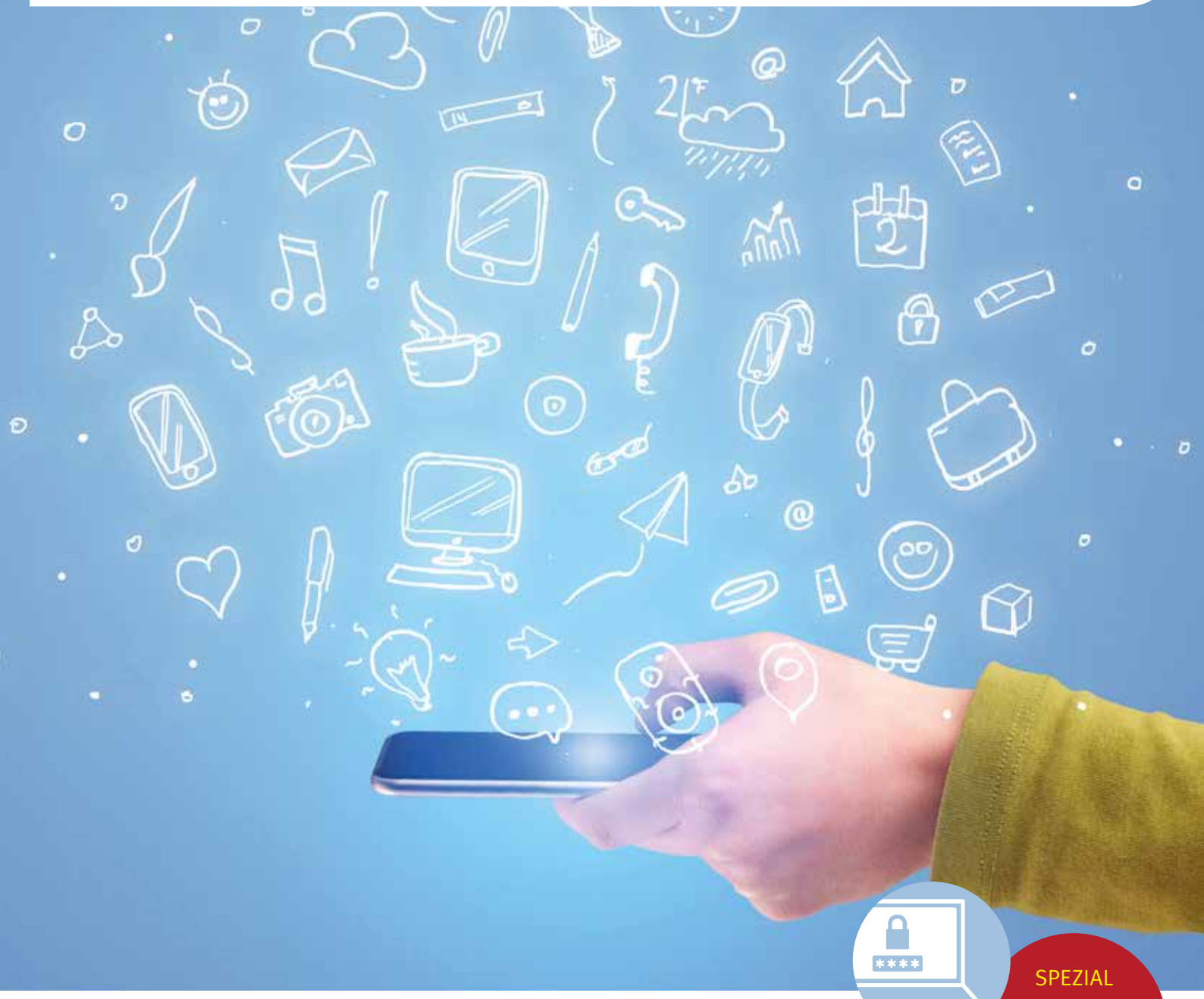
Verbraucher **konkret**

Themenheft der VERBRAUCHER INITIATIVE e.V.



SPEZIAL
BASISTIPPS: SICHERHEIT IM INTERNET

INTERNET-MYTHEN

Informieren.
Motivieren.
Gestalten.

Bundesverband
Die Verbraucher Initiative e.V.

GEGENSTÄNDE: SMARTPHONE, AUTO, STAUBSAUGER & CO.
KI: PRAKTISCHE ANWENDUNGEN & DUMME ALGORITHMEN

ISSN 1435-3547 • A12 114

LIEBE LESERIN, LIEBER LESER,

Computer und Internet revolutionierten in den 80er und den 90er Jahren die Arbeitswelt und erfreuten sich auch im privaten Bereich großer Beliebtheit. Dank mobiler Endgeräte wie Notebooks, Tablets oder Smartphones ist es inzwischen selbstverständlich, nicht nur zu Hause sondern auch unterwegs im Netz zu surfen oder zu mailen.

SPEZIAL
BASISTIPPS: SICHERHEIT IM INTERNET

Durch die rasant fortschreitende Technik können sich nicht nur Computer mit dem Internet verbinden. Gegenständen wie Autos, Kühlschränken, Heizungen, Türschlössern, Alarmanlagen, Fernsehern oder Fitnessarmbändern ist dies ebenfalls möglich. Das kann Vorteile haben, etwa Energie oder Strom sparen, für mehr Sicherheit sorgen oder das Leben bequemer machen. Doch diese Geräte sammeln Informationen über Lebensgewohnheiten, Vorlieben und andere persönliche Daten, die sie weitergeben. Privatsphäre und Datenschutz werden bedroht, der Verbraucher wird immer „gläserner". Der Missbrauch öffnet Kriminellen im wahrsten Sinne des Wortes Tür und Tor.

Hinzu kommen immer mehr Anwendungen der sogenannten „Künstlichen Intelligenz" (KI). Doch: Wie intelligent sind diese wirklich? Zwischen der Werbung der Anbieter, den Wünschen und Vorstellungen der Verbraucher und der Wirklichkeit klaffen bisweilen Lücken. Wir wollen helfen, die wichtigsten davon zu schließen.

Eine „smarte" Lektüre wünscht Ihnen

Guido Steinke
Fachreferent 60+ und Internet der VERBRAUCHER INITIATIVE e. V.

IMPRESSUM | Verbraucher konkret, September 2024 | ISSN 1435-3547 | „Internet-Mythen" – Themenheft der VERBRAUCHER INITIATIVE e. V. • Redaktionsanschrift: Wollankstraße 134, 13187 Berlin, Tel. 030/53 60 73-3, mail@verbraucher.org, www.verbraucher.org | Konzept & Text: Georg Abel (V.i.S.d.P.), Guido Steinke | Fotos: S. 2 privat, alle anderen: iStock | Papier: Diese Broschüre wurde klimaneutral auf Offset/Naturpapier weiß, FSC-zertifiziert, gedruckt. Hinweis: Wenn im Text z. B. vom „Verbraucher" die Rede ist, ist dies ein Zugeständnis an die Flüssigkeit der Sprache, gemeint sind natürlich alle Verbraucherinnen und Verbraucher. |

Die einmalige Anforderung der Themenhefte ist im Mitgliedsbeitrag der VERBRAUCHER INITIATIVE e. V. (100,00 Euro/Jahr, ermäßigt 80,00 Euro/Jahr, online 50,00 Euro/Jahr) enthalten. Einzelverkaufspreis für Nichtmitglieder: 2,00 Euro zzgl. Versand (abhängig vom Umfang der Bestellung).

SMARTPHONE, AUTO, STAUBSAUGER & CO. KONTROLLIEREN

Selbstfahrende Autos, das „Internet der Dinge“ (Internet of things, kurz IoT) und „Smart Home“ sind in aller Munde, vor allem denen der Wirtschaft. Der Verbraucher wird mit immer neuen Begriffen und Geräten konfrontiert. Nicht alle halten, was die Werbung verspricht. Neben Vorteilen lauern Risiken und Gefahren, vor denen Daten- und Verbraucherschützer warnen.

Wenn Haushaltsgeräte und -technik, Geräte der Unterhaltungs- und Sicherheitselektronik Informationen erfassen, verarbeiten und ins Internet übermitteln können, wird das als „Internet der Dinge“ bezeichnet. Die Hersteller bringen immer mehr Dinge der täglichen Nutzung ins Internet, Möglichkeiten und Markt wachsen. Werden Haushaltsgeräte und -technik oder einzelne Bereiche davon vernetzt, spricht man vom „Smart Home“ oder „intelligentem Haus“ (smart = pfiffig, klug, schlau).

INTELLIGENTES ZUHAUSE

Es kann praktisch sein, „intelligente“ Geräte in seiner Wohnung zu haben, z. B. Bewegungsmelder, die dafür sorgen, dass das Licht angeht, wenn es benötigt wird und ausgeht, wenn niemand mehr im Raum ist. So spart man Strom. Machbar wird das z. B. dank intelligenter Sensoren, die menschliche Aktivität, Helligkeiten oder Raumtemperaturen messen können. Alternativ können Geräte im Smart Home direkt über ein Smartphone oder Tablet gesteuert werden. Die Heizung lässt sich von unterwegs aktivieren, das Licht gedimmt einschalten oder der Backofen anstellen sobald man sich dem Haus nähert. Das ist komfortabel, aber „smart“? Wenn das eigene Smartphone so etwas kann, können das auch Fremde.

