Security Lektion 5
Sicherheit im WWW und Sicherheit beim Bezahlen

- Sicheres Surfen
- Browser-Einstellungen
- Popupblocker
- 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, www.shopinfo.net, www.euro-label.com

1. Sicheres Surfen

Das Internet bietet über das World Wide Web Zugang zu untereinander verlinkten Websites an. Google hatte bereits 2005 Zugriff auf 8 Mrd. Sites! Da stellt sich die Frage, wie sicher die Webseiten, wie überprüft und vertrauenswürdig die Informationen und wie sicher die selber eingegebenen Informationen sind.

Möchten Sie wissen wie es um die Vertrauenswürdigkeit einer Website gestellt ist, dann prüfen Sie unter anderem folgende Kriterien:

- inhaltliche Qualität
- Aktualität
- gültige URL
- Information zum Inhaber der Webseite (Impressum)
- Kontaktdaten
- Eventuell Sicherheitszertifikat
- Eventuell Überprüfung der Domain-Inhaberschaft

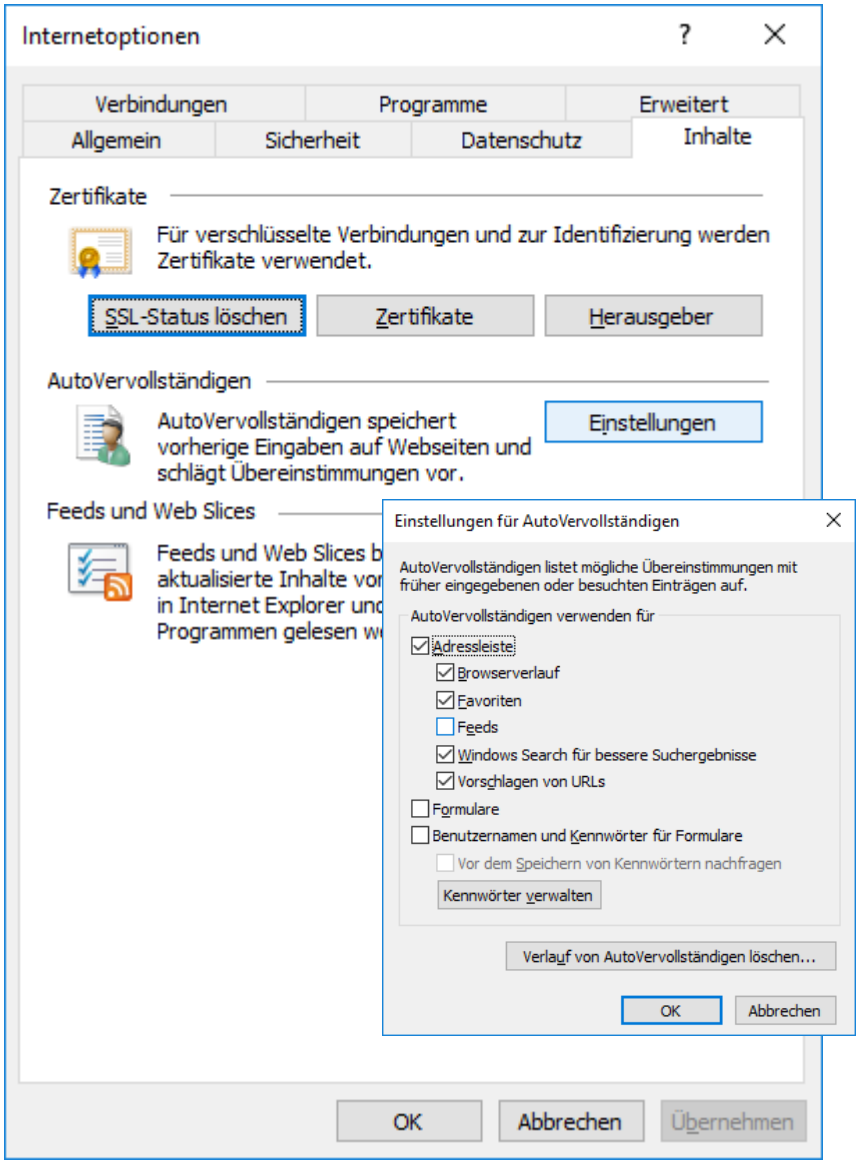
Zum Schutz von Kindern und Jugendlichen bietet sich Software zur Inhaltskontrolle an:

- Internet- Filterprogramme
- Kinderschutz-Software

Damit wird die Zeit für die Internet-Nutzung limitiert und mit Filtersystemen bestimmt, welche Websites, Apps nd Spiele verwendet werden dürfen. Zu Inhaltskontrollen gibt es im Laufe dieser Lektion noch eine kurze Information.

