

Gut zu wissen!

RAN ANS INTERNET!



Ein Ratgeber für Einsteiger jedes Alters

Bayerisches Staatsministerium der
Justiz und für Verbraucherschutz



INITIATIVE **D21**

Inhaltsverzeichnis

Grußwort	3
Einführung	4
Hardware	4
Software	6
Was man sonst so braucht . . .	8
Internet, E-Mail & Co.	10
Erste Schritte	10
Sicherheit	11
Wie gehe ich ins Netz?	12
1. Informationsrecherche	13
Nachrichten	13
Suchmaschinen	13
Wikipedia	15
Blogs	15
2. Online-Shopping	16
Internet-Gütesiegel	17
Ihre Rechte beim Online-Kauf	18
eBay	20
Zu guter Letzt: Bewertungsportale	21
3. Kommunikation	22
E-Mail	22
Chatten	26
Skypen	27
Glossar, hilfreiche Links und Informationsseiten	28
Glossar	28
Kurz und knapp	30
Links/weiterführende Informationen	31
Impressum	32

Grußwort

Liebe Leserin, lieber Leser,

das Internet ist heutzutage allgegenwärtig. Es gibt kaum ein Angebot, das man nicht bequem online bestellen und kaum eine Dienstleistung, die man nicht vom heimischen Sofa in Anspruch nehmen kann. Kurzum: Das Internet ist in der Gesellschaft angekommen – mehr als 76% der deutschen Wohnbevölkerung sind online. Das heißt zugleich aber auch, dass ein Viertel noch nicht „drin“ ist und der Anteil der über 60jährigen ist in dieser Gruppe überproportional hoch. Dabei sind die Vorteile des Internets immens: Ob nun online einkaufen, mit der Familie auch über weite Distanzen in Kontakt bleiben oder für die Informationsrecherche. Das Internet erleichtert das tägliche Leben. Und: Es ist einfacher als man denkt, man muss sich nur trauen.

Natürlich wollen wir aber die Gefahren nicht verhehlen. Es gibt sogenannte „Abzockangebote“, es gibt Schadsoftware im Netz oder E-Mails mit kriminellen Inhalt, um nur einige Beispiele zu nennen. Man kann sich jedoch davor schützen: Mit gesundem Menschenverstand und den Tipps und Tricks, die wir Ihnen in unserer Broschüre verraten.

Wir wünschen Ihnen eine interessante und informative Lektüre!



Ihre Dr. Beate Merk, MdL
Bayerische Staatsministerin der
Justiz und für Verbraucherschutz



Ihr Hannes Schwaderer
Präsident der Initiative D21

Einführung

Für den Gang ins Internet braucht man:

- ▶ **Hardware**
Unter Hardware versteht man einen PC, ein Notebook, ein Tablet oder ein Smartphone.
- ▶ **Software**
Programme, die auf dem PC oder dem Notebook laufen.
- ▶ **Internetanschluss**
... etwa von der Deutschen Telekom, Vodafone oder Kabel Deutschland.

Hardware

Bevor Sie ins Internet gehen können, brauchen Sie geeignete, das heißt in diesem Fall internetfähige Hardware: einen PC, ein Notebook, ein Tablet oder ein Smartphone. Und wenn Sie etwas ausdrucken möchten, benötigen Sie darüber hinaus noch einen Drucker.

Personal-Computer (kurz: „PC“)

Ein PC ist ein stationärer meist kastenförmiger Computer. Zusätzlich benötigen Sie in der Regel noch weitere Geräte, wie etwa einen Bildschirm, eine Tastatur und eine Maus.



Notebook (oder auch „Laptop“)

Ein Notebook ist ein kleiner tragbarer aufklappbarer Computer mit einer Tastatur und einem Bildschirm. Auch die Maus ist hier schon mit an Bord. Notebooks sind in der Regel etwas teurer als PCs, dafür ist aber auch schon alles dabei und man kann sie überallhin mitnehmen.



Tablet (engl. für „Tafel“) oder auch „Tablet-PC“

Ein Tablet ist ein flacher, tragbarer und durch die besondere Speichertechnologie sehr schneller Computer mit einem berührungsempfindlichen Bildschirm („Touchscreen“). Auch hier ist bereits alles dabei und das Gerät ist aufgrund seines geringen Gewichts noch besser zum Mitnehmen geeignet als ein Notebook.



Smartphone

Ein Smartphone ist ein modernes, mit Computerfunktionen ausgerüstetes leistungsstarkes Mobiltelefon, das auch für den Gang ins Internet genutzt werden kann. Da der Bildschirm aber sehr klein ist, empfehlen sich Smartphones nicht für die ersten Schritte ins Internet.



Software

Neben der Hardware, braucht man noch Programme (die „Software“), die auf dem jeweiligen Gerät laufen. Im Regelfall sind schon einige Programme vorinstalliert, mit denen man für den Einstieg gut auskommt.

Betriebssystem

Das Betriebssystem ist die Nutzeroberfläche auf dem Gerät. Es variiert je nachdem, ob man einen **PC**, ein **Notebook** oder ein **Tablet** beziehungsweise **Smartphone** benutzt. Bei PCs und Notebooks am verbreitetsten ist das System „Windows“ von Microsoft, die neueste Version hiervon ist Windows 8.

E-Mail-Programme

Zum Empfangen oder Versenden von E-Mails benötigt man spezielle E-Mail-Programme, zum Beispiel „**Outlook**“ von Microsoft oder „**Thunderbird**“ von Mozilla.



<http://office.microsoft.com/de-de/outlook>



www.mozilla.org

Alternativ kann man auch eine sogenannte Web-Anwendung benutzen, mit der man seine E-Mails mit Hilfe eines Browser ansehen oder versenden kann. Hier gibt es zahlreiche – oft auch kostenfreie Angebote – wie etwa **WEB.DE**, **GMX** oder **Gmail**.



www.web.de



www.gmx.de



www.gmail.com



HINWEIS:

Hinweis: Kostenfreie E-Mail-Programme im Internet finanzieren sich durch Werbung. Daher erhält man hier oft Werbe-E-Mails.

Browser

Ein Browser ist ein spezielles Programm zur Anzeige von Internetseiten. Am beliebtesten sind der „**Firefox**“ von Mozilla und der „**Internet Explorer**“ von Microsoft.

Die meisten Browser sind ähnlich aufgebaut: Gibt man oben in die Adressleiste die Adresse der zu besuchenden Seite ein, lädt der Browser nach Drücken der Eingabetaste der Eingabetaste auf der Tastatur die Inhalte der gewünschten Seite. Eine Internetadresse beginnt in der Regel mit „www.“



Sicherheitsprogramme

Zum Schutz des eigenen Rechners und der eigenen Daten benötigt man eine **Firewall** und ein **Virenschutzprogramm**. Ein Virenschutzprogramm verhindert zum Beispiel, dass sich Schadsoftware auf dem eigenen Gerät installieren kann. Es sollte daher immer auf dem neuesten Stand sein; am besten die Funktion „automatische Updates“ aktivieren. Auch sollte man in regelmäßigen Abständen die eigenen Dateien auf einem anderen Ort sichern („Backup“). Am besten eignet sich dafür eine externe Speicherfestplatte.

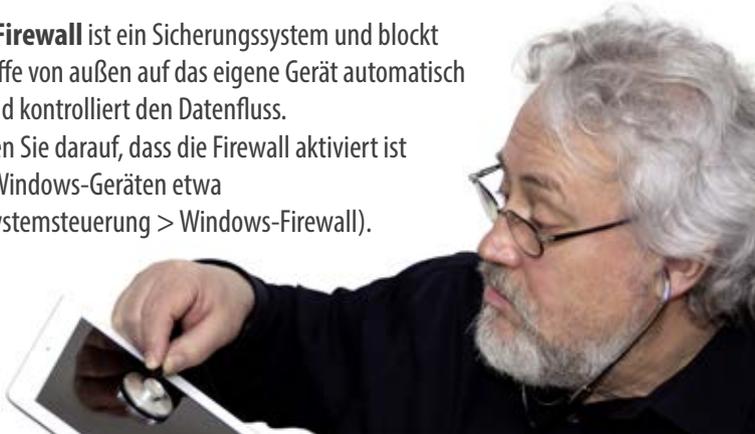
EMPFEHLUNG:

Sollte die Schrift auf einer Seite mal zu klein sein, einfach gleichzeitig die Tasten „strg“ (= „Steuerung“) und „+“ auf der Tastatur drücken.



