Digital Kompass

Digital-Kompass kompakt

www.digital-kompass.de

Herausgeber:

DsiN Deutschland sicher im Netz

Mit Unterstützung von:

bagso

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Digital Kompass

Impressum

Herausgeber:
Digital-Kompass c/o Deutschland sicher im Netz e.V.
Albrechtstraße 10 c
10117 Berlin
info@digital-kompass.de
www.digital-kompass.de

V.i.S.d.P.:
Dr. Michael Littger

Redaktion:
Die VERBRAUCHER INITIATIVE e. V. (Bundesverband)

Gestaltung und Satz:
www.nadine-kreuder.com

Druckerei:
WIRmachenDRUCK GmbH, www.wir-machen-druck.de

Erscheinungsjahr:
1. Auflage 2021

Titelbild:

Liebe Leserinnen und Leser,

das Internet bietet eine Fülle von Chancen, unseren Alltag zu erleichtern. Das gilt in besonderem Maße für ältere Generationen. Der Digital-Kompass stellt kostenfreie Angebote für Seniorinnen und Senioren rund um Internet und Co. bereit. Er ist Treffpunkt für persönlichen Austausch an bundesweit 100 Standorten, für Schulungen – vor Ort und online – und Quelle für zahlreiche Lehr- und Lernmaterialien. Die vorliegende Publikation gehört dazu: mit kompakten Informationen rund um eine sichere Internetnutzung. Der Digital-Kompass ist ein Verbundprojekt von Deutschland sicher im Netz e.V. und der Bundesarbeitsgemeinschaft der Seniorenorganisationen in Partnerschaft mit der Verbraucher Initiative e.V.

Viel Vergnügen beim Lesen!

Ihr Joachim Schulte
Projektleiter Digital-Kompass
Deutschland sicher im Netz e.V.

Ihr Georg Abel
Bundesgeschäftsführer,
Die VERBRAUCHER INITIATIVE e. V.

Inhalt

Online sicher unterwegs

Das Internet bietet älteren Verbraucherinnen und Verbrauchern viele Vorteile und Möglichkeiten. Da wundert es nicht, dass die Zahl älterer Internetnutzerinnen und -nutzern stetig wächst. Rund die Hälfte aller Menschen über 60 Jahre ist online unterwegs. Wir sagen Ihnen, worauf Sie dabei achten sollten.

Das Internet hilft Menschen, die nicht mehr so mobil sind, weiterhin am gesellschaftlichen Leben teilzuhaben. Ob Kommunizieren oder Informieren, Einkaufen oder unterschiedliche Services nutzen – das Internet bietet viele Vorteile. Doch auch im Internet gibt es Fallen, die Sie durch vorsichtiges Verhalten und technische Sicherheitseinstellungen umgehen können.

Für Menschen ohne eigenen Online-Zugang gibt es die Möglichkeit, in Hotels, Bibliotheken oder in Internetcafés zu surfen. Für einen bestimmten Zeitraum wird hier der Zugang zum Internet verkauft. Wollen Sie Ihre E-Mails oder andere persönliche Daten von hier aus bearbeiten, ist Vorsicht geboten. Sie wissen nicht, ob die Sicherheitseinstellungen eingerichtet und aktuell sind. Vermeiden Sie deshalb, Bankgeschäfte oder Online-Käufe über öffentlich aufgestellte Computer abzuwickeln. Löschen Sie nach jeder Sitzung sämtliche im Webbrowser gespeichert Daten. Der Webbrowser merkt sich alle von Ihnen besuchten Seiten. Diesen „Verlauf“ sollten Sie leeren, sonst kann der oder die nächste Benutzer:in Ihre Nutzung nachvollziehen.

Richtiger Computer

Vor dem Kauf eines eigenen Computers sollten Sie überlegen, wozu Sie den Computer nutzen wollen: Schreiben Sie viel, surfen Sie oft im Internet oder spielen Sie gerne? Für einfache Büro- und Internetanwendungen genügt ein preiswerter Rechner. Für höhere Leistungsfähigkeit müssen Sie allerdings mehr bezahlen. Klären Sie vorab auch, wo Sie das Gerät verwenden werden. Desktop-PCs, Notebooks oder Tablets sind auf die unterschiedlichen Bedürfnisse, von der Schreibtischnutzung bis zum Einsatz unterwegs, zugeschnitten.

Sicherer Computer

Um sich vor unberechtigten Zugriffen anderer Menschen oder Schadsoftware zu schützen, müssen Sie Ihren Computer sichern. Sie sollten in einem ersten Schritt die Zugriffsrechte für andere Nutzer:innen beschränken, indem Sie ein individuelles Nutzerprofil und Passwort für Ihren Computer festlegen.

Eine aktivierte Firewall verhindert, dass Viren oder andere Schadprogramme auf Ihren Rechner gelangen. Ein Antivirenscanner kann den Rechner von Schadprogrammen reinigen, die den Rechner

befallen haben. Es ist notwendig, dass das Betriebssystem, die Firewall und der Antivirenscanner immer auf dem neuesten Stand sind. Aktivieren Sie deshalb die automatischen Updates auf Betriebssystemebene und in den Einstellungen der Firewall sowie des Antivirenscanners. Ein Antivirenscanner muss nicht immer kostenpflichtig sein, oftmals erzielen auch die kostenlosen Programme gute Resultate. Hilfe bei der Auswahl bieten beispielsweise Testergebnisse von Computerfachmagazinen.

Ein weiteres Einfallstor sind Kriminelle, die versuchen, Ihre Zugangsdaten oder Passwörter „mitzuhören". Dies kann über ein ungesichertes oder geknacktes WLAN (Drahtlose Netzwerkverbindung) geschehen. Aus diesem Grund ist es wichtig, dass das WLAN verschlüsselt ist und Unbefugte keinen Zugriff auf das Netzwerk und die sich darin befindenden Rechner haben. Ändern Sie das Standard-Administratorenpasswort Ihres Routers, damit Andere nicht darauf zugreifen können. Verschlüsseln Sie den Zugang zu Ihrem WLAN, indem Sie ein WLAN-Passwort festlegen (z. B. mit der Verschlüsselungsmethode WPA2). Verändern Sie Ihren WLAN-Namen oder verstecken Sie Ihre WLAN-Kennung (SSID) direkt in den Einstellungen des Routers.

