VERBRAUCHERFORUM 60+

CHANCEN UND HERAUSFORDERUNGEN DES INTERNETS

Themenheft zu den
regionalen Verbraucherveranstaltungen
in Baden-Württemberg

Landesseniorenrat Baden-Württemberg e.V.

Bundesverband Die Verbraucher Initiative e.V.

Baden-Württemberg
Ministerium für Ernährung,
Ländlichen Raum und Verbraucherschutz

WEITERE THEMEN FÜR DIE ZIELGRUPPE DER VERBRAUCHER 60+

Im Rahmen der Verbraucherkonferenzen in Baden-Württemberg wurden in den letzten Jahren folgende Themen behandelt:

- Verbraucher 60+: Aktiv und selbstbewusst im Gesundheitsbereich
- Verbraucher 60+: Sicher im Internet
- Verbraucher 60+: Energie und Kosten sparen
- Verbraucher 60+: Ihr gutes Recht: So schützen Sie sich vor Abzocke im Alltag

Die Abgabe erfolgt – solange der Vorrat reicht – kostenlos. Die jeweils 20-seitigen Publikationen werden gedruckt gegen Versandkosten abgegeben und sind außerdem auf der Webseite der VERBRAUCHER INITIATIVE e. V. unter http://verbraucher.org/informieren/kostenlose-informationen herunterladbar.

Impressum

Herausgeber: Die VERBRAUCHER INITIATIVE e. V. (Bundesverband), Georg Abel (V.i.S.d.P.), Mitarbeit: Guido Steinke, Alexandra Borchard-Becker, Wollankstr. 134, 13187 Berlin. Die Texte der Seiten 3 bis 19 stammen aus der gleichnamigen NRW-Broschüre. Fotonachweis: S. 3: VERBRAUCHER INITIATIVE; alle anderen: IStockphoto. Für die Inhalte sind die jeweiligen Autoren verantwortlich. Nachdruck und Vervielfältigungen, auch auszugsweise, nur mit Genehmigung des Herausgebers (10/2025).

Hinweis: Wenn im Text z. B. vom „Verbraucher" die Rede ist, ist dies ein Zugeständnis an die Flüssigkeit der Sprache. Gemeint sind selbstverständlich Verbraucherinnen und Verbraucher.

Gefördert durch | Baden-Württemberg Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz

VORWORT

LIEBE VERBRAUCHERINNEN UND VERBRAUCHER,

aus unserer wissens- und dienstleistungsorientierten Gesellschaft ist das Internet nicht mehr wegzudenken. Der Umgang mit den unterschiedlichen Möglichkeiten gehört sicherlich zu den Schlüsselkompetenzen. Auch immer mehr ältere Verbraucher sind online unterwegs. Sie besuchen Informationsportale, kaufen Waren und buchen Reisen. Das Internet bietet auch die wichtige Möglichkeit einer gesellschaftlichen Teilhabe, gerade für Ältere. Die neue Freiheit birgt jedoch auch Gefahren wie Schwachstellen in der Datensicherheit und Kostenfallen wie als Gratis-Angebote getarnte kostenpflichtige Abonnements.

Als unabhängige Verbraucherorganisation verfolgen wir das Leitbild der mündigen, verantwortlichen Verbraucher. Um diese Rolle wahrnehmen zu können, sind glaubwürdige Informationen eine Voraussetzung. Wer als mündiger Konsument selbstbewusst und selbstbestimmt die vielfältigen Online-Angebote nutzen will, muss seine Handlungsoptionen sowie seine Rechte und Pflichten als Kunde kennen. Dies gilt natürlich auch für den Umgang mit dem neueren Thema der Künstlichen Intelligenz.

Ihre Dr. Bettina Knothe

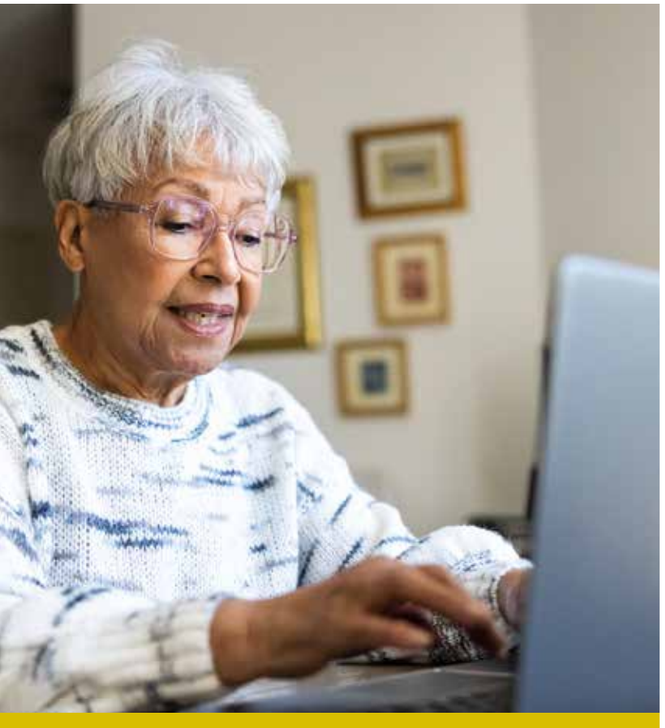
Bundesvorsitzende
Die VERBRAUCHER INITIATIVE e. V.

INHALT

VORBEUGEN

COMPUTER, KONTEN & DATEN SCHÜTZEN

Von zu Hause aus einkaufen, mit Freunden und Familie in Kontakt bleiben, Informationen finden oder Bankgeschäfte erledigen – das Internet bietet gerade für ältere Verbraucherinnen und Verbraucher eine Menge Vorteile. Um es sicher nutzen zu können, sind technische Sicherungsmaßnahmen und umsichtiges Verhalten gefragt. Wir sagen, worauf Sie achten können.



Überlegen Sie, welche privaten Informationen Sie „öffentlich" machen.

Soziale Netzwerke

Sichern Sie Ihren PC und mobile Geräte wie Notebook, Tablet und Smartphone, um sie vor unbefugten Zugriffen anderer Menschen oder fremder Programme (Viren) zu schützen. Beschränken Sie die Zugriffsrechte für andere Nutzer, z. B. durch ein Passwort.

Firewall & Virenscanner

Eine aktivierte Firewall verhindert, dass Viren oder andere Schadsoftware (Malware) auf Ihren Rechner gelangen. Apps bieten diese Funktion ebenfalls für Smartphones an. Ein Virenschutzprogramm bzw. Virenscanner warnt vor Schädlingen, spürt sie auf und entfernt sie, falls sie die Geräte befallen haben.