Eine **Firewall** ist ein Sicherungssystem und blockt Zugriffe von außen auf das eigene Gerät automatisch ab und kontrolliert den Datenfluss.

Achten Sie darauf, dass die Firewall aktiviert ist (bei Windows-Geräten etwa → Systemsteuerung > Windows-Firewall).



EMPFEHLUNG:

- ✓ Virenschutzprogramm installieren
- ✓ Backup erstellen
- ✓ Firewall aktivieren



Was man sonst so braucht ...

Hat man das erforderliche Equipment beisammen, benötigt man noch einen Internetanschluss. Man unterscheidet im Wesentlichen zwischen stationären Lösungen und solchen über Funk.

- ▶ Stationäre – also **leitungsgebundene** – Angebote sind zum Beispiel DSL-/VDSL oder auch die Lösungen über Glasfaser und das Fernseekabel. Auch immer mehr Versorgungsunternehmen wie Stadtwerke oder Energielieferanten finden sich mittlerweile unter den Anbietern.
- ▶ **Funklösungen** wie LTE- oder UMTS bekommt man in der Regel über Mobilfunkanbieter (zum Beispiel T-Mobile oder Vodafone).



Der Anbieter („Provider“) liefert die Internetsignale bis zum – in der Regel mitgelieferten – **Modem** (oder „Router“) in Ihren Haushalt. Im Haus selbst können Sie an dieses ein sogenanntes **LAN-Kabel** anschließen, das Ihre Hardware direkt mit dem Modem verbindet, oder eine sogenannte **WLAN-Lösung** einsetzen, bei der das Signal dann per Funk in Ihrem Haus vom Modem an Ihren PC, Ihr Notebook oder Ihren Tablet weitergesendet wird.

Generell ist darauf zu achten, dass man eine Übertragungsgeschwindigkeit von **wenigstens 6 MBit/s** wählt, um möglichst alle angebotenen Dienste adäquat nutzen zu können. Bei Funkbasierten Lösungen muss man besonders auf **Sicherheitsaspekte** achten, da hier die Daten leichter von Dritten eingesehen werden können. Dasselbe gilt, wenn Sie bei sich ein WLAN einrichten. Hier sind zwingend Sicherheitsvorkehrungen wie etwa die **Verschlüsselung des Funknetzes** mit dem **Sicherheitsstandard WPA2** zu treffen. Die Einstellung erfolgt über das Modem/den Router. Die Provider oder die Hersteller geben im Regelfall hierzu ausführliche Anleitungen.



Mehr zum Thema: www.verbraucher-sicher-online.de/artikel/kabellos-aber-nicht-sorglos

Da immer mehr Provider auf den Markt drängen und somit im Regelfall eine große Konkurrenz herrscht, bekommt man ein adäquates Internetangebot bereits für ca. 30,- EUR im Monat. Ein sogenanntes Flatrate-Angebot schützt vor unliebsamen Kostenüberraschungen. Eine Flatrate beinhaltet die Zusage des Anbieters, eine bestimmte Datenmenge mit einer bestimmten Übertragungsgeschwindigkeit zur Verfügung zu stellen. Oft ist da auch schon das Festnetztelefonieren mit dabei.

EMPFEHLUNG:



- ✓ Die Datenverbindung sollte mindestens 6 MBit/s im Downstream leisten. Das bedeutet, dass man Daten mit einer Geschwindigkeit von bis zu 6 Megabit in der Sekunde herunterladen kann.
- ✓ Wer ein WLAN zuhause betreibt, muss es sichern (bspw. mit dem WPA2-Standard). Ansonsten drohen haftungsrechtliche Probleme bei Missbrauch durch Dritte.
- ✓ Am besten ein sogenanntes „Flatrate-Angebot“ wählen. Das schützt vor unliebsamen Kosten Überraschungen.

Übrigens:

Viele Unternehmen/Händler bieten die Einrichtung der Hardware und der Internetverbindung gleich mit an.

Sicherheit

Im Internet lauern viele Gefahren. Man kann sich Viren und andere Schädlinge einfangen, die Daten können missbraucht werden oder man kann auf unseriöse Angebote hereinfallen. Das ist jedoch kein Grund, auf die vielen Vorteile, die das Netz bietet, zu verzichten. Das ist nur ein Grund, Vorsicht walten zu lassen und vor allem die notwendigen **Sicherheitsvorkehrungen** zu treffen – das gilt für das Surfen genauso wie für den Umgang mit E-Mails.

Neben genereller Sicherheitsbedenken wird oft die Sorge um die **eigenen Daten** als Grund genannt, warum jemand nicht das Internet nutzen möchte. Und in der Tat gibt es hier Gefahren, beispielsweise beim Einkaufen im Netz. Eine 100%ige Sicherheit gibt es wie im realen Leben auch hier nicht, die Gefahren lassen sich jedoch mit einem Mindestmaß an Sorgfalt erheblich minimieren. Und zu guter Letzt hilft einem auch immer der gesunde Menschenverstand.

EMPFEHLUNG:

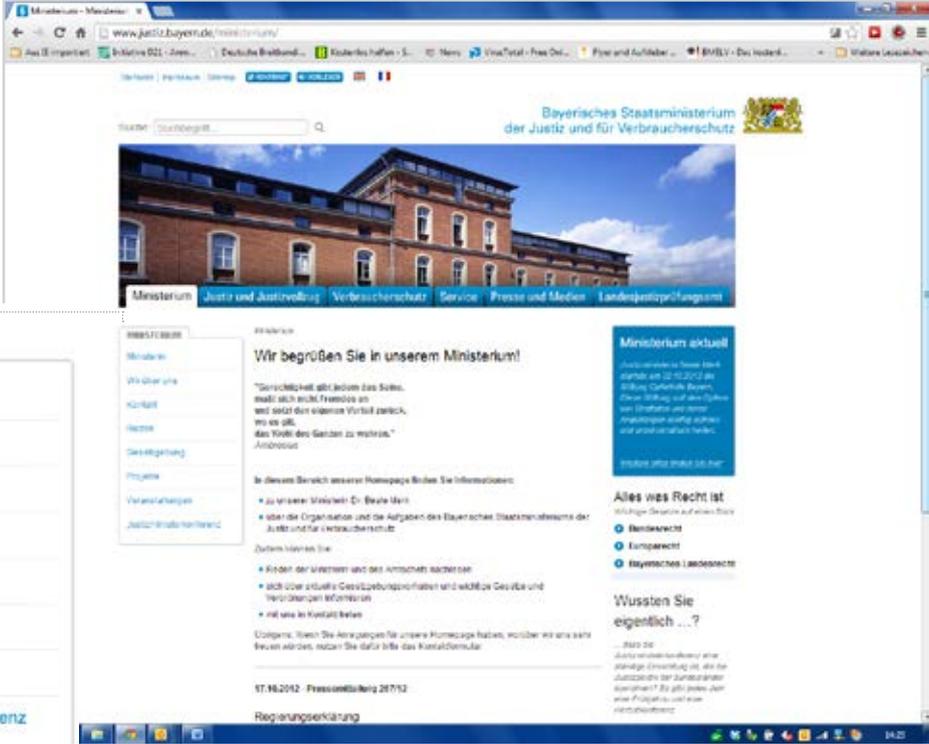


- ✓ Verwenden Sie immer ein aktuelles **Virenschutzprogramm**. Achtung: Kostenfreie Lösungen schützen oft nicht vollumfänglich. Wichtig ist auch der Schutz beim Surfen im Netz, da manipulierte Seiten schon durch das bloße Aufrufen einen Rechner infizieren können. Prüfen Sie regelmäßig, ob Updates vorhanden sind oder nutzen Sie die automatische Updatefunktion.
- ✓ **AntiSpy (= Anti-Spionage)-Programme** schützen vor unerwünschten Beobachtern oder davor, dass Daten (zum Beispiel bei der Passworteingabe) unbemerkt übermittelt werden.
- ✓ Nutzen Sie eine **Firewall**, die den Datenverkehr überwacht und zusätzlichen Schutz vor Eindringlingen bietet.
- ✓ Installieren Sie regelmäßig die **Updates** des Betriebssystems oder sonstiger Software (zum Beispiel Java).
- ✓ Erhöhen Sie die Sicherheitseinstellungen Ihres Browsers. Tipps dazu finden Sie in der Regel beim Anbieter selbst (zum Beispiel: www.internet-explorer.de).
- ✓ Öffnen Sie **keine unbekannt Dateien**, zum Beispiel Dateianhänge aus E-Mails.
- ✓ Verwenden Sie keine **Datenträger** (CD-ROM, USB-Sticks, etc.) unbekannter Herkunft.