Wenn Sie das WLAN nicht nutzen, empfiehlt es sich, dieses abzuschalten. Das ist bei den meisten Routern möglich. Aufgrund der Vielzahl an technischen Geräten, die mittlerweile mit dem Internet (u. a. über WLAN) kommunizieren, ist das in vielen Haushalten allerdings keine praktikable Lösung. Eine bessere Variante wäre es, ein sicheres, nur sehr schwer knackbares Passwort zu verwenden, z. B. eine Kombination aus Zahlen und Ziffern, Groß- und Kleinschreibung und Sonderzeichen. Verwenden Sie einen ganzen Satz als Passwort oder die Anfangsbuchstaben der einzelnen Wörter und wechseln Sie Ihr Passwort regelmäßig. Geben Sie Ihr Passwort nicht weiter. Achten Sie darauf, dass in Ihrem Router die „automatische Aktualisierung" eingestellt ist.

» Link-Tipp:

Unsere Handreichung #1 „Was ist das Internet? Eine Einführung" unterstützt bei den ersten Schritten in die Online-Welt:

https://www.digital-kompass.de/materialien/handreichung-1-was-ist-das-internet-eine-einfuhrung

Soziale Netzwerke

Soziale Netzwerke helfen, alte Freunde wiederzufinden oder Kontakt zu entfernten Freunden zu halten. Sie erwirtschaften aber den Großteil ihres Umsatzes durch zielgerichtete Werbung. Um sicherzustellen, dass die richtige Werbung zu den passenden Nutzer:innen kommt, müssen die Netzwerke viel über diese wissen und speichern deshalb eine Menge Daten.

Dadurch sind Soziale Netzwerke in der Lage, Unternehmen passgenaue Zielgruppen für deren Werbung anzubieten. Es liegt in der Verantwortung der Nutzer:innen, sparsam mit den eigenen, aber auch mit den persönlichen Daten Anderer umzugehen. Fügen Sie nur Personen Ihrer Freundesliste hinzu, die Sie auch persönlich kennen. Beachten Sie auch: Wenn Daten, Videos oder Fotos erst einmal im Internet sind, ist es fast unmöglich, diese wieder zu entfernen.

Mails

E-Mails sind eine einfache und in der Regel kostenlose Möglichkeit der Kontaktaufnahme. Auch hier sollten Sie vorsichtig mit Ihrer Adresse umgehen. Achten Sie darauf, wo Sie diese öffentlich machen. Verschicken Sie keine E-Mails an Hunderte von Empfängern, da die Adressen im CC-Feld von allen Empfängern gelesen und verwendet werden können. Beachten Sie, dass Hinweise wie „Vom ... bis ... sind wir im Urlaub“ in einer Abwesenheitsnotiz Einbrecher auf den Plan rufen können.

Online-Banking

Kontostand abfragen, Überweisungen tätigen oder einen Dauerauftrag einrichten – Bankgeschäfte lassen sich einfach online abwickeln. Dabei loggen Sie sich in das Online-Banking-Portal Ihrer Bank ein, üblicherweise mit einem Nutzernamen und einem dazugehörigen Passwort. Um einen Vorgang zu autorisieren, muss eine einmalig verwendbare Transaktionsnummer (TAN) eingegeben werden. Diese kann mit einem TAN-Generator für jeden Vorgang erzeugt werden oder wird im Mobile-TAN-Verfahren an eine hinterlegte Mobilfunknummer gesendet.

Mobiles Internet

Auch bei der Nutzung von Smartphone oder Tablet sollten Sie einige Sicherheitstipps beachten. Falls das Gerät verloren geht, sind alle auf dem Smartphone hinterlegten Daten (u.a. Passwörter) nutzbar. Sichern Sie deshalb die Geräte durch einen Zugangscode und speichern Sie dort keine Passwörter, PIN-Codes, Kreditkartendaten oder Ähnliches.

Achten Sie in der Öffentlichkeit auf eventuellen Sichtschutz bei der Eingabe kritischer Informationen wie z. B. Passwörtern. Deaktivieren Sie das WLAN und Bluetooth, wenn Sie diese Funktionen nicht brauchen. Sind diese Schnittstellen geöffnet, bieten sie die Möglichkeit eines Angriffs von außen. Nebenbei schonen Sie die Akkulaufzeit, wenn Sie diese Funktionen ausschalten.

Achten Sie darauf, dass die aktuellste Betriebssystemversion auf Ihrem Gerät installiert ist. Bei der Installation von Apps gilt es darauf zu achten, von welcher Quelle die App installiert wird. Verwenden Sie möglichst nur die App-Stores der jeweiligen Hersteller – der Link ist normalerweise auf Ihrem Gerät vorinstalliert („Apple App Store“, „Google Play Store“, „Windows Store“).

Datensicherung

Sichern Sie Ihre Daten regelmäßig, um Datenverlust zu vermeiden. Eine Möglichkeit ist die Cloud. Cloud bedeutet, dass Ihre Daten in einer „Datenwolke“ im Internet gespeichert sind und nicht lokal auf Ihrem PC oder einer Festplatte. Beachten Sie, dass sich die Cloud-Server auch im Ausland befinden können, wo andere Datenschutzgesetze gelten.

Für eine lokale Synchronisierung eignen sich im Falle eines Apple-Betriebssystems iTunes und im Falle eines Android-Betriebssystems der MyPhoneExplorer Client. Auch beim Smartphone gibt es mittlerweile Viren, d. h. es kann notwendig sein, sich eine Sicherheitssoftware zu installieren (z. B. Avast Mobile Security für Android), um sich vor dieser Gefahr zu schützen.

ÖFFENTLICHES WLAN

Wenn Sie sich dort einloggen, achten Sie darauf, dass Sie keine Anwendungen ausführen, die vertrauliche Informationen benötigen oder verwenden. Besonders die Zugangscodes zu Ihrem Online-Banking-Portal sind interessant für Kriminelle. Personen, die sich ebenfalls in diesem

WLAN aufhalten, können die versendeten Informationen mitlesen, wenn sie nicht verschlüsselt sind. Es ist besser, diese Aktivitäten über das normale Mobilfunknetz abzuwickeln.

Wenn Sie das Gerät verlieren, rufen Sie sofort Ihren Mobilfunkanbieter an und lassen Sie die Karte sperren. Viele Hersteller bieten Fernwartungsfunktionen an, die helfen sollen, verschollene Telefone zu finden und Daten zu löschen. Hierzu braucht das Telefon allerdings noch ausreichend Akku und Empfang.

