

## Sicherheit Lektion 5

### Sicherheit im WWW und Sicherheit beim Bezahlen

- ✗ Browser-Einstellungen
  - ✗ Cookies
  - ✗ Browserverlauf
  - ✗ Inhaltskontrollen
  - ✗ Digitale Zertifikate und https
  - ✗ Einmal-Kennwort
  - ✗ E-Commerce und Tele-Banking
- ✓ Bestimmt nutzen Sie das Internet. Wissen Sie, dass Sie im Browser verschiedene Einstellungen finden, die das Surfen sicherer machen? Haben Sie schon einmal das digitale Zertifikat einer Website geprüft und kennen Sie Strategien, um zu ermitteln, ob ein Einkauf in einem Online-Shop sicher ist? Mit diesen Themen beschäftigt sich Lektion 5.

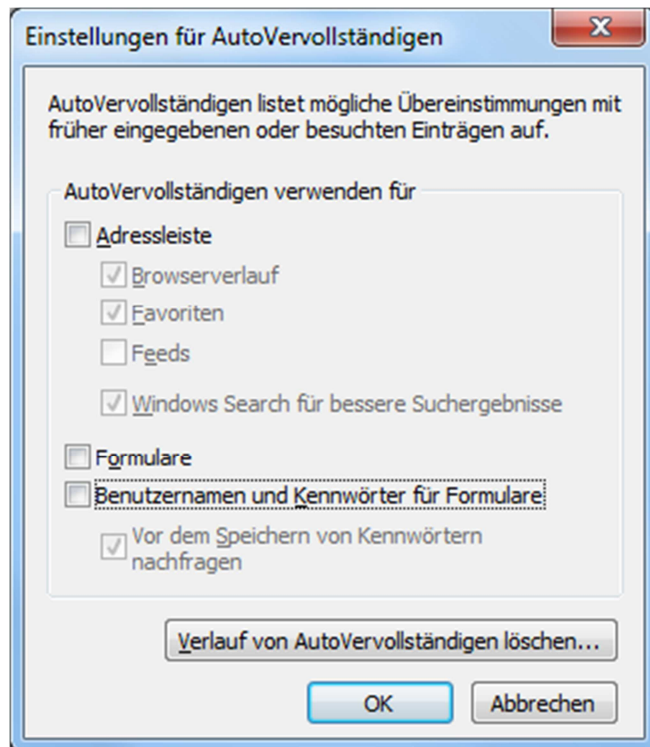
#### 🔒 Aufgabe

Recherchen: [www.guetezeichen.at](http://www.guetezeichen.at),  
[www.shopinfo.net](http://www.shopinfo.net), [www.euro-label.com](http://www.euro-label.com)

#### 1. Browser-Einstellungen

Füllen Sie Formulare aus, schlägt der Internet Explorer 9 die persönlichen Daten bereits vor. Dieses sogenannte *AutoVervollständigen* birgt leider ein Sicherheitsrisiko. Deaktivieren Sie diese Einstellungen über EXTRAS | INTERNETOPTIONEN | INHALTE.

- ▶ Deaktivieren Sie die Kontrollkästchen und bestätigen Sie mit **OK** (siehe Abbildung).



### **TIPP: InPrivate-Browsen**

Öffnen Sie den Internet Explorer 9 und hier die Befehlsschaltfläche SICHERHEIT. Klicken Sie auf INPRIVATE-BROWSEN. Bleiben Sie in diesem Fenster, denn so werden keine Daten über Ihre Browsersitzung gespeichert (Cookies, temporäre Internetdateien, Verläufe, etc.). Ihre IP-Adresse bleibt aber nicht geheim.

### **TIPP: Tracking-Schutz**

Es kann vorkommen, dass beim Besuchen einer Website gleichzeitig andere Inhalte mitgeladen werden. Wieder versucht man, personenbezogene Daten über Sie zu sammeln. Im Internet Explorer 9 blockieren Sie diesen Ladevorgang über SICHERHEIT | TRACKING-SCHUTZ. Aktivieren Sie im Dialogfeld ADD-ONS ANZEIGEN UND VERWALTEN den **Tracking-Schutz**.

