Verbraucher **konkret**

Themenheft der VERBRAUCHER INITIATIVE e.V.

SPEZIAL

TIPPS GEGEN FALLEN IM NETZ

INTERNET

Informieren.
Motivieren.
Gestalten.

Bundesverband
Die Verbraucher Initiative e.V.

HINTERGRUND: DAS INTERNET IST ÜBERALL

KÜNSTLICHE INTELLIGENZ: VOM HYPE ZUR ANWENDUNG

ISSN 1435-3547 • A12 114

LIEBE LESERIN, LIEBER LESER,

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. Seit der Jahrtausendwende verbreitet sich eine technologische Entwicklung immer mehr: Künstliche Intelligenz.

SPEZIAL

TIPPS GEGEN FALLEN IM NETZ

Das Internet hat die Grundlagen für weitere Anwendungen geschaffen, wie Übersetzungsdienste, Sprachassistenten oder Sprachmodelle wie ChatGPT. Sie kommen in immer mehr Geräten und Diensten zum Einsatz. Durch die rasant fortschreitende Technik können sich längst nicht mehr nur Computer mit dem Internet verbinden. Anderen Gegenständen wie Autos, Heizungen, Türschlössern, Alarmanlagen, Fernsehern oder Fitnessarmbändern ist das ebenfalls möglich.

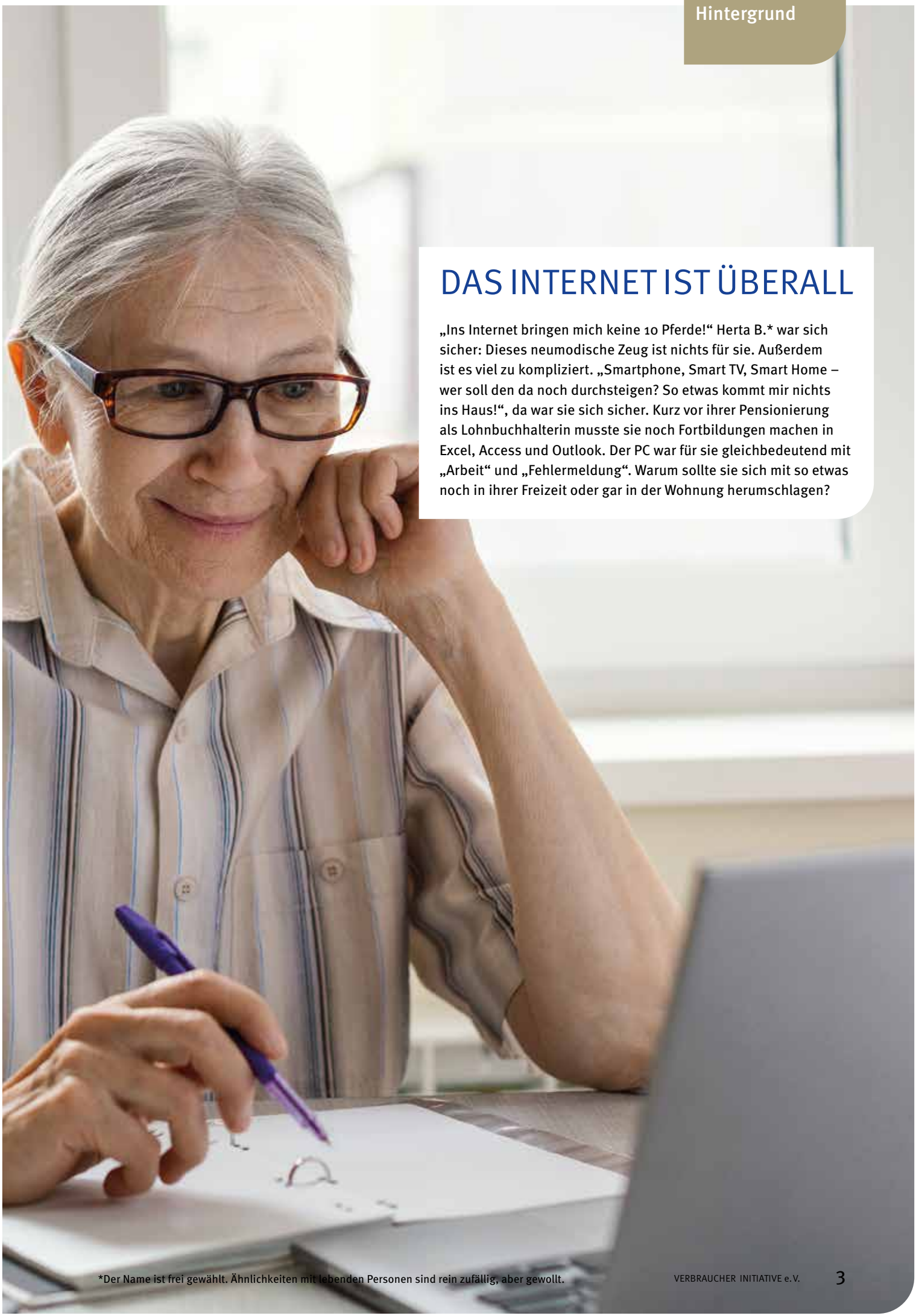
Das kann Vorteile haben, etwa Energie oder Strom sparen, für mehr Sicherheit sorgen oder das Leben bequemer machen. Gleichzeitig sammeln diese Geräte Informationen über Lebensgewohnheiten und persönliche Daten.

Pessimisten sehen das Ende der Menschheit heraufdämmern: Maschinen übernehmen die Herrschaft. Allerdings müssen diese von Menschen konzipiert, gebaut, programmiert, gestartet, trainiert und eingesetzt werden. Es gibt also viele Ansatzpunkte, die Entwicklung in eine gute Richtung zu lenken. Wir wollen Ihnen helfen, dabei den Überblick zu behalten.