APPS

Wenn Sie eine App installieren, achten Sie darauf, welche Freigaberechte die App von Ihnen einfordert. Manche Apps verlangen Zugriff auf das Adress- und Telefonbuch, auf Ihre Standortdaten, Ihre Identität, Ihre Fotos und Videos. Das ist manchmal gerechtfertigt, beispielsweise kann eine Navigations-App Zugriff auf Ihre Standortdaten benötigen, um Sie in Echtzeit zu Ihrem gewünschten Ziel zu navigieren. Warum eine Taschenlampen-App allerdings Zugriff auf diese Daten benötigt, ist nicht ersichtlich. Seien Sie deshalb vorsichtig, welcher App Sie welche Zugriffsrechte geben.

» TIPPS:

- Seien Sie sparsam mit persönlichen Informationen. Überlegen Sie, welche privaten Daten und Fotos Sie „öffentlich“ machen wollen.
- Erkundigen Sie sich nach den Allgemeinen Geschäftsbedingungen und den Datenschutzbestimmungen, bevor Sie ein Profil anlegen. Nutzen Sie Optionen, mit denen Ihre Informationen und Bilder nur eingeschränkt „sichtbar“ sind.
- Seien Sie wählerisch bei Kontaktanfragen, besonders von Personen, die Sie nicht „real“ kennen.
- Fallen Sie nicht auf gut klingende Profile herein. „Unechte Profile“ werden nachweislich dazu genutzt, anderen Personen zu schaden.
- Melden Sie „Cyberstalker“, die Sie unaufgefordert und dauerhaft über das Soziale Netzwerk kontaktieren, beim Netzwerkbetreiber. Bei schwereren Belästigungen sollten Sie die Polizei einschalten.
- Sind Sie in verschiedenen Sozialen Netzwerken unterwegs, sollten Sie unterschiedliche Passwörter verwenden.
- Prüfen Sie, welche Rechte Sie den Betreibern Sozialer Netzwerke an den von Ihnen eingestellten Bildern und Informationen einräumen.
- Denken Sie daran: Das weltweite Netz vergisst nichts.

Sicher online einkaufen

Ob Reisen, Kleidung, CDs oder Bücher – der Einkauf im Internet bietet viele Vorteile. Bequem von daheim aus rund um die Uhr in einem weltweiten Warenangebot auswählen zu können, ist ein Vorteil. Die Ware nicht vorab prüfen zu können, ist eher ein Nachteil. Wir sagen Ihnen, worauf Sie beim Online-Einkauf achten sollten.

Online sind Produkt- und Preisvergleiche oft nur einen Mausklick entfernt. Allerdings gibt es im Internet nicht immer günstigere Preise, so sind Bücher wegen der Preisbindung online genauso teuer wie im Ladengeschäft. Falls es nach dem Kauf zu einem Problem mit dem Produkt kommt, ist ein Besuch beim Fachhändler oft einfacher als das Einfordern von Garantie- oder Gewährleistungsfällen bei einem weit entfernten Internetanbieter.

GÜTESIEGEL & CO.

Wenn Sie im Netz bei einer Ihnen bisher unbekannten Webseite einkaufen möchten, sollten Sie vor der Kaufabwicklung einige Dinge prüfen. Es ist wichtig, sich hinsichtlich der Seriosität nicht ausschließlich auf ein schönes Webseiten-Design zu verlassen. Suchen Sie online nach Erfahrungsberichten über den Händler: Geben Sie dazu den Namen des Händlers in

Kombination mit dem Suchbegriff „seriös“ oder „unseriös“ in eine Suchmaschine ein. Lesen Sie die Kundenbewertungen. Treten ähnliche Beschwerden gehäuft auf, sollten Sie einen anderen Anbieter wählen.

Verstärkt nutzen Online-Shops unterschiedliche Siegel. Anbieterunabhängige Informationen zu einzelnen Siegeln bietet die Webseite www.label-online.de der VERBRAUCHER INITIATIVE. Beispiele für seriöse Siegel sind „Trusted Shops“, das Siegel „Geprüfter Online-Shop“ oder das Siegel des TÜV Süd. Allerdings können Siegel in einem Internetshop auch gefälscht sein. Machen Sie deshalb den Doppelcheck beim Gütesiegelanbieter und gehen Sie von der Seite eines seriösen Gütesiegelanbieters auf die Seite des entsprechenden Händlers.

Hilfreich für Kunden sind ebenfalls Bewertungsportale. Die meisten haben Vorkehrungen gegen Bewertungsmanipulation getroffen. Ganz ausschließen kann man jedoch nicht, dass positive Bewertungen selbst oder Negatives von Konkurrenten verfasst wurden. Achten Sie daher auf die Zahl der Bewertungen. Auch eine Werbesprache oder auffallend ähnliche Bewertungen könnten Hinweise auf Manipulationen sein. Berücksichtigen Sie den Inhalt der Bewertungen: So ist es bei privaten Urlaubsreisen egal, ob ein Geschäftsreisender kritisiert, dass es um 06:00 Uhr noch kein Frühstück gab.

SERIÖSER INTERNETSHOP

Die Angabe eines Impressums auf einer Webseite ist in Deutschland wie in der EU gesetzlich vorgeschrieben. Dort müssen die genaue Adresse (kein Postfach) und eine verantwortliche Person aufgeführt sein. Prüfen Sie auch, ob der Händler telefonisch gut zu erreichen ist, und berücksichtigen Sie beim Kauf im Ausland, ob Sie in deutscher Sprache betreut werden.

Achten Sie auf die Allgemeinen Geschäftsbedingungen (AGB). Sie sollten leicht zu finden und verständlich formuliert sein. Lesen Sie diese vor dem Kauf, da sie Vertragsbestandteil sind. Zu einem seriösen Händler gehört, dass er Kunden über das Widerrufs- und Rückgaberecht informiert. Üblicherweise geschieht das über die AGB. Händler lassen sich in der Regel von den Kunden mit einem Häkchen zusichern, dass diese gelesen wurden. Informieren Sie sich, ob Sie bei einer Rücksendung die Kosten tragen müssen.

PREISE

Berücksichtigen Sie vor dem Kauf das gesamte Preis-Leistungs-Verhältnis. Wägen Sie ab, ob es nicht vorteilhafter ist, wenn ein örtlicher Händler Ihnen zwar einen teureren Gerätepreis berechnet, dafür aber dieses anschließt und das alte Gerät entsorgt.