Achten Sie darauf, dass die Firewall und der Virenscanner immer auf dem neuesten Stand sind. Ein weiterer zentraler Faktor für die Sicherheit ist das Betriebssystem. Halten Sie es bei den verschiedenen Geräten ebenfalls unbedingt aktuell. Aktivieren Sie dazu die automatischen Updates in den jeweiligen Einstellungen. Installieren Sie bei Tablets und Smartphones zudem nur Apps aus vertrauenswürdigen Quellen, z. B. aus den App-Stores der jeweiligen Hersteller.

TIPP Virenschutzprogramm

Sie können ein Virenschutzprogramm kaufen oder ein kostenloses Programm nutzen. Tests von Computerfachzeitschriften oder Verbrauchermagazinen zeigten, dass beide Varianten gute Ergebnisse erzielen können. Sie bieten Hilfestellung bei der Auswahl.

Starke Passwörter

Verwenden Sie für Ihre Kundenkonten bei Banken, Online-Shops, E-Mail- und Messenger-Diensten sowie sozialen Netzwerken Passwörter, die mindestens 10 Zeichen lang sind. Nutzen Sie dafür eine Kombination aus Buchstaben, Zahlen, Groß- und Kleinschreibung sowie Sonderzeichen.

Nehmen Sie unbedingt verschiedene Passwörter für die einzelnen Nutzerkonten. Und denken Sie daran, das Startpasswort zu ändern, wenn Sie sich bei einem neuen Anbieter angemeldet haben.

Halten Sie die Passwörter geheim und bewahren Sie sie an einem sicheren Ort auf. Speichern Sie weder Passwörter noch PIN-Codes, Kreditkartendaten oder Ähnliches auf dem PC oder auf mobilen Geräten. Eine Ausnahme gilt, wenn Sie einen Passwortmanager mit starkem Master-Passwort nutzen.

Zusätzliche Sicherung

Sichern Sie sensible Online-Konten für einen besseren Schutz zusätzlich mit einer Zwei-Faktor-Authentisierung. Bei diesem Verfahren müssen Sie sich in zwei Schritten mit unterschiedlichen Methoden identifizieren, bevor Sie Zugang zu dem Account bekommen.

Üblicherweise geben Sie zunächst Ihren Benutzernamen und Ihr Passwort ein. Im zweiten Schritt erhalten Sie einen weiteren Zugangscode, z. B. per SMS oder E-Mail. Andere Varianten sind TAN-Generatoren, Apps auf dem Smartphone wie beim Online-Banking oder biometrische Kennzeichen wie der Fingerabdruck.

Daten schützen

Daten sind die begehrte Währung in der digitalisierten Welt. Gehen Sie bei den verschiedenen Nutzungen ausgesprochen sparsam damit um.

- **Bei Kundenkonten**: Geben Sie bei der Anmeldung so wenig persönliche Daten wie möglich an.

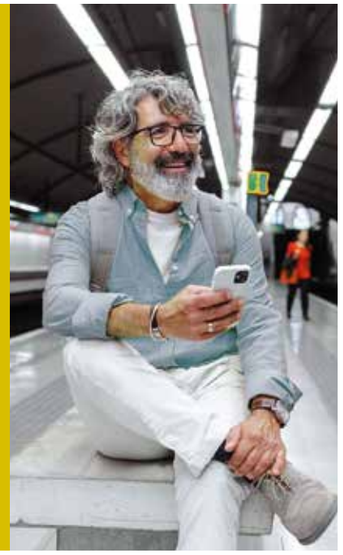
TIPPS Passwörter

- Erstellen Sie Passwörter, indem Sie beispielsweise die Anfangs- oder Endbuchstaben von Wörtern aus einem ganzen Satz nehmen, die Sie durch Zahlen und weitere Zeichen ergänzen.
- Nutzen Sie Passwortmanager zum Generieren und Verwalten von Passwörtern.
- Achten Sie in der Öffentlichkeit auf eventuellen Sichtschutz bei der Eingabe von kritischen Informationen wie Passwörtern.
- Verzichten Sie aus Sicherheitsgründen auf die sogenannte Single-Sign-On-Funktion, mit der Sie die Zugangsdaten für ein Google-Konto oder einen Social-Media-Account wie Facebook für die Anmeldung bei diversen Online-Shops oder -Plattformen verwenden.

- **In sozialen Netzwerken:** Überlegen Sie genau, welche privaten Daten und Fotos Sie „öffentlich" machen wollen. Denken Sie daran: Das weltweite Netz vergisst nichts.
- **Bei Apps**: Schränken Sie deren Zugriffsrechte auf Ihren Smartphones und Tablets soweit wie möglich ein. Nicht alle Berechtigungen sind für die Nutzung tatsächlich notwendig. In den Geräteeinstellungen finden Sie eine Übersicht über die Apps auf dem Gerät und können die Berechtigungen verwalten.

Seien Sie bei Zugriffen auf das Adress- und Telefonbuch, Ihre Standortdaten, Fotos sowie Videos besonders zurückhaltend. Bei Ihren Kontakten sind auch die Daten von anderen Menschen betroffen. Bedenken Sie, dass bei einer dauerhaften Standortfreigabe ein Bewegungsprofil erstellt werden kann. Viele Apps benötigen den Zugriff auf den Standort aber nur dann, wenn Sie die App verwenden.

Seien Sie vorsichtig bei öffentlichen WLAN-Netzen.



Öffentliches WLAN

Seien Sie vorsichtig bei öffentlichen WLAN-Netzen, z. B. in Regional- und Fernzügen, Cafés, Hotels oder Innenstädten. Da die Übertragung der Daten nicht gesichert wird, können sie abgefangen werden oder andere Personen, die das WLAN ebenfalls nutzen, können die versendeten Informationen mitlesen. Achten Sie beim Surfen auf verschlüsselte „https://"-Seiten und deaktivieren Sie gegebenenfalls die Datei- bzw. Verzeichnisfreigabe. Informieren Sie sich vor der Nutzung über die jeweiligen Sicherheitstechnologien.

