende Beispiel führt Sie zu den Seiten der Firma Microsoft. Sie können den Microsoft-Besuch auf der aktuellen oder auf einer neuen Registerkarte öffnen. Löschen Sie aber vorher die Registerkarten, die Sie nicht mehr benötigen. Sollte der Internet Explorer geschlossen sein, starten Sie ihn wieder, wie es auf der Seite 13 beschrieben ist.

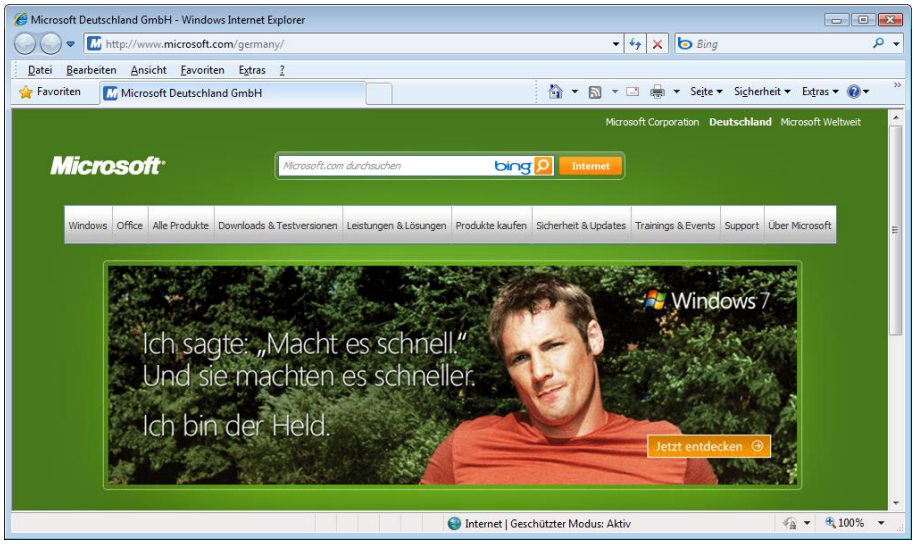
Auf der aktuellen Registerkarte öffnen

Geben Sie in die Adressleiste www.microsoft.com/germany ein, und schließen Sie die Eingabe mit der [↵] Return-Taste ab. Sollte sich unterhalb der Adressleiste nach dem Eintippen der ersten Zeichen eine Liste öffnen, dann haben Sie vorher schon einmal Adressen eingegeben, die mit diesen Zeichen beginnen. Ist die gewünschte Adresse dabei, klicken Sie auf diese Zeile. Sie sparen sich so das weitere Eintippen:



Aus einer Liste auswählen

Übrigens: Auch die Eingabe www.microsoft.de hätte Sie auf die richtige Seite geführt. Besonders die großen Firmen haben meistens mehrere Webadressen. Der Internet-Server der Firmen leitet Sie automatisch an die richtige Stelle.



Eine Homepage von Microsoft

Auf einer neuen Registerkarte öffnen

Um eine Webseite auf einer neuen Registerkarte zu öffnen, geben Sie in der aktuellen Adressleiste die URL vollständig ein, schließen aber die Eingabe mit der Tastenkombination Alt+↵ ab!

Bei dieser Vorgehensweise können Sie allerdings nicht aus der oben beschriebenen Liste eine Adresse auswählen. Eine Webseite aus der Liste wird immer in der aktuellen Registerkarte geöffnet. Wenn die Liste erscheinen soll, klicken Sie erst auf diese Schaltfläche , und eröffnen eine neue Registerkarte. Nun geben Sie die ersten Buchstaben ein und wählen aus der Liste aus, wie es oben gemacht wurde.

Bis die Seite vollständig auf Ihrem Bildschirm erscheint, vergeht manchmal etwas Zeit. Dies hängt von der Übertragungsgeschwindigkeit Ihres Internetzugangs ab. Während der Ladedauer sehen Sie einen optischen Hinweis unten in der Statuszeile. Zusätzlich dreht sich ein türkis-farbiger Kreis in dem Tab der Registerkarte und am Mauszeiger.

Der Internet Explorer lässt beim Einladen einer Seite aus dem Web die darin eingebundenen Grafiken zunächst einmal außen vor. Diese sind für den eigentlichen Informationsgehalt der entsprechenden Seite in der Regel nicht dringend erforderlich. Grafiken benötigen allerdings den größten Teil der Übertragungszeit. Wenn alle Textinformationen vorhanden und lesbar sind, werden die Seiten mit den Bildern ergänzt.

Ein Computer, der Ihnen im Internet Daten übermittelt, wird in der Fachsprache Web- oder Internet-Server genannt.

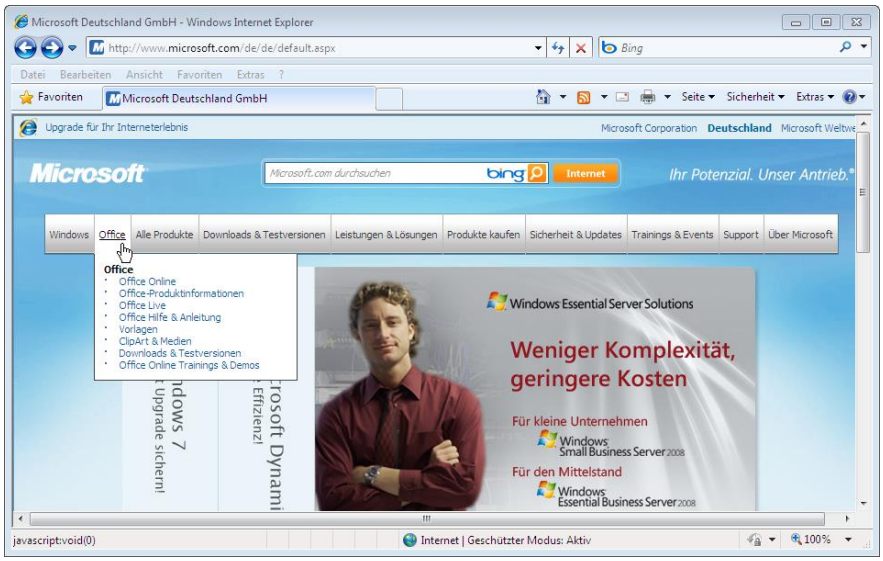
Da sich die Internetseiten ständig ändern, wird die Homepage der Firma Microsoft, die Sie in der Abbildung sehen, vermutlich anders aussehen. Das ist aber nicht von Bedeutung. Hier geht es lediglich um die grundsätzliche Vorgehensweise.

Um in den Vollbildmodus zu schalten, drücken Sie die F11-Taste. Der Internet Explorer passt die Elemente an die neue Fenstergröße an. Mit der Tastenkombination Strg+⇆-Tabtaste wechseln Sie auch im Vollbildmodus zwischen den geöffneten Registerkarten. Die F11-Taste bringt Sie wieder in den Normalmodus zurück.

4.4 Verknüpfungen und Registerkarten

Von der Homepage aus können Sie nun zu bestimmten Themen der Firma Microsoft gelangen. Zum nachfolgenden Beispiel kommen Sie, wenn Sie in der Navigationsleiste auf den Link **Office** zeigen und in dem aufgeklappten Menü auf eine Verknüpfung klicken:

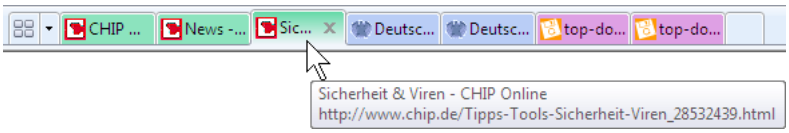
- Wenn Sie mit der linken Maustaste und ohne zusätzliche Taste auf einen Link klicken, wird in der Standardeinstellung die verknüpfte Webseite in der *aktuellen* Registerkarte geöffnet. Dies kann allerdings von den Webgestaltern auch anders festgelegt werden. Über diese Schaltfläche kommen Sie wieder auf vorherige Webseiten zurück.
- Drücken Sie zusätzlich mit der linken Maustaste die Strg-Taste, wird das verknüpfte Webdokument auf einer *neuen* Registerkarte geöffnet. Oder Sie drücken nur die mittlere Radtaste allein, ohne Strg-Taste. Eventuell müssen Sie noch oben auf den neuen Tab klicken, damit die neue Registerkarte im Vordergrund steht. Dies kann aber in den **Internetoptionen** (Seite 80) eingestellt werden.
- Soll die Verknüpfung in einem ganz neuen, zusätzlichen Explorerfenster geöffnet werden, dann drücken und halten Sie zuerst die ⇧-Taste (Umschalt- oder Shift-Taste) und klicken dabei auf eine Verknüpfung.



Navigation bei Microsoft

Registerfarben (Tab-Gruppierung mit Farbcodes)

Wenn Sie ein verknüpftes Webdokument auf einer *neuen* Registerkarte öffnen, werden oben in der Registerleiste die Kartenreiter (Registerlasche oder auch Tab), die zu einem Thema gehören, in einer einheitlichen Farbe dargestellt. Dadurch erkennen Sie auf den ersten Blick, welche Registerkarten thematisch zusammengehören, z.B.:



Registerkarten-Gruppierung

4.5 Vorwärts und Zurück

Um zu der vorherigen Webseite zurückzukehren, klicken Sie oben links auf die Schaltfläche **Zurück**. Mit der entsprechenden Anzahl an Mausklicks auf diese Schaltfläche kommen Sie oft, aber nicht immer, auf die Ausgangsseite zurück.

Über die Schaltfläche **Vorwärts** gehen Sie wieder eine Seite nach vorn, aber es sind immer nur Webseiten, die Sie seit dem Öffnen dieser Registerkarte bereits besucht haben.