Achten Sie auch auf die Versandkosten, so sind Auslandspaketsendungen erheblich teurer als der Versand innerhalb Deutschlands. Bei einigen Anbietern entfallen diese Kosten ab einem gewissen Lieferwert.

Prüfen Sie, ob alle Artikel zu einer Bestellung zusammengefasst und eine Versandkostenpauschale berechnet wird oder ob die Versandkosten für jeden einzelnen Artikel erhoben werden. Nicht nur beim

Versand ist es wichtig, dass alle einzelnen Posten auf der Rechnung aufgeschlüsselt sind. Es muss eindeutig feststellbar sein, wie sich der Kaufpreis zusammensetzt. Das bedeutet auch, dass die Mehrwertsteuer ausgewiesen sein muss.

PRODUKTBESCHREIBUNG

Achten Sie auf die detaillierte Beschreibung des Produkts oder der Dienstleistung. Prüfen Sie, ob die Beschreibung mit dem aktuellen Produkt übereinstimmt oder ob es sich vielleicht um ein Auslaufmodell oder ein älteres Produkt handelt. Achten Sie darauf, dass die Artikelbezeichnung mit dem abgebildeten Bild übereinstimmt. Klären Sie vor dem Kauf eventuelle Unstimmigkeiten. Lassen Sie sich nicht durch äußerst günstige Preise blenden, auch im Internet gibt es nichts zu verschenken.

BESTELLUNG

Der vorgeschriebene Bestellbutton weist darauf hin, dass nun ein kostenpflichtiger Kaufvertrag abgeschlossen wird. Der Button muss farbig herausgehoben vom Rest der Webseite eindeutig erkennbar sein und ist meist mit „Kostenpflichtig bestellen“, „Zahlungspflichtig bestellen“ oder „Jetzt kaufen“ beschriftet.

BEZAHLUNG

Achten Sie darauf, dass mehrere Bezahlmöglichkeiten angeboten werden. Bezahlen Sie nur per Vorkasse, wenn Sie sich sicher sind, dass der Händler vertrauenswürdig ist. Wählen Sie am besten eine andere Zahlungsart, sollten Sie sich unsicher sein. Die Zahlung per Rechnung ist dabei die bequemste und sicherste aller Zahlungsarten. Die Zahlung per Nachnahme kostet Sie als Kunde Nachnahmegebühren und bei Erhalt des Pakets oder Päckchens kann auch nicht geprüft werden, was sich darin befindet.

Wenn Sie direkt per Sofort-Überweisung, Überweisung, Paydirekt, Paypal, Kreditkarte oder mittels anderweitiger Methoden bezahlen, sollten Sie darauf achten, dass die Verbindung verschlüsselt erfolgt. Dies erkennen Sie daran, dass am Anfang des Adressfelds im Browser „https“ statt nur „http“ steht. Das zusätzliche „s“ weist darauf hin, dass die Verbindung „secure“/ gesichert ist. Falls Sie mit einer Kreditkarte oder per Lastschriftverfahren bezahlen, gibt es die Möglichkeit zur Rückbuchung ungerechtfertigt abgebuchter Beträge. Informieren Sie sich bei Ihrer Bank über die genauen Modalitäten und Fristen.

DATENSICHERHEIT

Speichern Sie niemals Ihre Zugangsdaten zum Bezahlsystem auf dem Rechner. Gehen Sie sparsam mit Ihren persönlichen Daten um.

Cookies sind kleine Dateien, die eine Internetseite auf Ihrem Rechner speichert, um Sie beim nächsten Besuch wiederzuerkennen. Deaktivieren Sie Cookies in Ihrem Browser für Seiten, bei denen Ihnen die Cookies keinen Nutzen bringen.

RÜCKGABERECHT

Es besteht üblicherweise ein 14-tägiges Rückgaberecht für Waren, die im Internet bestellt wurden. Diese Regelung gilt nur bei Verträgen zwischen Händler und Privatkunden, nicht für gewerbliche Geschäftsbeziehungen. Diese Regel dient als Ausgleich dafür, dass im Internet bestellte Ware nicht im Vorfeld vor Ort begutachtet werden kann. Falls der Händler vergisst, Sie beim Kauf der Ware über dieses Widerrufs- bzw. Rückgaberecht aufzuklären, verlängert sich die 14-tägige Frist um ein Jahr, d. h. die Widerrufs- bzw. Rückgabefrist beträgt dann 1 Jahr und 14 Tage.

Diese Regeln gelten nicht für Flugtickets, personalisierte Sonderanfertigungen, Hygieneartikel, verderbliche Waren, stark preisschwankende Artikel sowie geöffnete Software- oder Musikdatenträger. Eine detaillierte Auflistung aller Dienstleistungen und Produkte, für die das Widerrufsrecht nicht besteht, finden Sie im § 312g des Bürgerlichen Gesetzbuches.

Im Falle einer Rücksendung ist der Händler berechtigt, die Versandkosten den Kunden tragen und sich einen gewissen Wert erstatten zu lassen, wenn das Produkt intensiver getestet wurde als es im Laden möglich wäre.

MAHNUNGEN

Prüfen Sie, ob die Mahnung berechtigt ist und Sie die Leistung überhaupt erhalten haben. Reagieren Sie nicht auf unberechtigte Mahnungen und unterschreiben Sie kein Angebot, Ihre Schuld zu begleichen, denn so akzeptieren Sie die Forderung.

Bewahren Sie die Schreiben von Händlern oder Inkassobüros auf. Teilen Sie in einem Widerspruch ausdrücklich mit, dass Sie die Forderung als unberechtigt ansehen. So müssen Sie sich vor einem Beweis des Gegenteils keine Sorge um einen Schufa-Eintrag machen.