TIPPS Cookies

- Schränken Sie Cookies in den Datenschutz- und Sicherheitseinstellungen Ihres Browser so weit wie möglich ein. Unterbinden Sie Drittanbieter-Cookies und stellen Sie ein, dass Cookies nach dem Schließen des Browsers gelöscht werden.
- Auch wenn es lästig und aufgrund der unübersichtlichen Gestaltung der Cookie-Banner oftmals mühsam ist, nehmen Sie sich Zeit, die Einstellungen bei der Auswahl der Cookies aufmerksam zu lesen und Ihre Wahl zu treffen.

Um die Datenübertragung in einem öffentlichen WLAN sicherer zu machen, können Sie VPN nutzen, das steht für Virtual Private Network. Dabei werden die Informationen verschlüsselt übertragen. VPN lässt sich über eine App oder über eine Verbindung zum heimischen Router einrichten.

Verzichten Sie darauf, datensensible Anwendungen auszuführen, bei denen Sie Passwörter und andere Zugangscodes eingeben müssen. Es ist besser, diese Aktivitäten über das normale Mobilfunknetz abzuwickeln.

Unterwegs: Flugmodus

Deaktivieren Sie bei mobilen Geräten WLAN und Bluetooth, wenn Sie diese Funktionen unterwegs nicht brauchen. Ist WLAN aktiv, sucht das Gerät permanent nach verfügbaren Netzen und versendet dabei Daten. Sie erlauben Rückschlüsse auf das Gerät, die eigenen Bewegungen und Standorte. Zudem erhöhen Sie die Sicherheit des Systems, wenn Sie WLAN und Bluetooth ausschalten. Diese geöffneten Schnittstellen können theoretisch einen Angriff von außen ermöglichen. Nebenbei schonen Sie die Akkulaufzeit.

Löschen Sie gespeicherte Netzwerke in den Verbindungseinstellungen. So vermeiden Sie, dass sich das Gerät möglicherweise in gefälschte Netzwerke einwählt. Sie tragen den Namen von bekannten öffentlichen Netzwerken, sind aber eine Kopie, über die beispielsweise Schadsoftware auf Ihre Geräte gelangen kann.

Cookies anpassen

Ein zurückhaltender Umgang mit persönlichen Daten ist ebenfalls bei Cookies angezeigt. Diese kleinen Dateien werden von Internetseiten auf Ihrem Rechner gespeichert, um Sie beim nächsten Besuch wiederzuerkennen. Sie können in bestimmten Fällen sinnvoll sein, z. B. wenn Sie mehrere Produkte in einem Online-Shop bestellen, einen Warenkorb anlegen und speichern wollen. Die Webseite erkennt Sie über die Cookies wieder und Sie müssen die Daten nicht noch einmal eingeben.

Deutlich häufiger dienen Cookies jedoch dem Sammeln von Informationen über Sie als Nutzer. Sie erfassen besuchte Seiten und erlauben Rückschlüsse auf Surfverhalten, Interessen, eingekaufte Produkte, finanzielle Möglichkeiten, Bildungsstand, E-Mail-Adresse und andere Daten, die Sie eingegeben haben. Auf diese Weise lässt sich im Laufe der Zeit ein umfangreiches Nutzerprofil erstellen, das für die Anbieter bares Geld wert ist. Es kann beispielsweise für Werbung genutzt oder verkauft werden.

Cookie-Banner prüfen

Wenn Sie eine Webseite aufrufen, erscheint aufgrund der aktuellen Datenschutzgrundverordnung meistens ein sogenanntes Cookie-Banner und fragt, welche Informationen über Sie gespeichert werden dürfen. Webseiten, die nur technisch notwendige Cookies nutzen, müssen kein Cookie-Banner verwenden.

Lassen Sie nur erforderliche Cookies zu, die auch als essentielle oder notwendige Cookies bezeichnet werden, und lehnen Sie grundsätzlich alle anderen ab. Dazu gehören Tracking-Cookies sowie Marketing- oder Analyse-Cookies.

Datensicherung

Sichern Sie Ihre gesamten Daten regelmäßig. Mit diesem sogenannten Backup vermeiden Sie einen Datenverlust durch technische Probleme oder einen Befall mit Schadsoftware.

Bei der klassischen Variante verwenden Sie eine externe Festplatte oder USB-Sticks ausschließlich für die Datensicherung und trennen sie dann wieder vom PC oder Notebook.

Alternativ steht eine Cloud zur Verfügung, das ist eine Art Festplatte im Internet. Microsoft und Apple bieten Clouds an, daneben gibt es weitere Clouddienste. Stellen Sie vor der Nutzung sicher, dass sie ausreichend Platz bietet und prüfen Sie, inwieweit der Datenschutz durch Verschlüsselung gewährleistet wird. Es gibt zudem Programme, die Ihre Daten verschlüsseln, bevor sie in die Cloud hochgeladen werden.

TIPP Datensicherung

Mit Programmen zur Datensicherung, die von den gängigen Betriebsystemen angeboten werden, sparen Sie sich das Kopieren der einzelnen Dateien. Nach einmaliger Einstellung erfolgt der Backup automatisch.

WEITERE INFORMATIONEN

Ministerium für Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen, www.mlv.nrw > Themen > Verbraucherschutz > Verbraucherschutz im Alltag > Verbraucherschutz in der digitalen Welt ■ Verbraucherzentrale Nordrhein-Westfalen, www.verbraucherzentrale.nrw > Digitale Welt > Sicher im Internet – Handy, Tablet und PC schützen ■ Landeskriminalamt Nordrhein-Westfalen (LKA NRW), Kampagne „Mach Dein Passwort stark": www.mach-dein-passwort-stark.de/ ■ Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de > Themen > Verbraucherinnen und Verbraucher

ABZOCKE ERKENNEN

Gelegenheit macht Diebe – dieser Spruch gilt auch für das Internet. Die Gauner haben es auf Ihre Daten und Ihr Geld abgesehen. Dafür nutzen sie beispielsweise E-Mails, Webseiten, Messenger-Dienste oder soziale Netzwerke. Wir stellen häufige Betrugsmaschen vor und sagen, wie Sie sich schützen können.

Die Kriminellen nehmen gezielt die Internet-Nutzer ins Visier und versuchen, sie mit Manipulationen oder Täuschungen dazu zu bringen, sensible Daten preiszugeben oder Geld zu überweisen. Hilfsbereitschaft, Vertrauen, Respekt oder Angst der Opfer werden ausgenutzt. Sie werden über die Identität des Absenders getäuscht und mit Problemen, Notlagen oder falschen Versprechungen geködert.