Eine „intelligente" Lektüre wünscht Ihnen

Guido Steinke (Fachreferent Verbraucher60+ und Internet)

IMPRESSUM | Verbraucher konkret, Mai 2024 | ISSN 1435-3547 | „Internet" – 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.), Alexandra Borchard-Becker, 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. | Nachdruck und Vervielfältigungen, auch auszugsweise, nur mit Genehmigung des Herausgebers und Quellenangabe. | 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).



DAS INTERNET IST ÜBERALL

„Ins Internet bringen mich keine 10 Pferde!“ Herta B.* war sich sicher: Dieses neumodische Zeug ist nichts für sie. Außerdem ist es viel zu kompliziert. „Smartphone, Smart TV, Smart Home – wer soll den da noch durchsteigen? So etwas kommt mir nichts ins Haus!“, da war sie sich sicher. Kurz vor ihrer Pensionierung als Lohnbuchhalterin musste sie noch Fortbildungen machen in Excel, Access und Outlook. Der PC war für sie gleichbedeutend mit „Arbeit“ und „Fehlermeldung“. Warum sollte sie sich mit so etwas noch in ihrer Freizeit oder gar in der Wohnung herumschlagen?

*Der Name ist frei gewählt. Ähnlichkeiten mit lebenden Personen sind rein zufällig, aber gewollt.

Als 1969 Wissenschaftler die ersten Rechner in verschiedenen Städten über Telefonleitungen miteinander verbanden, dachte noch keiner daran, dass diese Technologie unsere Wissenschaft, Wirtschaft und unser Leben generell verändern würde. Begriffe wie „Smartphone“, „Smart Shopping“, „Smart Home“ oder „Smart Grid“ kamen erst in den ersten Jahren dieses Jahrhunderts auf.

Hinzu kamen in den letzten Jahren vermehrt mobile Anwendungen, auch „Apps“ genannt. Mit Hilfe dieser Programme auf dem Smartphone lassen sich das Wetter vorhersagen, Radio hören oder auch Fotos austauschen. Es kommen aber auch immer mehr hinzu, die sehr viel über uns wissen (wollen). Standort, gelaufene Schritte oder besuchte Internetseiten sind nur ein Ausschnitt davon.

Computer, d. h. immer kleinere Mikrochips, stecken in immer mehr Dingen des Alltags. Was früher großen Industrieanlagen und Banken vorbehalten war, steckt heute in Telefon und Automobil. Heute hat ein durchschnittliches Telefon mehr Rechenleistung als die Computer, mit denen die Astronauten der Apollo-Missionen den Mond erreichten. Aber auch Etiketten von teureren Modeprodukten oder der Personalausweis und die Gesundheitskarte enthalten Computer, die RFID-Chips. Über Funkwellen werden sie mit anderen Computern verbunden – und könnten so auch ins Internet – theoretisch.

Den nächsten Entwicklungsschub gab es mit den Drahtlos-Technologien, d. h. der Verbindung der Computer über Funkwellen. Ob WLAN zu Hause oder Bluetooth im Auto, die Geräte verbinden sich heute fast von allein. Der Kühlschrank, der Rezepte aus dem Internet lädt, ist schon Realität, genauso wie Autos, die Staumeldungen austauschen.

Wenn man früher in eine neue Stadt fuhr, besorgte man sich einen Reiseführer, fragte einen Kollegen, der schon einmal dort war und ging zur Touristen-Information. Dieses Vorgehen hat sich bewährt, auch bei allen Fragen rund um das Internet und KI. In jeder Stadtbücherei gibt es inzwischen eine Abteilung mit Ratgebern („für Dummies“ – dabei sind die Leser eher klug: Sie machen sich schlau, bevor sie etwas Neues ausprobieren!), die Volkshochschulen bieten Kurse an, PC-Klubs Fragestunden und die Verbraucherzentralen haben ein ganzes Bündel an Ratgebern und Checklisten. Keine Angst also vor dem Internet: Man muss nur wissen, wie und wo man sich orientieren kann.

HERAUSFORDERUNG INTERNET

Mit dem „Turbo KI“ erreichen damit auch Gauner und Ganoven fast alle Lebensbereiche. Aber auch vermeintlich seriöse Nutzer wie Firmen und demokratische Regierungen bewegen sich beim Einsatz von KI oft in einer Grauzone. War die Datensammlung zulässig? Wer hat noch alles Zugang zu diesen Daten? Wofür werden sie noch genutzt? Gesetze kommen da oft zu spät, Selbstschutz ist gefragt. Wenn man seine Geräte und die Anwendungen kennt, kann man vorbeugen.

Jeder hat inzwischen seine eigene Internetseite, sein Facebook-Profil, seinen Instagram-Account. Manche wären dabei gerne jung, schön, sportlich. KI macht es möglich. Mit Filtern und anderen Werkzeugen wird das eigene Profilbild verschönert.

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“ und „Fake-Shops“.

Auch hier hat Künstliche Intelligenz einen Turbo eingelegt. Erkannte man früher gefälschte E-Mails noch am schlechten Deutsch, werden die Texte immer besser, dank einer Übersetzungssoftware, die KI nutzt. So unterscheiden sich E-Mails von Kriminellen kaum von echten. Auch die Internetseiten, auf die man Sie locken möchte, um Ihre Daten abzugreifen, sind kaum von den Originalen zu unterscheiden.

Gefälschte Online-Shops (Fake Shops) arbeiten ausschließlich mit Vorkasse. Dabei sehen sie aus, wie jeder andere, seriöse Shop im Netz. Aber sie haben Angebote, die zu gut sind, um wahr zu sein: Rabatte von 50 Prozent auf begehrte Markenartikel sind keine Seltenheit. Der Haken: Man erhält die Ware nie, oder minderwertigen Schrott. Hat man dann bereits bezahlt, ist das Geld oft verloren.