» Link-Tipp:

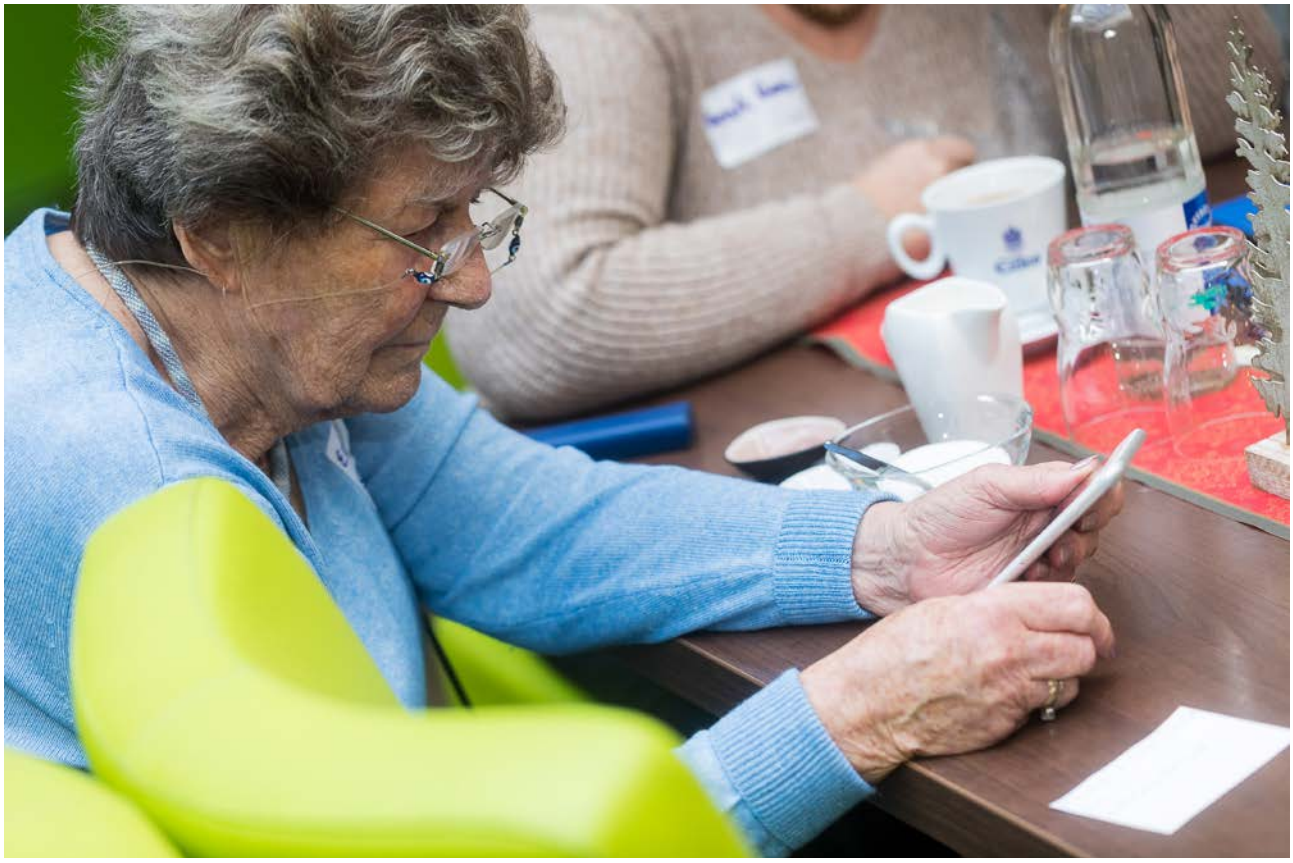
Unsere Handreichung #5 „Online-Einkaufen und Online-Banking – Sicher im Internet bestellen und bezahlen“ gibt weiteführende Informationen zu Online-Shopping & Co.:

https://www.digital-kompass.de/materialien/handreichung-5-online-einkaufen-und-online-banking-sicher-im-internet-bestellen-und

» Medikamente per Mausklick

Immer mehr Verbraucherinnen und Verbraucher kaufen Medikamente online ein. Wir geben Hinweise, worauf Sie hierbei achten sollten.

- Arzneimittel dürfen nur mit Vorlage eines Originalrezeptes versandt werden; eine Kopie per Mail oder Fax reicht nicht aus. Preisnachlässe auf diese Medikamente sind nicht gestattet.
- Auf der Internetseite der Versandapotheke muss ein Impressum angegeben sein, in dem die Adresse der Apotheke und des Betreibers aufgeführt sind sowie die jeweilige Aufsichtsbehörde und die zuständige Apothekerkammer genannt werden.
- Persönliche Daten sollten nur weitergegeben werden, wenn der Anbieter ein Verschlüsselungssystem anwendet.
- Es muss eine Beratungsmöglichkeit vorhanden sein. Seriöse Internetapotheken informieren per Telefon und E-Mail oder veröffentlichen den Beipackzettel zum jeweiligen Angebot. So können sich Verbraucherinnen und Verbraucher vor dem Kauf über eventuelle Risiken und Nebenwirkungen der Medikamente informieren.
- Vor der Bestellung sollten die „Allgemeinen Geschäftsbedingungen“ gelesen werden. Dort sind Einzelheiten zu Lieferbedingungen, Mindestbestellmengen und zur Abrechnung festgehalten.
- Beim Kauf sollte auf mögliche Nebenkosten, z. B. für den Versand oder die Zahlung per Nachnahme, geachtet werden.
- Bei nicht verschreibungspflichtigen Medikamenten kann sich ein Preisvergleich unter Berücksichtigung aller Kosten lohnen.
- Bei Zweifeln helfen die zuständigen Apothekenkammern, Krankenkassen oder die Beratungsstellen der Verbraucherzentralen. Die Stiftung Warentest (www.test.de/medikamente) bietet eine Arzneimitteldatenbank mit Bewertungen über die meistverkauften rezeptfreien Medikamente. Das Deutsche Institut für Medizinische Dokumentation und Information (https://versandhandel.dimdi.de/pdfs/vhr-apo.pdf) bietet ein Register mit der Auflistung aller Apotheken, die behördlich zum Versandhandel zugelassen sind.



Fallen im weltweiten Netz

Gelegenheit macht Diebe – dieser Spruch gilt auch für das Internet. Betrüger sind auch im weltweiten Netz unterwegs und haben es auf fremde Daten und Finanzen abgesehen. Wir zeigen, wie Sie sich schützen können.

Viele Angebote im Internet kosten Geld. Die legalen Angebote sind deshalb oft entweder kostenpflichtig oder werden durch Werbung finanziert. Jedoch mischen sich unter diese Angebote auch dubiose Internetseiten, die es auf arglose Kunden abgesehen haben. Zu den fragwürdigen Angeboten zählen Gewinnspiele, fingierte IQ-Tests, Partnervermittlungsbörsen, Astrologieseiten, Lebenserwartungsrechner oder Anbieter, die Familienstammbaumanalysen versprechen.