ACHTUNG: Einbrecher werden sich nicht damit aufhalten, die Heizung hoch und das Licht herunterzufahren. Sie haben es auf das elektrische Garagentor, die Jalousien oder die Schließanlage abgesehen, die vernetzt und mit dem Smartphone zu steuern sind. Hacker testen regelmäßig Lücken in den Systemen, die ans Internet angeschlossen sind. Bei PCs ist bekannt, dass eine gute Firewall und ein Antivirenschutz wichtig sind, genauso wie aktuell gehaltene Programme. Ob es ausreichende Sicherungssysteme für Heizung & Co. gibt, sollte daher unbedingt geprüft werden, bevor das Haus „smart“ wird.

TIPPS

- Lassen Sie bei der Einrichtung eines „klugen Hauses“ die gleiche Sorgfalt walten wie bei WLAN und PC: Verschlüsseln, sichere Passwörter und PINs verwenden, die Software immer aktuell halten und – sofern möglich – Firewall und Virenschutz installieren.
- Bedenken Sie: Alle Geräte, die Sie über Ihr Smartphone steuern können, können von anderen übernommen werden. Sie sollten es den digitalen Einbruchshelfern so schwer wie möglich machen.

ICH „WHATSAPPE“ BLOSS

Früher benötigte man für den Gang ins Internet noch einen Computer und ein Telefon. Heute sind alle Smartphones internetfähig. Dank der Funkübertragung per WLAN (Wireless Local Area Network, engl. für drahtloses lokales Netzwerk) können auch andere Geräte ins Netzwerk eingebunden werden und ins Internet gehen, zum Beispiel der Fernseher. Die Technik hinter Anwendungen wie WhatsApp tritt gar nicht mehr in Erscheinung. So kann es passieren, dass man jemanden statt über das Telefonnetz über WhatsApp anruft.

TIPPS

- Achten Sie darauf, ob Sie das mobile Datennetz oder das Telefonnetz nutzen (bei Ihrem Smartphone). Je nachdem können unterschiedliche Kosten entstehen (Anrufe, SMS, mobile Daten).
- Verwenden Sie ein gesichertes Funknetz.
- Klären Sie, welche Daten durch das Gerät übertragen werden und an wen.

ANONYM?

Das Internet macht‘s möglich – endlich wieder jung, sportlich, gut aussehend! Schließlich bestimme ich, welches Geburtsdatum ich angebe und welche Fotos ich zu meinem Profil hochlade. Noch schnell eine Kiste Wein bestellt und dann mit dem jungen Mädel im Chat geflirtet. Mir kann ja keiner nachweisen, wer ich wirklich bin. Kann man nicht?

Welche Adresse und welchen Namen gebe ich für die Lieferung des Weins an? Und mit welcher E-Mail-Adresse habe ich mich registriert, zur Sicherheit noch meine Mobilnummer angegeben (2-Faktor-Authentisierung). Nicht nur die Polizei kann so schnell herausfinden, wer ich wirklich bin. Im realen Leben mag es amüsant sein, in eine andere Person zu schlüpfen. Tut man das

im Internet, kann man nicht belangt werden, wenn man nicht die (Rechts-)Kreise anderer stört.

Im Internet können sich folgende Probleme ergeben:

- Das „junge Mädel“, das ich kontaktiert habe, ist wirklich jung. Die Eltern der 11-Jährigen kommen dahinter und ich habe eine Anzeige wegen sexueller Belästigung Minderjähriger am Hals.
- Die Firma, bei der ich den Wein bestellt habe, stellt fest, dass unter dieser Adresse gar kein Mensch mit meinem erfundenen Namen gemeldet ist. Die meisten Melderegister stellen Firmen ihre Daten gegen Bezahlung zur Verfügung. Sie stellen in so einem Fall eine Anzeige wegen Betruges oder geben die Information weiter an die Meldebehörden.
- In einem Kommentar lasse ich mich zu deutlichen Worten gegenüber Politikern hinreißen. Dann kann es passieren, dass ich Post von der Staatsanwaltschaft bekommen, wegen Beleidigung oder Bedrohung.

Halten Sie sich daher an gewisse Spielregeln wie im realen Leben auch. Eine gute Übersicht zur sog. „Netiquette“ findet sich z. B. bei Wikipedia (www.wikipedia.de › Suchbegriff „Netiquette“).

Im Internet ist man nicht wirklich anonym – außer man bewegt sich professionell im Darknet. Dieses „dunkle Netz“ existiert parallel zum frei zugänglichen Internet, ist aber durch Verschlüsselung abgeschirmt.

WAS IST SCHON SCHNELL?

Die Internetanbieter überschlagen sich mit Angeboten. „Highspeed Internet Flat zum Top-Preis“, „Telefon, Internet, Fernsehen – alles zum Sparpreis“. Wenn man genau hinsieht, entdeckt man immer eine Einschränkung, den *Sternchen-Hinweis: „Nur die ersten 12 Monate, danach doppelt so teuer“ oder „bis zu 50 Mbit/s.“

TIPPS

- Achten Sie auf die Technik, die dahinter steckt. Ob Glasfaser, Kabel, DSL oder mobile Daten, jede hat ihre Grenzen.
- WLAN ist bequem, weil man damit viele Geräte mit dem Internet verbinden kann. Die WLAN-Box hat aber Übertragungsgrenzen. Manchmal ist ein (LAN-)Kabel die schnellere Variante, oder eine neue Box mit größerer Kapazität. Sie wird z. B. in Mbit/s (= Megabits pro Sekunde) angegeben. 50–100 Mbit/s sollten es sein, wenn Sie auch fernsehen möchten.
- Mit einem im Auftrag der Bundesnetzagentur entwickelten Test können Sie die Übertragungsgeschwindigkeit Ihres Breitbandschlusses ermitteln und mit den Daten im Vertrag vergleichen: www.breitbandmessung.de. Ergibt die Messung tatsächlich eine größere Diskrepanz, sollten Sie die Messergebnisse sichern, mit den Angaben in der Leistungsbeschreibung vergleichen, bei Ihrem Anbieter nachfragen, und wenn es keine Lösung des Problems gibt, sich an die Verbraucherzentralen wenden. Sie können den Vertrag prüfen und ggfs. gegen falsche Werbeversprechen vorgehen.
- Sie können den monatlichen Betrag kürzen und unter Umständen fristlos kündigen, wenn Sie einen zu langsamen Festnetzanschluss bekommen haben. Die Verbraucherzentrale hat dazu Musterbriefe.
- Wechseln Sie den Anbieter, beachten Sie jedoch die Kündigungsfristen. Manchmal hilft schon ein Wechsel des Tarifs oder der verwendeten Technik.

Das gleiche gilt für die „Alles inklusive Flat“ beim Mobiltelefon. Ist wirklich alles „inklusive“, auch die Nutzung im und ins Ausland? Durch SMS ins Ausland oder Sondernummern können horrende Kosten entstehen.

ONLINE EINKAUFEN

Wenn der Kunde Rechnung, Kontoauszug und Bestellbestätigung selber abruft (und zu Sicherungszwecken ausdruckt), spart das dem Anbieter Zeit und Geld. Er muss diese Systeme sowieso vorhalten, aber statt seiner Mitarbeiter bedient sie nun der Kunde und wird zum „Prosument“ (aus „Pro-duzent“ und „Kon-sument“).

Bei Bestellungen von standardisierten Produkten oder Nachbestellungen kann sich das Internet lohnen. Das Fachgeschäft (vor Ort) hat Vorteile bei:

- komplexeren Buchungen wie Reisen mit Sonderwünschen, Flügen und Zugfahrten mit Zwischenstopps.
- hochwertigeren Anschaffungen. Zwar haben Sie beim Online-Kauf ein Widerrufsrecht, um sich die Ware vor der Nutzung anzuschauen. Wer schickt aber schon gerne teuren Schmuck oder Porzellan quer durch die Republik? Es muss alles gut verpackt und versichert werden, was die Kosten erhöht.
- Spezialanfertigungen: Dabei gibt es kein Widerrufsrecht. Wenn etwas nicht zu Ihrer Zufriedenheit geliefert wird, müssen Sie auf die Kulanz des Anbieters setzen oder den schwereren Weg der Gewährleistung gehen.

SMARTPHONE, AUTO & CO.

Das Internet ist überall. Manchmal möchte man aber nicht überall erreichbar und damit überwachbar sein.

Über das Mobilfunknetz lässt sich eine Verbindung zum Internet aufbauen. Wer schon versucht hat, im Zug längere Telefongespräche zu führen oder seine E-Mails zu beantworten, kennt die Grenzen der ständigen und grenzenlosen Erreichbarkeit. Ziel ist, sie selbst zu bestimmen, ebenso wie das, was man damit über sich preisgibt.