So können Sie sich schützen:

- Ihre Bank fordert Sie nie per E-Mail zur Angabe von Nutzernamen, PIN und TANs auf.
- 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 nur zur Vorkasse animieren.
- Lassen Sie sich nicht auf Vorkasse ein. Das Risiko mag bei kleineren Beträgen noch überschaubar sein. Bei größeren Summen empfehlen sich Einzugsermäch-

tigung, Kreditkarte oder die gute, alte 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.
- Schauen Sie vorab bei den Fakeshop-Findern vorbei! Diese gibt es auf den Internetseiten der Verbraucherzentralen (www.verbraucherzentrale.de › Digitales › Online-Handel)

FALSCHE ENKEL

Vom „Enkeltrick“ haben viele schon gelesen. „Omi, ich habe eine neue Handynummer!“ Reagiert man dann auf diese Nachricht von Kriminellen, wird man über die neue Nummer zum Beispiel über WhatsApp in Dialoge verwickelt, die oft darin gipfeln, dass der vermeintliche Enkel dringend Geld braucht, weil er in der Klemme steckt. „Freunde“ holen das Geld dann ab. Dank KI können die Ganoven nicht nur die Nachrichten fälschen. Wenn sie Stimmproben vom Enkel haben, hinterlassen sie neuerdings Sprachnachrichten mit der Stimme des Enkels. Oder noch dreister: Jemand ruft mit der Stimme des Enkels an!

So können Sie sich schützen:

- Gesunde Skepsis: Meist kommen die Nachrichten oder Anrufe überraschend, also zu Zeiten, zu denen der Enkel oder die Tochter sich nie meldet. Oder sie haben noch nie nach Geld gefragt.
- Da hilft dann meist schon ein Rückruf: „Ich kann gerade nicht sprechen, kann ich Dich in fünf Minuten zurückrufen?“ Dann natürlich unter der alten, richtigen Nummer.
- Vereinbaren Sie ein Codewort oder stellen sie eine Frage, die nur der echte Enkel beantworten kann.
- Ziehen Sie jemanden zu dem Gespräch hinzu, zum Beispiel den Ehepartner. Zwei Menschen lassen sich schwieriger übertölpeln.
- Seien Sie datensparsam! Wenn die Kriminellen Ihre Handynummer oder E-Mail-Adresse nicht kennen, können Sie auch keinen Kontakt mit Ihnen aufnehmen.

Diese Verbrechensvariante wird auch „Social Engineering“ genannt (englisch frei übersetzt: „Zwischenmenschliche Manipulation“). Beim Social Engineering nutzt der Täter den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.

Sie macht nicht bei Großeltern oder Eltern halt. Geködert werden Menschen auch durch vermeintliche Jobangebote, „günstige“ Mietwohnungsanzeigen, E-Mails vom Chef oder Anrufe von Mitarbeitern von Microsoft, Paypal und vieles mehr. Allen Varianten gemeinsam ist, dass durch Überraschung, Angst, Gier oder Mitgefühl der oder die Betroffene dazu gebracht werden soll, wichtige Daten wie Zugangscodes preis zu geben, oder sogar Geld zu zahlen.

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. Ortungsdienste sind der „letzte Schrei“. 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.

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 nur 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 wahlweise seinen Kindern oder dem Ehepartner nachspionieren kann, z. B. die App „mSpy“. Die Nützlichkeit ist umstritten. Bei Neuwagen wird Ortung ab Werk eingesetzt, um bei Unfällen den Rettungskräften schnellstmöglich den Weg zu weisen (eCall). Das ist sinnvoll. Was aber ist, wenn der Partner einen überraschen möchte? Das fällt schwer, wenn man sieht, dass die Gattin gerade bei der Geschäftsstelle des Fußball Clubs ist, obwohl sie sonst mit Fußball nichts am Hut hat. Ganz abgesehen davon benötigt jeder einen eigenen, privaten Bereich. Dies wird aber in Frage gestellt, wenn eine permanente Überwachung droht.

Schlimm wird es, wenn diese neuen Überwachungsmöglichkeiten vom Staat eingesetzt werden. In China wurde großflächig in Städten Gesichtserkennung eingesetzt, um zum Beispiel Massnahmen gegen die Corona-Pandemie zu überwachen. Aber auch demokratische Regime setzen durch KI erzeugte oder verbesserte Software ein, um auf das Smartphone zuzugreifen.

So können Sie sich schützen:

- Aktivieren Sie Ortungsdienste nur dann, wenn Sie diese wirklich brauchen.
- Prüfen Sie die Hersteller der Apps und installieren Sie keine aus dubiosen Quellen.
  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. Prüfen Sie die Finanzierung: Ist der Preis angemessen? Schauen Sie bei kostenlosen Apps, ob sie werbefinanziert oder von öffentlichen Stellen getragen werden.
- Schalten Sie das Smartphone zwischendurch aus.
- Wenn Sie nur mobil telefonieren und fotografieren möchten, genügen vielleicht noch ein älteres Handymodell – und ein Fotoapparat.

TIPPS

- Klicken Sie nicht auf Links in Nachrichten oder E-Mails, die sie nicht kennen!
- Lassen Sie Ihr Telefon auch einmal aus, oder zu Hause!
- Wenn man sein Telefon auf die Grundeinstellungen zurück setzt, werden in der Regel schädliche Apps entfernt – aber auch alle anderen Daten.
- Nutzen Sie die Sicherheitsangebote, die Ihnen Ihr Telefon macht. 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 sichere Passwörter, auch bei der Nutzung von geld-relevanten Apps (Online-Banking, In-App-Käufe)
  - Verwenden Sie beim Onlinebanking nicht dasselbe Smartphone, an das auch die mobile TAN geschickt wird!