2. Browser-Einstellungen

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



- Klicken Sie auf EINSTELLUNGEN.
- Deaktivieren Sie die gewünschten Kontrollkästchen und bestätigen Sie mit **OK** (siehe Abbildung oben).

TIPP: InPrivate-Browsen

Öffnen Sie den Internet Explorer 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 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 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.

3. Popupblocker

Oft wird beim Öffnen einer Webseite ein Werbefenster eingeblendet. Dieses zusätzliche Fenster wird *Popup* genannt. Im Internet Explorer 11 ist ein POPUP-BLOCKER aktiviert.

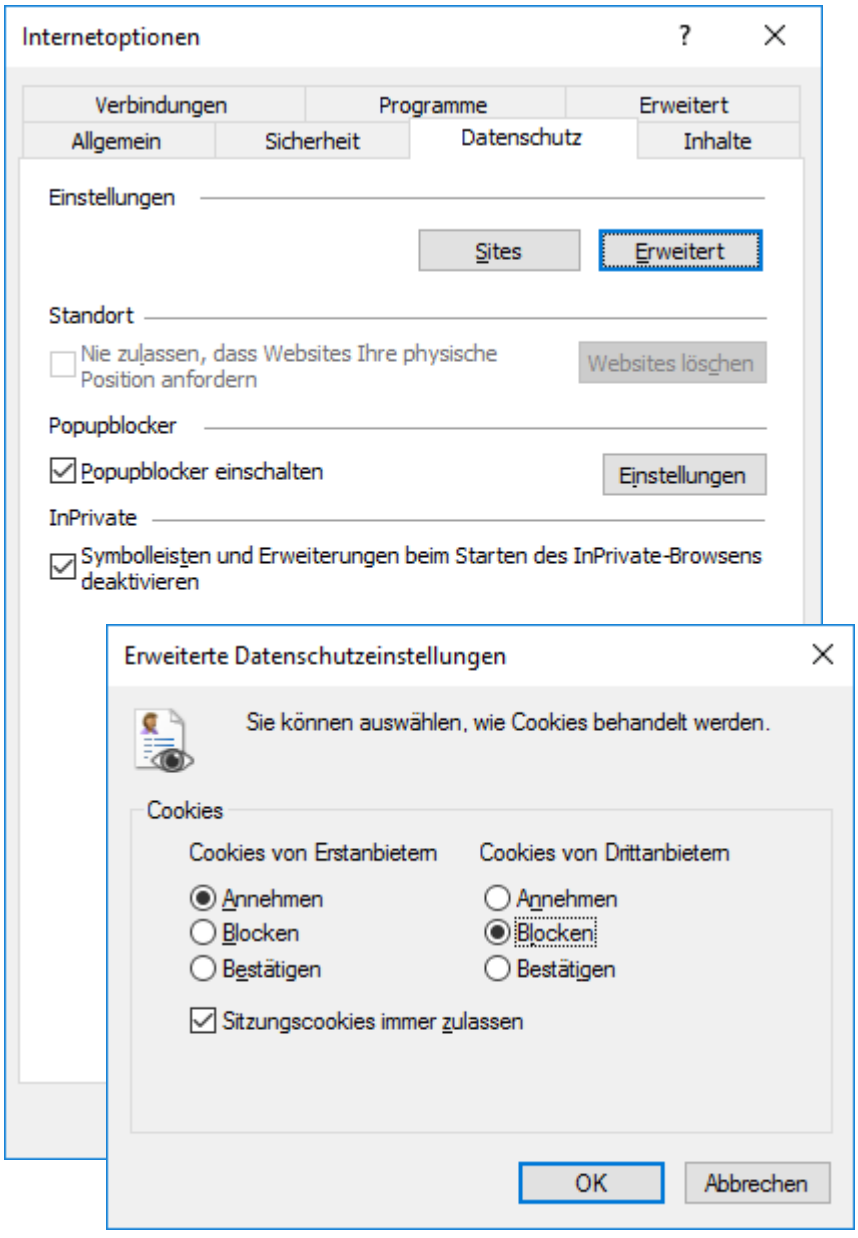
Leider blockiert dieser Blocker auch Seiten, die eingeblendet werden, wenn Sie Programme downloaden möchten oder Telebanking durchführen wollen. Sie deaktivieren diese Einstellung über EXTRAS | INTERNETOPTIONEN | DATENSCHUTZ. Alternativ dazu arbeiten Sie über EXTRAS | POPUPBLOCKER.