PSYCHOTRICKS

Eine beliebte Methode ist es, in die psychologische Trickkiste zu greifen und beispielsweise das Ergebnis eines bereits abgeschlossenen IQ-Tests nur anzuzeigen, wenn ein Premiumkonto eingerichtet wird. Bei Angeboten, die mit „Gratisangebot“, „Clubmitgliedschaft“ oder „Gewinnspiel“ werben, lohnt sich ein Blick in das Impressum und die Allgemeinen Geschäftsbedingungen.

Bei Partnerportalen kommt es vor, dass Betrüger über Chat, E-Mail oder sogar WhatsApp eine Vertrauensbeziehung zum Opfer aufbauen und so die Hoffnung auf einvernehmliche Liebe ausnutzen, um an Geld zu gelangen. Nach erfolgreichem Vertrauensaufbau wird plötzlich Geld für eine Operation oder eine unbezahlte Inkassoforderung gefordert. So etwas kann passieren, muss es aber nicht. Versuchen Sie bei Online-Bekanntschaften generell Vorsicht walten zu lassen und nicht zu schnell in eine emotionale Abhängigkeit zu geraten. Für diesen Internetbetrug gibt es einen eigenen Begriff: Romance-Scamming.

SPAM-MAILS

Bei manchen Internetangeboten ist es nötig, seine Kontaktdaten einzugeben. Deshalb sollten Sie vorher nachdenken, ob eine Registrierung bei allen Portalen mit vollem Namen und kompletter Anschrift nötig ist.

Bei Sozialen Netzwerken, über die man Freunde finden oder wiederfinden möchte, mag das noch sinnvoll sein, beim Online-Einkauf sowieso, weil Sie die Lieferung andernfalls nicht erreichen wird. Wenn Sie jedoch beispielsweise bei einem IQ-Test nach Ihrem Namen und Ihrer Adresse gefragt werden, sollten Sie vorsichtig sein.

Mit einer zweiten bzw. dritten E-Mail-adresse, die man für die Anmeldung bei Internetseiten verwendet, können Sie auch ein weiteres Problem im Internet reduzieren: unerwünschte Spam-Mails. Nichts verstopft den E-Mail-Posteingang so sehr wie Spam-Mails, also unverlangt zugesandte Werbung.

Abzocker arbeiten mit unlauteren Methoden. Die Palette reicht von unberechtigten und scharf formulierten Schreiben bis zu unverhohlenen Drohungen, die per Post oder auch per E-Mail an Sie gerichtet werden. Lassen Sie sich hiervon nicht einschüchtern, sondern überlegen Sie, wie Sie besonnen, aber trotzdem bestimmt reagieren können.

Überlegen Sie: Wie ist der Anbieter überhaupt an Ihre Daten gekommen? Haben Sie möglicherweise bei einem Gewinnspiel mitgemacht und die Weitergabe der Daten erlaubt? Falls Sie ausschließen können, dass Sie Ihre Daten freiwillig übergeben haben, bzw. Ihre Daten fehlerhaft sind, brauchen Sie überhaupt nicht reagieren. Reichen Sie den Betrügern bei fehlerhaften Daten keinesfalls Ihre korrekten Daten nach.

Wenn Sie Ihre Daten selbst hinterlassen haben, aber nicht ausreichend auf ein kostenpflichtiges Angebot hingewiesen wurden, reagieren Sie mit einem Widerspruch. Musterbriefe finden Sie unter https://www.verbraucherzentrale.de/musterbriefe/digitale-welt.

DATENSICHERHEIT

Online oder auf dem Computer hinterlegte Informationen sind bequem, da sie nicht immer wieder eingegeben werden müssen. Dieser Komfortgewinn geht jedoch einher mit gewissen Sicherheitsproblematiken, da alle hinterlegten Informationen auch von Dritten ausgelesen und weiterverwertet werden können. Als

Leitsatz gilt demnach in der Regel: „Mehr Komfort ist weniger Sicherheit und weniger Komfort ist mehr Sicherheit“.

Ein kompletter Schutz vor Spam-Mails und Risiken im Internet ist nur schwer möglich, obwohl die Filtertechnologie erhebliche Fortschritte gemacht hat. Verwenden Sie eine E-Mail-Adresse für Ihre private Kommunikation und eine gesonderte für die Anmeldung bei Online-Portalen.

PHISHING

„Phishing” ist ein Kunstwort aus „Passwort” und „Fishing” (abfischen) und sind ungleich gefährlicher. Gefälschte E-Mails oder Internetseiten dienen als Köder und sollen von den Empfängern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen „abfischen“.

Hierzu verwenden die Betrüger als Absender oftmals E-Mailadressen von Firmen, bei denen viele Verbraucherinnen und Verbraucher Kunden sind oder ein Konto haben. Ob Visa- oder Mastercard, Banken oder Sparkassen, DHL oder Telekommunikationsanbieter – betroffen sind viele großen Firmen. Schnell öffnet man die E-Mail und klickt auf den dort enthaltenen Link. Meistens sind diese Seiten kaum von den Originalseiten der jeweiligen Firmen zu unterscheiden. Viele Verbraucherinnen und Verbraucher folgen gewohnheitsgemäß den Anweisungen, die eigenen Benutzerdaten und auch eine Transaktionsnummer einzugeben.

Sind die Betrüger im Besitz dieser Informationen, ist es ihnen ein Leichtes, Bankgeschäfte in Ihrem Namen zu tätigen.

Größere Unternehmen werden Ihnen niemals E-Mails senden, in denen Sie dazu aufgefordert werden, Benutzerdaten und Kontoinformationen preiszugeben oder auf einem Portal einzugeben. Falls Sie Zweifel haben, rufen Sie bei Ihrer Bank an und fragen nach, ob Ihnen eine E-Mail gesendet wurde.

Sie können Ihrer Bank auch mitteilen, dass Sie keine weiteren E-Mails erhalten möchten. Falls Sie danach weiterhin E-Mails von Ihrer vermeintlichen Bank erhalten, können Sie sicher sein, dass es sich um Betrugsversuche handelt. Geben Sie auf Internetseiten, bei denen Sie nicht sicher sind, dass es sich um eine vertrauenswürdige Seite handelt, niemals Ihre Kontonummer, PIN und TAN etc. ein. Besondere Vorsicht ist geboten, wenn Sie nach mehreren TANs gefragt werden. Löschen Sie fragwürdige E-Mails ungelesen.