Oder Sie klicken auf den Listenpfeil neben der Schaltfläche **Vorwärts** und wählen aus der sich öffnenden Liste direkt eine vorher besuchte Webseite aus.

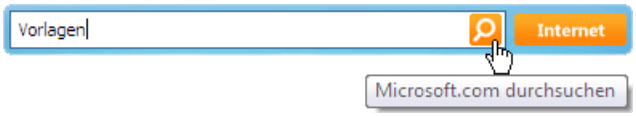
Wenn Sie diese Schaltflächen anklicken, muss der Explorer die zuletzt betrachteten Seiten nicht erneut laden, sondern hält sie sofort bereit. Das funktioniert, weil er diese Seiten auf dem Speicher Ihres eigenen Rechners (Cache) kurzzeitig ablegt. Der Vorteil ist, dass die Seiten mit den Verweisen (Links) dabei voll funktionsfähig bleiben.

Aktualisieren

Wenn Sie den Verdacht haben, dass die angezeigte Webseite nicht auf dem neuesten Stand ist, so können Sie über die Taste F5, über die Schaltfläche **Aktualisieren** in der Adressleiste oder über den Menüweg **Ansicht**, **Aktualisieren** die Webseite neu laden.

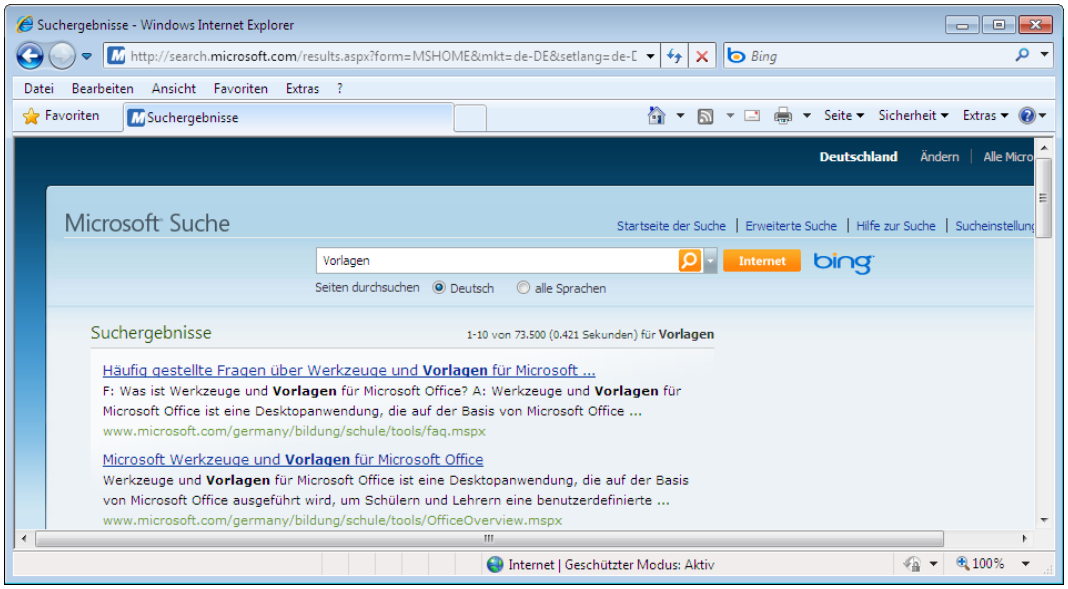
4.6 Suchen innerhalb einer ganzen Website

Besonders bei einem sehr großen Informationsangebot bieten die Betreiber einer Website (hier Microsoft) eine Suchmöglichkeit. Geben Sie in das Suchfeld im Microsoft Webdokument einen Begriff ein, z.B. **Vorlagen**, und klicken Sie auf die Suchen-Schaltfläche. Wie bei allen anderen Themen kann allerdings die Internetseite bereits wieder verändert worden sein, wenn Sie diesen Text lesen.



Suchfeld

Dieses Suchfeld innerhalb einer Website darf aber nicht mit der Suche im Internet Explorer ganz oben rechts verwechselt werden. In diesem Feld wird nach Begriffen im *ganzen* Internet gesucht. Diese Websuche wird ab der Seite 58 vorgestellt.



Suchergebnisse

4.7 Nach Texten auf der aktuellen Seite suchen

Über den Menüweg **Bearbeiten**, **Auf dieser Seite suchen** oder mit der Tastenkombination Strg+F können Sie nach Texten nur in der aktuellen Webseite suchen:

Nach Texten im aktuellen Webdokument suchen

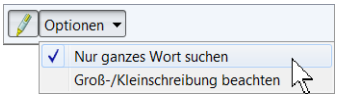
Tragen Sie in die oben stehende Dialogleiste den Suchtext ein. Die Suche starten Sie über die Schaltfläche Weiter. Wenn der Explorer die Suchdaten gefunden hat, wird der Text markiert. Danach klicken Sie wieder auf Weiter. Über die Schaltfläche Zurück gehen Sie in der Suchrichtung wieder nach oben.

Optionen in der Dialogleiste Suchen

Alle Übereinstimmungen hervorheben: Wenn diese Schaltfläche eingedrückt, also aktiviert ist, werden *alle* gefundenen Suchbegriffe markiert. Mit einem Mausklick aktivieren bzw. deaktivieren Sie eine Schaltfläche.

Nur ganzes Wort suchen: Bei eingeschaltetem Kontrollkästchen markiert der Explorer keine Texte, die nur Teil eines Wortes sind.

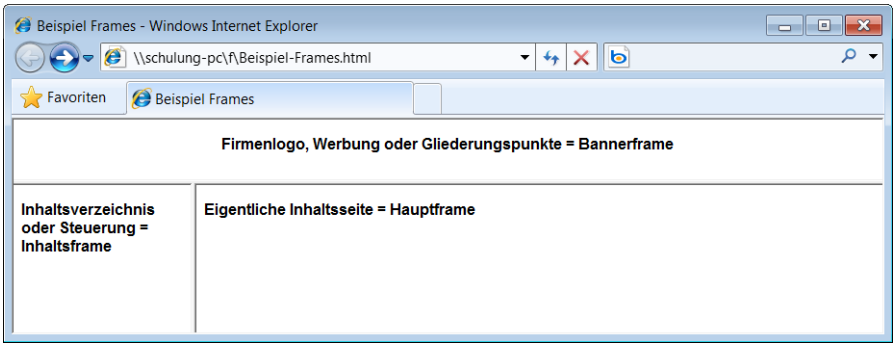
Groß-/Kleinschreibung beachten: Bei ausgeschaltetem Kontrollkästchen wird die Groß- oder Kleinschreibung des Suchtextes ignoriert.



Optionen

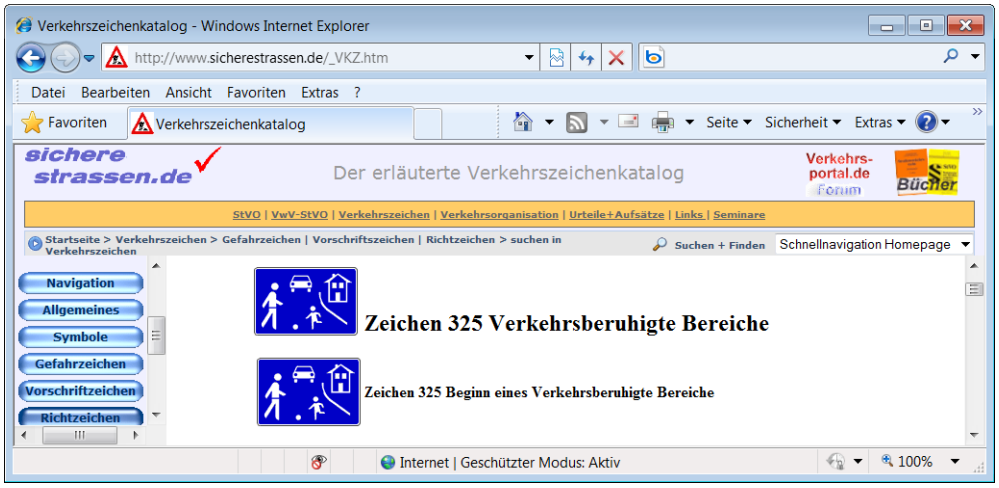
4.8 Frames

Mit Frames (Rahmen) haben die Webdesigner eine Möglichkeit, das Browser-Fenster in mehrere Unterfenster zu unterteilen. In jedem dieser Unterfenster kann eine andere HTML-Seite platziert werden. In einem der Frames wird ein Inhaltsverzeichnis angezeigt, beim Klick auf einen Link im Inhaltsverzeichnis sehen Sie die dazugehörende Seite in einem anderen Rahmen. Die Struktur sieht vielleicht folgendermaßen aus:



Schematische Darstellung eines Framesets

Eventuell ist in jedem Frame eine Bildlaufleiste zum Blättern zu sehen. Dies kann aber von Ihnen nicht beeinflusst werden, es wird von den Webseiten-Gestaltern festgelegt.



Ein Beispiel für ein Frameset

Sollte die Radmaus zum Blättern und Zoomen in Frameseiten nicht wie erwartet funktionieren, dann ist vielleicht in dem Moment der gewünschte Rahmen nicht das aktive Element. Klicken Sie in den Frame hinein, aber nicht auf eine Verknüpfung. Danach sollte das Blättern und Zoomen auch mit der Radmaus funktionieren.

4.9 Text kopieren

Sie können häufig einzelne Textteile oder auch den ganzen Text einschließlich der Bilder und Verknüpfungen auf einer Webseite in die Windows-Zwischenablage kopieren und diesen Text beispielsweise in ein Worddokument einfügen. Die Zwischenablage wird von allen Dokumenten benutzt. Damit haben Sie die Möglichkeit, Text zwischen verschiedenen Programmen auszutauschen. Zum Ausprobieren starten Sie Word, WordPad, OpenOffice.org Writer oder ein anderes Textprogramm mit einem leeren Dokument, ohne den Internet Explorer zu schließen.