### **TIPP: ActiveX-Steuerelemente filtern**

ActiveX ist eine Technologie, um beispielsweise Videos und Animationen abzuspielen oder um bestimmte Dateiarten anzuzeigen. Die Gefahren dabei gehen vom Sammeln personenbezogener Daten, über das Verlangsamen des Rechners hin zum Manipulieren des Rechners. Aktivieren Sie die ActiveX-Filterung über SICHERHEIT | ACTIVEX-FILTERUNG.

### **TIPP: SmartScreen-Filter**

Aktivieren Sie den SmartScreen-Filter. Der Internet Explorer 9 blockiert den Ladevorgang für Sites, von denen bekannt ist oder vermutet wird, dass sie Malware oder andere Sicherheitsrisiken - wie Phishing-Websites – enthalten. Klicken Sie auf SICHERHEIT | SMARTSCREEN-FILTER | SMARTSCREEN-FILTER EINSCHALTEN. Aktivieren Sie das Optionsfeld SMARTSCREEN-FILTER EINSCHALTEN und klicken Sie auf **OK**.

Sobald Sie einen Link zu einer anderen Site anklicken oder einen URL eingeben, wird die Adresse an Microsoft übermittelt und dort mit einer vorhandenen Blacklist abgeglichen. Auch Sie können eine verdächtige Site melden. Klicken Sie auf SICHERHEIT | SMARTSCREEN-FILTER | UNSICHERE WEBSITE MELDEN.

---

*Cookies werden im HTML-Format im Ordner Temporary Internet Files gespeichert.*

## **2. Cookie**

Cookies sind Informationsdateien, die auf Ihrem Rechner im Auftrag des Webserver der besuchten Website gespeichert werden. Meist sind sie nützlich, weil Sie zB Anmeldedaten speichern, die man dann beim wiederholten Besuch einer Website nicht mehr eingeben muss. Doch gibt es auch Cookies, die zum Ausspionieren verwendet werden. Surft man auf fremden Rechnern, sind Informationen über Ihre Daten unerwünscht – löschen Sie die Cookies.

- ▶ Zum Löschen öffnen Sie EXTRAS | INTERNETOPTIONEN | ALLGEMEIN | BROWSERVERLAUF | LÖSCHEN. Hier löschen Sie unter anderem die Cookies.
- ▶ Möchten Sie die Sicherheitseinstellungen für Cookies ändern, so öffnen Sie EXTRAS | INTERNETOPTIONEN | DATENSCHUTZ und ziehen Sie den Schieberegler ganz hinauf. Damit sind alle Cookies blockiert.

### Popupblocker

Oft wird beim Öffnen einer Webseite ein Werbefenster eingeblendet. Dieses zusätzliche Fenster wird *Popup* genannt. Im Internet Explorer 9 ist ein POPUPBLOCKER aktiviert.

Leider blockiert dieser Blocker auch Seiten, die eingeblendet werden, wenn Sie Programme downloaden möchten oder Telebanking durchführen wollen. Sie deaktivieren diese Einstellung über EXTRAS | INTERNETOPTIONEN | DATENSCHUTZ. Alternativ dazu arbeiten Sie über EXTRAS | POPUPBLOCKER.

### 3. Browserverlauf

Wenn Sie mit dem Internet Explorer surfen, werden die Links zu besuchten Seiten, temporäre Internetdateien, Passwörter, Cookies und Formulardaten gespeichert. Löschen Sie den Browserverlauf.

- ▶ Öffnen Sie die INTERNETOPTIONEN über EXTRAS | INTERNETOPTIONEN.
- ▶ Öffnen Sie SICHERHEIT | BROWSERVERLAUF LÖSCHEN oder EXTRAS | INTERNETOPTIONEN | ALLGEMEIN | BROWSERVERLAUF | LÖSCHEN.
- ▶ Damit wird das Dialogfeld BROWSERVERLAUF LÖSCHEN angezeigt.

#### Bevorzugte Websitedaten beibehalten

Aktivieren Sie dieses Kontrollkästchen, wenn die Cookies und Dateien nicht gelöscht werden sollen, die Websites in der Favoritenliste zugeordnet sind.

#### Temporäre Internetdateien

Beim Surfen wird eine große Menge an aufgerufenen Daten zeitlich begrenzt (temporär) nicht nur im Verlauf, sondern auch auf der Festplatte gespeichert. Löschen Sie diese Dateien.