URHEBERRECHTE

Das Internet ist voll von Bildern, Videos und Musikschnipseln – auch hier sind sowohl die unbegrenzten Möglichkeiten als auch die Gefahren oft nur einen Mausklick entfernt. Zwar ist die Privatkopie in Deutschland nicht unter Strafe gestellt, die unerlaubte Vervielfältigung und Nutzung der Werke Anderer allerdings schon. Falls Sie also ungefragt ein Bild im Internet herunterladen, um dieses auf die eigene Homepage zu stellen, verstoßen Sie gegen geltendes Urheberrecht. Laden Sie deshalb keine fremden Inhalte auf Ihren Computer und achten Sie darauf, dass Sie, falls Sie Fotos oder Musik anderer verwenden, vorher die Rechtsfrage abgeklärt haben.

» TIPPS:

- Lesen Sie die Allgemeinen Geschäftsbedingungen (AGB).
- Machen Sie bei Unsicherheit einen Screenshot von der Internetseite.
- Gehen Sie mit Ihren persönlichen Daten sparsam um.
- Recherchieren Sie online, ob die Webseite seriös ist.
- Prüfen Sie im Impressum, wer für das Angebot verantwortlich ist und wie Kontakt zum Anbieter hergestellt werden kann.
- Lassen Sie sich nicht von der Teilnahme an einem Gewinnspiel blenden.
- Fallen Sie nicht auf Lockvogelangebote herein, die Ihnen die gewollten Informationen erst nach Abschluss eines kostenpflichtigen Vertrags anzeigen.
- Achten Sie darauf, ob Sie über das Widerrufsrecht informiert wurden.
- Verwenden Sie für Ihr Passwort eine Kombination aus Ziffern, Zahlen, Groß- und Kleinschreibung und Sonderzeichen.

» Link-Tipp:

Unsere Handreichung #2 „Surfen im Internet – Zuhause und mobil“ liefert hilfreiche Hinweise zur sicheren Nutzung des Internets:

https://www.digital-kompass.de/materialien/handreichung-2-surfen-im-internet-zuhause-und-mobil

Online persönlich vernetzt

Soziale Netzwerke gehören heute zu den wichtigsten Anwendungen im Internet. Egal wo man sich befindet – man kann jederzeit mit Familie, Freunden oder Bekannten verbunden sein. Wir geben Tipps zum richtigen Umgang.

Steigende Beliebtheit erlebten Soziale Netzwerke um die Jahrtausendwende, da seitdem auch die private Kommunikation zunehmend online erfolgte. In Deutschland sind rund zwei Drittel der Internetnutzerinnen und -nutzer aktive Mitglieder in Sozialen Netzwerken. Bekannte Soziale Netzwerke im privaten Bereich sind beispielsweise Facebook, der Kurznachrichtendienst Twitter, Google+ oder StayFriends, mit dem Sie Schulfreunde finden können. Für einzelne Zielgruppen oder Medienformen gibt es eigene Angebote. Dazu gehören die Videoplattform Youtube oder die Fotodienste Instagram, Pinterest oder Flickr. Zunehmend mehr ältere Nutzerinnen und Nutzer posten, liken, chatten und vernetzen sich mittlerweile im Netz.

Persönliche Angaben

Zur Nutzung der Sozialen Netzwerke ist eine Anmeldung erforderlich. Dies ist oft möglich, ohne den vollen Namen, die echte Adresse oder die richtige Telefonnummer anzugeben. Hier sollten Sie zumindest sparsam mit Ihren Daten umgehen, vielleicht auch einen Spitznamen verwenden. Werden weitere Daten wie Geburtsdatum oder Mailadresse erfragt, sollte diese für Dritte nicht einsehbar sein. Denken Sie daran, das Internet vergisst nie. Das gilt auch für Ihre Telefonnummer, Ihre Mailadresse oder Ihre Fotos.

Wer sich bei Sozialen Netzwerken anmeldet, muss den Allgemeinen Geschäftsbedingungen (AGB) des Anbieters zustimmen und deren Datenschutzerklärungen zur Kenntnis nehmen. Wer nicht zustimmt, kann den Dienst nicht nutzen. Durch Akzeptanz der Allgemeinen Geschäftsbedingungen kommt rechtlich ein Vertrag zustande. Es empfiehlt sich daher diese zu lesen. In der Praxis ist diese Empfehlung jedoch häufig schwer umsetzbar, da die AGB vieler Anbieter sich über viele Seiten erstrecken und nicht immer leicht verständlich sind.

Viele Freunde

In den Sozialen Netzwerken suchen Nutzerinnen und Nutzer häufig andere Menschen mit ähnlichen Interessen. Dazu ist eine gewisse Selbstdarstellung notwendig. Durch die Pflege eines Profils können die unterschiedlichsten persönlichen Angaben wie Beziehungsstatus, Hobbies oder Interessen angegeben werden. Fotos oder Videos können diese persönlichen Informationen ergänzen. Ein Adressbuch ermöglicht den weltweiten Kontakt zu Familie, Freunden oder Bekannten. Innerhalb des Netzwerkes können Untergruppen gleichen Interesses angelegt werden. Soziale Medien erleichtern es, in Kontakt zu bleiben, können aber einen persönlichen Kontakt nicht ersetzen. Berücksichtigen

Sie auch, dass nicht jede Online-Bekanntschaft Ihnen zwangsläufig wohlgesonnen ist. Geben Sie deshalb nicht zu viel Persönliches preis.

Vielfältige Möglichkeiten

Followen, liken, posten … dies sind Begriffe aus der Welt der Neuen Medien. In den Sozialen Netzwerken stehen das Teilen von Informationen, Erfahrungen und Meinungen sowie die Vernetzung im Mittelpunkt. Andere können am eigenen Leben und man selbst am Leben Anderer teilnehmen. So lässt sich in Erfahrung bringen, was jemand denkt oder tut. Dies kann mithilfe eines Texts, eines Fotos oder auch eines Videos passieren. Geteilte Inhalte können kommentieren, favorisiert und weitergeleitet werden.