Text markieren

Wechseln Sie wieder in den Internet Explorer, über die Taskleiste oder mit der Tastenkombination [Alt]+[⇆] Tabtaste. Zuerst muss der zu kopierende Text markiert werden. Hierzu stehen Ihnen zum Teil die Möglichkeiten zur Verfügung, die Sie vielleicht aus einem Textprogramm kennen. Ein gravierender Unterschied ist aber zu beachten: Es gibt keinen Cursor (Eingabemarke) wie in Word, da Sie natürlich im Internet Explorer direkt keinen Text eingeben können, außer in einem extra dafür vorgesehenen Formular. Hier verschiedene Methoden, um Elemente auf einer Webseite zu markieren:

- Zeigen Sie mit der Maus vor das erste Zeichen, an dem die Markierung beginnen soll. Aber zeigen Sie nicht auf eine Verknüpfung. Bei gedrückter linker Maustaste ziehen Sie die Maus über den Text. Wollen Sie dabei auch Teile einschließen, die nicht im sichtbaren Bildschirmbereich stehen, bewegen Sie den Mauszeiger einfach über den Fensterrand hinaus. Wenn der gewünschte Bereich markiert ist, lassen Sie die Maustaste wieder los.
- Mit einem Doppelklick (2x) wird ein Wort und mit einem Dreifachklick (3x) ein ganzer Absatz markiert.
- Oder Sie markieren mit einem Doppelklick das erste Wort, an dem die Markierung beginnen soll, aber nicht eine Verknüpfung. Bei gedrückter ⇧-Taste klicken Sie dann an das Ende des Textbereichs.

☞ Falls Sie den markierten Bereich *nachträglich* vergrößern oder verkleinern wollen, müssen Sie *zuerst* die ⇧-Taste drücken und *festhalten* und nun das neue Ende der Markierung mit einem Mausklick festlegen.

- Mit der Tastenkombination Strg+A oder über Menü **Bearbeiten**, **Alles auswählen** können Sie die komplette *aktuelle* Webseite markieren.

Nach der Text-Markierung ist Ihnen vielleicht das rechts stehende Symbol neben der Markierung aufgefallen. Mit dieser Schaltfläche für **Schnellinfos**, auch **Smart-Tag** genannt, möchte der Internet Explorer Ihnen die Arbeit zusätzlich erleichtern. Weitere Informationen stehen auf der Seite 48.

Schnellinfo

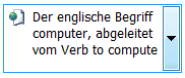
In die Zwischenablage kopieren
Mit den üblichen Befehlen kopieren Sie den markierten Bereich in die Zwischenablage:

- Tastenkombination Strg+C oder
- Menü **Bearbeiten**, **Kopieren** oder
- mit der *rechten* Maustaste auf die Markierung klicken und aus dem Kontextmenü den Befehl **Kopieren** auswählen.

Text einfügen
Wechseln Sie wieder über die Taskleiste oder mit der Tastenkombination Alt+⇆ Tabtaste in das Textprogramm. *Links von der Cursorposition* wird der Inhalt einer Zwischenablage eingefügt:

- Symbol **Einfügen** aus der Symbolleiste (Programm abhängig) oder
- Tastenkombination Strg+V oder
- Menü **Bearbeiten**, **Einfügen** (Programm abhängig) oder
- Kontextmenü mit *rechter* Maustaste, **Einfügen** oder
- falls geöffnet, ein Symbol aus dem Aufgabenbereich **Zwischenablage** anklicken (Programm abhängig).

Symbol Einfügen in Word 2007



Ein Eintrag in der Office Zwischenablage im Aufgabenbereich

Drag and Drop

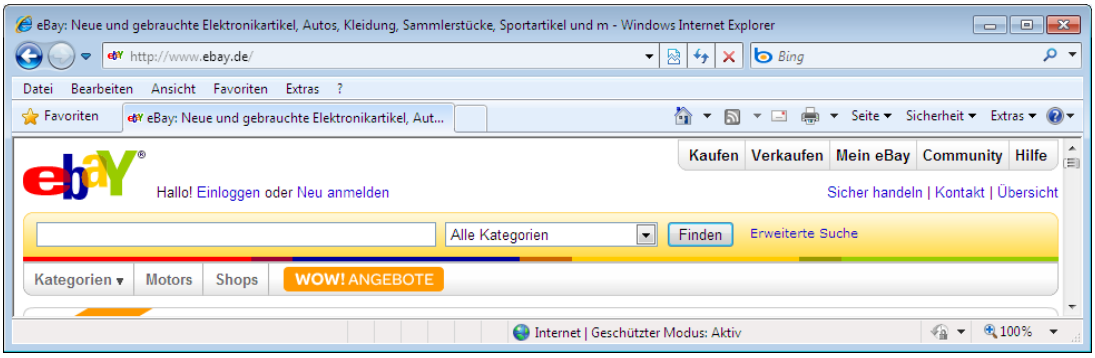
Mit der Editierfunktion Drag and Drop haben Sie noch eine weitere Möglichkeit, mit der Maus Textteile zu kopieren. Als Drag and Drop (Ziehen und Fallenlassen) wird das Kopieren eines *markierten* Textes bei gedrückter *linker* Maustaste bezeichnet.

Dazu platzieren Sie die beiden Fenster **Word** und **Internet Explorer** im Wiederherstell-Modus neben- oder untereinander, markieren den Text im Explorer und ziehen den markierten Text in das Wordfenster. In Word wechselt der Mauszeiger beim Ziehen sein Aussehen, und in der Word-Statuszeile erscheint die Frage: „Wohin kopieren?“ Durch eine kleine Markierung wird die Einfügestelle in Word dargestellt und beim Loslassen der Maustaste das Element abgelegt.

Falls allerdings bei diesem Vorgang eine Sicherheitsmeldung erscheint, klicken Sie auf die Schaltfläche [Zulassen]. Nun müssen Sie das Drag and Drop noch einmal durchführen.

4.10 Handel (eCommerce)

Immer stärker wird das Internet auch für den Handel eingesetzt. Die umfangreichen Kataloge der traditionellen Versandhandelshäuser können Sie jetzt auch (oder nur noch) im Web einsehen und dort auch gleich bestellen. Die Bezahlung erfolgt allerdings häufig noch auf traditionellen Wegen, da doch noch teilweise Bedenken bestehen, die Kreditkartendaten im Internet weiterzugeben. Sehr große Zuwachsraten verzeichnen die Auktionen im Internet. Auf diesen Marktplätzen können Sie neue oder gebrauchte Waren aller Art anbieten oder kaufen:



Auktionen bei eBay

Gefahren des Internet-Handels

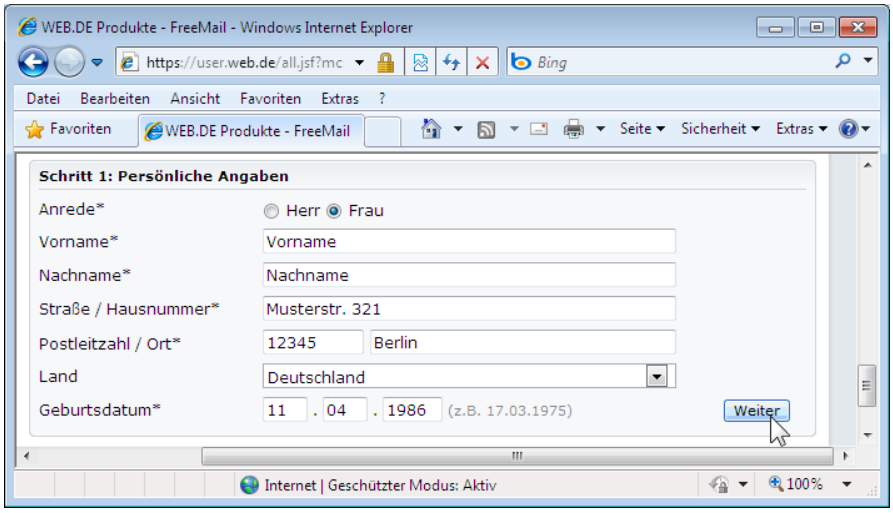
Leider ist das Internet auch immer mehr zum Tummelplatz für Betrüger geworden. Es sind nicht nur die bereits erwähnten gefälschten E-Mails, in denen Sie aufgefordert werden, Ihre Online-Banking- oder Kredtikarten-Daten anzugeben. Oft genug verlangen die Verkäufer Vorauskasse und der Käufer bekommt nichts geliefert. Dabei werden auch häufig sehr phantasievolle Tricks angewendet, um an Ihr Geld zu kommen. Extrem vorsichtig sollten Sie sein, wenn der Verkäufer seinen Sitz im Ausland hat und/oder Sie auf ein Bankkonto im Ausland überweisen sollen, da Sie nur selten jemanden im Ausland belangen können. Es fallen auch immer noch Leute auf den Trick herein, man möge doch bei einem geheimnisvollen Geldtransfer aus dem Ausland behilflich sein, aber man solle vorher bitteschön 3.000,- $ als Spesen überweisen. Danach bekäme man ganz sicherlich 1, 2 ja 10 Millionen $ auf seinem Konto gutgeschrieben.