#### Cookies

Cookies sind kleine Informationsdateien, die unter Umständen auch zum Ausspionieren verwendet werden. Löschen Sie diese Cookies.

#### Verlauf

Löschen Sie die Links zu den in den vergangenen Tagen besuchten Seiten.

#### Downloadverlauf

Löschen Sie die Liste der getätigten Downloads.

#### Formulardaten

Löschen Sie alle Informationen, die Sie über Formulare eingegeben haben.

#### Kennwörter

Entfernen Sie auch hier Ihre Spuren und aktivieren Sie das Kontrollfeld zum Löschen der Kennwörter.

---

*Diese Themen werden ebenfalls im Training Internet besprochen*

### Daten der ActiveX-Filterung und des Tracking-Schutzes

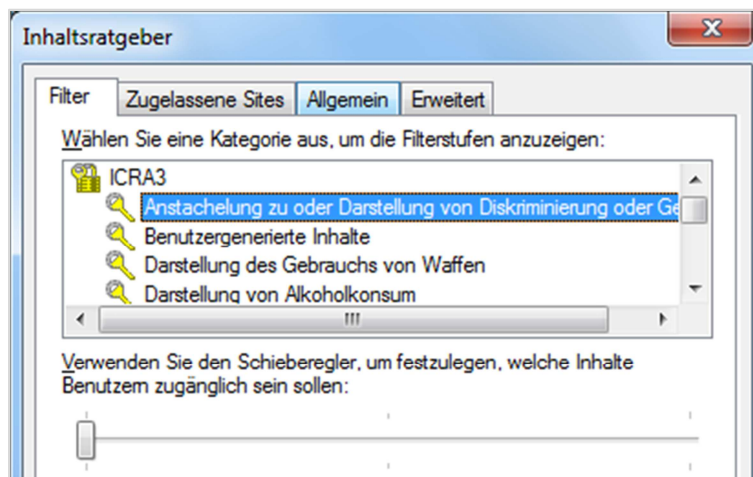
Wie weiter oben bereits erwähnt, ist ActiveX ist eine Technologie, um beispielsweise Videos und Animationen abzuspielen oder um bestimmte Dateiarten anzuzeigen. Jedoch kann ActiveX auch ein Sicherheitsrisiko darstellen und die Geschwindigkeit des Computers beeinträchtigen, personenbezogene Daten sammeln oder den Rechner manipulieren.

- ▶ Klicken Sie auf LÖSCHEN und sehen Sie in der Verlaufsleiste nach – es dürfen keine Links mehr aufgelistet sein.

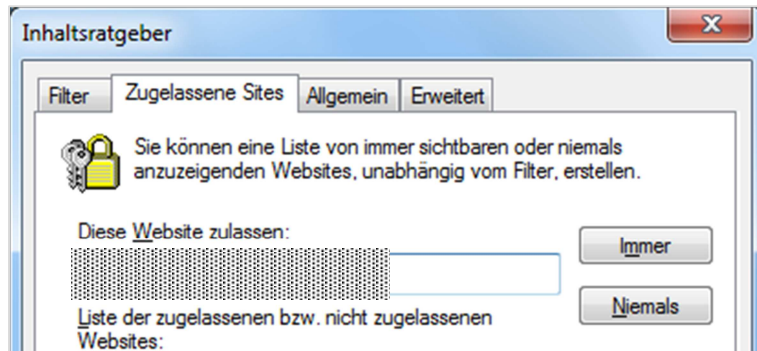
## 4. Inhaltskontrollen

Im Netz gibt es auch ungeeignete Seiten, vor allem für Ihre Kinder. Beugen Sie dem Besuch dieser Sites rechtzeitig durch Inhaltskontrollen vor. Zuerst melden Sie sich am Rechner als Administrator mit Kennwort an. Ihre Kinder bekommen ein normales Konto oder ein Gast-Konto. Nutzen Sie dazu die Einstellungen in der SYSTEM-STEUERUNG unter BENUTZERKONTEN.