ÜBERWACHUNGS-WUNDER SMARTPHONE

E-Mails abrufen, Bahnverbindungen suchen und Tickets buchen, Wettervorhersagen und Restauranttipps, schnell mal was im Internet recherchieren – es gibt fast nichts, was diese kleinen Super-Computer in der Hosentasche nicht können. Vermehrt werden sie außerdem als Portemonnaie und Gesundheitscoach eingesetzt, von den „spielerischen" und unterhaltenden Möglichkeiten (Musik, Video, Spiele) ganz zu schweigen. Statt einer dicken Geldbörse mit Dutzenden von Karten reicht das Telefon.

Als Computer wird das Smartphone immer öfter Ziel von Hackern und 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. Oder Geld per Online-Banking auf ein eigenes Konto überweisen oder kostenpflichtige SMS an teure Nummern versenden.

SPRICH MIT MIR

Die Übertragungsgeschwindigkeiten in den Mobilfunknetzen nehmen zu. Damit einhergehen immer mehr Dienste, die über das Internet funktionieren. Siri (der Sprachassistent von Apple) und der Google-Assistant hören alles und reagieren auf menschliche Stimmen, mehr oder weniger. Dies geht allerdings nur mit einer Verbindung zu den Servern von Apple und Google. Dort wird die Stimme analysiert und es werden entsprechende Reaktionen vorgeschlagen. Wenn Sie das nicht deaktivieren, hört also „Big Brother" ständig mit.

Das Auto misst die Parklücke aus und parkt selbständig ein, es bremst für spielende Kinder und hängt sich auf der Autobahn in sicherem Abstand hinter den Vordermann – bequeme neue Werbewelt! 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. Zwei Hackern war es beispielsweise Mitte 2015 in den USA gelungen, einen Jeep Cherokee zu hacken und fern zu steuern.

TIPPS

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

- Fahren Sie Ihr altes, nicht mit Elektronik vollgestopftes Auto so lange wie möglich. Dies ist nebenbei 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 aus, das von der elektronischen Revolution weitestgehend verschont wurde.

IN DER „WOLKE"

Kontakte aktualisieren, seinen Kalender teilen, alle Dokumente immer parat haben, Fotos sichern und nicht zuletzt die gesamte E-Mail-Korrespondenz. Immer mehr Anwendungen werden vom Laptop und PC in die „Wolke", die sogenannte Cloud, verlagert. Der Vorteil: Man hat seine Dateien immer synchron auf vielen Geräten (Laptop, Smartphone, Tablet) parat, kann sie mit anderen teilen und braucht sich nicht um Datensicherungen zu kümmern. Das machen die Anbieter. Man könnte sich im „7. Himmel" wähnen, wären da nicht ein paar Haken:

TIPPS

- Sichern Sie die Daten immer auch lokal, z. B. auf einer externen Festplatte.
- Wählen Sie einen Cloud-Anbieter in Deutschland. Hier ist das deutsche Datenschutzrecht anwendbar.
- Nehmen Sie einen kostenpflichtigen Anbieter, denn er muss die Daten nicht zu Werbezwecken nutzen.
- Verschlüsseln Sie die Dateien, bevor Sie sie in die „Wolke" hochladen.

Ohne Internetverbindung kommen Sie nicht in die „Wolke".

- Sollten die Daten beim Anbieter verloren gehen, ist es oft mühselig, sie wieder herstellen zu lassen, sofern das überhaupt möglich ist.
- kostenlose Cloud-Dienste wie Google nutzen die Daten für eigene (Werbe)-Zwecke, unter anderem zum Trainieren ihrer KI-Anwendungen
- unerwünschten Zugriff können auch Andere haben, entweder per Gesetz (z. B. Patriot Act in den USA) oder faktisch als Hacker.

SICHERES ONLINE-BANKING

Ob zu Hause am PC oder über mobile Geräte – Bankgeschäfte wie Kontostand abfragen, Überweisungen tätigen oder einen Dauerauftrag einrichten lassen sich einfach und schnell über das Internet abwickeln. Auch mobiles Bezahlen per Smartphone ist möglich.

Um sich in das Online-Portal Ihrer Bank einzuloggen, benötigen Sie einen Nutzernamen und ein Passwort. Zusätzlich müssen Sie als zweiten Faktor eine einmalig verwendbare Transaktionsnummer (TAN) eingeben. Für die Freigabe einer Überweisung oder eines anderen Vorganges benötigen Sie ebenfalls eine TAN als eine Art digitale Unterschrift.

GÄNGIGE TAN-VERFAHREN

- Das Push-TAN-Verfahren läuft über eine zugehörige App Ihrer Bank, die Sie auf einem Smartphone oder Tablet nutzen können. Die TAN wird in der App erzeugt.
- Für das Chip-TAN-Verfahren benötigen Sie Ihre Bankkarte und einen TAN-Generator. Je nach Verfahren kann er eine Grafik, einen QR-Code® oder eine Matrix auf dem Bildschirm erkennen und die TAN generieren.
- Das Photo-TAN-Verfahren funktioniert ähnlich, nur dass Sie hier statt des TAN-Generators ein Smartphone mit einer zugehörigen App verwenden, die ein Bild oder einen QR-Code® auslesen kann. Eine Alternative sind spezielle Lesegeräte.
- Bei der sms-TAN (oder mTAN) wird die TAN per SMS an eine hinterlegte Mobilfunknummer gesendet.

Experten stufen das Chip-TAN-Verfahren als sehr sicher ein. Wenn bei Push-TAN und Photo-TAN separate Geräte für das Online-Banking und die App verwendet werden, gelten sie ebenfalls als sicher. Das mTAN-Verfahren wird als weniger sicher angesehen, da beispielsweise SMS abgefangen werden könnten. Viele Banken bieten es nicht mehr an oder planen die Abschaffung.