HILFE, ICH WERDE ÜBERWACHT

In älteren Krimis musste dafür noch ein Sender am Auto befestigt werden. Heute kann dies fast jedes kleine Programm auf dem Smartphone. Fast alle Apps (= Applikationen), d. h. kleine Programme mit unterschiedlichen Funktionen, die auf dem Smartphone oder Tablet installiert werden können, verlangen nach einer Freigabe dafür. Was bedeutet das und was ist davon zu halten? Bequemlichkeit vs. Datenschutz: Die meisten Programmierer interessiert nicht, wo Sie gerade sind. Auch die Firmen haben kein konkretes Interesse an Ihnen als Individuum. Sie wollen „nur“ Geld verdienen und das geht im Internet über Werbung oder über Dienste, die Ihnen kostenpflichtig verkauft werden. Das Sammeln von Ortungsdaten ist daher nicht per se gefährlich. Es kann aber dazu führen, dass Sie Werbung von der Pizzeria an der Ecke erhalten oder Ihnen eine neue App angeboten wird.

Es gibt inzwischen Programme, mit denen man seine Kinder oder dem Ehepartner nachspionieren kann, z. B. die App „mSpy“. Die Nützlichkeit ist umstritten. Bei Neuwagen wird diese Technik seit 2018 eingesetzt, um bei Unfällen den Rettungskräften schnellstmöglich den Weg zu weisen (eCall). Das ist sinnvoll. Das Recht auf Privatsphäre ist höchstrichterlich verbrieft (Bundesverfassungsgericht, Urteil vom 2. März 2006, Az. 2 BvR 2099/04). Dies wird in Frage gestellt, wenn eine permanente Überwachung machbar ist.

TIPPS

- Aktivieren Sie Ortungsdienste nur dann, wenn Sie diese wirklich brauchen.
- Prüfen Sie die Hersteller der Apps und installieren Sie keine aus dubiosen Quellen.
- Schalten Sie das Smartphone zwischendurch aus.
- Wenn Sie nur mobil telefonieren und fotografieren möchten, genügen vielleicht noch ein älteres Handymodell – und ein Fotoapparat.

SMARTPHONE

E-Mails abrufen, Bahnverbindungen suchen und Tickets buchen, etc. – es gibt fast nichts, was diese kleinen Super-Computer nicht können. Vermehrt werden sie außerdem als Portemonnaie und Gesundheitscoach eingesetzt, von den „spielerischen“ und unterhaltenden Möglichkeiten (Musik, Video, Spiele) ganz zu schweigen.

TIPPS

Schauen Sie sich Apps genau an, bevor Sie sie installieren:

- Wer ist der Herausgeber und gibt es schon Beschwerden über ihn? Dazu den Namen in eine Suchmaschine eingeben mit dem Zusatz „Probleme“ oder „Beschwerden“.
- Lesen Sie Rezensionen oder seriöse Tests.
- Schauen Sie bei kostenlosen Apps, ob sie werbefinanziert oder von öffentlichen Stellen herausgegeben werden.

FEIND IN MEINER HAND

Das Smartphone wird immer öfter Ziel von Cyber-Kriminellen. Mit einem Trojaner können sie das Gerät übernehmen und dann an Ihrer Stelle:

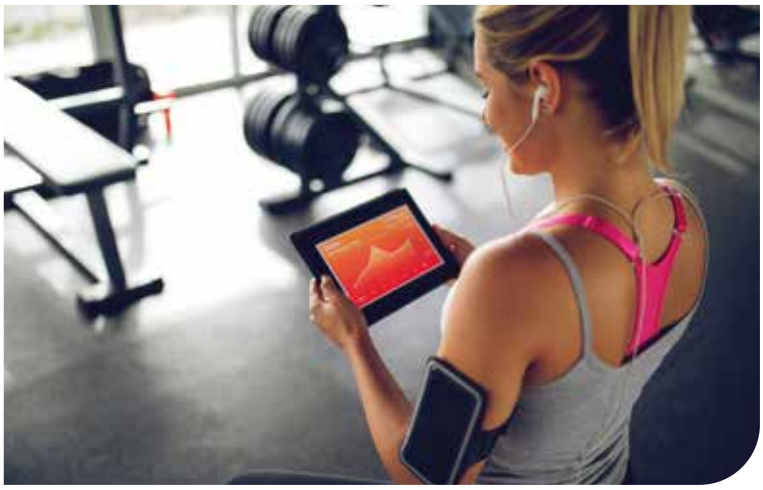
- Einkäufe tätigen, die über Ihr Bankkonto abgerechnet werden – aber nicht bei Ihrer Adresse ankommen
- Geld per Online-Banking auf ein Betrugskonto Konto überweisen
- kostenpflichtige SMS an teure Nummern versenden, gleich hundertfach und vieles mehr.

TIPPS

- Nutzen Sie Sicherheitsangebote, des Telefons. Das sind:
  - Bildschirm-Sperrcode einrichten
  - Automatische Updates aktivieren
  - Virenschutz und Firewall (zumindest bei Android-Geräten, Apple-Geräte sind besser ab Werk geschützt).
- Aktivieren und nutzen Sie starke Passwörter, auch bei der Nutzung von geldrelevanten Apps.
- Verwenden Sie beim Onlinebanking nicht dasselbe Smartphone, an das auch die mobile TAN geschickt wird!

FITNESS APPS

Vor allem Fitness-Armbänder erfreuen sich großer Beliebtheit. Gaukeln sie einem doch vor, dass das Smartphone nicht nur zu einem krummen Nacken führen kann, sondern auch zu einer besseren Figur. Die kleinen Fitness-Überwacher funktionieren nämlich mit einer App, über die dann mit Hilfe des Smartphones Daten und Auswertungen an Anbieter im Internet übertragen werden. Ob jemand dadurch tatsächlich fitter geworden ist, als mit „analogem“ Training, ist noch nicht geklärt. Sicher ist jedoch, dass dadurch eine Menge Daten über den Nutzer anfallen, die im Zweifel den Anbieter der App reicher machen (sollen).



MEIN AUTO FÄHRT ALLEIN

Das Auto parkt selbständig ein, es bremst für spielende Kinder und hängt sich auf der Autobahn in sicherem Abstand hinter den Vordermann: In der Realität erkennt die Einparkhilfe nicht jedes Hindernis, der „Active City Stop“ bremst auch für aufgewirbelte Blätter. Wenn nach der Vollbremsung der LKW hinter Ihnen seine 40 Tonnen nicht so schnell zum Stehen bekommen sollte wie Sie Ihre 1,5 Tonnen, kann es lebensgefährlich werden. Zumindest ist Ärger vorprogrammiert. Denn keiner der Hersteller übernimmt die Haftung für Unfälle. Die Verantwortung trägt der Fahrer oder Halter, ebenso für die Absicherung der Elektronik gegenüber An- und Eingriffen von außen.

TIPPS

Wenn Sie auf Nummer sicher gehen wollen, bleiben Ihnen letztendlich nur drei Wege:

- Nutzen Sie Ihr altes, nicht mit Elektronik vollgestopftes Auto so lange wie möglich. Dies ist auch umweltfreundlicher – allein die Herstellung eines Neuwagens verschlingt Unmengen an Energie und Ressourcen.
- Versuchen Sie, Ihre Werkstatt davon zu überzeugen, die unnötige Elektronik abzuschalten.
- Wählen Sie ein Auto, das von der elektronischen Revolution weitestgehend verschont wurde.

MEINE VERSICHERUNG WEISS, WIE ICH FAHRE

Autoversicherer sind auf den Zug der „smart-mobility“ aufgesprungen. Sie locken mit günstigen Tarifen, wenn der Fahrer sein Fahrverhalten überwachen lässt. Bei diesen sogenannten Telematik-Tarifen verpflichten sich die Kunden, eine Überwachungs-Box im Auto oder eine App auf dem Smartphone zu installieren, die Daten über ihre Fahrweise an die Versicherung übermittelt: Brems- und Beschleunigungsverhalten genauso wie Geschwindigkeit und Leerlaufzeiten.

Die Stiftung Warentest rät ab, vor allem, so lange nicht klar ist, wer letztendlich Zugriff auf die Daten erhält. Hinzu kommt, dass man bei manchen Versicherern für die Technik bezahlen muss. Die Ersparnis relativiert sich dann schnell, vor allem, wenn man kein Fahranfänger ist und sowieso schon eine günstige Beitragsklasse hat.

Vergleichen Sie die Konditionen von verschiedenen Versicherern und wechseln Sie zu einem günstigeren Anbieter, z. B. zum Ende des Jahres.

HOTSPOTS

Öffentliche WLANs (Wireless Local Area Networks = Drahtlose lokale Funknetzwerke), also Internetzugänge über Funknetzwerke sind oft kostenlos. Sie sparen Datenvolumen, z.B. bei Mobilfunkverträgen und sind oft schneller als der Weg ins Internet über das Mobilfunknetz. Das Problem: Sie sind öffentlich, d.h. es können auch andere in dem Netz fischen, in dem Sie gerade unterwegs sind. Die Betreiber haften in erster Linie für Urheberrechtsverstöße, die über WLANs passieren, nicht aber bei Datenklau der Nutzer untereinander. Das bedeutet: Wenn jemand in Ihren Laptop oder Ihr Smartphone einbricht und z.B. Passwörter klaut, ist das in erster Linie Ihr Problem.