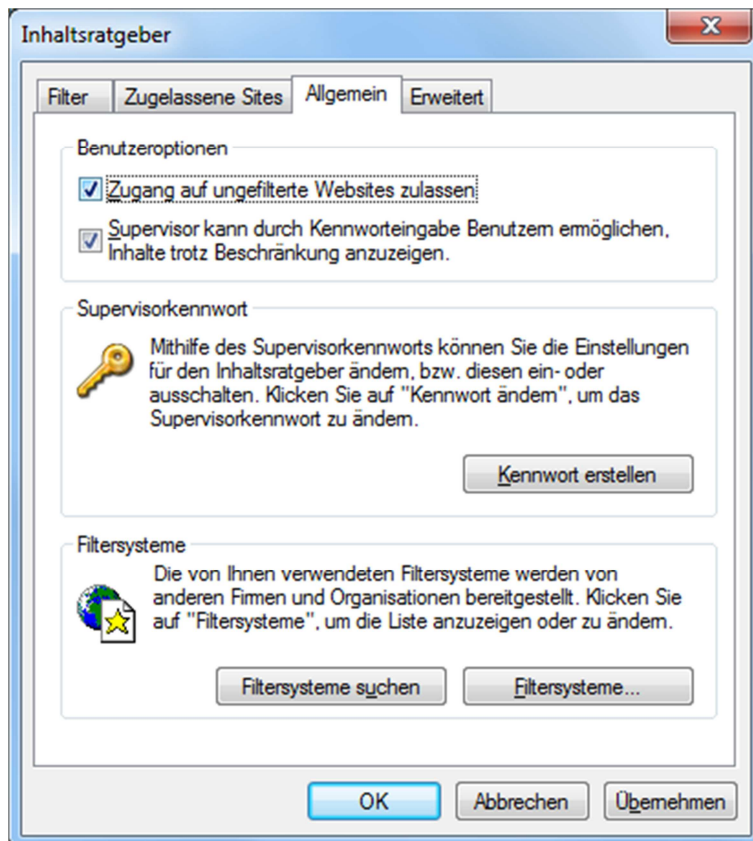
- ▶ Im Internet Explorer 9 wählen Sie als Administrator / -in EXTRAS | INTERNET-OPTIONEN | INHALTE. Klicken Sie unter INHALTSRATGEBER auf die Schaltfläche **Aktivieren**.
- ▶ Klicken Sie die aufgelisteten Kategorien nacheinander an und nutzen Sie jeweils den Schieberegler zum Einstellen, welche Inhalte zugänglich sein sollen (siehe Abbildung). Die Erläuterungen zu einer Filterstufe finden Sie gleich darunter.



- ▶ Wechseln Sie auf die Registerkarte ZUGELASSENE SITES. Geben Sie hier eine komplette Adresse ein. Darf diese Site nie angezeigt werden, dann klicken Sie auf die Schaltfläche **Niemals** (siehe Abbildung auf der nächsten Seite).



- ▶ Wechseln Sie auf die Registerkarte ALLGEMEIN. Das Filtersystem blockt alle Websites, die nicht im Filter enthalten sind. Das kann dazu führen, dass gar keine Websites angezeigt werden. Aktivieren Sie darum das Kontrollkästchen ZUGANG AUF UNGEFILTERTE WEBSITES ZULASSEN (siehe Abbildung).
- ▶ Aktivieren Sie auch das zweite Kontrollkästchen. Wenn Sie nämlich eine geblockte Site laden möchten, erhalten Sie ein Dialogfeld, in das Sie Ihr Supervisionskennwort eintragen. Dann können Sie die Website öffnen.