4. Cookie

Möchten Sie die Sicherheitseinstellungen für Cookies ändern, so öffnen Sie EXTRAS | INTERNETOPTIONEN | DATENSCHUTZ und klicken Sie auf ERWEITERT (siehe Abbildung auf der nächsten Seite).

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

Bei meinem letzten Besuch auf msn wurden 65 Cookies gesetzt! Facebook; Amazon oder Google sind nicht besser. Sehen Sie einmal in den Einstellungen Ihres Browsers nach. Einzelne Cookies mögen dabei aber sinnvoll sein, beispielsweise, um die Darstellung einer Website automatisch an die Größe des Ausgabegerätes anzupassen.



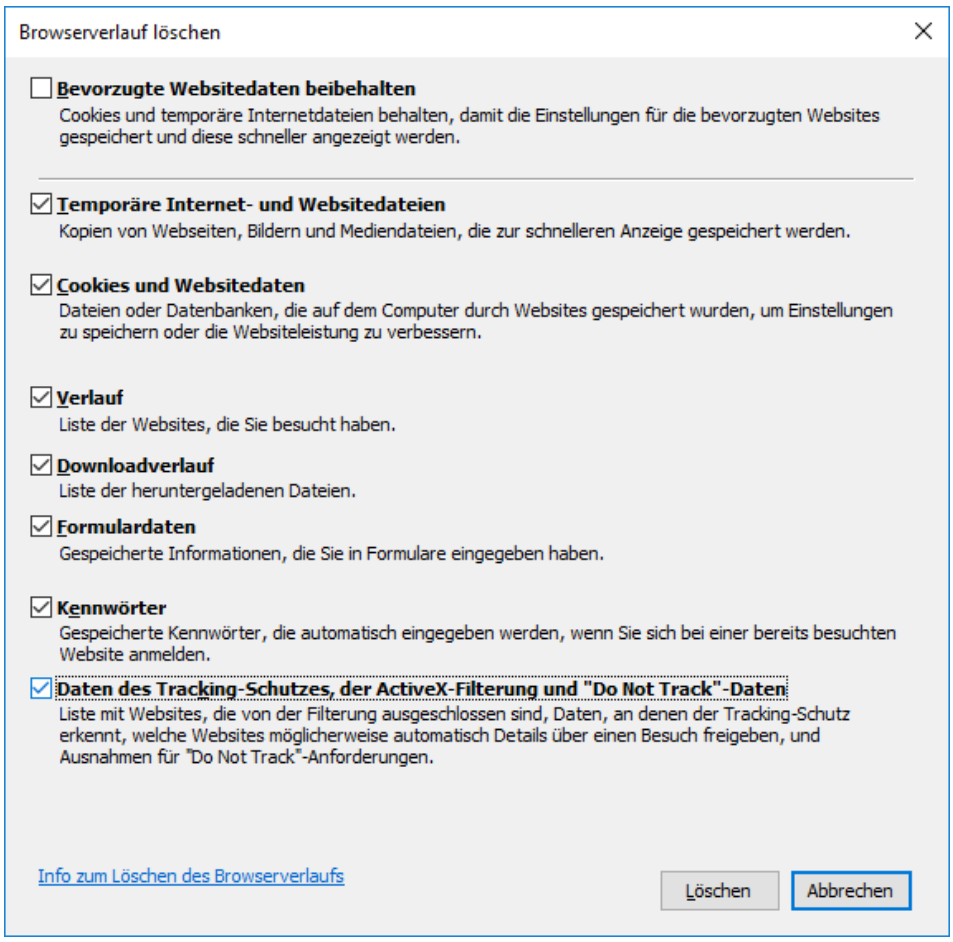
Cookies sind Informationsdateien, die auf Ihrem Rechner im Auftrag des Webservers der besuchten Website gespeichert werden. Früher waren sie nützlich, weil Sie zB Anmeldedaten speichern, die man dann beim wiederholten Besuch einer Website nicht mehr eingeben musste. Doch heute werden Cookies zum Ausspionieren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

5. Browserverlauf

Diese Themen werden ebenfalls im Training Internet besprochen.

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 (siehe Abbildung).



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.

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.

6. 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.

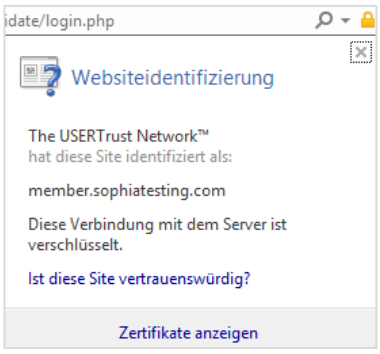
- Im Internet Explorer wählen Sie als Administrator / -in EXTRAS | INTERNET-OPTIONEN | INHALTE. Klicken Sie FAMILY SAFETY. Hier können Sie einstellen, was Ihre Kinder online sehen dürfen und legen Zeitbegrenzungen zum Surfen fest.