Beachten Sie ein paar Regeln, um sich in öffentlichen Hotsports sicher zu bewegen. Zu den wichtigsten, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammengestellt hat, gehören:

- Schalten Sie die WLAN-Funktion nur ein, wenn Sie diese benötigen! Viele Geräte haben die WLAN-Funktion immer aktiviert, z.B. Smartphones. Wenn Sie nicht mit dem Netzwerk verbunden sind, kann auch keiner einbrechen.

- Versenden Sie keine vertraulichen Daten über ein fremdes WLAN-Netz! Online-Banking, Bestellungen oder die Eingabe von anderen wichtigen Daten wie Passwörtern: Wenn Sie nicht wollen, dass Ihr Nachbar hier mitliest, dann seien Sie bei fremden WLANS zurückhaltend.
- Achten Sie auf verschlüsselte Hotspots. Sie sind sicherer als unverschlüsselte.
- Deaktivieren Sie die Datei- und Verzeichnisfreigaben.
- Deaktivieren Sie nach Möglichkeit die automatische Anmeldung an bekannten Hotspots. Den Namen seines WLANs kann jeder frei wählen. Daher ist es denkbar, dass Betrüger WLANs errichten, die „Telekom“ heißen, und dann darauf warten, dass Sie sich mit Ihren Geräten einbuchen. So können sie nicht nur Ihre Zugangsdaten abgreifen, sondern auch den gesamten Datenverkehr mitlesen.

ONLINE IM AUSLAND

Auch im Ausland können kleine Internethelfer wie Smartphones oder Tablets sehr nützlich sein. Allerdings schlagen die Anbieter bei den Kosten zu. Wer einen alten Vertrag hat oder gar auf eine Kreuzfahrt geht, kann davon ein Lied singen. Auf Kreuzfahrten kann das Handy eine Kostenfalle sein, z.B. wenn es sich ins Bordnetz einwählt.

Die Falle heißt „Hintergrundaktualisierung". Seien es nun Karten oder E-Mails, Wetterdaten oder Fotos. Viele Apps sind so voreingestellt, dass sie ständig nach aktuellen Daten im Internet suchen – oder permanent Daten an ihren Herausgeber übermitteln (wie z.B. Facebook). Was im Inland (bei einer günstigen Flatrate = Pauschalvertrag mit großem Datenvolumen und niedrigem Preis) praktisch ist, kann im Ausland Hunderte, ja sogar Tausende an Euros kosten. Dem Autor ist ein Fall bekannt, bei dem eine Woche Smartphone-Nutzung auf den Hurtigruten 1.700 Euro kosten sollte.

TIPPS

- Informieren Sie sich vor der Reise bei Ihrem Anbieter nach günstigen „Auslandspaketen" – und buchen Sie sie rechtzeitig.
- Innerhalb der EU gilt der Grundsatz „Roam like at home", das heißt telefonieren oder surfen wie zu Hause, ohne Zusatzgebühren.
- Achten Sie im Grenzgebiet auf die Mobilnutzung, denn schnell hat man sich z. B. in Konstanz ins Schweizer Netz eingewählt.
- Die Gerichte verpflichten die Anbieter regelmäßig, Sie bei „ungewöhnlichem Nutzungsverhalten" zu warnen. Ignorieren Sie diese Warnungen nicht.
- Auf Schiffen gelten meist Sonderbestimmungen. Informieren Sie sich vor dem Ablegen, ansonsten kann es zu Hause eine böse Überraschung geben. Schiffe sind über das Satellitennetz verbunden, das oft besonders teuer ist.

BIBLIOTHEK IN DER JACKENTASCHE

Schwere Bücher schleppen war gestern. Heute passen in jede Jackentasche hunderte, sogar tausende von Büchern mit einem der modernen Lesegeräte (z. B. Kindle oder Tolino). Sie ersetzen nicht das haptische Erlebnis des „Begreifens" eines Buches, auch Randnotizen zu machen, ist etwas schwierig. Doch Vorteile haben sie schon. So lassen sich der Kontrast und die Helligkeit verändern, genauso wie die Buchstabengröße und der Hintergrund. Außerdem wiegen diese Geräte nur ein paar Hundert Gramm. Das ist ein immenser Vorteil, wenn man z. B. im Urlaub nicht eine Bücherkiste mitschleppen möchte.

Diese Geräte erhalten die Buchdateien über das Internet, sei es per Onleihe oder direkt in der Internet-Buchhandlung. Manchmal muss man dazu die Geräte mit einem Computer verbinden, der Zugang zum Internet hat. Einige Geräte haben aber auch direkten Internetzugang, z. B. Tablets. Für ungetrübte Lesefreude sind dabei ein paar Punkte zu beachten. Hier gilt im Grunde das gleiche wie bei anderen Geräten mit direktem Zugang zum Internet.

TIPPS

- Gehen Sie nicht über ungesicherte Netzwerke ins Internet, z. B. in Cafés.
- Versehen Sie Ihr Gerät mit einem PIN- oder Passwort-Schutz, damit nicht jeder Ungebetene mitlesen kann – oder für Sie teure Einkäufe bei Ihrem Buchhändler tätigt, falls Ihnen das Gerät abhandenkommt.
- Lassen Sie es bei einem Verlust unverzüglich sperren.
- Halten Sie die Software aktuell durch regelmäßige Updates.

KANN ICH DIGITALE BÜCHER WEITERGEBEN?

Bei einem Buch in Papierform ist den meisten Menschen die Lage klar: man kann es verleihen, weiterverkaufen, sogar darin herumschreiben… und man hat ein 14-tägiges Widerrufsrecht beim Erwerb über das Internet. Bei den E-Books dagegen streiten sich die Verbraucherschützer noch mit den Anbietern und den Gerichten. Bei Amazon heißt es stellvertretend für viele Anbieter in den AGB: „Sofern nichts anderes ausdrücklich angegeben ist, dürfen Sie die Rechte an den Kindle-Inhalten oder Teilen davon nicht verkaufen, vermieten, verleihen, vertreiben, im Rundfunk ausstrahlen, unterlizenzieren oder anderweitig an Dritte abtreten".

Im März 2013 hat das Landgericht Bielefeld einem anderen Anbieter dazu Recht gegeben (LG Bielefeld, Urteil vom 5.3.2013, Az. 4O 191/11): Er durfte ähnliche lautende AGB verwenden, d. h. die Nutzung für die Verbraucher entsprechend einschränken.

BASISTIPPS: SICHERHEIT IM INTERNET

Mit dem Internet holt man sich die halbe Welt ins Haus. Damit dabei keine ungebetenen Gäste Zutritt erhalten, gilt es ein paar Dinge zu beherzigen.

Die Geräte, mit denen man ins Internet geht sollten abgesichert sein. Dazu gehört ein aktueller Virenschutz nebst Firewall.

Zu diesen Geräten zählen nicht nur der WLAN-Router zu Hause, Computer, Smartphone oder Tablet. Auch bei anderen vernetzten Geräten, die mit Schnittstellen ausgestattet sind (Bluetooth oder WLAN) wie Überwachungskameras, Fernseher, oder Saugrobotern lohnt es sich, vor Kauf und Inbetriebnahme einen Blick in die Sicherheitseinstellungen zu werfen. Man möchte ja nicht, dass die Einbrecher per Überwachungskamera nachsehen können, ob man zu Hause ist und ob sich ein Einbruch lohnt.

ONLINE-ZUGÄNGE UND -DIENSTE

Vor der Inbetriebnahme verlangen viele Geräte eine Registrierung beim Hersteller. Auch so praktische Dienste wie App-Stores bei den Smartphones oder E-Mail funktionieren nur nach einer Anmeldung auf den Servern der Anbieter, genauso wie viele Online-Händler oder Facebook und Co.. Wenn diese Anmeldedaten, also die „Schlüssel“ zu diesen Diensten, in falsche Hände gelangen, könnte jemand mit ihrem Namen, also ihrer Internet-Identität, E-Mails verschicken, sich bei anderen Diensten mit dieser E-Mail-Adresse anmelden und z.B. einen Fake-Shop betreiben. Oder er bestellt „nur“ in ihrem Namen Waren, die er dann an eine andere Adresse schicken lässt, natürlich auf ihre Kosten.Dies lässt sich vermeiden mit

- starken und komplexen Passwörtern und
- einer Authentifizierung mit einem zweiten Faktor.