Wie gehe ich ins Netz?

Der Gang ins Netz ist denkbar einfach. Man öffnet den **Browser** und tippt in die **Adressleiste** oben die gewünschte Internetadresse ein, zum Beispiel www.ard.de oder www.bayern.de. Nach Drücken auf die Eingabetaste auf der Tastatur lädt der Browser die gewünschte Seite. Sollte bis zu diesem Zeitpunkt noch keine Internetverbindung bestanden haben, wird man jetzt gefragt, ob nun eine aufgebaut werden soll.

Die Internetseiten selbst folgen in der Regel einem einheitlichen – oft hierarchischem – Aufbau: Von der Startseite (der sog. „Landingpage“) gelangt man durch Klicken auf die einzelnen Unterpunkte auf die einzelnen Unterseiten mit weitergehenden Informationen und Inhalten.



The image shows a screenshot of a web browser displaying the homepage of the Bavarian State Ministry of Justice and Consumer Protection. The browser's address bar shows the URL www.justiz.bayern.de/ministerium/. The page features a search bar, a navigation menu with links to 'Ministerium', 'Justiz und Justizvollzug', 'Verbraucherschutz', 'Service', 'Presse und Medien', and 'Landesgesetzprüfungsamt', and a main banner image of a building. A sidebar on the left contains a 'MINISTERIUM' menu with links to 'Ministerin', 'Wir über uns', 'Kontakt', 'Reden', 'Gesetzgebung', 'Projekte', 'Veranstaltungen', and 'Justizministerkonferenz'. The main content area includes a welcome message, a quote by Ambrosius, and a list of links to various pages. A right sidebar contains 'Ministerium aktuell' and 'Alles was Recht ist' sections.

1. Informationsrecherche

Einer der herausragenden Vorteile des Internets ist der **nahezu unbegrenzte Zugang zu Wissen und Informationen**. Auf keine andere Weise lässt sich derart schnell in Erfahrung bringen, wie das Wetter in den nächsten Tagen wird, wie man am schnellsten von A nach B kommt, welche Zutaten in ein bestimmtes Gericht gehören oder wer die Wahlen in einem bestimmten Land gewonnen hat. Und es gibt quasi nichts, was sich nicht irgendwo finden lässt. Und das oft auch noch kostenfrei.

Nachrichten

Fast alle Printmedien wie Tageszeitungen oder Journale haben mittlerweile einen Online-Auftritt. Auf Portalen wie www.zeit-online.de, www.spiegel.de oder www.augsburger-allgemeine.de findet man aktuelle Informationen, die man ansonsten erst am nächsten Tag in der Zeitung lesen könnte.

Suchmaschinen

Wenn man nach bestimmten Dingen im Netz sucht, etwa nach Reiseberichten, sollte man eine so genannte **Suchmaschine** benutzen. Dies ist eine eigens für die Suche nach bestimmten Schlagworten oder Namen programmierte Internetseite. Bei der Recherche über eine Suchmaschine wie Google, Bing oder ixquick muss man jedoch auf ein paar Dinge achten, um nicht mit Informationen überhäuft zu werden oder ganz woanders zu landen, als man eigentlich möchte. Die meisten Suchmaschinen sind „dumm“ – zumindest noch. Neue „mitdenkende“ Suchverfahren sind mehr und mehr im Kommen. Derzeit muss man aber die meisten Suchmaschinen mit exakten Informationen, wonach man genau sucht, füttern.

ANLEITUNG:

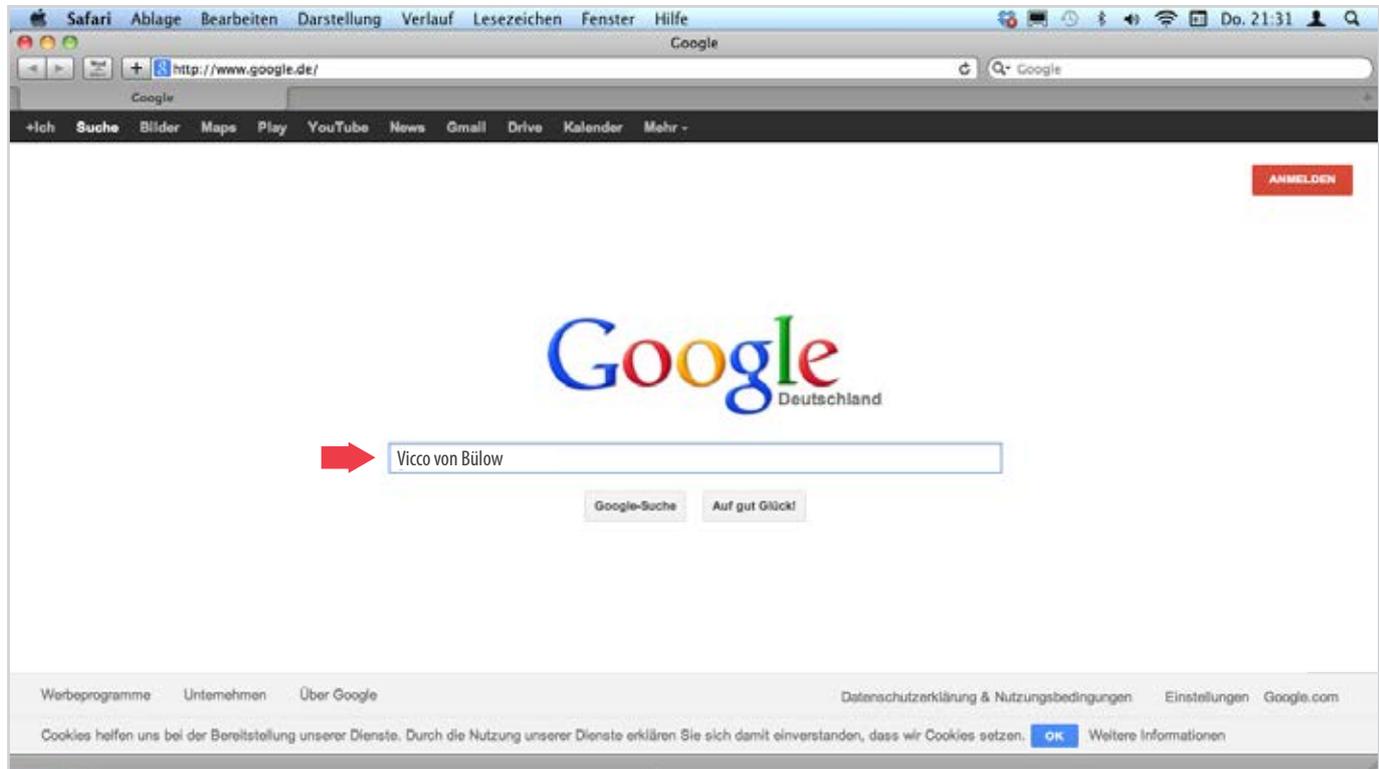


- ✓ Öffnen Sie die Homepage der Suchmaschine (zum Beispiel www.google.de).
- ✓ Geben Sie in das Suchfeld (oft in der Mitte der Seite) die zu suchenden Begriffe ein und drücken Sie die „Enter-Taste“ oder „Return“.
- ✓ Um die Ergebnisse zu präzisieren sollte man immer mehrere Begriffe eingeben, beispielsweise wenn man nach Fußballergebnissen aus der Bundesliga sucht, neben „Fußball“ noch „Ergebnisse“ und „1. Bundesliga“.
- ✓ Oft hilft auch, wenn man eine Frage in die Suchmaske eingibt, zum Beispiel „Wie baue ich ein Türschloss ein?“ In der Regel bekommt man eine Vielzahl von Ratgeberseiten genannt oder findet sogar Hinweise auf veranschaulichende Film- und Videobeiträge.
- ✓ Bei der Suche nach Personen empfiehlt es sich, den Vor- und den Nachnamen in Anführungszeichen zu setzen (Beispiel „Vicco von Bülow“). Dann erkennt die Suchmaschine, dass die Wörter zusammengehören und filtert andere Ergebnisse weitgehend aus.