MOBILES BEZAHLEN

Für das Bezahlen mit dem Smartphone oder einer Smartwatch benötigen Sie eine entsprechende App, die Sie mit einem Zahlungsmittel verknüpft haben, z. B. einer Kreditkarte oder Ihrem Girokonto. Ab einem bestimmten Betrag ist zusätzlich die Eingabe einer PIN oder einer TAN erforderlich.

Sichern Sie das Gerät und die App sorgfältig, beispielsweise mit Passwörtern oder ähnlichen Verfahren. Halten Sie das Betriebssystem und die App stets aktuell.

Bezahl-Apps werden u. a. von Banken, Sparkassen, Apple, Google oder einigen Händlern angeboten.

TIPPS GEGEN FALLEN IM NETZ

Betrügerische Maschen im Internet richten sich zunehmend gegen Privatpersonen. Solche Straftaten, die moderne Informations- und Kommunikationstechnologien nutzen, werden unter dem Begriff Internetkriminalität (Cybercrime) zusammengefasst. Dazu gehören u. a. Phishing, Diebstahl und Missbrauch von Daten sowie Betrug bei Online-Shops. Bei den folgenden Adressen erfahren Sie, wie Sie sich gut gegen diese Fallen im Netz wappnen und wie Sie im Ernstfall handeln können.

www.bsi.bund.de

Das Bundesamt für Sicherheit in der Informationstechnik bietet in der Rubrik „Themen“ unter dem Menüpunkt „Verbraucherinnen und Verbraucher“ umfangreiche Tipps und Handlungsempfehlungen, wie Sie Ihren digitalen Alltag sicher gestalten können. Dazu gehören beispielsweise Beiträge zu geeigneten Passwörtern, zum sicheren Online-Banking, Online-Shopping und mobilen Bezahlen sowie zur Sicherheit bei der Nutzung von E-Mails, Messenger-Diensten und sozialen Netzwerken. Außerdem stehen Informationen zu aktuellen Themen wie Methoden der Cyberkriminalität und zu Sicherheitsvorfällen bereit.

www.digital-kompass.de

Der Digital-Kompass richtet sich vorrangig an ältere Verbraucher sowie insbesondere an Menschen mit Sinnes- und Mobilitätsbeeinträchtigungen. Ziel ist, ihnen digitale Kompetenzen zu vermitteln, so dass sie die Vorteile des Internets für sich sicher nutzen können. In der Rubrik „Materialien“ gibt es unter dem Menüpunkt „Sicherheit und Recht“ zahlreiche Informationen zu den Themen Sicherheit, Datenschutz und Verbraucherrechte.

Das Projekt „Digital-Kompass“ wird von der Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V. (BAGSO) gemeinsam mit Deutschland sicher im Netz e. V. durchgeführt. Die VERBRAUCHER INITIATIVE ist einer der Projektpartner. Weitere Bausteine sind Treffpunkte für persönlichen Austausch, Schulungen und zahlreiche Lehr- und Lernmaterialien.

www.sicher-im-netz.de

Ein Ziel des Vereins Deutschland sicher im Netz e. V. (DsiN) ist es, Verbraucher beim sicheren Umgang mit der digitalen Welt zu unterstützen. Zu seinen Angeboten gehören vielfältige Informationen und praktische Tipps, die Sie in der Rubrik „Verbraucher“ finden. In den Beiträgen geht es beispielsweise um einen digitalen Basisschutz sowie die sichere Nutzung der verschiedenen Anwendungen und Möglichkeiten im Netz.

www.verbraucher60plus.de

Die VERBRAUCHER INITIATIVE bietet mit dem Portal Verbraucher 60 plus ebenfalls Informationen für die wachsende Zielgruppe der älteren Verbraucher an. In den Rubriken Internet und Abzocke können Sie sich beispielsweise zu den Themen Online-Shopping, soziale Netzwerke und Fallen im weltweiten Netz informieren. Neben praktischen Tipps finden Sie jeweils Hinweise auf weitere Informationsquellen und auf Beratungsangebote. Unter „Veranstaltungen“ finden Sie Hinweise auf (Online-) Veranstaltungen zum Thema Internet.

Informieren.
Motivieren.
Gestalten.

Bundesverband
Die Verbraucher Initiative e.V.

www.verbraucherzentrale.de

Das Verbraucherportal der Verbraucherzentralen und des Verbraucherzentrale Bundesverbandes hält in der Rubrik „Digitales“ viele praktischen Empfehlungen zur Internetsicherheit bereit. Hier ist u. a. der Beitrag „Sicher im Internet – Handy, Tablet und PC schützen“ zu finden, der umfassend Tipps zum Schutz vor Datenklau, Viren und unsicheren Netzwerken bietet. Er informiert über sichere Accounts und Passwörter, Online-Shopping und Fake-Shops, Datensicherung und das richtige Verhalten bei Cybercrime-Angriffen sowie Betrugsversuche und Manipulationen, z. B. Phishing.

www.vis.bayern.de

Im Verbraucherportal Bayern stehen in der Rubrik Digitale Welt Hintergrundinformationen und Handreichungen parat, beispielsweise zu den Themen „Sicher im Internet“, „Online einkaufen und bezahlen“ sowie zum Datenschutz.

www.klicksafe.de

Im Fokus dieser EU-Initiative stehen Kinder und Jugendliche sowie Eltern, Lehrkräfte und andere Multiplikatoren. Klicksafe möchte sie dabei unterstützen, einen sicheren, kompetenten und selbstbestimmten Umgang mit dem Internet zu entwickeln. Nutzer erhalten einen Überblick über aktuelle Online-Themen sowie konkrete Tipps für den digitalen Alltag, beispielsweise über Kinder- und Jugendschutzprogramme, soziale Netzwerke, Messenger-Dienste, Cybermobbing, Cybergrooming und Privatsphäre. Die Beiträge sind erreichbar über den Menüpunkt „Alle Themen“.

https://koeln.polizei.nrw

Die Podcast-Reihe „Sicherheit in der digitalen Welt“ der Polizei Nordrhein-Westfalen in Köln richtet sich an Personen, die nicht in und mit der digitalen Welt aufgewachsen sind, sondern das weltweite Netz erst als Erwachsene kennengelernt haben. Darüber hinaus richtet sie sich an alle, die wissen möchten, welche Gefahren es birgt und wie sie sich dagegen schützen können.