SICHERES SMARTPHONE

Das Smartphone ist eines der wichtigsten Geräte geworden, mit denen man ins Internet geht. Vieles ist mit diesen Alleskönnern machbar. Neben Fotos und Kontakten verbleiben auch Kontodaten und Zugangscodes auf dem Handy. Das macht das Smartphone zur persönlichen Datensammelstelle und zum begehrten Ziel für Hackerangriffe. Hier die wichtigsten Tipps:

- SIM und Bildschirmsperre: Die Eingabe von PINs ist nervig. Sie schützen aber davor, dass Unbefugte Ihr Smartphone weiter nutzen, wenn sie es einmal verlieren oder vergessen sollten.
- Schnittstellen nur bei Bedarf einschalten: Über Schnittstellen wie Bluetooth oder auch WLAN können sich Unbefugte Zutritt zu ihrem Gerät verschaffen.
- Manche Apps verlangen oder benötigen Zugriff auf viele Funktionen: Kontakte, Kamera, Mikrofon, Standort uvm. Daher prüfen Sie die Apps, bevor Sie sie installieren.
- Keine Bezahldaten, keine Abzocke: Die meisten „Einbrecher“ haben es auf Ihr Geld abgesehen. Wenn Sie keine Bezahldaten im System oder den Apps hinterlegt haben und dazu noch eine Drittanbietesperre aktiviert ist, laufen diese Angriffe ins Leere.
- Aktuell bleiben: Was für den Computer und den WLAN-Router gilt, ist auch beim Smartphone wichtig. Sofortige, am besten automatische Updates.
- Daten, aber sparsam: Bei vielen Apps bezahlen Sie mit Ihren Daten. Wer wissen möchte, ob eine App besonders hungrig ist, kann bei www.mobilsicher.de nachschauen, › „Check Deine Apps“
- Backup wichtiger Daten: Smartphone sofort sperren (bei Diebstahl, online im Konto von Apple oder Google und die SIM unter 116 116, www.sperr-notruf.de).

Informieren.
Motivieren.
Gestalten.

Bundesverband
Die Verbraucher Initiative e.V.

ONLINE EINKAUF

Fake-Shops: So können Sie sich schützen

- Ist die Ware 50, 60 oder sogar 70 Prozent günstiger als im Laden, hat die Sache meist einen Haken. Entweder es ist Hehlerware, oder die Ware gibt es gar nicht und man möchte Sie zur Vorkasse verleiten.
- Lassen Sie sich nicht auf Vorkasse ein. Das Risiko mag bei kleineren Beträgen noch überschaubar sein. Bei größeren Summen empfehlen sich Einzugsermächtigung, Kreditkarte oder Rechnung. Wie bei der Einzugsermächtigung können Sie sich innerhalb bestimmter Fristen auch bei der Kreditkarte das Geld u. U. zurückholen – schauen Sie in Ihre Kreditkartenbedingungen!
- Achten Sie auf Siegel für vertrauenswürdige Online-Shops und scheuen Sie sich nicht, den Namen des Shops mit einer Suchmaschine auf Beschwerden hin zu untersuchen oder in Übersichten über Fake-Shops zu recherchieren.

Weitere Tipps beim Online-Einkauf

- Nehmen Sie den Händler unter die Lupe. Prüfen Sie das Impressum auf Vollständigkeit (Name der Firma, Rechtsform, verantwortliche Person, vollständige Postadresse – kein Postfach! Telefonnummer, E-Mail-Adresse) sowie die angebotenen Kontaktmöglichkeiten (Ansprechpartner, Telefonnummern, E-Mail-Adressen). Machen Sie im Zweifel einen Testanruf.
- Lesen Sie die Produktbeschreibung und beachten Sie die Versand- und Lieferbedingungen (Allgemeine Geschäftsbedingungen).

FAKE SHOPS: VON ANGEBOTEN, DIE ZU GUT SIND, UM WAHR ZU SEIN

Jeder hat inzwischen seine eigene Internetseite, seinen Online-Shop, sein Facebook-Profil. Manche wären dabei gerne jung, schön, sportlich. Gefährlicher sind aber diejenigen, die professionell an das Geld anderer Leute wollen. Sie versuchen dies mit gefälschten E-Mails und täuschend echten Internetseiten, den sogenannten „Phishing-Mails“1und „Fake-Shops“. Diese haben es auf Ihr Geld abgesehen.

- Achten Sie bei der Bestellung auf eine sichere Datenübertragung (ssl-Protokoll, im Browser zu erkennen an dem httpS://www... oder dem Schlosssymbol) und ein starkes Passwort.
- Wählen Sie eine sichere Art der Bezahlung, z.B. gegen Rechnung oder per Einzugsermächtigung.
- Das Widerrufsrecht ist bei kommerziellen Anbietern Pflicht. Bevor der Kaufvertrag abgeschlossen wird, muss der Verkäufer Sie über den Widerruf belehren und Ihnen mitteilen, bis wann und an wen Sie ihn richten können. Die gesetzliche Widerrufsfrist beträgt 14 Tage ab Erhalt der Ware.
- Achten Sie auf den Umgang mit Ihren Daten und werfen Sie einen Blick in die Datenschutzerklärung!

Folgen Sie Ihrem Instinkt! Angebote, die zu günstig sind, um wahr zu sein, sind es oft auch nicht. Und es gibt nicht nur betrügerische Shops, auch bei der Werbung mit Produkttests sind schwarze Schafe unterwegs.

INFORMATIONEN

- Verbraucher 60 plus – ein Informationsportal der VERBRAUCHER INITIATIVE zu vielen Themen für die ältere Generation: https://www.verbraucher60plus.de/ › Internet
- Verbraucherzentrale NRW: https://www.verbraucherzentrale.nrw/ › Wissenswertes zu... (unten auf der Seite) Thema wählen › Digitale Welt
- Zu Fake Shops: www.watchlist-internet.at › Unseriöse Webseiten › Betrügerische Online-Shops (Fake-Shops) und https://www.verbraucherzentrale.de/fakeshopfinder
- „Mach Dein Passwort stark“ eine Informationsseite der Polizei NRW: https://www.mach-dein-passwort-stark.de/
- Europäisches Verbraucherzentrum Deutschland, www.evz.de › Einkaufen und Internet
- Digital Kompass: Eine Informationsseite mit einer vielseitigen Fundgrube an Broschüren, Präsentationen, Checklisten, Vorträgen u.v.m.: https://www.digital-kompass.de/ › Materialien, dann runterscrollen zu den Themen
- Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de › Themen › Verbraucherinnen und Verbraucher › Tipps für den digitalen Alltag › Basistipps

Künstliche Intelligenz

- Eine gute Einführung findet man bei der Landeszentrale für Politische Bildung NRW: https://www.politische-bildung.nrw.de/ › Themen › Digitalisierung/Digitale Gesellschaft › Künstliche Intelligenz
- KI und Alter: Eine Informationsseite der BAGSO: https://ki-und-alter.de/kiwissen/
- KI Konkret: Künstliche Intelligenz einfach erklärt: https://www.ki-konkret.de/
- KI-Campus: Eine Lernplattform zum Thema KI, mit vielen guten Materialien, z. B. https://ki-campus.org/videos/wasistki
- Das Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI): Projekt von iRightsLab in Zusammenarbeit mit den Fraunhofer-Instituten AISEC und IAIS sowie der FU Berlin: https://www.zvki.de/

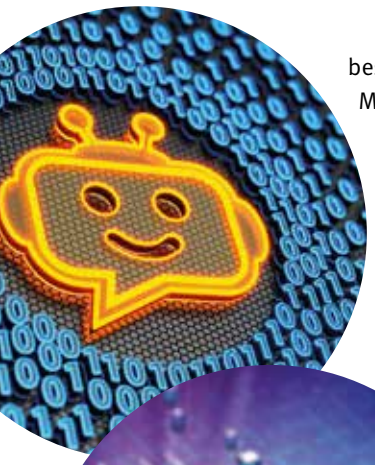
Verbraucher konkret „Internet-Mythen“ - Themenheft der VERBRAUCHER INITIATIVE e. V., Wollankstraße 134, 13187 Berlin, Tel. 030/53 60 73-3, www.verbraucher.org | Konzept & Text: Georg Abel (V.i.S.d.P.), Guido Steinke | Fotos: iStock | Nachdruck und Vervielfältigungen, auch auszugsweise, nur mit Genehmigung des Herausgebers und Quellenangabe. 09/2024

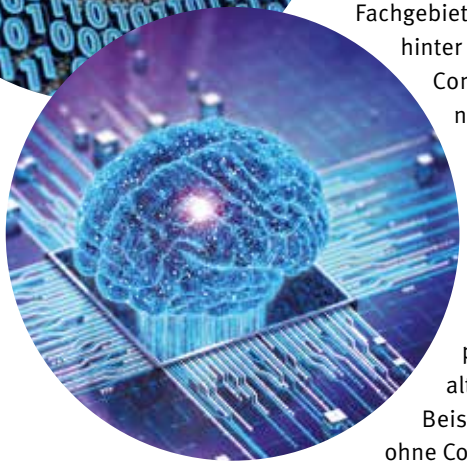
PRAKTISCHE ANWENDUNGEN & DUMME ALGORITHMEN

Es vergeht kein Tag, an dem Künstliche Intelligenz/KI (oder englisch „AI“ für „Artificial Intelligence“) nicht in den Schlagzeilen ist. Die Anwendungsgebiete sind schier grenzenlos. Jedes Unternehmen und jede Organisation, die technologisch auf der Höhe der Zeit sein will, nutzt KI oder plant dies zumindest. Was bedeutet es für die Verbraucherinnen und Verbraucher? Woran sollen wir uns orientieren? Die folgenden Punkte können bei der Einordnung helfen – und Missverständnissen vorbeugen.