WARNUNG:

Mit der Auswertung von Suchanfragen können Suchmaschinen ein relativ exaktes Profil von jedem Nutzer erstellen, das zum Beispiel Aufschluss über Vorlieben, Interessen, Freundschaften, Hobbys und andere Eigenschaften geben kann. Dies erkennt man daran, dass sich die Suchergebnisse (und die in der Regel zusätzlich geschaltete Werbung) an die von der Suchmaschine gewonnenen Erkenntnisse über den Nutzer anpassen. Und dieser kann sich kaum davor schützen. Alternativen bieten etwa Anbieter wie „ixquick“ (www.ixquick.com), die bewusst auf die Sammlung persönlicher Daten bei der Suche verzichten..



2. Online-Shopping

Der Handel mit Waren im Internet wächst und wächst. Allein im Jahr 2012 wurden in Deutschland via Internet Waren im Wert von fast **40 Milliarden Euro** umgesetzt. Die Vorteile liegen auf der Hand: Bequem im Netz nach Schnäppchen suchen und vom Sofa aus bestellen, warten bis es geliefert wird und wenn's nicht gefällt, kann man es in der Regel einfach zurückschicken – und das alles ohne Stau, Parkplatzsuche und Schlangestehen. Aber: Vorsicht! Zwar ist der Verbraucher in der Regel durch die bestehenden Gesetze gut geschützt, aber trotzdem gilt es, einige Punkte zu beachten und die Augen offen zu halten.

Wie immer wenn es um Geld geht, **birgt** auch der **Einkauf** über das Internet **Gefahren**. Verbraucher bekommen ihre Ware nicht, auch wenn sie diese schon bezahlt haben, sensible Kunden-Daten werden unberechtigt an Dritte weitergegeben oder gehen gar ganz verloren. Richten Sie Ihr Augenmerk daher auf Punkte wie:

▶ **Seriosität des Anbieters**

Wirkt der Internetauftritt seriös? Ist die Seite gut strukturiert und kundenfreundlich aufgebaut? Achtung zum Beispiel auch bei Angeboten, die preislich deutlich unter dem von anderen Anbietern liegen. Das könnte auch eine Falle sein. Nutzen Sie Ihren gesunden Menschenverstand!

▶ **Werden die rechtlichen Vorgaben eingehalten?**

Der Anbieter ist verpflichtet, ein Impressum mit seinen vollständigen Kontaktdaten anzugeben, seine Allgemeinen Geschäftsbedingungen (AGB) zugänglich zu machen und auf das Widerrufsrecht hinzuweisen, wenn der Kunde Verbraucher ist. Der Bestellvorgang darf erst mit einem deutlich erkennbaren Hinweisbutton (etwa „zahlungspflichtig bestellen“) ausgelöst werden.

▶ **Sind meine Daten sicher?**

Geben Sie Ihre Daten nur ein, wenn die Seite besonders geschützt ist. Das erkennt man an dem Schloss- oder Schlüsselsymbol im Eingabefenster Ihres Browsers. Außerdem beginnt die Internetadresse mit einem „**https**“.

▶ **Sind die angebotenen Zahlungsmethoden sicher?**

Am sichersten ist die Zahlung auf Rechnung; man bezahlt erst, wenn man die Ware bekommen hat. Auch das Lastschriftverfahren hat Vorteile: Man kann sein Geld durch Widerruf der Belastung im Notfall zurückbekommen. Treuhänder oder Zahlungsdienstleister wie PayPal oder Click & Buy bieten einen gewissen Schutz, wenn der Verkäufer zum Beispiel nicht liefert. Aber ebenso wie bei Kreditkartenzahlungen muss man seine Daten zusätzlich einem Dritten preisgeben. Vorkasse birgt dagegen immer die Gefahr, dass man etwas bezahlt und hinterher mit leeren Händen da steht.

Internet-Gütesiegel

Findet sich auf der Internetseite des Shopping-Anbieters ein Gütesiegel oder ein Label, kann dies ein Indiz für Seriosität sein. Dabei ist aber nicht jedes Siegel gleich zu bewerten. Es gibt immer wieder Anbieter, die eine solche Auszeichnung selbst erfinden oder der Einfachheit halber auf eines zurückgreifen, das ohne sonderliche Anforderungen oder besondere Prüfung durch einen seriösen Zertifizierer verliehen wird.

Umso wichtiger ist es darauf zu achten, dass das Siegel selbst auch eine gewisse Qualität mit sich bringt. Die vier Internet-Gütesiegel, die sich seit Jahren in einem Projekt der Initiative D21 engagieren (www.internet-guetesiegel.de) und die sich freiwillig zu mehr und besserem Verbraucherschutz im Netz verpflichtet haben, sind an dieser Stelle zu empfehlen. Sie haben sich den D21-Qualitätskriterien und damit einer besonderen Aufsicht und zusätzlichen Prüfung unterworfen.



Trusted Shops
www.trustedshops.de



TÜV SÜD
www.tuev-sued.de



Geprüfter Online-Shop
www.gepruefter-webshop.de



Internet privacy standards
www.datenschutz-cert.de

Eine Umfrage aus dem letzten Jahr hat ergeben, dass bereits 76% aller „Internetshopper“ diese vier Siegel kennen und dass diese für sie bei unsicheren Zahlungsverfahren – wie etwa Vorkasse – oder bei Shops, die ihren Sitz im Ausland haben, umso wichtiger werden.

Diese vier Gütesiegelanbieter haben in Deutschland aktuell bereits mehr als 13.000 Internet-Shops zertifiziert. Sie bieten die Gewähr für einen sichereren Online-Handel mit den von ihnen geprüften Anbietern.

Und sollte doch einmal etwas schiefgehen, dann bieten Siegel-Anbieter wie Trusted Shops die **Streitschlichtung** oder gar die **Erstattung etwaiger Auslagen** mit an. Alternativ kann man sich auch an die Online-Schlichtungsstelle wenden (www.online-schlichter.de).

HINWEIS:

Eine 100%ige Sicherheit gibt es – wie auch im stationären Handel – nicht. Umso wichtiger ist es, seine Rechte als Verbraucher zu kennen.



Ihre Rechte beim Online-Kauf

✓ **Rückgabe der Ware ohne Angabe von Gründen oder Widerruf:**

Der Verbraucher hat bei Unternehmern grundsätzlich ein **Widerrufsrecht**. Innerhalb von 14 Tagen ab Lieferung der Ware kann er sich in der Regel vom Vertrag lösen (Achtung: Ausnahmen gibt es bei speziell angefertigten, bei verderblichen und bei entsiegelten Waren). Der Käufer muss die Ware innerhalb dieses Zeitraums **einfach zurücksenden**, ab einem Wert von über 40 EUR muss er noch nicht einmal die Rücksendungskosten tragen. In einigen Fällen muss man zusätzlich noch den **Widerruf erklären**. Ein Blick in die Anbieterinformationen klärt darüber auf. Fehlt die Belehrung, verlängert sich die 14-Tage-Frist sogar noch.