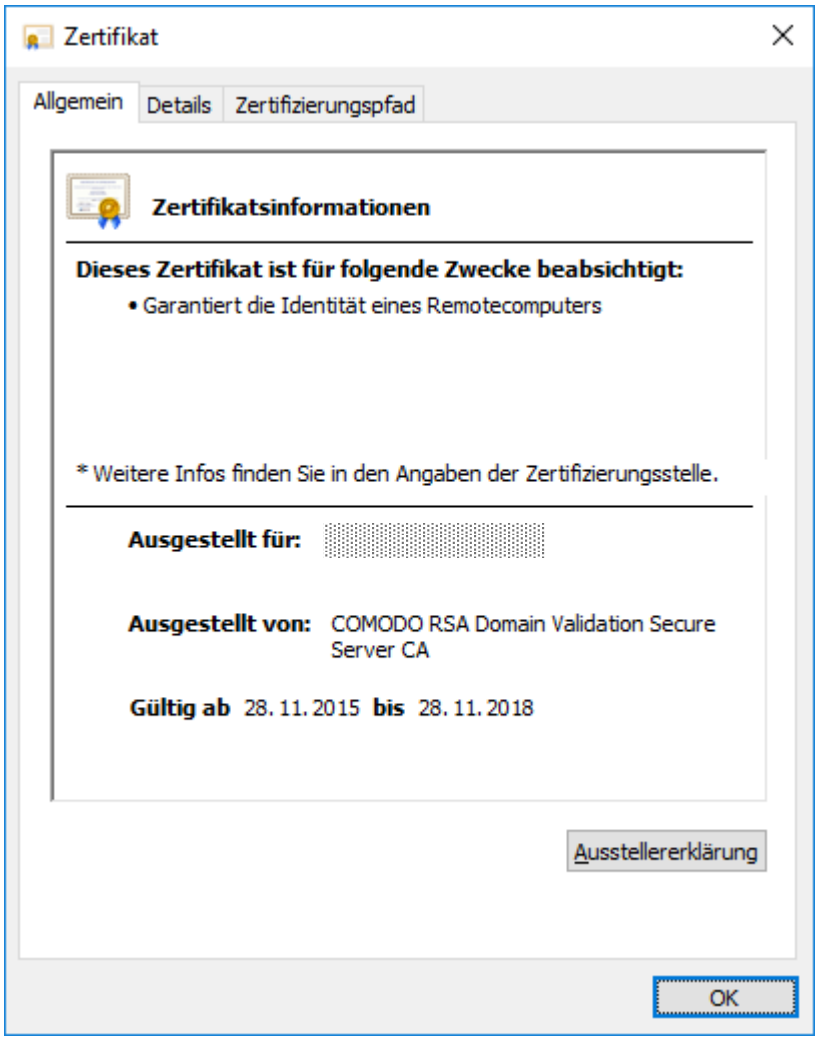
7. Digitale Zertifikate und https

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, www.thawte.de, www.a-trust.at oder 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 rechts).
- Das Zertifikat wird angezeigt (siehe Abbildung unten).





8. 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 ausgestrichen. Diese Nummer ist nur für einen Vorgang gültig.

9. E-Commerce und Tele-Banking

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

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-Gesetzt gibt es **Informationspflichten.**

  Digitale Zertifikate und Gütezeichen kosten Geld. Nur große Anbieter können sich das leisten. Checken Sie daher, ob ein Online-Shop den Informations-pflichten nachkommt. 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 Nutzungsgebühr 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.

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.

Diese Labels gibt es auch für Italien, Frankreich, Polen und Spanien. Informieren Sie sich auf www.euro-label.com.

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

Zahlen Sie mit dem Handy (www.paybox.at) oder nutzen Sie für Online-Geschäfte unter anderem Paypal GmbH unter www.paypal.com oder Click & buy International AG unter www.clickandbuy.com oder Giropay GmbH unter www.giropay.de.

Sicherheit Schritt fünf
Sicherheit im www
Sicherheit beim Bezahlen

Übung und Selbststudium

1. Löschen Sie alle Formulardaten.
2. Löschen Sie die Cookies.
3. Aktivieren Sie den Popupblocker.
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 Sei 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

In der nächsten Lektion beschäftigen wir uns mit Online Communities.