Spam & Phishing

Besonders häufig kommen Spam- und Phishing-Mails vor. Spam sind unverlangt zugesandte Werbe-Mails. Handelt es sich tatsächlich nur um Werbung, sind sie lästig, aber nicht gefährlich. Doch es gibt auch Spam-Mails, in denen einige Fallen lauern können. „Phishing" ist ein Kunstwort aus „Passwort" und „Fishing" (abfischen). Ziel ist es, Passwörter und weitere vertrauliche Informationen zu erbeuten.

Aktivieren Sie den Spam-Filter Ihres E-Mail-Dienstes.

Folgende Gefahren können von diesen betrügerischen E-Mails ausgehen:

Schadstoffsoftware: Sie kann sich in den E-Mails selbst, den Anhängen oder enthaltenen Bildern verstecken. Die Viren, Würmer und andere Schädlinge können sensible Daten ausspionieren, Ihren Computer oder Teile davon manipulieren oder lahm legen.

Betrug: Mit falschen Versprechungen sollen Sie verleitet werden, Geld zu überweisen, z.B. um eine angebliche Erbschaft anzutreten, einen lukrativen Job zu bekommen, vermeintlichen Freunden Geld zu leihen oder in erfundenen finanziellen Notlagen zu helfen. Oder sie enthalten Mahnungen und Inkasso-Forderungen über angeblich nicht bezahlte Rechnungen.

Datenklau: Gefälschte E-Mails oder Internetseiten dienen als Köder, um sensible Daten wie Passwörter, Zugangsdaten zu Bankkonten oder anderen Konten „abzufischen".

Falschmeldungen: Diese Spam-Mails werden Hoax genannt und sollen Meinungen beeinflussen. Sie können auch als Kettenbrief daherkommen und mit der Aufforderung verbunden sein, sie weiter zu verbreiten. Leiten Sie solche E-Mails auf keinen Fall weiter.

Vorbeugen

- Aktivieren Sie den Spam-Filter Ihres E-Mail-Dienstes.
- Gehen Sie sparsam mit der Angabe Ihrer E-Mail-Adresse und anderen Kontaktdaten um. Besondere Vorsicht ist bei vermeintlichen Gewinnspielen geboten.
- Stimmen Sie der Weitergabe Ihrer Daten nicht automatisch zu. Der Handel mit Adressen ist ein großes Geschäft. Und je mehr Anbietern oder Unternehmen Sie Ihre private E-Mail-Adresse geben, desto größer ist das Risiko, dass sie in unseriöse Hände gerät.
- Nutzen Sie mehrere E-Mail-Adressen, z. B. eine für die private Kommunikation, eine andere für die Anmeldung bei Online-Diensten und eine dritte für das Online-Shopping. So reduzieren Sie das Spam-Aufkommen in Ihrem Haupt-E-Mail-Account und können notfalls eine Adresse löschen, wenn der Spam überhand nimmt. Wählen Sie dabei Adressen, die keine Rückschlüsse auf Ihren vollständigen Namen zulassen.

Auch Adressen von Bekannten könnten gefälscht sein.

Erkennen

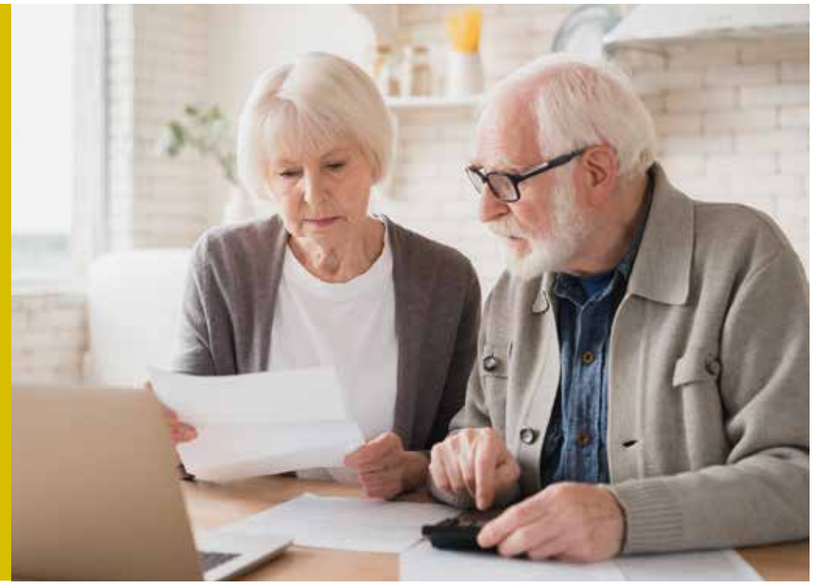
Die betrügerischen E-Mails weisen einige Gemeinsamkeiten auf:

Falsche Absender: Die Kriminellen verwenden oftmals gefälschte E-Mailadressen von Firmen, bei denen viele Verbraucher Kunden sind, z. B. Banken, Sparkassen, Visa, Mastercard, Paypal, DHL, Amazon, Telekommunikationsanbieter, andere große Unternehmen und soziale Netzwerke. Sie sehen oftmals nur auf den ersten Blick genau so aus wie die bekannten Firmenadressen. Aber auch Adressen von Bekannten oder Freunden können gefälscht sein.

Abfrage von Kundendaten: Werden Sie in der E-Mail darum gebeten, auf einen Link zu klicken und persönliche Daten preiszugeben oder unbedingt angeblich wichtige Dateien herunterzuladen, haben Sie es mit ziemlicher Sicherheit mit Phishing zu tun. Beim Inhalt können zudem Rechtschreib- und Grammatikfehler sowie merkwürdig klingende Formulierungen auffallen.

Gefälschte Webseiten: Wer die betrügerischen E-Mails öffnet und auf den enthaltenen Link klickt, landet auf gefälschten Abzockerseiten, die den Originalseiten täuschend ähnlich sehen. Verbraucher werden dazu verleitet, Zugangsdaten, Transaktionsnummern (TAN) oder Kreditkarteninformationen einzugeben, die missbräuchlich verwendet werden.

Prüfen Sie die Seriösität des Händlers.