Häufig sind es auch die vermeintlich kleineren Beträge von 50,- oder 100,- € mit denen einige Leute große Gewinne machen. Viele Geschädigte scheuen sich wegen dieser Beträge die Gerichte anzurufen und zahlen lieber die Rechnung, um keinen Ärger mehr zu haben. Aber man muss halt vorher schon sehr vorsichtig sein, damit ein angeblich "kostenloses" Angebot (Free-Irgendwas) sich nicht als ein kostenpflichtiges Abonnement für zwei Jahre entpuppt. Lesen Sie sich die betreffenden Webseiten ganz genau durch, einschließlich der kleingeschriebenen oder versteckten Texte. Und auch die unbeliebten AGBs (Allgemeine Geschäftsbedingungen) sollten Sie besonders genau studieren.

Natürlich gibt es die gleichen Probleme auch beim Handel außerhalb des Internets. Aber durch die Anonymität der Handelspartner und das vielfältige Angebot sind die Gefahren doch deutlich größer. Die großen Internet-Auktionshäuser, z.B. eBay, bieten online viele Informationsmöglichkeiten über den Internet-Handel. Diese Informationen sollten Sie unbedingt nutzen. Und am besten fragen Sie auch im Bekannten- und Kollegenkreis die erfahrenen Internet-Käufer, auf welche Stolpersteine Sie achten sollten.

4.11 Ein Formular ausfüllen

Beim Surfen im Internet, beim Einkaufen im Web oder bei einem Behördengang, den Sie vielleicht schon von Hause aus über das Web erledigen können, sind hin und wieder Formulare auszufüllen. Oder Sie möchten für sich privat eine Free-Mail-Adresse einrichten, beispielsweise bei www.web.de:

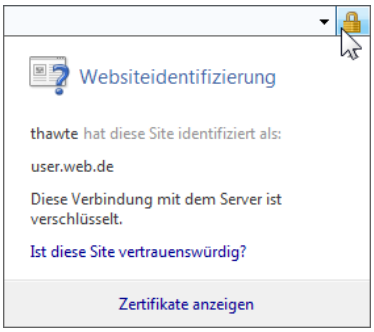


Ein Formular ausfüllen

Geben Sie Ihre Daten in die entsprechenden Felder ein, oder wählen Sie sie aus einem Listenfeld ▼ aus. Mit der Maus oder noch besser mit der [⇥] Tabtaste springen Sie die einzelnen Felder an. Die Tastenkombination [⇧]+[⇥] Tabtaste führt Sie wieder ein Feld zurück. Nach dem Abschluss klicken Sie im Formular auf eine Schaltfläche, z.B. [Weiter] oder [Abschicken]. Falls das Formular aus mehreren Seiten besteht, gibt es im Regelfall die Schaltfläche [Zurück], damit Sie Ihre Eingaben auch berichtigen können. Möchten Sie die Formulareingabe vorzeitig abbrechen, dann schließen Sie einfach diese Registerkarte ✕ oder den Internet Explorer ✕.

4.12 Sicherheitsstatusleiste

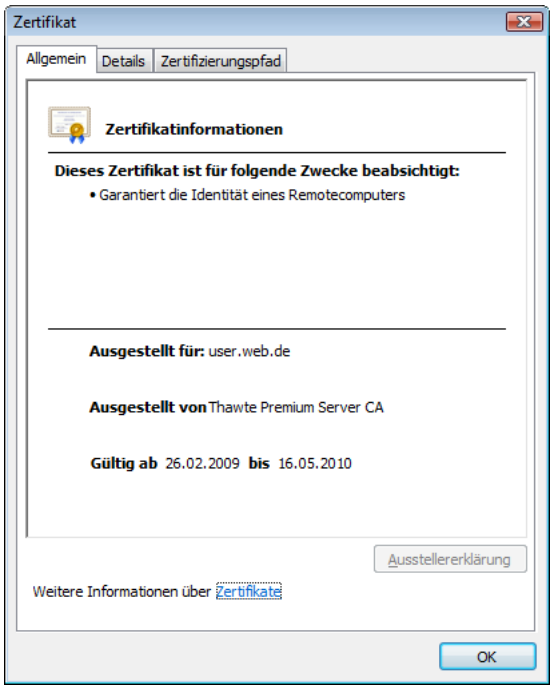
In dem oberen Bild sehen Sie am Anfang der Adressleiste die Art des Protokolls: **https**. Dabei steht das **s** für Sicherheit. Zusätzlich weist noch ein Vorhängeschloss 🔒 in der so genannten **Sicherheitsstatusleiste** im rechten Teil der Adressleiste auf diese *einigermaßen* abhör- und fälschungssichere Übertragung der Daten hin. Mit einem Klick auf das **Schloss** bekommen Sie die im rechten Bild zu sehenden Informationen angezeigt. Achten Sie bitte darauf, dass bei allen sensiblen Transaktionen immer diese Sicherheitshinweise im Internet Explorer angezeigt werden, beispielsweise bei der Eingabe von persönlichen Daten, bei Kreditkarten-Angaben oder bei der Abwicklung von Bank-



Diese Sicherheitsinformationen bekommen Sie mit einem Klick auf das Schloss

geschäften.

Bei dem HTTPS-Protokoll werden die Daten zwischen Webserver und dem Internet Explorer verschlüsselt übertragen. Die geschützte Identifikation und Authentifizierung des Webservers kann durch ein **Zertifikat angezeigt** werden. Dazu klicken Sie in dem Rahmen **Websiteidentifizierung** auf die Verknüpfung am unteren Rand. Das nachfolgende Dialogfenster wird geöffnet:



Zertifikatsinformationen

Das Zertifikat, das zum Verschlüsseln der Verbindung verwendet wird, enthält auch Informationen über die Identität des Betreibers der Website oder der zugehörigen Organisation.

Besonders beim Online-Banking ist es üblich, ein noch strengeres Verfahren zur Identifikation und Authentifizierung des Webservers durchzuführen. Dies erkennen Sie an der **grünen Hintergrundfarbe** in der Adressleiste und in der Sicherheitsstatusleiste:

Eine besonders sorgfältige Identifizierung erkennen Sie an der grünen Hintergrundfarbe

Umgekehrt bedeutet eine **rote Hintergrundfarbe**, dass das Zertifikat nicht gültig ist, es kann beispielsweise gefälscht worden sein. In dem Fall sollten Sie diese Webseite sofort schließen. Bei einer **gelben Hintergrundfarbe** kann das Zertifikat nicht überprüft werden. Auch das ist problematisch.

Aber: Trotz der vielfältigen Bemühungen der Fachleute, eine größere Sicherheit im Internet duch die verschiedensten Verfahren zu erreichen, muss immer wieder daraufhin gewiesen werden:

Es gibt keine absolute Sicherheit im Internet!!!

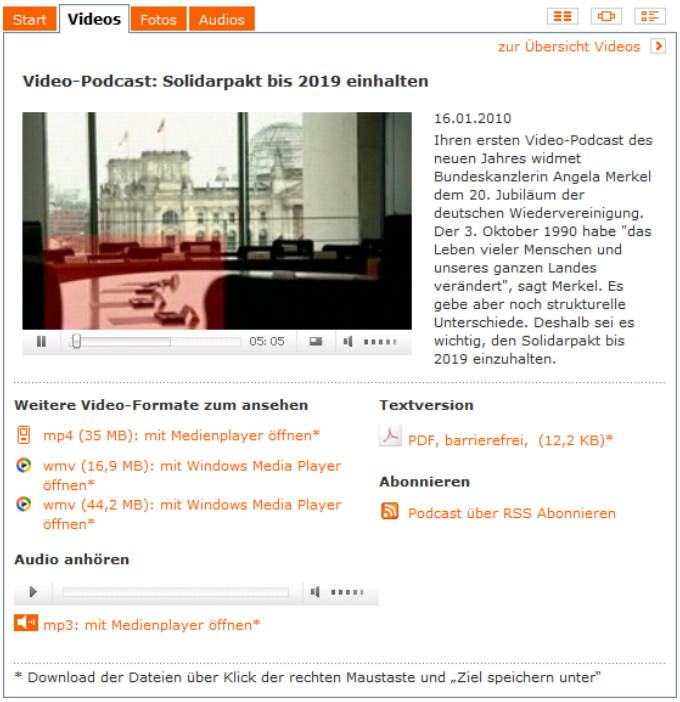
Sie können besonders durch Ihr eigenes Verhalten versuchen, sich vor den Betrügereien zu schützen. Rufen Sie möglichst nur Webseiten auf, denen Sie vertrauen können.

4.13 Blog und Podcast – neue Darstellungsformen

Ein **Blog** ist eine Abkürzung der Wörter **Web** und **Logbuch**, auch **Weblog** genannt. Wie bei einem Tagebuch werden auf einer Blog-Webseite Informationen meist in chronologischer Reihenfolge dargestellt. Ein typisches Beispiel: Die Seminarleiterin stellt in ein paar Worten noch einmal den vergangenen Seminartag dar. Darüber hinaus werden auch weiterführende Links für die Seminarteilnehmer in den Blog gestellt oder auch andere Informationen, die für das Seminar wichtig sind.

Auch **Podcast** oder **Podcasting** sind Kunstwörter, gebildet aus dem Namen des Kult-MP3-Players **iPod** der Firma Apple und dem englischen Wort **broadcasting**, das wohl in diesem Zusammenhang mit Rundruf am besten übersetzt wird. Beim Podcasting werden Mediendateien im Internet zum Anschauen und Anhören meist kostenlos angeboten. Ein Podcast ist also eine kurze Audio-/Videodatei, man kann auch sagen ein Audio-/Videoschnipsel, das auch zum Abspielen auf mobilen Geräten geeignet ist, wie Handy und iPod.