Der Begriff steckt schon im Namen: Künstliche Intelligenz. Doch was ist Intelligenz? Da scheiden sich die Geister. Es gibt keine allgemein anerkannte Definition der Intelligenz, die mehr besagt als: Geistige Fähigkeiten zur Lösung eines logischen, sprachlichen, mathematischen oder sinnorientierten Problems. Da einzelne kognitive Fähigkeiten unterschiedlich stark ausgeprägt sein können und keine Einigkeit darüber besteht, wie diese zu bestimmen und zu unterscheiden sind, gibt es keine weiterführende, allgemeingültige Definition der Intelligenz. Für die Künstliche ist es ähnlich.

KI ÜBERTRUMPFT DEN MENSCHEN





Bestimmte Aufgaben kann KI besser als der Mensch, zum Beispiel Muster in großen Datenmengen schnell erkennen. Aber gerade dafür baut der Mensch seit Beginn der Menschheit Werkzeuge und Maschinen: Damit man mit ihnen Aufgaben schneller und besser erledigen kann.

Künstliche Intelligenz ist ein Fachgebiet der Informatik. Dahinter steckt der Versuch, Computern das Wahrnehmen, Denken und Handeln beizubringen, damit sie eigenständig Probleme erkennen und lösen können. Also: Ohne Computer, keine KI. Der alte VW-Käfer fuhr zum Beispiel noch komplett ohne Computer.

VON MENSCHEN EINGESETZT

Künstliche Intelligenz wird von Menschen (Unternehmen, Verwaltung, Organisationen, usw.) eingesetzt. Computer und Software werden zu bestimmten Zwecken gebaut, programmiert und verwendet. Dahinter stecken menschliche Entscheidungen und Motive. Kenne ich diese, kenne ich die KI, die eingesetzt wird. Man sollte sich also immer fragen: Wer setzt diese KI ein, zu welchem Zweck?

KI kann überall da zum Einsatz kommen, wo jetzt schon Computer und Software eingesetzt werden – also fast überall. Computerchips und damit die Computer werden immer kleiner. Sie stecken inzwischen in Glühbirnen und Personalausweisen. Theoretisch kann daher auch die Glühbirne „intelligent“ werden, also angehen, wenn ich das für richtig halte- oder wenn sie das für „richtig“ hält. Dazu müsste ich sie aber „trainieren“, ihr also zeigen, wann ich Licht haben möchte und wann nicht.

Bei der „Weltherrschaft“ wäre das genauso. Wer sollte die KI so trainieren, dass sie die Aufgaben, für die man sie gebaut hat, nicht mehr erfüllen wollen, und stattdessen über Menschen herfallen und sie versklaven? Wer würde dafür Geld und andere Ressourcen zur Verfügung stellen? Und: Jeder Computer benötigt Strom. Im Zweifel zieht man den Stecker. Es dürfte auffallen, wenn ein Computer plötzlich anfängt, eigene Kraftwerke zu bauen.

Natürlich können Menschen sie einsetzen und entsprechend bauen, aber das haben sie schon bei weitaus gefährlicheren Maschinen gemacht wie den Atombomben.

TURBO FÜR EDV-SYSTEME

KI beschleunigt die Verarbeitung von Daten, durch neue Systeme (z. B. neuronale Netze) und Programmierverfahren (Maschinelles Lernen). Dadurch ist sie leistungsfähiger und schneller als ältere EDV-Systeme, erheblich schneller. Ein Beispiel: Fotos konnte man auch früher schon retuschieren, im Fotolabor. Bei digitalen Fotos musste man dazu teilweise Pixel für Pixel ändern, was sehr zeitraubend war. Heute geht das mit zwei Klicks. Diese Schnelligkeit hat ihren Preis. Für das Training benötigt die KI riesige Datenmengen. Um diese zu verarbeiten, braucht es große Rechenzentren, die wiederum viel Strom verbrauchen. Experten schätzen, dass eine Suchanfrage mit KI 10 Mal mehr Energie verbraucht als eine herkömmliche.

KI: SINNVOLLE ANWENDUNGEN

Viele Lebensbereiche sind schon digitalisiert. In allen anderen können Computer zumindest unterstützen bei Beobachtungen und Auswertungen. Hierbei kann und wird oft auch KI eingesetzt. Sie kann zwei Dinge besser als herkömmliche Software: Große Datenmengen durchsuchen und Muster erkennen. Voraussetzung ist jedoch, dass sie zuvor gut trainiert wurde. Daran hapert es meist noch. Es gibt noch keine allgemeingültigen Standards für Trainingsdaten, die z. B. eine Diskriminierung nach Geschlecht oder Alter verhindern.

„FINDEMASCHINEN“ STATT SUCHMASCHINEN

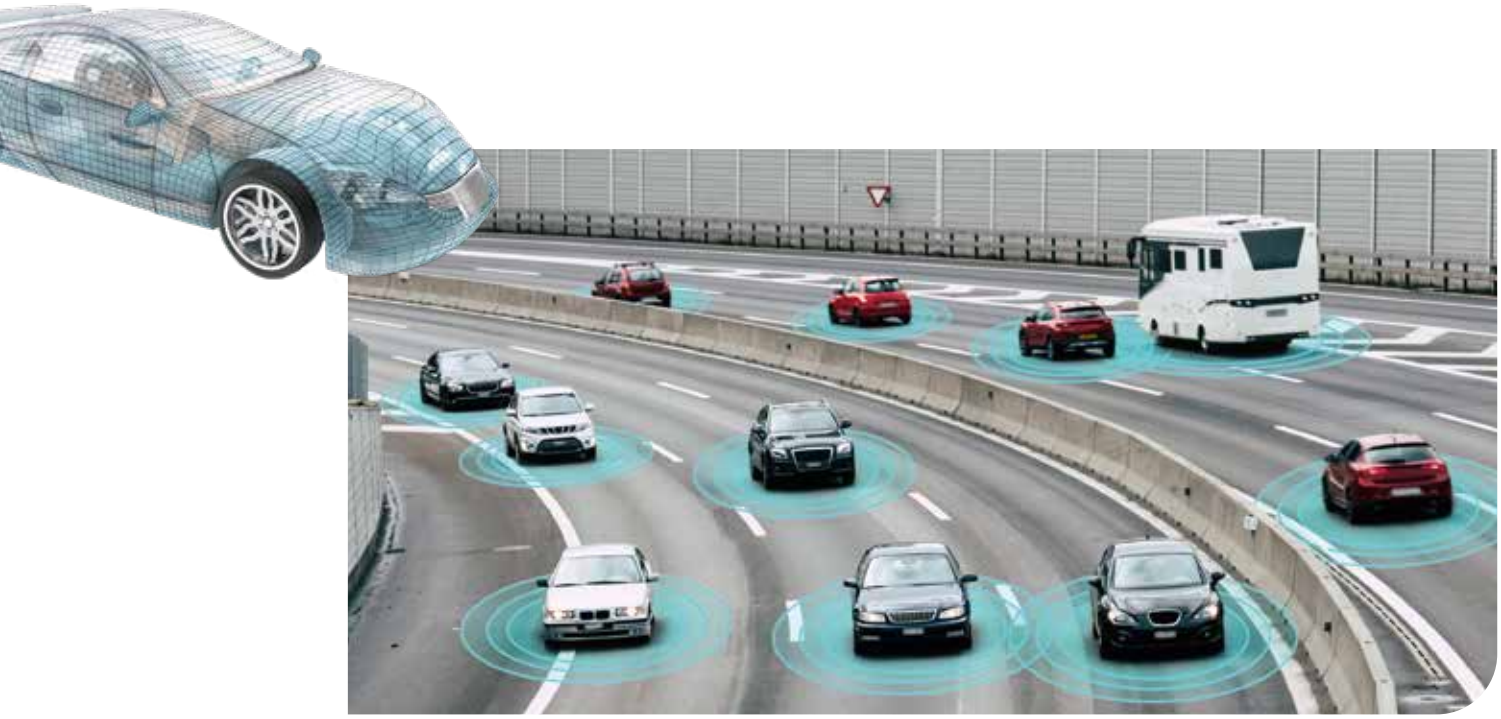
Dank des „Turbos“ der künstlichen Intelligenz schaffen es „Maschinen“ wie Google oder Bing in sehr kurzer Zeit, Abermillionen von Internetseiten nach den gefragten Begriffen zu durchsuchen. Inzwischen sind sie so weit fortgeschritten, dass ganz normale Fragen gestellt werden können, ähnlich wie bei einem menschlichen Gesprächspartner. Dennoch muss man die Ergebnisse immer noch überprüfen. Teilweise sind sie durch Werbung beeinflusst, teilweise fehlerhaft, weil sie falsche von wahren Informationen nicht unterscheiden können (Fake News).