✓ **Ware bezahlt, aber sie kommt nicht:**

Auch bei einem Versandhändler kann mal etwas schief gehen. Also sollte man ihn erst einmal anrufen oder eine E-Mail mit entsprechendem Hinweis schreiben. Folgt keine Reaktion, sollte man dem Verkäufer **schriftlich** (am besten per Einschreiben mit Rückschein) **eine Frist für die Lieferung setzen**. Lässt er diese verstreichen, kann der Verbraucher entweder die Lieferung **auf rechtllichem Wege durchsetzen** oder **vom Vertrag zurücktreten** und sein Geld zurückverlangen. Hier empfiehlt es sich, auch die Rücktrittserklärung per Einschreiben mit Rückschein zu versenden.

✓ **Ware ist mangelhaft:**

Ist die von einem gewerblichen Anbieter gelieferte Ware mangelhaft, hat der Verbraucher **Gewährleistungsansprüche**. Ein Mangel liegt dann vor, wenn die sog. „**Ist-Beschaffenheit**“ von der „**Soll-Beschaffenheit**“ abweicht (Eselsbrücke: „Es ist nicht wie es soll“) oder der Kaufgegenstand nicht die für den üblichen Gebrauch **erforderlichen Eigenschaften** aufweist. Dies ist zum Beispiel dann der Fall, wenn ein Reifen Luft verliert.

Der Verbraucher muss dem Verkäufer zunächst eine angemessene **Frist zur Nacherfüllung** (Reparatur oder Neulieferung der Ware) setzen. Verstreicht diese erfolglos, kann der Verbraucher entweder **vom Vertrag zurücktreten** oder weiterhin auf einer **mangelfreien Ware bestehen**. Der Rücktritt muss gegenüber dem Verkäufer **erklärt** (zum Beispiel durch Einschreiben mit Rückschein) und die Ware zurückgeschickt werden. Der Verkäufer muss daraufhin schon bezahltes Geld zurückerstaten. Möchte der Käufer die Ware trotz des Mangels behalten, kann er dem Verkäufer zum Beispiel eine Reduzierung des Kaufpreises anbieten.



Achtung: Durch die Umsetzung der EU-Verbraucherrechterichtlinie (VRRl) ändern sich voraussichtlich einige Dinge.

Diese betreffen zum Beispiel die Übernahme der Rücksendekosten durch den Verbraucher. Es wird von einem Inkrafttreten des Gesetzes im Juni 2014 ausgegangen.

CHECKLISTE



- ✓ Impressum (Name des Anbieters, Anschrift, Kontaktdaten & Erreichbarkeit, Firmierung, Hinweis auf das Registergericht etc.) vorhanden?
- ✓ Hat der Shop seinen Sitz in Deutschland? Die Rückabwicklung mit einem Shop im Ausland kann unter Umständen schwieriger sein (z. B. Sprache, erhöhte Portokosten, etc.).
- ✓ Sind Allgemeine Geschäftsbedingungen (AGB) ersichtlich?
- ✓ Gibt es einen Hinweis auf Widerrufs- oder Rückgabemöglichkeit?
- ✓ Sind die Versandkosten und die Gesamtkosten klar und deutlich angeben?
- ✓ Werden sichere Bezahlformen angeboten? Vorkasse kann risikobehaftet sein, besser ist Rechnungskauf oder die Teilnahme am Lastschriftverfahren.
- ✓ Ist eine Datenschutzerklärung vorhanden (sind meine Daten sicher)? Sind die Daten in einem geschützten Bereich („https“ & Schlosssymbol) einzugeben?
- ✓ Hat der Shop ein seriöses Internet-Gütesiegel?





Der Kauf von Produkten über Internetauktionsplattformen wie eBay birgt einige Besonderheiten: Neben kommerziellen Anbietern, die Neuwaren verkaufen, finden sich auch unzählige Privatleute, die zum Beispiel gebrauchte Kindersachen oder den Schrank von der Großmutter auf diese Weise veräußern möchten.

Bei den **gewerblichen Anbietern** ändert sich im Großen und Ganzen zum Vorhergesagten nicht viel. Sie sind genauso Unternehmer wie die Anbieter, auf deren Seiten man direkt Waren kaufen kann. Der Verbraucher hat in diesem Fall also alle oben genannten Rechte. Man erkennt kommerzielle Anbieter bei eBay daran, dass sie als „gewerblicher Verkäufer“ benannt sind. Einzige Einschränkung: Beim Kauf von gebrauchten Sachen kann der **gewerbliche Verkäufer** die Gewährleistungsfrist auf ein Jahr (sonst: 2 Jahre) verkürzen. Es ist im Übrigen grundsätzlich egal, ob man etwas ersteigert oder in Form des „Sofort-Kaufs“ die Transaktion sofort auslöst.

Beim Kauf von **Privaten** müssen Käufer dagegen darauf vertrauen, dass mit dem ersteigerten Produkt alles in Ordnung ist. Der private Verkäufer kann nämlich **seine Gewährleistungsrechte** ausschließen.

Man kann daher zum Beispiel die Sache nicht einfach zurückschicken, wenn sie einem nicht gefällt.

Angaben zum Verkäufer

██████████ (29 ★)

100% Positive Bewertungen

[Diesen Verkäufer speichern](#)

[Andere Artikel aufrufen](#)

Angemeldet als **privater Verkäufer**

Solange nicht strafrechtlich relevantes Verhalten beim Verkäufer zu verzeichnen ist (etwa eine eindeutige Betrugsabsicht), **hat man beim Privatverkäufer daher schlechtere Karten als beim gewerblichen**. Umso wichtiger sind hier die Bewertungen der anderen Nutzer: Neben dem Namen des Verkäufers findet sich eine Zahl und ein Stern. Wenn man auf diese Zahl klickt, gelangt man zu den **Bewertungen des Vertragspartners** aus früheren Transaktionen. Mithilfe dieser Bewertungen kann man sich ein Bild vom Verkäufer machen. Und wenn doch etwas schief geht: Der Plattformanbieter eBay bietet ein Schlichtungsverfahren an und probiert, eine gütliche Einigung herbeizuführen. Das Unternehmen eBay selbst ist übrigens nie der Vertragspartner, sondern stellt lediglich die Plattform zur Verfügung.

Zu guter Letzt: Bewertungsportale

Auf der Suche nach Rat oder Hinweisen orientiert sich ein Großteil der Verbraucher daran, was andere Internetnutzer über einen Anbieter oder ein Produkt schreiben. Oftmals geschieht dies in extra dafür eingerichteten **Bewertungsportalen** wie etwa www.qype.com oder www.ekomi.de. Positive Bewertungen können ein Indiz für ein gutes Produkt oder auch einen seriösen Anbieter sein. Vor allen Dingen, wenn sich viele davon finden lassen. Man muss sich aber darüber im Klaren sein, dass sich Bewertungen oft recht einfach manipulieren lassen – im Positiven wie auch im Negativen. Da werden Bewertungen einfach erfunden, um der Konkurrenz zu schaden oder es werden Anbieter rein aus Gefälligkeit über den grünen Klee gelobt. Keinesfalls sollte man sich also blind auf die Angaben in einem derartigen Portal verlassen. Lieber über eine Suchmaschine noch nach weiteren Hinweisen zu dem Produkt oder dem Anbieter suchen. Je mehr positive oder negative Äußerungen sich finden lassen, desto unwahrscheinlicher ist eine zielgerichtete Manipulation der Bewertungen.

EMPFEHLUNG:



Weitere Informationen: www.kaufenmitverstand.de ist die Homepage der Kampagne „Online Kaufen – mit Verstand!“ vom Bundesverband des Deutschen Versandhandels (bvh) und eBay für mehr Sicherheit im Onlinehandel mit Tipps und Tricks für den Notfall.