Das Presse- und Informationsamt der Deutschen Bundesregierung veröffentlicht jeden Samstag ein neues Podcast (www.bundeskanzlerin.de):



Podcasting des Presse- und Informationsamtes der Bundesregierung (Ausschnitt)

Interessant sind die verschieden Formen, in denen hier das Podcast angeboten wird:

- Flash-Player: Hierzu ist die einmalige Installation des kostenlosen Add-On-Programms Adobe Flash Player Voraussetzung. Das Podcast kann direkt in dem Flash-Fenster oben auf dieser Webseite angeschaut und angehört werden, eine Speicherung ist nicht vorgesehen. Gesteuert wird das Video über die Recorder-Icons am unteren Flash-Fensterrand:

Steuerung

- Video-Podcast (mp4): Diese Datei kann heruntergeladen und gespeichert und damit auch auf ein mobiles Gerät kopiert werden. Ein Programm zum Abspielen von mp4-Dateien gehört nicht zum Standardumfang von Windows.

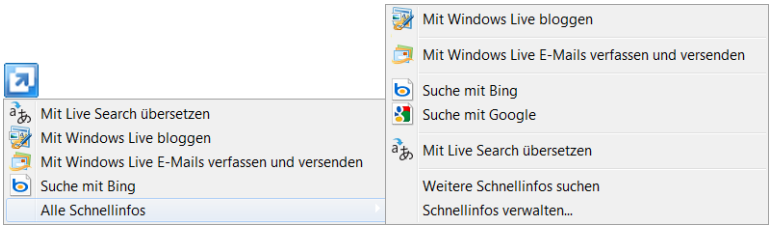
- Video-Podcast (wmv): Mit einem Links-Klick auf diese Verknüpfung wird die Datei in dem Programm Windows Media Player in einem eigenen Fenster abgespielt. Möchten Sie diese Datei herunterladen und speichern, klicken Sie mit *rechts* auf diesen Link und wählen im Kontextmenü den Befehl **Ziel speichern unter**.
- Audio-Podcast (mp3): Das Podcast wird im Windows Media Player abgespielt.
- Textversion: PDF-Dokument, das Sie speichern und mit dem kostenlosen Programm Adobe Reader öffnen können.
- RSS-Abonnement: Das Thema RSS-Feed wird ab der Seite 77 besprochen.

4.14 Schnellinfos

Auf der Seite 43 wurde bereits auf die Schaltfläche **Schnellinfo** hingewiesen, die nach einer Auswahl in der Nähe der Markierung erscheint. Welche Möglichkeiten sich hinter diesem Symbol verstecken, soll an einem Beispiel gezeigt werden:

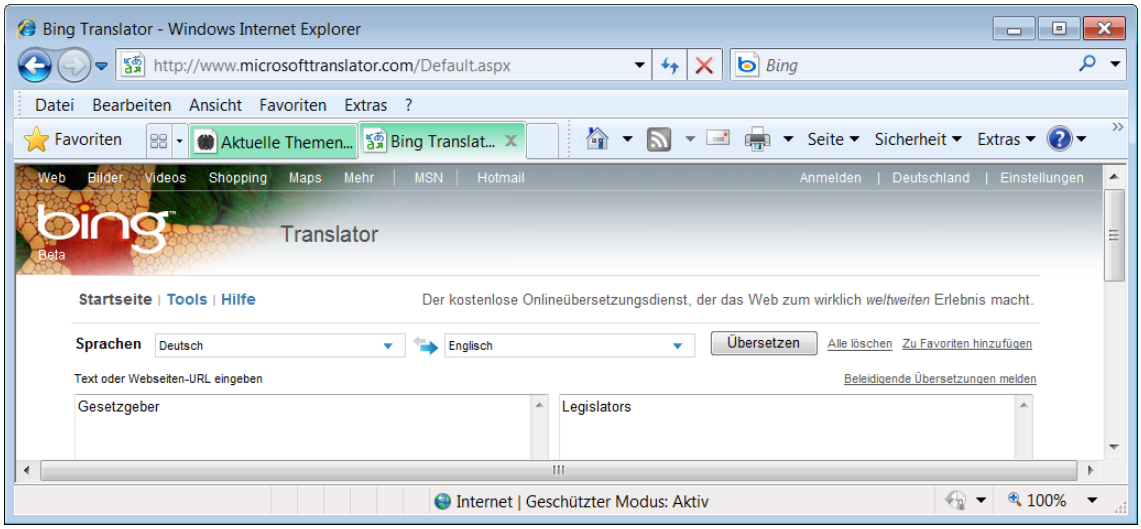
Schnellinfo

1. Auf einer Webseite des Deutschen Bundestages markieren Sie mit einem Doppelklick das Wort **Gesetzgeber** oder ein anderes beliebiges Wort.
2. Klicken Sie auf die Schaltfläche **Schnellinfo** und in dem geöffneten Menü auf den Befehl **Mit Live Search übersetzen**.



Schaltfläche Schnellinfo mit geöffnetem Menü

3. Nach einer kurzen Wartezeit wird auf einer neuen Registerkarte der **Translator** geöffnet.
4. Klicken Sie bei der Sprachenauswahl auf die kleinen blauen Pfeile ▾, und wählen Sie die Übersetzung vom Deutschen ins Englische aus.
5. Danach klicken Sie auf die Schaltfläche [Übersetzen]:



Schaltfläche Schnellinfo mit geöffnetem Menü

Das Ein- und Ausschalten der Schaltfläche **Schnellinfo** und die Verwaltung ist in den **Internetoptionen** ab der Seite 84 beschrieben.

4.15 Übungen

1. Schauen Sie sich doch einmal bei Apple um. Die Adresse lautet:
   www.apple.de
2. Wikipedia ist eine freie Enzyklopädie:
   http://de.wikipedia.org
3. Weitere interessante Web Adressen:
   www.tip.de
   www.stern.de
   www.whitehouse.gov
   www.keywest.com

9 Anhang

9.1 Virus Teil 2

Ab der Seite **Fehler! Textmarke nicht definiert.** haben Sie schon einen ersten Überblick über das doch recht schwierige und umfangreiche Thema Viren bekommen. Nun, nachdem Sie sich im Windows Explorer mehr eingearbeitet haben, folgen noch weitere Informationen und ein Einblick in die Benutzung eines Anti-Viren-Programms.

Virenarten

Es gibt eine riesige Anzahl bekannter und unbekannter Viren, und viele sind besonders gefährlich. Es werden aber auch immer wieder neue Viren in Umlauf gebracht. Nachfolgend sind einige der bedeutendsten Kategorien genannt:

- **Bootsektorviren**
  verstecken sich im Startbereich (Bootsektor) der Festplatten und Wechseldatenträger (z.B. USB-Stick, Diskette, CD/DVD). Sie werden bei einem Neustart des Computers und beim Wechseln des Datenträgers aktiv.

- **Programmviren**
  schleichen sich in ein Programm ein und aktivieren sich jedes Mal, wenn das Programm gestartet wird.

- **Makroviren**
  verstecken sich in den Makros der Dokumente, z.B. in Word-Dokumenten oder in Excel-Tabellen. Ein Makro ist ein kleines Programm und kann beim Öffnen des Dokuments automatisch aktiv werden.

- **Polymorphe Viren**
  besitzen die Fähigkeit, verschiedene Virenformen anzunehmen.

- **Stealth Viren**
  diese Tarnkappen-Viren können sich vor einem Viren-Suchprogramm verstecken.

- **Trojanisches Pferd oder Trojaner**
  bezeichnet einen Virus, der sich hinter nützlichen Funktionen eines Programms verbirgt. Beispiel: Es wird ein falsches Anmeldefenster angezeigt, um die Zugangsdaten oder die Kreditkartennummer beim Internet-Einkauf oder beim Online-Banking auszuspionieren.

- **Backdoor**
  versucht einem anderen Programm den Zugriff zum betroffenen Computer zu ermöglichen.

- **Wurm**
  versucht eMails an alle auf dem Computer vorhandenen Adressen zu schicken. Bei jedem Empfänger wird der Wurm-Virus wiederum aktiv. Damit wird eine Lawine losgetreten, die teilweise zu einer Blockade von Millionen von Rechnern führt. Manchmal wird dieser Virus als harmlos bezeichnet. Dies muss aber bestritten werden, da durch den Ausfall der Computer ein großer wirtschaftlicher Schaden entsteht.

- **Hoax**
  ist kein Virus, sondern ein Ketten-eMail, das vorgibt, vor einem Virus zu warnen. Meist ist die Warnung mit der Aufforderung verbunden, das eMail an viele Leute weiterzuleiten, da das Virus sehr gefährlich sei. Dies führt zu einer Blockade der eMail-Server. Oft werden auch fälschlicherweise ein oder mehrere Dateinamen in dem Hoax mit dem Hinweis ge-

nannt, diese Dateien unbedingt auf dem Computer zu löschen. Das sollten Sie auf keinen Fall tun. Programme und Betriebssystem sind danach eventuell nicht mehr lauffähig.

- **Spyware**
  sind Spionageprogramme, die unbemerkt Informationen sammeln und versenden. Es wird beispielsweise versucht, Ihre persönlichen Daten zu erkunden und Ihr Kauf- und Surfverhalten an interessierte Firmen weiterzugeben, um Sie ganz gezielt zu bewerben.

- **Phishing**
  versucht vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen zu bekommen. Es wird mit gefälschten, aber echt wirkenden Schreiben gearbeitet.

☞ Banken und andere Institute fragen niemals nach Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per E-Mail, per SMS oder telefonisch!

- **Pharming**
  arbeitet mit gefälschten Webseiten, Sie können die Fälschung nur schwer erkennen. Wie beim Phishing, wird versucht, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN, von Online-Banking-Zugängen zu erhalten.