Inzwischen kann man das Internet auch nach Bildern durchsuchen. Auch dabei kommt KI zu Einsatz. Sie wurde zuvor unter anderem durch uns trainiert: Immer wenn eine Internetseite von uns wissen möchte, ob wir ein Mensch sind, können sogenannte Captchas dabei helfen (Englisch für: „Completely Automated Public Turing test to tell Computers and Humans Apart“ – „vollautomatischer öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen“). Eine Variante sind kleine Sammlungen von Bildern, bei denen man z. B. diejenigen mit einer Ampel anklicken muss, oder alle mit einem bestimmten Tier.

Suchergebnisse muss man immer noch überprüfen. Manchmal sind es auch so viele, dass man lieber auf das Lexikon oder Wikipedia zurückgreift. In vielen Bereichen gibt es spezialisierte Webseiten wie z.B. bei Gesundheitsinformationen (www.gesundheitsinformation.de).

DOKTOR KI

Ärzte haben schon immer viele Daten erhoben und sie anschließend ausgewertet. Dabei unterstützt sie KI mehr und mehr, beispielsweise hilft KI bei der Krebsdiagnose. Früher hat der Arzt Bilder aus dem Ultraschall, dem Computertomographen, dem MRT oder dem Mikroskop nacheinander betrachtet und verglichen. Dies kann KI parallel und sie zugleich mit tausenden von Trainingsbildern abgleichen. Auch in der Kardiologie (Herzheilkunde) sind Algorithmen im Einsatz. Diese können Langzeit-EKG‘s für einen Arzt auswerten und wichtige Rhythmusstörungen schneller finden. Für den Patienten gibt es Apps für das Smartphone, welche die Pulsfrequenz messen können Dies kann bei der Entdeckung von Vorhofflimmern unterstützen und damit das Schlaganfallrisiko anzeigen. KI ersetzt aber nie den Arzt, sondern sie ist auch für ihn nur ein Hilfsmittel, wie das Stethoskop. Berufe, die menschliches Urteilsvermögen erfordern, können nicht durch KI ersetzt werden.



MEIN AUTO FÄHRT BESSER

Hier gibt es mehrere Bereiche, in denen Künstliche Intelligenz unterstützen oder sogar eigenständig tätig werden kann. Selbständig fahrende Autos sind noch Zukunftsmusik. Neuere Fahrzeuge besitzen bereits Assistenzsysteme, die beispielsweise selbständig bremsen oder die Spur halten können. Dennoch sind sie nicht fehlerfrei. Der „active city stop“ bremst auch für aufgewirbelte Blätter, und der „Autopilot“ übersieht auch schon einmal eine Ampel oder ein parkendes Polizeiauto.

Auch die Bahn setzt KI ein, um Verspätungen zu minimieren. Ebenso kann KI in der Verkehrs- und Stadtplanung eingesetzt werden, bei der Datenanalyse und Entscheidungsunterstützung. KI kann große Mengen an Daten zu Faktoren wie Umwelt, Wetter, Verkehr oder Wirtschaft analysieren, um Muster und Trends zu erkennen. Dies unterstützt Stadtplaner dabei, fundierte Entscheidungen zu treffen und Städte nachhaltiger und lebenswerter zu gestalten.

Eine KI-Ampel in Essenbach/Niederbayern verärgert Autofahrer. Drei Monate nach der Inbetriebnahme einer Ampel, die mit Unterstützung von KI den Verkehr regelt, machen Autos lieber einen großen Bogen um die Kreuzung. Sie verzögere die Grünphasen. Verantwortliche bitten um Geduld. Die KI kümmere sich um Fußgänger und vulnerable Verkehrsteilnehmer. Autofahrer gehören scheinbar nicht dazu.

Es passieren immer wieder Unfälle mit selbst fahrenden Autos. Die Hersteller haben das erkannt oder gewusst: Bei einem Unfall haftet immer der Fahrer, nie das Auto.

SMART HOME

Smart Home Anbieter („smart“: Engl. für „klug“) setzen auf Computertechnologien, um das Leben in den eigenen vier Wänden zu erleichtern. Doch wie klug ist das Zuhause wirklich? Amazon musste seinen „Dash Button“, einen WLAN-fähigen Bestellknopf, vom Markt nehmen, wegen Bedenken der Verbraucherschützer. Damit konnte man per Kopfdruck Waren bestellen. Der Preis war allerdings nicht ersichtlich. Auf ähnliche Probleme dürften Kühlschränke treffen, die Lebensmittel selber bestellen.

Bei der Haussteuerung sieht es jedoch anders aus. In Kombination mit Sprachassistenten wie Alexa, Siri oder Google Assistant lassen sich Heizungsregler, der Fernseher oder das Licht per Sprachbefehl steuern. Wenn dann die Thermostate und Lampen noch mit einer KI und weiteren Sensoren zusammenarbeiten, weiß das „kluge Zuhause“, welche Temperaturen wann und wo bevorzugt werden, und wann Licht benötigt wird.

Im Forschungsprojekt „KI@Home“ wurde der Frage nachgegangen, ob künstliche Intelligenz dazu beitragen kann, die Sicherheit und Gesundheit älterer Menschen in ihrem Zuhause zu verbessern. Das Projekt entwickelte auf der Basis Künstlicher Intelligenz in Verbindung mit alltagsunterstützenden Assistenzlösungen ein selbstlernendes System, um sich anbahnende gesundheitliche Krisen frühzeitig erkennen zu können.

Die Ergebnisse zeigen jedoch, dass eine intensive Begleitung der Nutzerinnen und Nutzer durch den Menschen erforderlich ist. Die Akzeptanz der Technologie ist nicht selbstverständlich.

KI kann das Leben in den eigenen vier Wänden erleichtern und so dafür sorgen, dass man länger – vielleicht sogar bis zum Ende – zu Hause wohnen kann. Allerdings ist die Technik nicht selbsterklärend, der Einrichtungs- und Betreuungsaufwand ist hoch. Und: Was nutzt eine Technologie, die von den Menschen, denen sie helfen soll, nicht akzeptiert und daher nicht genutzt wird?

MEIN COMPUTER VERSTEHT MICH

„Computer: Schilde aktivieren!“ Welcher Fan der Star-Trek-Serien und -Filme kennt nicht diesen Befehl, den der diensthabende Offizier dem Bordcomputer gibt, um sich auf einen Angriff vorzubereiten. Was in den 70er-Jahren noch Zukunftsmusik war, steckt heute in jedem Smartphone: Ein Sprachassistent.

Ob Alexa von Amazon, der Assistant von Google oder Siri von Apple – sprachfähige Assistenten erobern immer mehr auch die Wohnzimmer der Welt. Sie können Musik abspielen, Fragen beantworten oder auch Einkaufszettel erstellen. Sie sitzen an der Schnittstelle zwischen dem Menschen und Computern, meist auf Servern im Internet. Um helfen zu können, hören die Systeme permanent zu. Dabei nutzten sie als Technologie auch künstliche Intelligenz, das heißt die Systeme lernen dazu und verstehen uns mit der Zeit immer besser.

IHR KIND ÜBERWACHEN

Neben dem Smartphone und Lautsprechern gibt es immer mehr Produkte, mit denen Sie „reden“ können. In die Schlagzeilen hat es eine Puppe geschafft, die mit Kindern eine Art von Dialog führen konnte. „Cayla“ wurde letztendlich von der Bundesnetzagentur verboten. Es steckt das gleiche Prinzip dahinter wie bei den Sprachassistenten des Smartphones: Die Daten werden über das Internet auf Server der Hersteller übertragen, wo die Fragen registriert, verarbeitet und entsprechende Antworten vorgeschlagen werden. „Zur Verbesserung der Sprachqualität“ werden die Fragen und Antworten gespeichert, oft in Übersee, da die meisten Hersteller aus den USA kommen. Hierzulande verbreitet sind die Lautsprecher von Amazon („Echo“ mit dem Assistent „Alexa“) oder Google („Nest“, „Home“ mit „Google Assistant“) und die Sprachassistenten von Apple („HomePod“ und „Siri“).

TIPPS

- Weniger ist mehr: Seien Sie sparsam mit der Angabe Ihrer persönlichen Daten.
- Nutzen Sie datenfreundliche Produkte oder Voreinstellungen. Verzichten Sie auf die Sprachassistenten, wenn Sie sie nicht unbedingt benötigen. Oder wählen Sie Befehle, die das Gerät (Smartphone) selber verarbeiten kann, ohne ins Internet gehen zu müssen.
- Lesen Sie die Datenschutzerklärung und beschweren Sie sich notfalls beim Landesdatenschutzbeauftragten oder den Verbraucherzentralen. Vorab: Sichten Sie gespeicherte Daten regelmäßig und löschen Sie; was Sie nicht (mehr) benötigen.
- Achten Sie auf das für den Datenschutz geltende Recht. Wenn die Daten in den USA verarbeitet werden, gelten die weniger strengen US-amerikanischen Gesetze.
- Schalten Sie sie bei Abwesenheit aus, um unberechtigte Zugriffe zu vermeiden.
- „Cayla“ wird vermutlich nicht das letzte fragwürdige KI-Spielzeug bleiben mit einer Abhörfunktion. Sollten Ihnen Produkte mit versteckten Abhörfunktionen auffallen, können sie diese bei der Bundesnetzagentur per E-Mail melden: spionagegeraete@bnetza.de.