Überlegt handeln

- Bedenken Sie, dass seriöse Unternehmen Sie niemals per E-Mail auffordern, Benutzerdaten und Kontoinformationen auf einem neuen Portal einzugeben oder Aktualisierungen für ein TAN-Verfahren vorzunehmen. Falls Sie Zweifel haben, fragen Sie dort nach, ob die E-Mail tatsächlich daher stammt.
- Seien Sie wachsam bei Absenderadressen, die Sie nicht kennen, vor allem bei unverständlichen Phantasienamen. Öffnen Sie die Mails nicht und antworten Sie nicht darauf.
- Prüfen Sie den Absender und die Betreffzeile von fragwürdigen E-Mails, ohne sie zu öffnen. Richten Sie dazu den Mauszeiger auf den Absender, dann wird die Adresse angezeigt. Löschen Sie die Mails und deaktivieren Sie die Vorschau-Funktion Ihres E-Mail-Programms.
- Falls Sie die Mails versehentlich geöffnet haben, klicken Sie keinesfalls auf die Links und öffnen Sie keine Datei-Anhänge oder Bilder.
- Seien Sie besonders vorsichtig, wenn Sie ohne erkennbaren Grund nach einer TAN oder gleich nach mehreren TANs auf einmal gefragt werden oder wenn Sie auf der Seite Ihrer Bank nach der Anmeldung eigentlich bekannte Informationen wie Kontonummer und Namen nochmals eingeben sollen. Brechen Sie den Vorgang sofort ab.
- Werden Sie in unbekannten E-Mails aufgefordert, schnell angeblich offene Rechnungen zu begleichen oder dringende Dokumente zu bearbeiten und werden Ihnen Konsequenzen wie die Sperrung von Accounts oder ähnliches angedroht, sollten Sie unbedingt Vorsicht walten lassen.

Im Ernstfall

Trotz aller Vorsicht kann es passieren, dass man auf eine Phishing-Mail hereinfällt.

Haben Sie auf den Link in der Mail geklickt oder die Anhänge geöffnet, kann sich Ihr Computer mit Schadsoftware infiziert haben. Aktualisieren Sie Ihren Virenscanner und starten Sie einen vollständigen Scan, der Ihr gesamtes Gerät checkt, z. B. Ihren PC, Notebook, Tablet oder Ihr Smartphone.

Meldet Ihr Virenscanner einen Befall mit Schadsoftware, bewahren Sie Ruhe. Lassen Sie sich nicht durch Drohungen oder Lösegeldforderungen unter Druck setzen und zu unüberlegten Handlungen verleiten.

Gehen Sie wie folgt vor

- Trennen Sie das Gerät sofort vom Internet sowie von allen verbundenen Geräten und schalten Sie es aus.
- Nutzen Sie ein nicht infiziertes Gerät, um sicherheitshalber Ihre Passwörter zu Ihren Online-Konten zu ändern. Sperren Sie außerdem Ihre Kreditkarte und beantragen Sie eine neue.
- Wenden Sie sich an Computerfachleute, um sich bei der Entfernung des Schädlings und Wiederherstellung des Computers helfen zu lassen.
- Verwenden Sie Ihr Gerät erst wieder, wenn es frei von Schadprogrammen ist.
- Zeigen Sie den Cyber-Angriff bei Ihrer örtlichen Polizeidienststelle an. Legen Sie die Mail als Beweis für den Betrug vor.

Haben Sie den Link zu einer betrügerischen Webseite geöffnet und dort persönliche Daten eingegeben, kommt es beim weiteren Vorgehen darauf an, welche Informationen Sie preisgegeben haben. Waren es Adresse und Telefonnummer, seien Sie in Zukunft aufmerksam bei Anrufen oder Briefen, die Sie zur Weitergabe anderer sensibler Daten oder zu Geldüberweisungen drängen wollen.

Haben Sie Passwörter, Konto- oder Kreditkartennummern eingegeben, wenden Sie sich umgehend an Ihre Bank, lassen Sie die Karten sperren und sich über das weitere Vorgehen beraten. Ändern Sie sofort Ihre Zugangsdaten zum Online-Banking, zu anderen Accounts und kontrollieren Sie regelmäßig Ihre Kontoauszüge.

Smishing & Co.

Phishing kann auch über SMS, WhatsApp, andere Messengerdienste oder per Telefon stattfinden. Das Prinzip ist vergleichbar und im Visier der Betrüger stehen ebenfalls Ihre Daten und Ihr Geld.

Beliebt sind beispielsweise gefälschte Nachrichten von Paketdiensten oder Banken sowie Anrufe von angeblichen Mitarbeitern bekannter Unternehmen oder Behörden und von vermeintlichen Freunden von Verwandten.

Geben Sie in solchen Fällen keine Daten heraus und gewähren Sie Unbekannten keinen Zugang zu Ihrem Rechner, sondern legen Sie auf. Rufen Sie nicht die angegebenen Telefonnummern zurück, die sind gefälscht. Nehmen Sie mit den jeweiligen Absendern unter den Ihnen bekannten Telefonnummern Kontakt auf, um zu klären, ob der Anruf echt war.

TIPPS Soziale Netzwerke

- Vorsicht ist bei Kontaktanfragen geboten, wenn sie von Unbekannten stammen oder wenn Freunde nochmalige Kontaktanfragen stellen. Dahinter können Betrüger stecken, die mithilfe eines kopierten Profils Kontakt mit den Online-Bekannten des Original-Profils aufnehmen, um sie durch Vortäuschung einer Notlage zur Überweisung von Geld zu bewegen.
- Kontaktieren Sie die betreffende Person über einen anderen Weg und fragen Sie nach, ob die Kontaktanfrage ihre Richtigkeit hat. Falls es sich um ein kopiertes Profil und damit um einen Identitätsdiebstahl handelt, melden Sie den Vorfall.

Schützen Sie sich vor Internetbetrügern und antworten Sie nicht auf erpresserische Mails.

Betrug über WhatsApp

Als Pendant zum „Enkeltrick“ am Telefon werden Nachrichten über WhatsApp und andere Messengerdienste verbreitet, um Notfälle von bekannten Personen vorzutäuschen und die Opfer auf diese Weise zu Zahlungen von hohen Geldbeträgen zu bewegen. Der Betrug beginnt meistens mit der Nachricht, dass der Absender angeblich eine neue Mobilnummer hat. Fragen Sie in solchen Fällen bei Ihren Kindern, Enkelkindern oder Freunden nach, ob die Nachricht von dort stammt. Nutzen Sie dafür die Ihnen bekannte Handynummer oder andere Kontaktmöglichkeiten.