- **Dialer**
  versucht heimlich, ohne Ihre Zustimmung, den Internetzugang über ein vorhandenes Telefonmodem oder eine ISDN-Karte auf eine sehr teure 0900–Nummer (früher 0190) umzustellen. Der Dialer-Virus funktioniert aber nicht bei einem DSL-Anschluss. Wenn sich ein Dialer-Programm auf Ihrem Computer ohne Ihr Wissen eingenistet hat, müssen Sie diese überhöhten Telefonkosten nicht bezahlen.

Regelmäßige Informationen über Viren und Hoaxes erhalten Sie bei dem
Bundesamt für Sicherheit in der Informationstechnik

www.bsi.bund.de/ oder www.bsi-fuer-buerger.de

Webseite des Bundesamtes für Sicherheit in der Informationstechnik

Auch bei den Herstellern der Anti-Viren-Programme können Sie nachschauen, z.B.:

www.free-av.de/ www.symantec.com/de/de/norton360

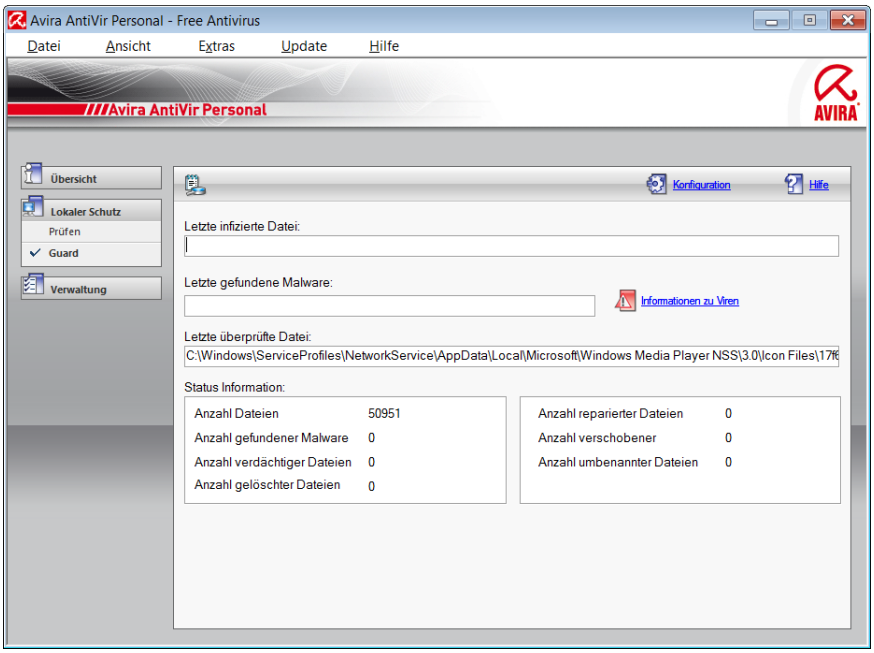
http://de.mcafee.com/virusInfo/default.asp

Beachten Sie bitte: Internetadressen können sich ändern!

Schutzmaßnahmen

Empfehlungen, um die Virengefahr zu verringern:

- Ein Anti-Viren-Programm im Hintergrund (Virenwächter) permanent mitlaufen lassen:



Anti-Viren-Programm

- Ein gutes Anti-Viren-Programm kann jederzeit kostenlos über das Internet aktualisiert werden (Update). Damit kann das Programm auch die allerneusten Viren aufspüren.
- Auch durch automatische Windows-Updates wird der Schutz vor Viren und anderen Sicherheitsbedrohungen deutlich erhöht (Seite 96).
- Eine E-Mail-Nachricht stets im Nur-Text-Format verschicken und empfangen. Nachrichten im HTML-Format können Viren enthalten.
- Keine Dateien von zweifelhafter Herkunft empfangen, öffnen bzw. speichern.
- Auch von einer vertrauensvollen Quelle sind alle externen Speichermedien (Wechsellaufwerke), die Sie in den Computer hineinschieben, anstecken oder sonst wie anschließen, zunächst mit einem Anti-Viren-Programm zu überprüfen. Als Beispiele sind hier zu nennen: CD/DVD, USB-Stick, Diskette, Speicherkarte.
- Auf einer gekauften Original-CD/DVD-ROM der großen Softwarefirmen dürften in der Regel keine Viren enthalten sein. Die Unternehmen betreiben einen sehr großen Aufwand, um dies zu verhindern. Wenn Sie aber eine selbst gebrannte CD/DVD beispielsweise mit Dokumenten bekommen, ist ein Virus auf diesem Medium nicht ausgeschlossen. Um CDs und DVDs vor dem Benutzen auf Viren zu überprüfen, drücken Sie beim Schließen der CD/DVD-Schublade gleichzeitig die ⇧-Taste (Shift-, Umschalttaste) und halten die Taste

ohne Unterbrechung ca. 15 - 30 Sekunden lang gedrückt. Diese Maßnahme verhindert den Autostart einer CD/DVD und damit den automatischen Start eines Virenprogramms auf dieser CD/DVD.

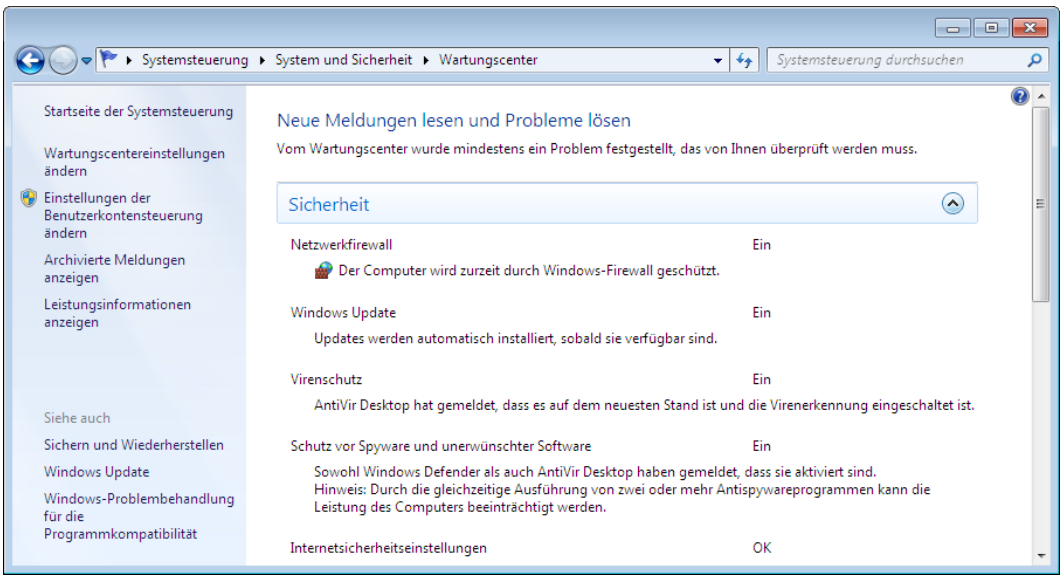
- Grundsätzlich sind alle neu gespeicherten Dateien, die von außen auf den Computer übertragen wurden (E-Mail-Anhang, Download aus dem Internet), sofort nach dem Speichern, aber spätestens vor dem Öffnen mit einem Anti-Viren-Programm zu überprüfen. Dies gilt auch, wenn das Virenwächter-Programm im Hintergrund permanent aktiv ist, denn es gibt Viren, die sich am Virenwächter vorbeimogeln!
- Zusätzlich sollte die gesamte Festplatte einmal am Tag nach Viren gescannt werden. Da das Anti-Viren-Programm dafür eine gewisse Zeit benötigt, können Sie dies vielleicht in die Arbeitspausen verlegen.
- Um einen unerlaubten Zugriff von außen abzuwehren, sollte im Netz und/oder auf den Anwendungscomputern eine Firewall (Seite 11) eingerichtet sein.
- Falls Sie besonders vorsichtig sein wollen und mehrere verschiedene Anti-Viren-Programme einsetzen, beachten Sie aber bitte: Es darf nur ein Anti-Viren-Programm gleichzeitig laufen. Mehrere Virenwächter, die im Hintergrund aktiv sind, können sich gegenseitig blockieren und Programme oder das Betriebssysteme (Windows) zum Absturz bringen!
- Regelmäßig Sicherungskopien (Backups) von Ihren virenfreien Daten anfertigen.

Aber es gibt keinen absoluten Schutz gegen Viren. Jeden Tag kommen neue Virenarten hinzu. Wenn Sie nicht sicher sind, sollten Sie die an eine eMail angehängte Datei nicht gleich öffnen, sondern die Datei zunächst speichern und danach mit einem Virensuchprogramm diese Datei überprüfen.

9.2 Das Wartungscenter

Wartungscenter

Windows gibt Ihnen mit dem **Wartungscenter** in der Systemsteuerung einen Überblick über den aktuellen Stand von wesentlichen Sicherheitsmaßnahmen. Mit den Ampelfarben Gelb und Rot werden Sie auf Probleme hingewiesen.

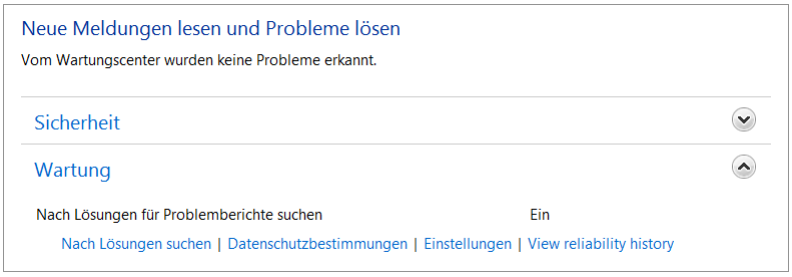


Wartungscenter

Zunächst einmal: Wenn in den Sicherheitszeilen keine Probleme angezeigt werden, und Sie mit Ihrem Computer zu Ihrer Zufriedenheit arbeiten können, ist es sehr zu empfehlen, dass Sie an den Sicherheitseinstellungen

nichts ändern!!!