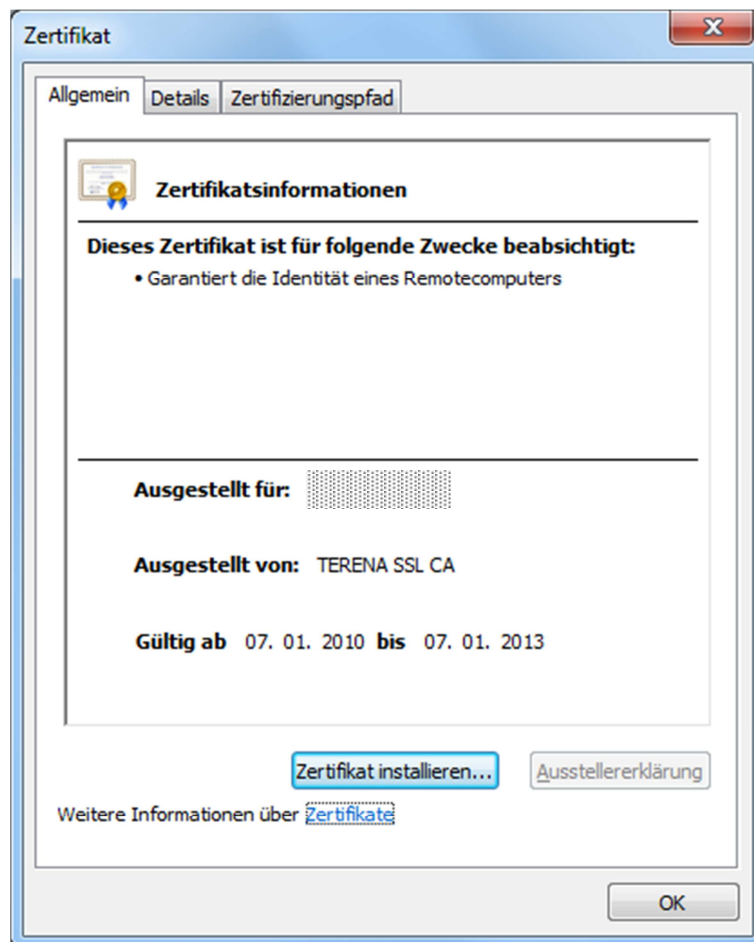
- ▶ Klicken Sie **auf Kennwort erstellen** (siehe Abbildung oben) und vergeben Sie ein Supervisionskennwort. So können Sie jederzeit im Register INHALTE die Einstellungen für den Inhaltsratgeber ändern oder deaktivieren.

## 5. Digitale Zertifikate und https

Verfügt eine Website über ein digitales Zertifikat, wird der Zugriff auf die Daten durch ein Sicherheitsprotokoll verhindert. Es wird automatisch ein Zertifikat zugesandt und in der Adressleiste erscheint zudem ein Schloss-Symbol. Das Zertifikat bescheinigt die Identität der Person / Firma bzw. die Sicherheit der Webseite. Zertifikate werden von unabhängigen Zertifizierungsstellen ausgestellt, unter anderem von [www.verisign.de](http://www.verisign.de), [www.thawte.de](http://www.thawte.de), [www.a-trust.at](http://www.a-trust.at) oder [www.terena.org](http://www.terena.org).

Auf sicheren Websites werden die Daten verschlüsselt übertragen. Sie erkennen das am Protokoll https für *hypertext transfer protocol secure* und an dem Schloss-Symbol im Browser.

- ▶ Klicken Sie auf das Schloss-Symbol.
- ▶ Klicken Sie auf ZERTIFIKATE ANZEIGEN (siehe Abbildung).



Wenn Sie mit dem Smartphone Ihre Bankgeschäfte erledigen, sollten Sie sich die TAN auf ein anderes Handy senden lassen.

## 6. Einmal-Kennwort

Einmal-Kennwörter verwendet man meist beim Tele-Banking. Eine für 5 Minuten gültige Transaktionsnummer wird per SMS auf das Handy gesendet oder aus einer Liste ausgedruckt. Diese Nummer ist nur für einen Vorgang gültig.

## 7. E-Commerce und Tele-Banking

Sie haben online dieses tolle Poster gefunden, das Angebot zum Musikdownload klingt verlockend und die Reise verspricht Sonne, Sand und Meer. Die Preise passen. Nun geht es ans Bezahlen. Was sollten Sie dabei beachten?

- ▶ Zuerst einmal Ihre eigenen Sicherheitseinstellungen im Betriebssystem und im Browser. Aktivieren Sie die Firewall und installieren Sie ein Anti-Viren-Programm. Betriebssysteme und Browser haben Sicherheitslücken. Darum führen Sie die automatischen Updates durch steigen Sie auf die jeweils aktuellste Browser-Version um.
- ▶ Übertragen Sie persönliche Daten über gesicherte Seiten, vor allem beim Bezahlen. Lassen Sie das digitale Zertifikat anzeigen und überprüfen Sie das Ablaufdatum.
- ▶ Kaufverträge im Internet unterliegen auch gesetzlichen Grundlagen. Laut E-Commerce-Gesetz gibt es **Informationspflichten**.