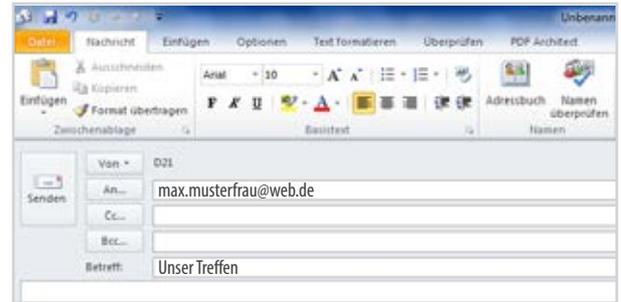
3. Kommunikation

E-Mail

► Aufbau einer E-Mail

Eine E-Mail ist eine elektronische Nachricht, sozusagen der Brief des Internets. Eine E-Mail kann man an alle die Personen schicken, deren E-Mail-Adresse man kennt.

Eine E-Mail-Adresse ist durch das „@“-Zeichen gekennzeichnet (z.B. „kontakt@initiated21.de“).



► E-Mailprogramme

Eine E-Mail kann man in einem eigens dafür entwickelten Programm wie zum Beispiel „Outlook“ von Microsoft oder „Thunderbird“ von Mozilla schreiben oder in einem sogenannten „webbasierten Online-Client“ wie web.de oder GMX, bei denen man für die E-Mail-Erstellung seinen Webbrowser nutzt.



ANLEITUNG:

„An“, „cc“, „bcc“

In das „An“-Feld trägt man die E-Mailadresse des Empfängers ein. Soll jemand die Nachricht in Kopie bekommen, so trägt man dessen E-Mailadresse in das „cc“-Feld ein. Wenn der Empfänger dies nicht mitbekommen soll, dann nutzt man für den Kopienempfänger statt des „cc“-Feldes das „bcc“-Feld.

Senden

Nachdem man eine E-Mail verfasst hat, klickt man auf den „Senden“-Button, um sie abzuschicken.

Empfangen

Mithilfe des „Empfangen“-Buttons ruft man seine E-Mails vom Mailserver ab. Oft ist „Senden/Empfangen“ auch als Funktion zusammen geführt.

Antworten/Weiterleiten

Möchte man auf eine E-Mail antworten, einfach oben auf „Antworten“ klicken. Soll die E-Mail nebst Anhängen an einen Dritten weitergeleitet werden, dann nutzt man dafür den „Weiterleiten“-Button.

„Netiquette“

„Netiquette“ ist ein Kunstwort und setzt sich aus „Net“ (englisch für „Netz“ (Internet)) und „Etiquette“) zusammen. Man umfasst damit die allgemeinen Regeln für den Umgang miteinander im Netz. Wichtig ist, dass man E-Mails im Prinzip wie einen herkömmlichen Brief strukturiert: In die Betreff-Zeile schreibt man einen kurzen Hinweis auf den Inhalt der E-Mail. Das ist wichtig, da ansonsten die Gefahr besteht, dass die E-Mail als sog. „Spam“ bewertet werden kann und dann nicht zugestellt wird.

Spam

Als „Spam“ oder auch „Junk“ (englisch für „Abfall“) wird die massenhafte Übersendung von elektronischen Nachrichten bezeichnet, deren Inhalte in der Regel Werbung sind. Nach Schätzungen sind beinahe 90% des gesamten weltweiten Mailaufkommens dem sogenannten „Spamming“ geschuldet. Daher bewirken Spams einen enormen volkswirtschaftlichen Schaden und verschwenden eine Unmenge an Ressourcen (Zeit, Energie, etc.).

Der Aufwand für den Spammer ist dabei überaus gering, die Adressen können in großer Zahl im Netz käuflich erworben oder mit speziell dafür entwickelten Programmen im Netz zusammengesammelt werden.

Die rechtliche Verfolgung von Spamming ist jedoch schwierig. Zwar hat der Empfänger grundsätzlich einen Unterlassungsanspruch gegen den Versender, aber die Geltendmachung erweist sich in der Realität oftmals als nahezu unmöglich.



HINWEIS:



Seit 2007 kann man sich an die SPAM-Beschwerdestelle des eco-Verbandes wenden und ihnen die Spam-Nachricht weiterleiten.

Vorgehensweise: Für Beschwerden über deutschen Spam bitte die E-Mail an die folgende E-Mail Adresse weiterleiten:

allgemeiner-spam@internet-beschwerdestelle.de

Sicherheit

Sicherheit ist ein großes Thema beim E-Mailverkehr. Kurz vorab: Die E-Mail ist nicht sicher und kann ohne weiteres abgefangen werden. Sie eignet sich daher nicht, vertrauliche Informationen oder sensible persönliche Daten über das Netz zu versenden. E-Mails können auch Schadsoftware übertragen und mit ihrer Hilfe kann auch versucht werden, an sensible Daten wie etwa Passwörter zu kommen:

Viren, Trojaner und Co.

Klicken Sie niemals auf Anhänge in E-Mails, deren Absender Sie nicht kennen. Ansonsten können Bilder und sonstige Daten auf dem eigenen Rechner ganz schnell zerstört sein. Auch finanzielle Schäden können drohen. Die größten Gefahrenquellen sind:

_Viren:

Programme, die sich selbst verbreiten. Einmal infiziert, kann die Hard- und die Software des Opfers manipuliert werden und Schaden nehmen. Das Virus wird in der Regel automatisch mit einem anderen (dem infizierten) Programm gestartet.

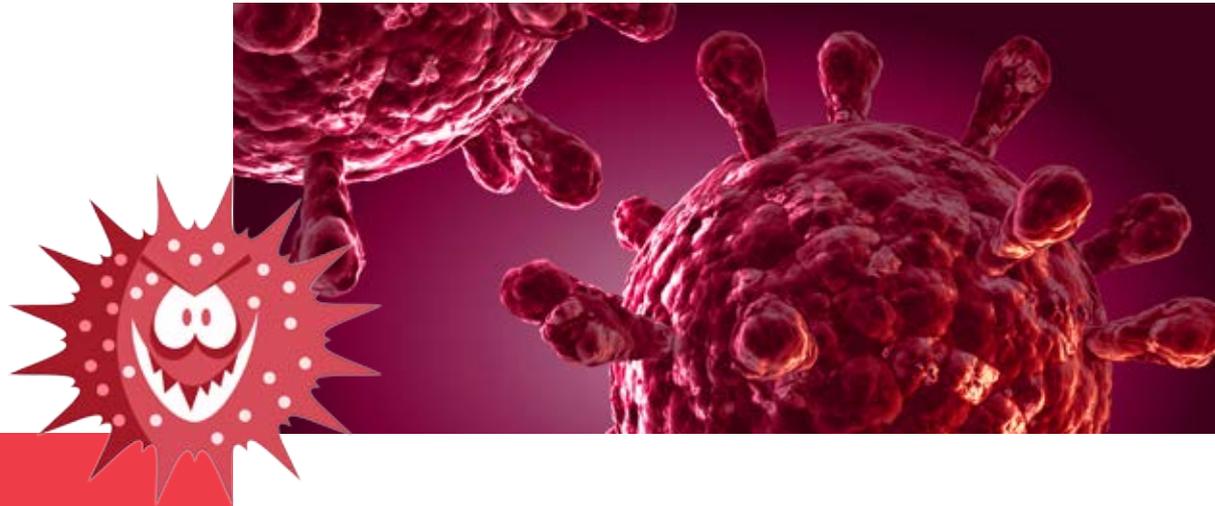
_Würmer:

Im Gegensatz zu einem Virus, versuchen Computerwürmer aktiv und eigenständig Prozesse zu manipulieren. Traurige Berühmtheit erlangte etwa der Computerwurm „I love you“, der unter anderem alle Bilder auf den infizierten Rechnern löschte.