Zu den Podcastfolgen mit Themen wie sichere Passwörter, Viren in E-Mails und sicheres Surfen gelangen Sie, wenn Sie auf der Webseite nach unten zu der Rubrik „Tipps und Beratungsangebote“ scrollen.

www.polizei.de

Im Falle einer Cybercrime-Attacke, beispielsweise in Form von Betrug oder Diebstahl, ist es ratsam, Anzeige bei der Polizei zu erstatten. Das geht auch online über die Online-Wachen der Polizeien der Länder. Über die Rubrik „Polizeiliche Einrichtungen“ gelangen Sie zur Übersicht und zur Internetadresse für Ihr Bundesland.

HILFREICHE INTERNETSEITEN

- https://ki-campus.org/: Der KI-Campus ist eine Lernplattform für Künstliche Intelligenz mit kostenlosen Online-Kursen, Videos und Podcasts zur Stärkung von KI- und Datenkompetenzen.
- https://www.ki-konkret.de/: Künstliche Intelligenz – einfach erklärt, mit Texten, Grafiken und Videos
- https://ki-und-alter.de/: Künstliche Intelligenz für ein gutes Altern: Projektseite der BAGSO, mit Lernorten und KI-Wissen

Verbraucher konkret „Internet“ - 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.), Alexandra Borchard-Becker, Guido Steinke | Fotos: iStock | Nachdruck und Vervielfältigungen, auch auszugsweise, nur mit Genehmigung des Herausgebers und Quellenangabe. 05/2024

VOM HYPE ZUR ANWENDUNG

Künstliche Intelligenz – abgekürzt KI – ist in aller Munde. 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. Dabei kommen Techniken zum Einsatz wie neuronale Netze und maschinelles Lernen.

Die Begriffe KI und Algorithmen sind verwandt, aber nicht identisch. Ein Algorithmus ist eine eindeutige Handlungsvorschrift für einen Computer zur Lösung eines Problems. Es ist also ein vorbestimmter Rechenweg. Ein Beispiel: Routenplanung mit einem Navigationssystem. Da kann man zwar mehrere Routen auswählen, verändert damit aber auch die Ankunftszeit.

Künstliche Intelligenz setzt auch Algorithmen ein. Durch das „maschinelle Lernen“ kann sich der Algorithmus aber verändern. Eine gute KI lernt ständig dazu, idealerweise, um Fehler auszumerzen. Die Ergebnisse können in Folge des „Lernprozesses“ also voneinander abweichen.

KI beschleunigt die Verarbeitung von Daten durch neue Systeme und Programmierverfahren. Dadurch ist sie leistungsfähiger und schneller als andere EDV-Systeme. Ein Beispiel: Um früher digitale Fotos zu retuschieren, musste man teilweise Pixel für Pixel ändern, was sehr zeitraubend war. Mit KI geht das inzwischen mit zwei Klicks.

VON MENSCHEN EINGESETZT

Künstliche Intelligenz wird von Menschen (z. B. Unternehmen, Verwaltung, Organisationen) 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 nutzt die KI und wozu?

KI kann dort zum Einsatz kommen, wo jetzt schon Computerchips und Software eingesetzt werden – also fast überall. Computerchips und damit Computer werden immer kleiner. Sie stecken inzwischen in Glühlampen und Personalausweisen. Theoretisch kann daher die Glühlampe „intelligent“ werden, also leuchten, wenn der Nutzer das für richtig hält. Dazu müsste er sie „trainieren“, ihr also zeigen, wann er Licht haben möchte und wann nicht.

Künstliche Intelligenz kann selbständig Aufgaben lösen. Diese können auch darin bestehen, den Menschen das Leben zu erleichtern. So ist es möglich, mit dem Computer zu reden und ihm zum Beispiel zu sagen, das Licht oder die Heizung einzuschalten – oder das selbständig zu tun, wenn man nach Hause kommt.

Überall, wo in kürzester Zeit riesige Datenmengen durchforstet werden müssen, kann KI ihre Stärken zeigen. Suchmaschinen wie Google oder Bing nutzen sie deswegen schon seit mehreren Jahren. Auch bei der Erkennung von Mustern kommt sie vermehrt zum Einsatz, zum Beispiel in der Medizin in der Krebsdiagnose.

Online-Geschäfte setzen sie für Empfehlungen ein, genauso wie Kreditinstitute bei der (Nicht-)Vergabe von Krediten. Die letzten beiden Beispiele zeigen, warum auch der Verbraucherschutz ein waches Auge auf diese Entwicklungen hat. Wenn Entscheidungen verlagert werden, muss klar sein, wer haftet und verantwortlich ist.

Eine der bekanntesten künstlichen Intelligenzen ist ChatGPT. Das steht für „Chat” (engl. „plaudern, sich unterhalten“) und GPT für „Generative Pre-trained Transformer” (engl. für „Generativer vortrainierter Transformer”), mit anderen Worten: Ein großes Sprachmodell, das eigenständig Texte erzeugen kann, inzwischen auch Bilder und Videos. ChatGPT kann, wie ein Mensch in einem Internet-Chat, auf Fragen reagieren und Gespräche führen. Allerdings sind die Antworten nicht immer richtig. Das dahinter stehende Computerprogramm geht von Wahrscheinlichkeiten aus. Es hat keine Möglichkeit, die Wirklichkeit zu überprüfen. Ein Beispiel: Auf die Frage „Wie ist das Wetter in Köln?” muss es sich im Internet Daten suchen und daraus schließen, welche Antwort am wahrscheinlichsten richtig ist. Wenn man es für wichtige Texte einsetzt oder glaubwürdige Informationen sucht, sollte man die Ergebnisse besser noch einmal überprüfen und zusätzlich andere Quellen nutzen.