Single- und Kontaktbörsen

Betrug mit falschen Accounts kommt ebenfalls bei Kontaktbörsen und Partnervermittlungen vor. Die Kriminellen bauen zunächst eine Vertrauensbeziehung zum Opfer auf. Hat es nach einiger Zeit des intensiveren Kontaktes Vertrauen gefasst, wird es um Geld gebeten. Das können durchaus größere Summen sein, z. B. für ein Flugticket, um sich endlich kennenlernen zu können, eine dringende Operation oder eine andere angebliche Notlage. Haben die Kriminellen das Geld erhalten, wird der Kontakt abgebrochen und das Profil gelöscht. Für diese Abzockmasche gibt es einen eigenen Begriff: Romance-Scamming.

Erpressung

Betrüger versuchen, Computer- und Internetnutzer auf verschiedenen Wegen zu erpressen. Eine Variante sind Schadprogramme, die als Ransomware bzw. als Verschlüsselungs- oder Erpressungstrojaner bezeichnet werden, eine andere Form sind erpresserische Mails. Aufhänger dieser E-Mails ist meistens, dass angeblich der Computer der Opfer gehackt wurde. Dadurch würden die Täter über brisante Informationen verfügen, die sie veröffentlichen, falls das Opfer nicht zahlt.

Antworten Sie nicht auf erpresserische Mails, denn damit bestätigen Sie, dass Ihre Mail-Adresse genutzt wird. Öffnen Sie auch die Anhänge nicht und zahlen Sie kein Lösegeld. Dann besteht die Gefahr, dass Sie als zahlungsbereites Opfer erneut erpresst werden könnten. Suchen Sie Computerfachleute auf, um die Schadsoftware professionell entfernen zu lassen. In den meisten Fällen können sie die Daten nicht entschlüsseln. Dann bleibt nur, sämtliche Dateien und Programme zu löschen und den Computer mithilfe einer Sicherungskopie wiederherzustellen. Da es sich um Erpressung handelt, können Sie Strafanzeige bei der Polizei erstatten.

WEITERE INFORMATIONEN

Verbraucherzentrale Nordrhein-Westfalen, www.verbraucherzentrale.nrw > Digitale Welt > Phishing-Radar ■ Die VERBRAUCHER INITIATIVE e. V., www.verbraucher60plus.de > Internet > Fallen im weltweiten Netz ■ Polizei Nordrhein-Westfalen/Köln, https://koeln.polizei.nrw/artikel/podcast-reihe-sicherheit-in-der-digitalen-welt: Podcast-Reihe „Sicherheit in der digitalen Welt“ ■ Landeskriminalamt Niedersachsen, www.polizei-praevention.de: Ratgeber Internetkriminalität ■ Deutschland sicher im Netz e. V., www.sicher-im-netz.de > Verbraucher ■ Digital-Kompass, www.digital-kompass.de

PRÜFEN

ÜBERLEGT ONLINE EINKAUFEN

Lebensmittel, Kleidung, Bücher, Haushaltsgeräte, Möbel oder andere Produkte in Ruhe aus einem breiten Warenangebot auszuwählen und nach Hause geliefert zu bekommen, ist praktisch und bequem. Worauf Sie achten können, um unliebsame Überraschungen zu vermeiden, haben wir hier zusammengestellt.

Prüfen Sie Online-Shops vor der Bestellung anhand der folgenden Punkte:

Vollständiges Impressum: Angegeben werden der Firmenname, die Rechtsform des Unternehmens, die verantwortliche Person und Postadresse. Zusätzlich müssen ein Handelsregistereintrag und eine Umsatzsteuer-Identifikationsnummer genannt werden.

AGB: Die allgemeinen Geschäftsbedingungen sind leicht zu finden und verständlich formuliert. Informationen zu Bestellmodalitäten, Lieferbedingungen, Versandkosten, Widerrufsrecht und Erstattung der Kaufpreise sind enthalten. Prüfen Sie, wie und wohin Sie Waren zurücksenden können (Deutschland oder Ausland) und welche Kosten dabei entstehen.

Datenschutz: Informationen zum Schutz und der Sicherheit Ihrer Daten sind ebenfalls gut auffindbar.

Kontakt: Der Shop ist auf verschiedenen Wegen erreichbar. Bei ausländischen Händlern sollte es eine Kontaktmöglichkeit in deutscher Sprache geben.

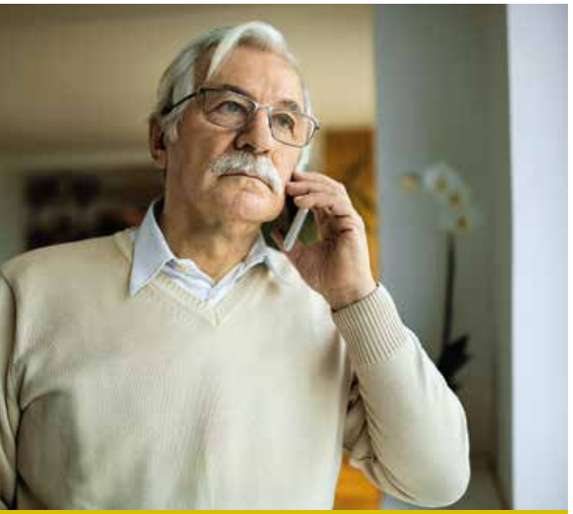
Datenübertragung: Die Browserzeile weist auf eine verschlüsselte Datenübertragung hin (erkennbar an https://www... oder dem Schlosssymbol). Achten Sie darauf vor allem beim Bestellen und Bezahlen. Mit einem Klick auf das Schlosssymbol können Sie zudem überprüfen, ob die Verbindung sicher und die Webadresse korrekt ist.

Prüfen Sie Online-Shops vor der Bestellung.

Produktinformationen: Sie sind klar, verständlich und umfassend, die Bilder passen zu der Ware.

Bestellbutton: Er ist eindeutig zu erkennen und trägt Hinweise wie „Kostenpflichtig bestellen“, „Zahlungspflichtig bestellen“ oder „Jetzt kaufen“. Begriffe wie „Anmelden“ oder „Weiter“ sind nicht zulässig.

Zahlungsmöglichkeiten: Mehrere Varianten werden angeboten, z. B. der Kauf auf Rechnung, die Zahlung per Kreditkarte, das Lastschriftverfahren, Online-Bezahldienste, Vorkasse oder Nachnahme.



TIPPS

- Machen Sie bei unbekannten Shops einen Testanruf, recherchieren Sie nach möglichen Kundenbeschwerden und kritischen Berichten, z. B. von Verbraucherorganisationen. Nutzen Sie den Fake-Shop-Finder der Verbraucherzentralen.
- Wickeln Sie bei Online-Marktplätzen, z. B. bei Amazon, den Kontakt, die Bestellung und Bezahlung ausschließlich über den Marktplatz mit den bekannten Funktionen „Warenkorb“ und „Kasse“ ab. So önnen Sie sich vor Betrug zu schützen, da vorhandene Sicherungsmaßnahmen und Käuferschutz greifen.