_Trojanische Pferde:

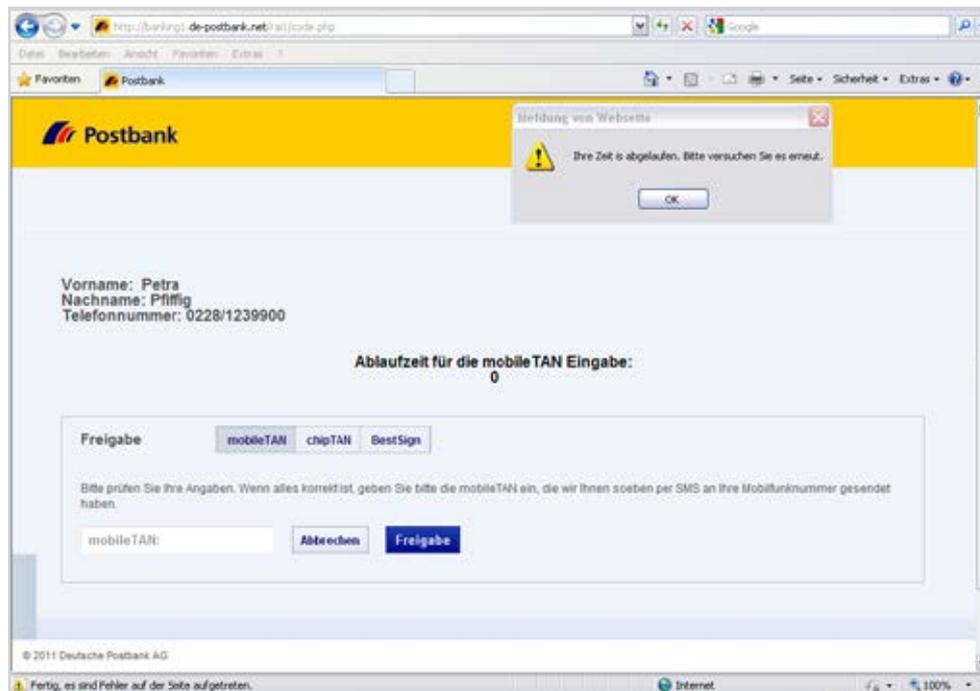
Schadsoftware, die oft an einem (scheinbar) nützlichen Programm angedockt sind. Hierunter fallen etwa viele Spionage-Programme („Spyware“), die es dem Täter erlauben, Vorgänge auf dem Rechner des Opfers mitzuverfolgen.

Oftmals treten auch Mischformen dieser sogenannten „Malware“ (Schachtelwort aus „malus“ = lat. für „schlecht“ und „ware“ von „Software“) in Erscheinung.



Phishing-Mails

Oft bekommt man E-Mails von **unbekannten Personen**, die einem Geschäftsvorschläge unterbreiten. Eine Person berichtet zum Beispiel von der unruhigen politischen Situation im Land X und das er deswegen dringend Geld ins Ausland transferieren müsse. Derjenige, der ihm sein Konto dafür zur Verfügung stellt, solle für diese kleine Dienstleistung einen hohen Betrag als Belohnung erhalten. Manchmal findet sich aber auch ein bekannter Name im Absenderfeld. Hintergrund ist oftmals, dass Adressbuchdateien von Dritten missbraucht werden, um so an sensible Daten ahnungsloser Opfer zu gelangen. Auch von **Banken** – möglicherweise sogar von der eigenen – können vermeintlicherweise verdächtige E-Mails kommen. Hier wird einem zum Beispiel angetragen, man solle doch dringend seinen Online-Banking-Zugang verifizieren. Zu diesem Zwecke müsse man auf dieser oder jenen Internetseite seinen PIN und seinen TAN eingeben.



E-Mails dieser Art haben in **keinem Fall einen realen Hintergrund**. Sie werden als „**Phishing-Mails**“ bezeichnet („phishing“ = Kunstwort, das sich an das englische „fishing“ anlehnt und im weitesten Sinn mit „etwas abfischen“ zu übersetzen ist). Ziel ist es, auf diese **Weise Daten des Nutzers zu erhalten** und diese missbräuchlich zu verwenden. Meist verraten sich die E-Mails durch eklatante Schreibfehler oder dergleichen. Aber manche sind mittlerweile doch täuschend ähnlich.

WARNUNG:

Es drohen Gefahren wie Kontoplünderungen und Identitätsdiebstahl.

Löschen Sie diese E-Mails daher sofort! Auf keinen Fall antworten oder auf in der E-Mail zu findende Verlinkungen auf andere Seiten klicken.



Chatten

Chatten ist eine besondere Form der Unterhaltung via Internet. Man kann sich Nachrichten schreiben, die sofort beantwortet werden können. In der Regel passiert dies in einem öffentlichen „Chatroom“ – für mehr Privatheit kann man den Chat jedoch in spezielle „Rooms“ (englisch für „Räume“), das heißt in besondere geschützte Bereiche, verlagern.

Chats erfreuen sich großer Beliebtheit, bieten sie doch die Möglichkeit, quasi in Echtzeit miteinander zu kommunizieren. Es gibt Chats für fast alles, am verbreitetsten sind sie jedoch im Bereich Kontaktanzeigen. Man sollte sich jedoch darüber im Klaren sein, dass man ähnlich wie in sozialen Netzwerken nie sicher sein kann, wer sein Gegenüber eigentlich ist. Also am besten keine **vertraulichen Informationen oder Fotos herausgeben** und immer den **gesunden Menschenverstand** benutzen.



Skypen



Mithilfe des Internets und des Programms „Skype“, einer Telefonie-Software des Unternehmens Microsoft, kann man auch **kostenfrei telefonieren**. Eine gute Möglichkeit, um etwa mit weit entfernten Familienmitgliedern in Kontakt zu bleiben. Über die **Webcam**, über die viele Geräte verfügen, kann man sich dabei sogar sehen. Aber Vorsicht, nur **Anrufe von Skype-Nutzer zu Skype-Nutzer** sind auch wirklich kostenlos. Da auch immer wieder Meldungen kursieren, dass Skype recht einfach abgehört werden kann, sollte man auch **keine besonders vertraulichen Dinge** zum Inhalt des Gesprächs machen.

Sie benötigen:

- ▶ das Programm „Skype“ (www.skype.de)
- ▶ eine Webcam und als Mindestausstattung ein Mikrofon und einen Lautsprecher (am besten eignet sich ein Headset)
- ▶ den Skypenamen des Anzurufenden



ANLEITUNG:

- ✓ Laden Sie Skype herunter und registrieren Sie sich.
- ✓ Am einfachsten ist es, bei Skype zunächst nach Freunden und Bekannten zu suchen. Haben Sie welche gefunden, fügen Sie sie zu Ihren Kontakten hinzu.
- ✓ Öffnen Sie die Kontaktkarte der Person, die Sie anrufen möchten. Klicken Sie auf „Anruf“ („Call“). Die Person, die Sie anrufen möchten, muss online sein (grünes Häkchen neben dem Bild des Nutzers).
- ✓ Alternativ: Wenn Sie eine Webcam haben, klicken Sie auf „Video-Anruf“ („Video call“).
- ✓ Die Farbe des Bildschirms ändert sich und im unteren Bereich wird eine Anrufliste eingeblendet. Sie hören einen Klingelton, bis der Anruf angenommen wird.
- ✓ Zum Beenden auf das rote Telefonhörersymbol klicken.
- ✓ Weitere Informationen und Anleitungen: <https://support.skype.com/de/>