RISIKEN UND SCHUTZ

Wie jede Technik kann auch KI missbraucht werden. Es kommt immer auf denjenigen an, der sie nutzt. So können Ganoven KI einsetzen, um Verbraucher zu täuschen, zum Beispiel beim „Enkeltrick“.

Heutzutage sind Sprachnachrichten oder sogar Anrufe möglich, die die Stimme des Enkels nachahmen können. Voraussetzung ist, dass er im Internet Sprachproben hinterlassen hat, zum Beispiel bei Youtube oder TikTok. Mit diesen Proben wurde die KI so trainiert, dass ein anderer mit dieser Stimme sprechen kann.

Auch ohne betrügerische Absicht sind KI-Systeme oft undurchschaubar. Da sie selbständig lernen und sich weiter entwickeln können, weiß oft der Anwender nicht, warum eine KI so und nicht anders reagiert. Dies kann problematisch sein, wenn auf KI gestützte Entscheidungen gefällt werden, zum Beispiel bei der Vergabe eines Kredites.

Wer weiß, was KI kann, kann sie einordnen und sich schützen. So könnte jemand anrufen, der wie der eigene Enkel oder ein anderer Verwandter klingt, und um Geld bitten. Wer aber weiß, dass es so etwas gibt, kann sich entsprechend schützen: Man legt auf und fragt bei der Person nach.

Bei Programmen wie ChatGPT rät das Bundesamt für Sicherheit in der Informationstechnik zur Vorsicht bei der Eingabe vertraulicher Themen, da eine Weitergabe an Dritte nicht

auszuschließen ist. Besondere Skepsis ist angebracht, wenn Ihnen in KI-Chats Links geschickt oder Sie nach sensiblen Daten wie Passwörtern gefragt werden.

Zugegeben: Es ist schwer, zu erkennen, ob in einem Computerprogramm oder Dienst im Internet bereits Künstliche Intelligenz eingesetzt wird. Daher fordern Verbraucherschützer unter anderem Transparenz bei Entscheidungen, um zum Beispiel überprüfen zu können, ob diese nicht diskriminieren, sowie eine Risikofolgenabschätzung durch den Anwender.

SINNVOLLE ANWENDUNGEN

Vielfach unbemerkt bahnt sich Künstliche Intelligenz ihren Weg in immer mehr Programme und Anwendungen. Sinnvoll eingesetzt kann sie die Arbeit erleichtern, Abläufe beschleunigen oder sogar Teilhabe ermöglichen. 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.

Bei „großen Datenmengen“ und „durchsuchen“ denkt man unweigerlich an 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.

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 zum Beispiel diejenigen mit einer Ampel anklicken muss, oder alle mit einem bestimmten Tier.

GESUNDHEIT: 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.

EINKAUFEN IM NETZ: „Wenn Ihnen dieses gefallen hat, gefällt Ihnen vielleicht auch…“ oder „Kunden, die jenes gekauft haben, kauften auch…“ Wer kennt sie nicht, diese Kaufempfehlungen nach einer Bestellung im Internet. Dazu wurden tausende von Bestellungen berücksichtigt und katalogisiert. Etwas, das KI ebenfalls gut beherrscht. Nicht immer treffen diese Empfehlungen den Geschmack. Oft machen sie einen aber aufmerksam auf noch unbekannte Bücher, Songs oder andere Produkte.

MOBILITÄT: Hier gibt es mehrere Bereiche, in denen Künstliche Intelligenz unterstützen oder sogar

eigenständig tätig werden kann. Neuere Fahrzeuge besitzen bereits Assistenzsysteme, die beispielsweise selbständig bremsen oder die Spur halten können. 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.

WOHNEN: Technikunterstütztes Wohnen und „kluges Zuhause“ (engl.: Smart Home) setzen auf Computertechnologien, um das Leben in den eigenen vier Wänden zu erleichtern. 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 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 Vorhaben 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 erforderlich ist. Die Akzeptanz der Technologie ist nicht selbstverständlich.

SPRACHASSISTENTEN: Früher kannte man es nur aus Science-Fiction-Filmen: Der Mensch redet mit einem Computer und der Computer antwortet. Ob Alexa von Amazon oder Siri von Apple – digitale Assistenten erobern immer mehr die Wohnzimmer der Welt. Sie können das Wetter vorhersagen, Fragen beantworten oder Musik spielen. Sie dienen sozusagen als intelligente Vermittler zwischen dem Menschen und der weiten Welt des 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.

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.

Diese Liste lässt sich beliebig verlängern. Künstler setzen KI bei der Erzeugung von digitalen Kunstwerken ein, Musiker beim Komponieren. Hier zeigen sich bereits einige Gefahren: Wer weiß mit Sicherheit, dass am anderen Ende des Internet-Chats ein Mensch sitzt? Wieviel hat der Musiker, oder der Student, noch selber geschrieben, was hat er schreiben lassen?

Gefährlicher sind jedoch die Nutzung und permanente Sammlung von riesigen Datenmengen, der Einsatz bei Entscheidungen, die der Mensch nicht mehr überblicken kann und der Missbrauch durch Kriminelle.