CHATGPT

Eine der bekanntesten künstlichen Intelligenzen ist ChatGPT. Dies ist ein sogenanntes „Large Language Model“ (englisch), ein großes Sprachmodell. Es kann eigenständig Texte erzeugen, inzwischen auch Bilder und Videos. Dabei reagiert ChatGPT auf Fragen wie ein Mensch in einem Internet-Chat und führt Gespräche.

Dagegen gibt es aber auch erhebliche Bedenken. Welche Daten wurden für das Training genutzt? Gab es dafür eine urheberrechtliche und datenschutztechnische Erlaubnis? Welche Vorkehrungen wurden gegen Diskriminierung getroffen, sowohl bei der Programmierung der Algorithmen als auch der Auswahl der Trainingsdaten? Was passiert mit meinen Daten, wenn ich eine Frage stelle, zum Beispiel mit höchstpersönlichen Angaben? Wer hat Zugriff auf diese Daten? Und nicht zuletzt: Oft stimmen die Anworten nicht, d.h. die KI fantasiert. Die Auswirkung auf bestimmte Berufe und Arbeitsplätze würde ein eigenes Kapitel füllen.

Forscher der Rice Universität in Houston, Texas, stellten fest: KI wird immer verrückter, wenn sie mit Trainingsdaten gefüttert wird, die selbst von KI erzeugt wurden. KI-Modelle könnten so an sich selbst ersticken. Sie könnten völlig dysfunktional werden.

Um die Technologie und ihre Risiken richtig einschätzen zu können, sollte man wissen, ob in einem Produkt oder einem Suchergebnis KI drin steckt. Viele Anbieter verlangen inzwischen eine Anzeigepflicht, ob KI genutzt wurde (z. B. Youtube). Die Europäische Union hat noch weitergehende Kennzeichnungspflichten in ihrer Verordnung über künstliche Intelligenz (KI-VO) niedergelegt.

THEMENHEFTE DER VERBRAUCHER INITIATIVE e. V.

Umfang: 16 Seiten (soweit nicht anders angegeben), Einzelpreis: 2,00 Euro zzgl. Versand
Allgemeine Geschäftsbedingungen und Versandkosten unter www.verbraucher.com

Gesundheit & Haushalt

- ○ Alltagsmythen (2014, 24 S.)
- ○ Basiswissen Bodenbeläge (2018)
- ○ Basiswissen Entspannung & Fitness (2017)
- ○ Basiswissen Fahrrad (2018)
- ○ Basiswissen Labels (2017, 24 S.)
- ○ Basiswissen Patientenrechte (2021)
- ○ Clever haushalten (2022, 20 S.)
- ○ Clever selbst machen! (2010, 24 S.)
- ○ Düfte und Duftstoffe (2022)
- ○ Erholsam schlafen (2022)
- ○ Erkältung & Selbstmedikation (2017)
- ○ Familienratgeber: Ernährung & Bewegung (2012, 24 S.)
- ○ Familienratgeber: Sitzender Lebensstil (2013, 20 S.)
- ○ Frauen & Gesundheit (2019)
- ○ Gesund älter werden (2020)
- ○ Gesund im Büro (2015)
- ○ Gut zu Fuß (2022)
- ○ Haushaltspflege (2015, 24 S.)
- ○ Heimwerken & Labels (2017)
- ○ Kinder & Gesundheit (2020)
- ○ Kinder & Übergewicht (2015)
- ○ Kindersicherheit (2015)
- ○ Kosmetik (2013, 32 S.)
- ○ Kosmetik für die reiferen Jahre (2024)
- ○ Kosmetik für junge Haut (2018, 20 S.)
- ○ Leben im Alter (2023)
- ○ Männer & Gesundheit (2019)
- ○ Nachhaltiger Haushalt (2019)
- ○ Nahrungsergänzungen (2024)
- ○ Naturheilverfahren (2016)
- ○ Natur- & Biokosmetik (2019)
- ○ Omas Hausmittel (2020)
- ○ Pflege organisieren (2024)
- ○ Rückengesundheit (2010, 28 S.)
- ○ Schadstoffarm wohnen (2017)
- ○ Schädlinge im Haushalt (2016)
- ○ Sonnenschutz (2016, 24 S.)
- ○ Unfällen im Alter vorbeugen (2024)
- ○ Vollwertig essen bei Diabetes Typ 2 (2024)
- ○ Yoga (2015, 32 S.)
- ○ Zähne pflegen (2014, 24 S.)

Essen & Trinken

- ○ Älter werden mit Genuss (2023)
- ○ Alkoholfreie Getränke (2023)
- ○ Ausgewählte Ernährungsrichtungen (2021)
- ○ Basiswissen Essen für Kinder (2017)
- ○ Basiswissen Fleisch (2018)
- ○ Basiswissen Gemüse & Obst (2018)
- ○ Basiswissen Gesund essen (2021)
- ○ Basiswissen Kochen (2015)
- ○ Basiswissen Öle & Fette (2018)
- ○ Clever kochen ohne Reste (2019)
- ○ Clever preiswert kochen (2019)
- ○ Clever preiswert kochen 2 (2014, 24 S.)
- ○ Clever saisonal kochen (2010, 24 S.)
- ○ Clever saisonal kochen 2 (2011, 24 S.)
- ○ Clever saisonal kochen 3 (2011, 24 S.)
- ○ Diäten (2016)
- ○ Essen macht Laune (2012)
- ○ Fisch & Meeresfrüchte (2020)
- ○ Insekten auf dem Teller (2023)
- ○ Klimafreundlich essen (2019)
- ○ Küchenkräuter (2009, 8 S.)
- ○ Lebensmittelallergien & Co. (2015)
- ○ Lebensmitteleinkauf (2016)
- ○ Lebensmittel selber machen (2022)
- ○ Lebensmittelvorräte (2020)
- ○ Obst & Gemüse selbst anbauen (2020)
- ○ Regionale Lebensmittel kaufen (2019)
- ○ Superfood (2022)
- ○ Süßigkeiten (2013, 24 S.)
- ○ Teller statt Tonne (2021)
- ○ Vegetarisch & vegan essen (2021)
- ○ Wie Oma backen (2014)
- ○ Wie Oma kochen (2011, 24 S.)
- ○ Wie Oma naschen (2012)
- ○ Zucker & Co. (2020)
- ○ Zusatzstoffe (2020)

Umwelt & Nachhaltigkeit

- ○ Abfall richtig entsorgen (2023)
- ○ Basiswissen Strom sparen (2018)
- ○ Beleuchtung (2016)
- ○ Besonders sparsame Haushaltsgeräte 2024 (2024)
- ○ Clever Energie sparen (2022)
- ○ Das neue EU-Energielabel (2021)
- ○ Einfach klimagerechter leben (2021, 20 S.)
- ○ Elektrosmog (2016)
- ○ Fairer Handel (2020)
- ○ Familie & Klima (2020)
- ○ Holz & Papier (2023)
- ○ Klimafreundlich einkaufen (2019)
- ○ Klimafreundlich gärtnern (2022)
- ○ Klimafreundlich haushalten (2022)
- ○ Klimafreundlich mobil (2022)
- ○ Konsum im Wandel (2015)
- ○ Mehrwegverpackungen (2022)
- ○ Nutzen statt besitzen (2020)
- ○ Nachhaltig digital konsumieren (2023)
- ○ Nachhaltig durch das Jahr (2019)
- ○ Nachhaltig feiern & schenken (2024)
- ○ Nachhaltig in der Freizeit (2023)
- ○ Nachhaltiger kleiden (2021)
- ○ Nachhaltige Verpackungen (2021)
- ○ Nachhaltige Mobilität (2012, 24 S.)
- ○ Nachhaltige Unternehmen (2008)
- ○ Nachhaltiger Handel(n) (2014)
- ○ Nanotechnologien in Alltagsprodukten (2021)
- ○ Permakultur (2019)
- ○ Plastikärmer leben (2021)
- ○ Schadstoffe im Alltag (2023)
- ○ Wasser – Lebensmittel Nr. 1 (2022)

Weitere Themen

- ○ Ehrenamt & Co. (2023)
- ○ Internet (2024)
- ○ Internet-Mythen (2024)
- ○ Langlebige Haushaltsgeräte (2018)
- ○ Online sicher unterwegs (2023)
- ○ Tierisch gut (2021)

DOWNLOADS FINDEN SIE UNTER WWW.VERBRAUCHER.COM

THEMENHEFTE EINFACH ONLINE, PER BRIEF ODER MAIL BESTELLEN

Bundesverband
Die Verbraucher Initiative e.V.

Wollankstraße 134, 13187 Berlin, mail@verbraucher.com