GLOSSAR, HILFREICHE LINKS UND INFORMATIONSEITEN

Glossar

AGB	Allgemeine Geschäftsbedingungen (eines Händlers oder Anbieters)
Anhang	(auch „E-Mail-Anhang“) Eine mit einer E-Mail mitgesendete Datei
AntiSpy	„Anti-Spionage-Programm“, das verhindert, dass zum Beispiel Passwörter bei der Eingabe durch Dritte mitgelesen werden
Backup	Sicherung der eigenen Dateien auf einem anderen (->) Speichermedium
Betriebssystem	Benutzeroberfläche eines (->) PC, (->) Notebooks, (->) Tablets oder (->) Smartphones
Bewertungsportal	Seiten im Internet mit Produktbewertungen anderer Nutzer (auch für Hotels und andere)
Blogs	Internetseite zu einem bestimmten Themengebiet für den Austausch mit anderen, oft durch Privatnutzer geführt
Browser	(->) Software für den Zugang ins Internet
Chatten	Direkter Austausch mit anderen Nutzern in einem (->) Chatroom
Chatroom	Plattform im Internet zum (->) Chatten
Datenträger	(->) Speichermedium wie eine CD-ROM oder ein USB-Stick
Downstream	Anhand des Downstreams kann man die Leistungsfähigkeit eines Internetzugangs messen (oft auch „Downloadrate“ genannt)
DSL/VDSL	Leitungsgebundene Datenübertragungstechnologien
E-Mail	Elektronischer Brief
E-Mail-Programm	(->) Software für die Erstellung und Bearbeitung einer (->) E-Mail
Firewall	(->) Sicherheitsprogramm, blockt Angriffe von Dritten auf das eigene System ab
Flatrate	Eine Flatrate impliziert in der Regel ein unbegrenztes Datenvolumen, das heißt, der Nutzer kann beliebig viel im Internet surfen
Hardware	Technische Ausstattung für den Gang ins Internet
Homepage	Internetseite, zum Beispiel einer Person, einer Organisation oder eines Unternehmens

https	(engl. „Hyper Text Transfer Protocol Secure“) Eine besonders gesicherte Seite im Internet
Internetanschluss	Zugang in das Internet, zur Verfügung gestellt durch einen (->) Provider
Internet-Gütesiegel	Qualitätssiegel für mehr und besseren Verbraucherschutz im Internet
Laptop (oder „Notebook“)	Computer, Tastatur und Monitor in einem Gerät, gehört zur (->) Hardware
LTE/UMTS	Funkübertragungstechnologien
Netiquette	Verhaltensregeln beim Verfassen von (->) E-Mails
Notebook (oder „Laptop“)	siehe Laptop
Online-Shopping	Einkauf im Internet
Phishing-Mail	Betrügerische (->) E-Mail, mit deren Hilfe Dritte zum Beispiel an Zugangsdaten wie Passwörter gelangen wollen
Provider	Internetzugangsanbieter
Sicherheitsprogramme	(->) Software, die dem Schutz des Rechners und der Sicherheit der Daten des Nutzers dient
Skype	Videotelefoniedienst der Firma Microsoft
Smartphone	Sehr leistungsstarkes Mobiltelefon, das auch für das Surfen im Internet genutzt werden kann
Software	Programme, die auf einem Rechner laufen
Spam	Massenhaft versendete E-Mails oft werblichen Inhalts
Suchmaschine	Internetseite für die Suche im Internet
Tablet	Kleiner Rechner mit einem berührungsempfindlichen Bildschirm („Touchpad“)
Updates (automatische)	Dienen der Aktualisierung der Programme
Virenschutzprogramm	(->) Software, die dem Schutz des Rechners dient
Wikipedia	Größte Online-Enzyklopädie im Internet
W-LAN	(Wireless Local Area Network, engl. = „kabelloses ortsbundenes Netzwerk“). Ein abgeschlossenes Funknetz für die Internetnutzung
www	Abkürzung für „World Wide Web“ (engl. = „weltweites Netz“). Das www ist die Summe aller über die Protokolle „http“ und „https“ übertragenen Hypertext-Dokumente und damit in etwa das, was man als Otto Normalverbraucher unter dem „Internet“ versteht

Kurz und knapp

Die Sicherung des eigenen Systems ist das A und O. Von daher sollte man immer die Grundregeln beachten.
Sicherheitsvorkehrungen – Checkliste:

- ✓ Immer ein aktuelles **Virenschutzprogramm** verwenden. Achtung: Kostenfreie Lösungen schützen oftmals nicht vollumfänglich. Wichtig ist zum Beispiel auch der Schutz beim Surfen im Netz, da manipulierte Seiten auch durch das bloße Aufrufen einen Rechner infizieren können. Prüfen Sie regelmäßig, ob Updates vorhanden sind oder nutzen Sie die automatische Updatefunktion.
- ✓ **AntiSpy-Programme** schützen vor unerwünschten Beobachtern oder davor, dass Daten (zum Beispiel bei der Passworteingabe) unbemerkt übermittelt werden.
- ✓ Nutzen Sie eine **Firewall**, die den Datenverkehr überwacht und zusätzlichen Schutz vor Eindringlingen bietet. Einstellen lässt sich diese bei Computern mit dem Betriebssystem Windows über die Systemsteuerung.
- ✓ Sichern Sie Ihre Dateien – am besten auf einem separaten Speichermedium (CD-ROM, DVD, USB-Stick, etc.).
- ✓ Installieren Sie regelmäßig die **Updates** des Betriebssystems oder sonstiger Software (zum Beispiel Java). Am besten die „Auto-Update-Funktion“ aktivieren.
- ✓ Erhöhen Sie die **Sicherheitseinstellungen Ihres Browsers**. Tipps dazu finden Sie in der Regel beim Anbieter selbst (zum Beispiel: www.internet-explorer.de).
- ✓ Öffnen Sie niemals **Dateien unbekannter Herkunft**, die Sie zum Beispiel als Anlage einer E-Mail oder über ein Speichermedium bekommen haben.
- ✓ Nutzen Sie nur **sichere Zugangsdaten und Kennwörter** und geben Sie diese nicht an Dritte weiter. Ein sicheres Passwort besteht aus der Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Nehmen Sie verschiedene Passwörter für verschiedene Anwendungen, aber speichern Sie diese nicht auf dem PC, dem Notebook oder dem Tablet.



LINKS / WEITERFÜHRENDE INFORMATIONEN:



- ▶ www.vis.bayern.de:
Verbraucherportal der Bayerischen Staatsregierung zu allen wichtigen Verbrauchertemen. Die Sicherheit im Netz bildet im Bereich Daten und Medien einen eigenen Schwerpunkt.
- ▶ www.bsi-fuer-buerger.de:
Informationsseite des Bundesamtes für Informationssicherheit über die Gefahren des Internets und wie man ihnen am besten begegnet.
- ▶ www.bagso.de/verbraucherthemen/internet.html:
Internetauftritt der Bundesarbeitsgemeinschaft der Senioren-Organisationen mit Tipps und Tricks zur Internetnutzung. Besonders hervorzuheben sind hier die „Internet-Sicherheitsbriefe“.
- ▶ www.verbraucher-sicher-online.de:
Vom Bundesverbraucherschutzministerium gefördertes Projekt der TU Berlin. Ziel ist es, Verbraucher über die sichere Internetnutzung sowie den Zugang zu digitalen Inhalten und Informationen verständlich zu informieren. Empfehlenswert sind auch die Hinweise über die richtige Einstellung von Programmen.
(www.verbraucher-sicher-online.de/thema/sicher-surfen).
- ▶ www.surfer-haben-rechte.de:
Eine Aufklärungskampagne des Verbraucherzentrale Bundesverbandes (vzbv) mit dem Ziel, Verbraucher zu befähigen, sich sicher im Netz zu bewegen.
- ▶ www.polizei-beratung.de:
Informationsseite der Polizeilichen Kriminalprävention der Länder und des Bundes mit ausführlichen Hinweisen zu den Gefahren im Internet.
- ▶ www.sicher-im-netz.de:
Seiten des Vereins „Deutschland sicher im Netz“ mit Hinweisen für Verbraucher für mehr IT-Sicherheit.



Herausgeber:

INITIATIVE D21

Bayerisches Staatsministerium der
Justiz und für Verbraucherschutz



Redaktion:

Martin Falenski (Initiative D21) – V.i.S.d.P.

Gestaltung:

Ulrike Miller, www.miller-partners.com

Kontakt:

Initiative D21, Reinhardtstraße 38, 10117 Berlin
kontakt@initiated21.de, www.initiated21.de

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz
Prielmayerstraße 7, 80335 München
poststelle@stmjv.bayern.de, www.justiz.bayern.de,
www.vis.bayern.de



**Aufbruch
Bayern** 