Mit einem Mausklick auf den Schalter am rechten Rand einer Sicherheitszeile vergrößern bzw. verkleinern Sie eine Zeile und erhalten dadurch mehr Informationen:



Verkleinerte Sicherheits- und vergrößerte Wartungszeilen

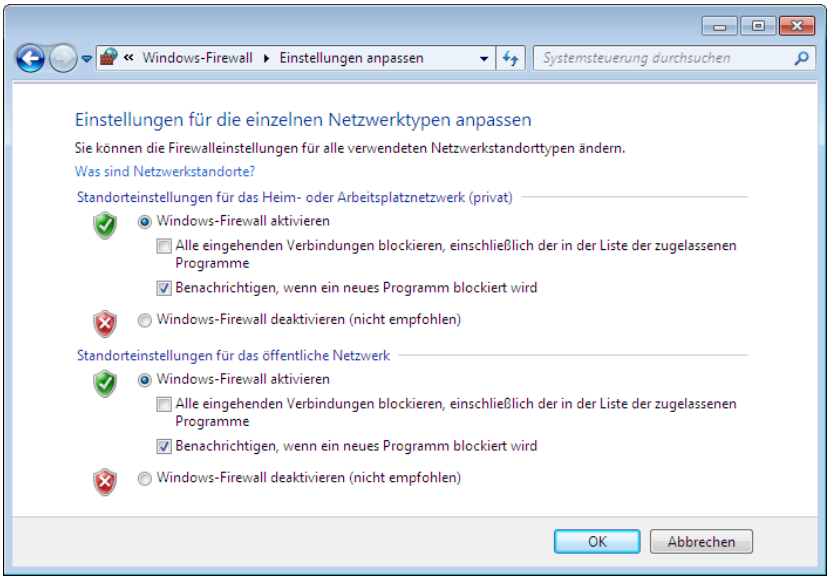
Sie können die verschiedenen Sicherheitseinstellungen aber auch direkt im Ordner **Systemsteuerung** verwalten.

9.3 Windows-Firewall

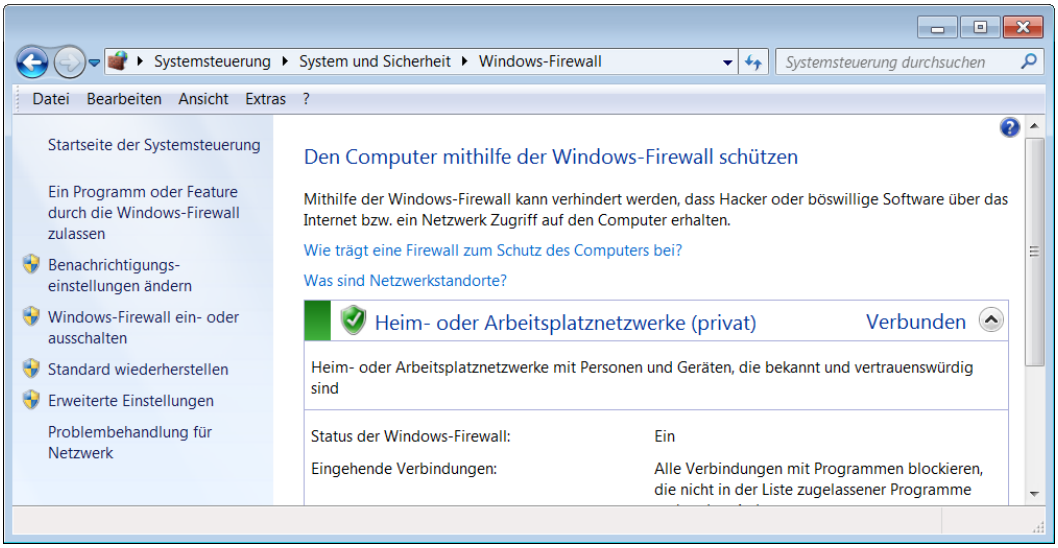
Windows-Firewall

Eine Firewall (Brandschutzmauer) ist ein System, einen Computer oder ein ganzes Netzwerk vor einem unbefugten Zugriff zu schützen. Sie soll den erlaubten Verkehr zwischen Computer/Netzwerk und dem Internet, anderen Computern oder Programmen zulassen und den nicht gewünschten Verkehr blockieren. Ein Hackerangriff soll damit abgewehrt werden. Die Firewall kann in einem speziellen Computer, in einem Router und/oder – wie in Windows – als Zusatz-Programm eingebaut sein.

Falls auf Ihrem Computer einzelne Programme oder Dienste nicht richtig arbeiten, können in den nachfolgenden Dialogfenstern (Kategorie **System und Sicherheit**) die Einstellungen der **Windows-Firewall** geändert werden.



Einstellung anpassen



Windows-Firewall

Die Einstellungsmöglichkeiten sind sehr vielfältig. Aber die Windows-Firewall ist auch "lernfähig". Falls Sie bei einem Programm- oder Diensteaufruf eine Sicherheitswarnung erhalten, können Sie den Zugriff festlegen.

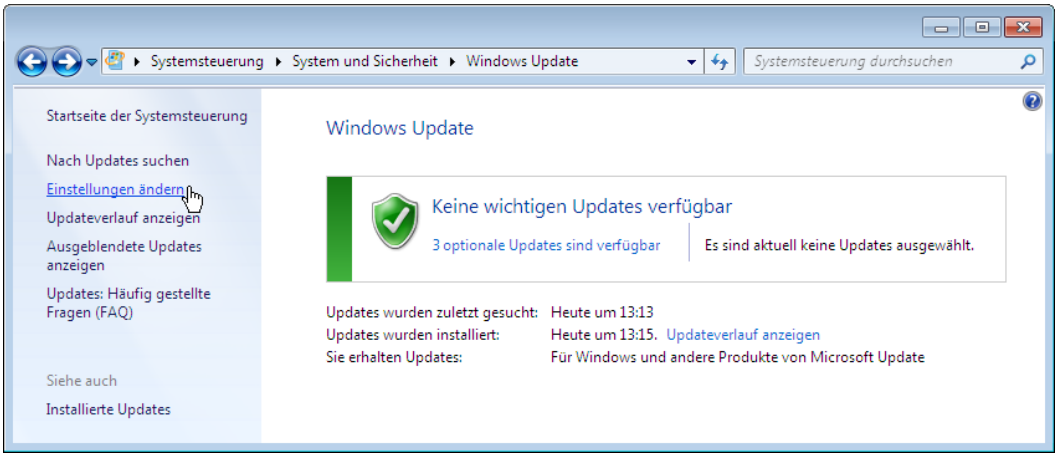
9.4 Windows Updates

Windows Updates

Wenn eine Internet-Verbindung vorhanden ist, kann Windows wichtige Programm-Erneuerungen (Updates) automatisch oder manuell aus dem Internet holen und auf Ihrem Computer installieren. Damit wird der Schutz vor neuen Viren und anderen Sicherheitsbedrohungen deutlich erhöht. Besonders bei Computern, die nicht von Fachleuten betreut werden, ist es sehr empfehlenswert, diese Sicherheitseinstellung eingeschaltet zu lassen:

Windows Update	Ein
Updates werden automatisch installiert, sobald sie verfügbar sind.	

Öffnen Sie das nachfolgende Dialogfenster in der **Systemsteuerung**. Bei dieser Einstellung werden die Programm-Erneuerungen (Updates) bei einer aktiven Verbindung automatisch aus dem Internet geholt:

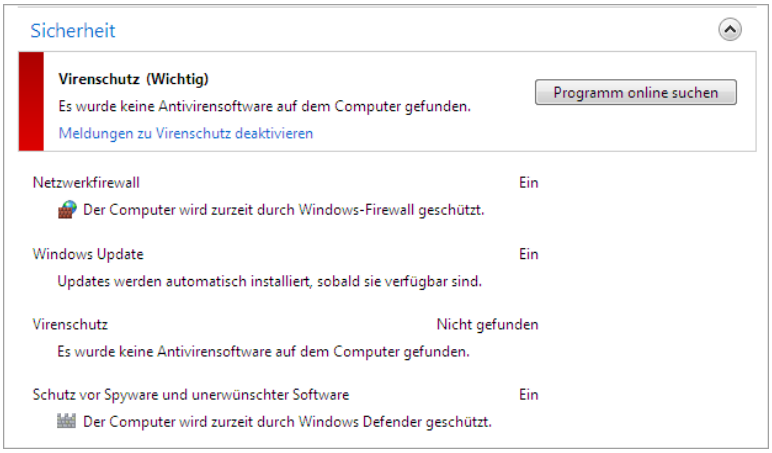


Über einen Link im Navigationsfenster die Einstellungen ändern

Die Installation wird automatisch gestartet, natürlich nur wenn der Computer eingeschaltet ist. Sie kann aber auch manuell durchgeführt werden. Über einen Link im Navigationsfenster nehmen Sie die Änderungen vor.