TIPPS FÜR EINEN BEWUSSTEN UMGANG

Künstliche Intelligenz – abgekürzt KI (oder englisch „AI“ für „Artificial Intelligence“) – ist in aller Munde. Jedes Unternehmen und jede Organisation, die technologisch auf der Höhe der Zeit sein will, nutzt sie oder plant es zumindest. Was bedeutet dies für die Verbraucherinnen und Verbraucher? Woran sollen wir uns als mehr oder weniger freiwillige Nutzerinnen und Nutzer orientieren? Die folgenden Punkte können dabei helfen.

- Keine KI ohne Computer (Software und Hardware)
- KI beschleunigt die (Datenverarbeitungs-)Prozesse – „Turbo für EDV-Systeme“
- Sie wird von Menschen (Unternehmen, Verwaltung, Organisationen, usw.) eingesetzt
- Sie kann überall da zum Einsatz kommen, wo jetzt schon Computerchips und Software eingesetzt werden – also fast überall.
- KI kann das Leben leichter machen
- Wie jede Technik kann sie auch missbraucht werden
- Wer weiß, was KI kann, kann sie einordnen und sich schützen

GLOSSAR

KÜNSTLICHE INTELLIGENZ: Künstliche Intelligenz ist ein Teilgebiet der Informatik, das sich mit der Automatisierung von intelligentem Verhalten befasst. Dabei ist weder festgelegt, was „intelligent“ bedeutet, noch welche Technik zum Einsatz kommt. Eine der Grundlagen der modernen Künstlichen Intelligenz ist das Maschinelle Lernen. Weitere wichtige Methoden sind logisches Schließen auf symbolischem Wissen, Wissensrepräsentation oder Planungsverfahren. In Fachkreisen wird zwischen Starker KI und Schwacher KI unterschieden.

MASCHINELLES LERNEN: Maschinelles Lernen bezweckt die Generierung von Wissen aus Erfahrungswerten, indem Lernalgorithmen aus Beispielen ein komplexes Modell entwickeln. Das Modell kann anschließend auf neue, potenziell unbekannte Daten derselben Art angewendet werden. Damit kommt das Maschinelle Lernen ohne manuelle Wissenseingabe oder explizite Programmierung eines Lösungswegs aus.

STARKE KI: Starke KI steht für die Vision, mit KI-Techniken menschliche Intelligenz in vollem Umfang und außerhalb einzelner, eng definierter Handlungsfelder nachzubilden. Starke KI findet man bisher nur in Science Fiction. Seit Künstliche Intelligenz in den 1950er Jahren entstand, gab es Prognosen, dass eine starke KI in wenigen Jahrzehnten realisierbar wird.

SCHWACHE KI: Schwache KI setzt KI-Methoden zur Lösung eng umrissener Aufgaben. Während sie in einzelnen Bereichen, wie z. B. der Bildanalyse, menschliche Fähigkeiten bereits übertreffen kann, erreicht Schwache KI bei weiter gefassten Aufgaben im größeren Kontext oder bei Aufgaben, die Weltwissen erfordern, bei weitem nicht das gleiche Niveau. Alle derzeitigen KI-Lösungen sind Beispiele Schwacher KI.

NEURONALE NETZE: Künstliche/Neuronale Netze sind Modelle des Maschinellen Lernens, deren Vorbild die natürlichen neuronalen Netze des Gehirns sind. Sie bestehen aus vielen in Software realisierten Schichten von Knoten, die als künstliche Neuronen bezeichnet werden. Mithilfe von Beispielen verändert ein Lernalgorithmus die Gewichte, Zahlenwerte an den Verbindungen zwischen den Knoten, solange, bis die Ergebnisse für die Aufgabe gut genug sind. Die Anzahl der Knoten, Schichten und ihre Verknüpfung untereinander wirkt sich maßgeblich auf die Lösungskompetenz des Modells aus.

GENERATIVE KI: Generative KI-Modelle werden eingesetzt, um neue Daten zu erzeugen, die ähnliche statistische Eigenschaften wie ein gegebener Datensatz haben. So können z. B. Text, Bilder, Audio, Video, Programmcode, 3D-Modelle oder Simulationen erzeugt werden, die den Anweisungen des Nutzenden folgen.

LARGE LANGUAGE MODELS: Große Sprachmodelle sind Basismodelle oder Foundation Models , die für die Verarbeitung natürlicher Sprache mit großen Mengen von Textdaten trainiert wurden. Die Modelle lernen, Texte fortzusetzen, indem sie statistische Beziehungen zwischen Wörtern herstellen, und damit Wissen über Syntax, Semantik und Ontologie der Sprache, aufbauen. Nach diesem Vortraining können die Modelle für ihren spezifischen Einsatz, z. B. als Chatbot, feinjustiert werden. Ihre Transformer-Architektur ermöglicht die effiziente Verarbeitung großer Datenmengen und die Berücksichtigung entfernter Abhängigkeiten in Daten.

ROBOTER: Als Roboter werden Maschinen oder Geräte bezeichnet, die darauf abzielen, bestimmte physische und kommunikative Aufgaben des Menschen zu übernehmen. Typische Beispiele sind Service- und Industrieroboter. Die Autonomie von Robotersystemen steigt in dem Maße, wie sie selbstständig durch Maschinelles Lernens komplexe Aufgaben lösen können. Ein Beispiel hierfür sind vollautonome Fahrzeuge.

Quelle: www.ki.nrw/ki-schluesselbegriffe/#1 © 2024 Kompetenzplattform KI.NRW

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

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)

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 (2018)
- ○ Rückengesundheit (2010, 28 S.)
- ○ Schadstoffarm wohnen (2017)
- ○ Schädlinge im Haushalt (2016)
- ○ Sonnenschutz (2016, 24 S.)
- ○ Vollwertig essen bei Diabetes Typ 2 (2024)
- ○ Yoga (2015, 32 S.)
- ○ Zähne pflegen (2014, 24 S.)

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 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)
- ○ 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