Überprüfen Sie unter anderem:

- Das Impressum
- Ist der Bestellvorgang erklärt
- Gibt es eine Telefonnummer, Kontakt-Adresse und E-Mail-Adresse
- Wird auf das Rücktrittsrecht und bei nicht digitalen Daten auf einen Umtausch hingewiesen
- Der Vertrag kommt erst nach einer Bestätigung zustande

### E-Commerce Gütezeichen

Weil es auch unseriöse Anbietende gibt, wurde ein Gütezeichen geschaffen, das den Kunden und Kundinnen auf einen Blick seriöse Online-Shops zeigt.

In Österreich beträgt die einmalige Prüfgebühr gibt es ab 500 € (für Unternehmen bis zu 3 Mitarbeitenden); danach kostet die jährliche Nutzungsgeld wieder ab 500 € bis zu 1.500 € (für Unternehmen bis zu 1000 Mitarbeitenden). Für Einzelunternehmen ist das leider nicht leistbar. Rechts abgebildet sehen Sie das Euro-Label für Österreich. Besuchen Sie [www.guetezeichen.at](http://www.guetezeichen.at).

*TIPP: Digitale Zertifikate und Gütezeichen kosten Geld. Nur große Anbieter können sich das leisten.*

*Checken Sie, ob ein Online-Shop den links angeführten Informationspflichten nachkommt.*



In Deutschland richtet sich die Gebühr nach dem jährlichen Bruttoumsatz. Für die kleinste Klasse bis 250.000 € beläuft sich die Gebühr auf 750 € im Jahr, die einmalige Setupgebühr beträgt 75 €. Links abgebildet sehen Sie das Euro-Label für Deutschland. Informieren Sie sich unter [www.shopinfo.net](http://www.shopinfo.net).



Diese Labels gibt es auch für Italien, Frankreich, Polen und Spanien. Informieren Sie sich auf [www.euro-label.com](http://www.euro-label.com).

---

*Klicken Sie im Online-Shop auf ein Gütezeichen, so kommen Sie auf die Website des Gütezeichens mit Informationen zum Shop-Inhaber bzw. der Inhaberin.*

Beim Kauf von Waren in der EU gilt das Herkunftslandprinzip. Das bedeutet, dass das Recht des Landes gilt, in dem sich der Anbieter oder die Anbieterin niedergelassen hat.

Zahlen Sie mit dem Handy ([www.paybox.at](http://www.paybox.at)) oder nutzen Sie für Online-Geschäfte unter anderem

Paypal Deutschland GmbH unter [www.paypal.de](http://www.paypal.de)

Click & buy International AG unter [www.clickandbuy.com](http://www.clickandbuy.com)

Giropay GmbH unter [www.giropay.de](http://www.giropay.de)

## **Sicherheit Schritt fünf**

### **Sicherheit im www und Sicherheit beim Bezahlen**

#### **Übung und Selbststudium**

1. Löschen Sie alle Formulardaten.
2. Löschen Sie die Cookies.
3. Aktivieren Sie den Popublocker.
4. Löschen Sie den Browserverlauf.
5. Wie lange werden Link zu den zuletzt besuchten Seiten im Verlauf angeführt?
6. Sie machen Ihre Bankgeschäfte über ein Smartphone. Erarbeiten Sie, warum Sie sich die TAN auf ein anderes Handy senden lassen sollten.
7. Besuchen Sie einige Online-Shops. Woran erkennen Sie eine gesicherte Verbindung?
8. Finden Sie heraus, welche Angaben Shop-Betreiber/ -innen im Internet laut E-Commerce-Gesetz machen müssen.

#### **Testen Sie Ihr Wissen**

1. Warum sollten Sie das AutoVervollständigen für Formulardaten deaktivieren?
2. Was sind Cookies?
3. Wie schützen Sie Ihre Kinder vor unangenehmen oder gefährlichen Sites im WWW?
4. Was ist eine TAN?

#### **Notizen**