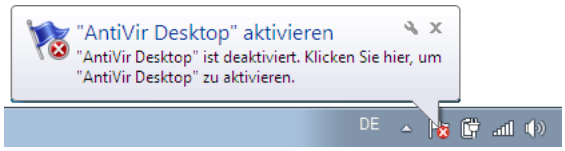
9.5 Virenschutz

Auf der Seite 12 wurde es schon erwähnt: In den aktuellen Windows-Versionen sind *standardmäßig* keine Viren-Suchprogramme enthalten. Dazu müssen Sie ein Fremdprogramm, ein Anti-Viren-Programm installieren. Windows überwacht nur den Status des Virenschutzes und im Wartungscenter bzw. im Virenprogramm können Sie den aktuellen Status ablesen:

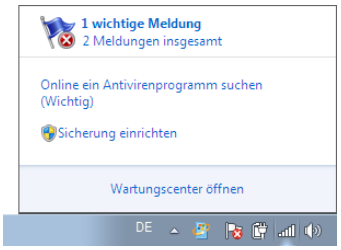


Kein Virenschutz

Falls der Virenschutz nicht ausreicht, werden Sie auch im Infobereich über das Problem informiert:

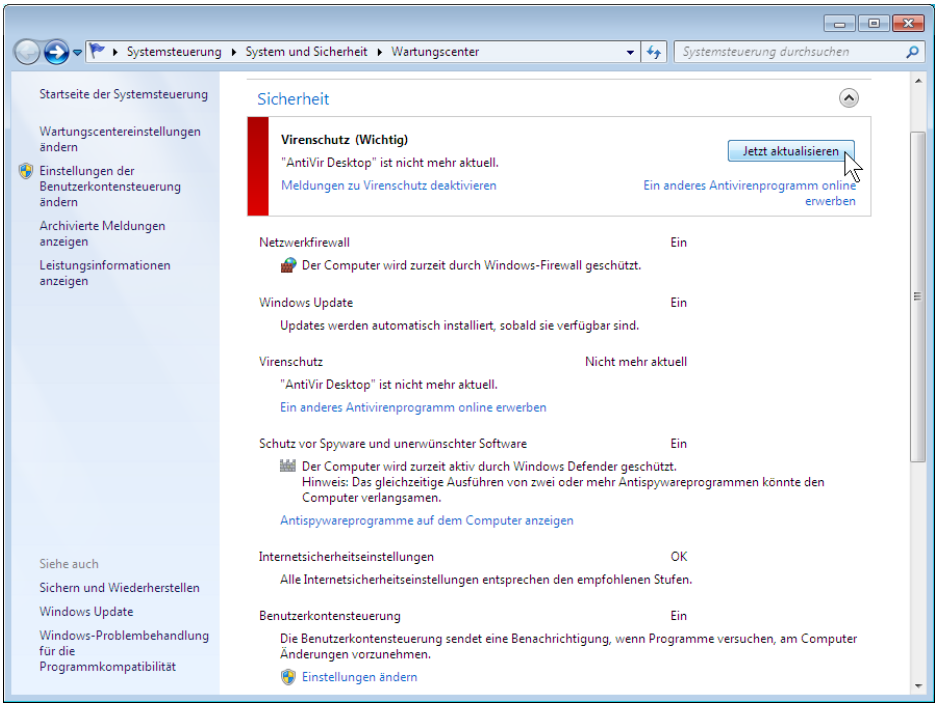


Hinweis im Infobereich



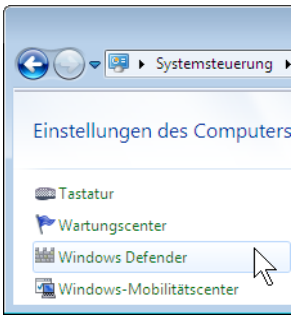
Klick auf das Symbol

Allerdings klappt manchmal das Zusammenspiel einiger Virenschutz-Programme mit dem **Wartungscenter** in Windows 7 nicht. Eventuell muss ein Update von der Internetseite des Anti-Viren-Programm-Herstellers installiert werden. Sie können über das Wartungscenter die Aktualisierung vornehmen oder direkt über das Virenprogramm:



Wartungscenter; Aktualität des Virenprogramms
Der Schutz vor Spyware ist aber eingeschaltet

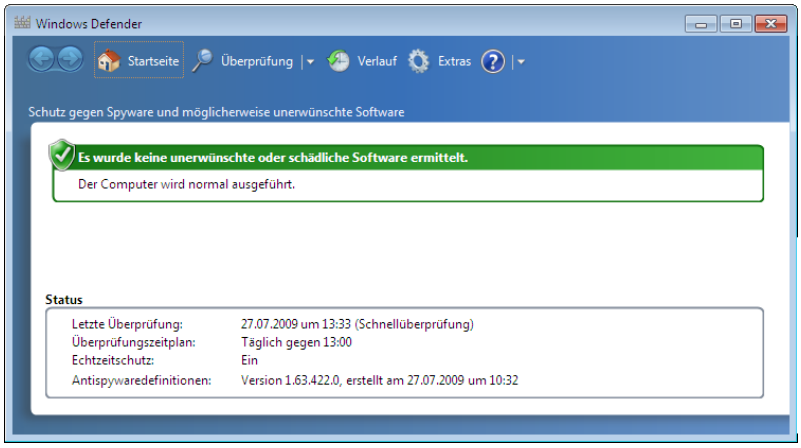
9.6 Windows Defender



Systemsteuerung
Ansicht Kleine Symbole
(Ausschnitt)

Im Wartungscenter erhalten Sie in der Sicherheitszeile **Schutz vor Spyware und unerwünschter Software** Informationen über das Programm **Windows Defender**. Spyware sind Spionageprogramme, die unbemerkt Informationen sammeln und versenden. Es wird beispielsweise versucht, Ihre persönlichen Daten zu erkunden und Ihr Kauf- und Surfverhalten an interessierte Firmen weiterzugeben, um Sie ganz gezielt zu bewerben.

Um das nachfolgende Defender-Fenster aufzurufen, klicken Sie beispielsweise in der Systemsteuerung auf die links stehende Verknüpfung. Die Symbolleiste bietet Ihnen einige Schaltflächen an, um dieses umfangreiche Programm optimal zu nutzen:



Schutz vor Spyware und anderer schädlicher Software

Die Schaltfläche Extras führt Sie zum nachfolgenden Fenster:

Defender: Einstellungen und Extras

Inhaltsverzeichnis

1 Vorbemerkungen ... 5
1.1 Tasten-Bezeichnungen ... 5
2 Grundlagen ... 6
2.1 Das Internet ... 6
2.2 Das Modem ... 9
2.3 Internet Service Provider (ISP) ... 10
2.4 HTML - Die Web-Sprache ... 10
2.5 Computerviren ... 11
2.6 Das Wartungscenter ... 11
2.7 Übungen ... 12
3 Der Internet Explorer ... 13
3.1 Der Internet Explorer-Bildschirm ... 15
3.2 Der Befehlsaufruf ... 16
3.3 Anzeigemodus ändern ... 20
3.4 Die Explorerleiste ... 22
3.5 URL ... 23
3.6 Blättern im Internet Explorer ... 27
3.7 Registerkarten ... 27
3.8 Hilfe ... 29
4 Surfen im Internet ... 32
4.1 Sicherheitswarnungen ... 33
4.2 InPrivate-Browsen – Surfen ohne Spuren ... 35
4.3 Eine weitere Internet-Tour ... 37
4.4 Verknüpfungen und Registerkarten ... 39
4.5 Vorwärts und Zurück ... 40
4.6 Suchen innerhalb einer ganzen Website ... 40
4.7 Nach Texten auf dieser Seite suchen ... 41
4.8 Frames ... 41
4.9 Text kopieren ... 42
4.10 Handel (eCommerce) ... 44
4.11 Ein Formular ausfüllen ... 45
4.12 Sicherheitsstatusleiste ... 45
4.13 Blog und Podcast – neue Darstellungsformen ... 47
4.14 Schnellinfos ... 48
4.15 Übungen ... 49
5 Webseiten speichern und drucken ... 50
5.1 Seiten speichern ... 50
5.2 Das Öffnen von gespeicherten Dateien ... 51
5.3 Die Druckvorschau ... 52
5.4 Das Seitenlayout ... 54
5.5 Webseiten drucken ... 55
6 Websuche ... 58
6.1 Verzeichnisdienste ... 58
6.2 Suchmaschinen ... 58
6.3 Meta-Suchmaschinen ... 59
6.4 Die Explorer-Suchhilfe ... 60
6.5 Suchvorschläge ... 62
6.6 Einen Suchbericht ausdrucken ... 62
6.7 Hilfe in den Suchmaschinen ... 63

6.8 Groß- und Kleinschreibung ... 64
6.9 Platzhalter * ... 64
6.10 Stoppwörter ... 64
6.11 Logische Operatoren ... 64
6.12 Auf der Suche nach aktuellen Informationen ... 68
6.13 Übungen ... 70
7 Lesezeichen (Favoriten) ... 71
7.1 Zu Favoriten hinzufügen ... 71
7.2 Die Explorerleiste Favoriten ... 72
7.3 Eine Favoriten-Webseite öffnen ... 73
7.4 Die Lebensdauer von Webadressen ... 74
7.5 Favoriten verwalten ... 75
7.6 Die Favoritenleiste ... 75
7.7 Die Explorerleiste Verlauf ... 76
7.8 Die Explorerleiste Recherchieren ... 76
7.9 Die Explorerleiste Feeds ... 77
8 Internetoptionen ... 80
8.1 Die Startseite ... 80
8.2 Einträge in der Explorerleiste Verlauf löschen ... 81
8.3 Den Anbieter für das Suchfeld ändern ... 82
8.4 Bilder, Klänge und Videos ... 83
8.5 Schaltfläche Schnellinfo ein- / ausschalten und verwalten ... 84
8.6 Web Slices ... 86
8.7 Übungen ... 87
8.8 Popupblocker-Einstellungen ... 87
8.9 SmartScreen-Filter-Einstellungen ... 89
8.10 Kompatibilitätsansicht ... 90
9 Anhang ... 91
9.1 Virus Teil 2 ... 91
9.2 Das Wartungscenter ... 94
9.3 Windows-Firewall ... 95
9.4 Windows Updates ... 96
9.5 Virenschutz ... 97
9.6 Windows Defender ... 98
10 Stichwortverzeichnis ... 100