Die Methoden haben Vor- und Nachteile. Der Kauf auf Rechnung ist am verbraucherfreundlichsten, da Sie die Lieferung prüfen können. Bei Kreditkarten oder Lastschriften können Sie das Geld innerhalb einer bestimmten Frist zurückbuchen lassen, falls etwas nicht stimmt. Bei Überweisungen ist das nur möglich, wenn das Geld noch nicht auf dem Empfängerkonto eingegangen ist. Bei Online-Bezahldiensten haben Sie keinen direkten Kontakt zum Händler und er erfährt Ihre Kontodaten nicht. Zudem bieten die Dienste Käuferschutzprogramme an. Von Vorkasse ist abzuraten, wenn der Händler nicht vertrauenswürdig erscheint. Auch Nachnahme hat erhebliche Nachteile. Und Vorsicht ist bei Angeboten wie „Buy now, pay later“ geboten. Der Überblick über fällige Zahlungen kann schwerer fallen und möglicherweise fallen Gebühren oder Zinsen an.

Labels: „Trusted Shops“, „EHI Geprüfter Online-Shop“ und „ips Gütesiegel“ (Internet Privacy Standards) weisen auf seriöse Online-Shops hin. Beim Anklicken werden Sie auf die Webseite des Siegelanbieters geleitet und können das Prüfzertifikat einsehen.

Fake-Shops erkennen

Betrügerische Online-Shops sind nicht auf Anhieb zu identifizieren. Sie sind professionell aufgemacht, wirken Vertrauen erweckend und orientieren sich nicht selten am Erscheinungsbild anderer bekannter Shops oder Marken.

Die Kunden werden auf mehreren Wegen abgezockt. Die gelieferten Waren entpuppen sich als minderwertiger Ramsch und sind ihr Geld nicht wert. Wenn es ungünstiger läuft, wird die bestellte und im Voraus bezahlte Ware gar nicht geliefert. Nachfragen beim Shop laufen ins Leere, Kunden werden wegen angeblicher Lieferverzögerungen vertröstet. Im ungünstigsten Fall werden die Adress- und Zahlungsdaten wie Kreditkarten- oder Kontonummern für kriminelle Handlungen missbraucht.

Folgende Anzeichen deuten auf einen Fake-Shop hin:

- Es werden durchweg sehr preisgünstige Waren angeboten und die Kundenbewertungen sind überschwänglich positiv.
- Der Name der Webadresse passt nicht zu den Produkten des Shops. Sie weist zudem ungewöhnliche Domainbezeichnungen auf, z. B. de.com. Häufig fehlt das Schlosssymbol für eine gesicherte Verbindung.
- Der Kontakt ist nur per E-Mail möglich. Bestellt werden kann nur gegen Vorkasse. Andere Bezahlmöglichkeiten werden zwar aufgeführt, aber lassen sich nicht nutzen.
- Das Impressum fehlt oder enthält falsche Angaben, auch die Allgemeinen Geschäftsbedingungen suchen Sie vergebens.
- Zu den abgebildeten Gütesiegeln sind keine weiteren Informationen hinterlegt.

Ware nicht bekommen

Haben Sie Waren bestellt und bezahlt, aber nicht bekommen, können Sie versuchen, das Geld zurückbuchen zu lassen, wenn Sie per Lastschrift oder Kreditkarte bezahlt haben. Bei einem Online-Bezahldienst wie Paypal oder Klarna kann der Käuferschutz greifen.

Stellen Sie Beweismittel wie E-Mails, Bestellbestätigungen und Screenshots zusammen und erstatten Sie Anzeige bei der Polizei.

Falsche Rechnungen

Bei drängenden Mahnungen von Online-Shops oder aggressiven Schreiben von Inkasso-Unternehmen checken Sie den Namen des Absenders, die Adresse des Shops und Ihre eigenen Daten. Nutzen Sie den kostenlosen Inkasso-Check der Verbraucherzentralen, um zu prüfen, ob Sie zahlen müssen.

Nutzerkonten gehackt

Handelt es sich bei dem Rechnungsabsender um ein seriöses Unternehmen mit korrekter Adresse und Ihre Angaben stimmen, aber Sie haben dort nichts bestellt, wurden möglicherweise Ihre Daten missbraucht. Die Betrüger können über Phishing Mails oder Datenlecks daran gekommen sein und haben in Ihrem Namen bei einem Online-Shop eingekauft.

Gehen Sie bei dem Verdacht, dass Konten bei Online-Shops sowie andere Accounts geknackt und Daten gestohlen wurden, folgendermaßen vor:

- **Passwörter ändern**: Vergeben Sie neue Zugangsdaten für die betroffenen Accounts und überprüfen Sie andere Online-Konten.
- **Online-Shops und andere Unternehmen informieren**: Sagen Sie, dass Sie den Verdacht eines Identitätsdiebstahls haben. Melden Sie sofort, wenn Sie keinen Zugriff mehr auf Ihre Accounts haben und lassen Sie sie zurücksetzen.
- **Bank kontaktieren**: Lassen Sie Ihre Kreditkarten sperren. Prüfen Sie Ihre Kontoauszüge auf unberechtigte Abbuchungen und lassen Sie sie gegebenenfalls zurückbuchen.
- **Anzeige erstatten**: Sichern Sie E-Mails, Bestelldaten sowie Kontoauszüge und erstatten Sie Strafanzeige bei der Polizei.
- **Widerspruch einlegen**: Legen Sie per Einschreiben Widerspruch gegen unberechtigte Forderungen beim Inkasso-Büro und bei dem betreffenden Unternehmen ein. Zahlen Sie auf keinen Fall den geforderten Betrag und leisten Sie auch keine Teilzahlungen.
- **Freunde und Bekannte informieren**: Teilen Sie ihnen mit, wenn Ihr E-Mail- oder Social-Media-Account gehackt wurde und warnen Sie vor Nachrichten mit Links oder Anhängen, die in Ihrem Namen verschickt werden.

WEITERE INFORMATIONEN

Verbraucherzentrale Nordrhein-Westfalen, www.verbraucherzentrale.nrw > Digitale Welt > Online-Handel; Suchbegriff „Inkasso-Check“ ■ Verbraucherzentralen Deutschland, Fakeshop-Finder: www.verbraucherzentrale.de/fakeshopfinder ■ Die VERBRAUCHER INITIATIVE e. V., www.verbraucher60plus.de > Internet > Sicher einkaufen im Netz

BEACHTEN

SICHERES ONLINEBANKING

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.

WEITERE INFORMATIONEN

Verbraucherzentrale Nordrhein-Westfalen, www.verbraucherzentrale.nrw > Geld & Versicherungen > Sparen und Anlegen ■ Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de > Themen > Verbraucherinnen und Verbraucher

KENNEN

KÜNSTLICHE INTELLIGENZ & ALGORITHMEN

Künstliche Intelligenz – abgekürzt KI – ist in aller Munde. Sie wird bereits von zahlreichen Unternehmen und Organisation genutzt oder soll künftig eingesetzt werden. Was KI und Algorithmen für Verbraucherinnen und Verbraucher bedeuten, welche Chancen und Risiken damit verbunden sind, haben wir anhand einiger Beispiele zusammengestellt.

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.

Turbo für EDV-Systeme

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.

Nutzen von KI

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.

Auch bei KI: Vorsicht bei der Eingabe vertraulicher Daten.

Beispiele

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.

Gesundheit: Riesige Datenmengen zu durchforsten und Muster zu erkennen, ist eine Stärke der KI. Das ist in der Medizin gefragt, wenn es darum geht, viele Daten auszuwerten. So unterstützt 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.

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 durchforstet und katalogisiert. Etwas, das KI ebenfalls gut beherrscht.

Mobilität: 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. Auch die Bahn setzt KI ein, um Verspätungen zu minimieren.

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 zusammen arbeiten, weiß das „kluge Zuhause“, welche Temperaturen wann und wo bevorzugt werden, und wann Licht benötigt wird.

ChatGPT: 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.

KI kann viele Daten auswerten und unterstützt die Krebsdiagnose.

Risiken

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.

Schutz

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.

Algorithmen

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-Gesetz

Angesichts der raschen technologischen Entwicklung der KI hat die EU beschlossen, gemeinsam zu handeln. Das KI-Gesetz ist die weltweit erste umfassende gesetzliche Regelung für KI. Ziel ist es, die Risiken für die Gesundheit, die Sicherheit und die Grundrechte zu mindern. Der Rechtsrahmen wird sowohl für öffentliche als auch für private Akteure innerhalb und außerhalb der EU gelten, sofern das KI-System in der Union in Verkehr gebracht wird oder Menschen in der EU von seiner Verwendung betroffen sind. Künftig müssen laut EU-Vorgaben Portale etc., die Künstliche Intelligenz einsetzen, gekennzeichnet werden. Weitere Informationen unter: https://ec.europa.eu/commission/presscorner/detail/de/QANDA_21_1683

WEITERE INFORMATIONEN

BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V., KI für ein gutes Altern, https://ki-und-alter.de > Wissen ■ Lernende Systeme – die Plattform für Künstliche Intelligenz, www.ki-konkret.de > Was ist KI?, Was kann KI?, Was darf KI? ■ Verbraucherzentrale Bundesverband, www.vzbv.de > Künstliche Intelligenz – Forderungen des vzbv ■ Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.bund.de > Suchbegriff „KI Sprachmodell“

PROJEKTPARTNER

Baden-Württemberg
Ministerium für Ernährung,
Ländlichen Raum und Verbraucherschutz

Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg

Kernerplatz 10, 70182 Stuttgart
Tel. 0711 / 126-0
poststelle@mlr.bwl.de-mail.de
www.mlr.baden-wuerttemberg.de

Das Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz Baden-Württemberg informiert im Verbraucherportal Baden-Württemberg (www.verbraucherportal-bw.de) über zahlreiche Verbraucherthemen. Auch auf der Homepage des Ministeriums (www.mlr.baden-wuerttemberg.de) finden Verbraucher 60+ unter „Unsere Themen" zahlreiche Informationen, beispielsweise zu Verbraucherrechten im Alltag oder Verbraucherschutz im Netz.

Bundesverband
Die Verbraucher Initiative e.V.

Die VERBRAUCHER INITIATIVE e. V. (Bundesverband)

Wollankstr. 134, 13187 Berlin
Tel. 030 / 53 60 73-3
mail@verbraucher.org, www.verbraucher.org

Der gemeinnützig anerkannte Bundesverband bietet seit 1985 unter www.verbraucher.org zahlreiche Informationen z. B. zu „Zusatzstoffen in Lebensmitteln". Rund 120 Broschüren zu den Themen Ernährung, Umwelt und Gesundheit können im Shop bestellt oder heruntergeladen werden. Die Webseite www.verbraucher60plus.de wendet sich gezielt an Ältere. Angeboten werden dort u. a. ein kostenfreies Online-Magazin und Weiterbildung über eine Online-Akademie.

Landesseniorenrat
Baden-Württemberg e.V.

Landesseniorenrat Baden-Württemberg e. V.

Kriegerstr. 3, 70191 Stuttgart
Tel. 0711 / 61 38 24
landesseniorenrat@lsr-bw.de, www.lsr-bw.de

Der Landesseniorenrat Baden-Württemberg e. V. ist der Zusammenschluss von rund 40 Kreis- und Stadtseniorenräten, 180 Orts- und Stadtseniorenräten und Landesorganisationen, die auf dem Gebiet der Altenarbeit tätig sind. 1974 als Dachverband gegründet, arbeitet der Landesseniorenrat als Interessenvertretung der älteren Menschen in Baden-Württemberg unabhängig, überparteilich und überkonfessionell.

Kooperationspartner

Verbraucherzentrale
Baden-Württemberg

Verbraucherzentrale Baden-Württemberg e. V.

Paulinenstr. 47, 70178 Stuttgart
Tel. 0711 / 66 91 10
info@vz-bw.de, www.vz-bawue.de

Die gemeinnützige Verbraucherzentrale Baden-Württemberg ist ein Verein, der seit dem Jahr 1958 in Fragen des privaten Konsums vor Ort, per Telefon, Videochat und Online informiert und berät. Die breite Themenpalette reicht dabei von Geld & Versicherungen über Lebensmittel, Energie und Haushalt bis zu Verträgen & Reklamation. Zum breitgefächerten Angebot gehören auch Erklärvideos und weitere Angebote zur Verbraucherbildung wie kostenfreie Online-Seminare.