Wenn Sie etwas gut finden – man liked etwas – genügt ein Klick. Die bekannteste Funktion von Facebook ist das Markieren eines Beitrages mit dem „Gefällt mir"-Button. Seit einiger Zeit ist es möglich, mit sogenannten Emojis, d. h. unterschiedlichen Symbole wie dem Smiley, die aktuelle Stimmung anzugeben.

Der Gebrauch der meisten Sozialen Netzwerke ist meist kostenlos. Dennoch zahlen die Nutzerinnen und Nutzer mit ihren privaten Daten. Ob Alter oder politische Präferenz, Wohnort oder Beziehungsstatus, Lieblingsportklub oder bevorzugtes Reiseziel – alles was hochgeladen, angeschaut oder geschrieben wird, wird registriert. Diese Informationen werten die Betreiber aus und schalten auf der Basis dieser Auswertung möglichst passende Werbung. Vorgeschlagen werden dabei die Inhalte

und die Werbung, die den Nutzerinnen und Nutzer gefallen könnten. Haben Sie sich beispielweise online für einen Urlaub im südlichen Afrika interessiert, werden Sie mit einer gewissen Wahrscheinlichkeit entsprechende Werbehinweise im Netz erhalten.

Bitte mit Stil

In Sozialen Netzwerken können Nutzer:innen mit Anderen diskutieren, Fragen stellen oder von eigenen Erfahrungen berichten. Das Internet funktioniert weltweit, einfach, spontan und formlos, ist aber kein rechts- oder benimmfreier Raum. Schnell ist eine unbedachte Äußerung oder ein Foto eingestellt und noch Jahre später im weltweiten Netz aufzufinden. Berücksichtigen Sie deshalb, online ist nichts wirklich privat. Geben Sie deshalb keine vertraulichen Informationen weiter und trennen Sie berufliche, ehrenamtliche und private Aktivitäten. Formulieren Sie immer wertschätzend.

Persönlichkeits- und Urheberrecht

Ob Texte oder Musik, Fotos oder Videos – in den Sozialen Netzwerken wird alles veröffentlicht. Bei eigenen Inhalten und Fotos gibt es meist kein Problem. Aber schon bei Ihrem Profilbild aus dem Fotostudio sollten Sie vorab die Rechte klären. Sind auf Ihrem Foto weitere Personen zu sehen, sollten Sie diese vor der Veröffentlichung um Erlaubnis bitten (Stichwort: Recht am eigenen Bild).

Auch bei Texten anderer Personen sollten Sie vorsichtig sein. Bei der Veröffentlichung sind die Urheberrechte, beispielsweise eines Autors oder einer Autorin, zu beachten. Dabei geht es nicht nur um den entsprechenden Quellennachweis, sondern auch um eventuelle Honorare für Text oder Foto. Rechtlich verantwortlich dafür ist, wer diese veröffentlicht, da die Anbieter nur die technische Plattform zur Verfügung stellen. Das Internet ermöglicht übrigens die schnelle Feststellung, ob und wo Entsprechendes veröffentlicht wurde.

» Link-Tipp:

Unsere Anleitung 2.1 „Soziale Netzwerke – Ein eigenes Profil einrichten am Beispiel Facebook“ gibt Ihnen wertvolle Informationen rund um die Kommunikation im Netz an die Hand:

https://www.digital-kompass.de/materialien/anleitung-21-soziale-netzwerke-ein-eigenes-profil-einrichten-am-beispiel-facebook

» TIPPS:

- Geben Sie nur persönliche Daten in Ihrem Profil an, die nötig sind und von denen Sie wollen, dass diese öffentlich sind. Die Veröffentlichung privater Informationen kann zu persönlichen Nachteilen führen.
- Achten Sie darauf, dass Ihre persönlichen Daten nicht für Dritte einsehbar sind. Eventuell sollten Sie zur Anmeldung eine zweite Mailadresse verwenden.
- Achten Sie auch in den Sozialen Netzwerken auf die Allgemeinen Geschäftsbedingungen (AGB) und den Regelungen des Datenschutzes.
- Prüfen Sie, welche Zugriffsrechte Sie den Betreibern Sozialer Netzwerke einräumen möchten.
- Überlegen Sie sich, wen Sie in Ihre Kontaktliste aufnehmen. Eine Nichtberücksichtigung ist legitim und nicht unhöflich.
- Überprüfen Sie regelmäßig Ihre Kontaktliste, entfernen Sie Personen mit denen Sie länger keinen Kontakt haben.
- Machen Sie sich Gedanken, wer welche Inhalte sehen darf. Gehen Sie eher restriktiv mit Ihren entsprechenden Einstellungen um.
- Freunden Sie sich online mit niemandem an, den Sie nicht bereits kennen.
- Wehren Sie sich gegenüber Nutzerinnen und Nutzern, die Sie unaufgefordert und dauerhaft kontakten wollen und melden diese dem Sozialen Netzwerk. Belästigen Sie natürlich auch Andere nicht.
- Veröffentlichen Sie nichts ohne vorher Persönlichkeits- und Urheberrechte zu berücksichtigen. Lässt sich dies nicht klären, verzichten Sie auf die Veröffentlichung.
- Sind Sie in mehreren Sozialen Netzwerken unterwegs, verwenden Sie dafür unterschiedliche Passwörter.
- Klicken Sie nicht vorschnell auf Links! Auch Soziale Netzwerke werden von Betrügern dazu genutzt, um Daten zu erlangen.
- Das Internet vergisst nichts: Ihre Informationen, Kommentare und Verlinkungen in Sozialen Netzwerken sind – auch nachdem Sie Ihren Account gelöscht haben – weiter im Netz. Veröffentlichen Sie also nichts, dass Sie später bereuen: Ihre Beziehungsprobleme, Ihre gesundheitlichen Probleme oder das Lästern über Andere haben dort nichts zu suchen.

Projektbeschreibung

Eine Publikation von Deutschland sicher im Netz im Rahmen des Verbundprojektes Digital-Kompass mit der BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen und ermöglicht durch Förderung durch das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz. Der Digital-Kompass ist ein Treffpunkt für alle Fragen rund ums Internet und Co., die ältere Menschen bewegen.

Auf www.digital-kompass.de gibt es vielfältige praxisnahe Materialien, Broschüren, Filme und Arbeitsblätter. Darüber hinaus finden Sie praktische Tipps für Treff en, Beratungen und Kurse rund um die digitale Welt.

Die Digitalen Stammtische ermöglichen einen Austausch zu aktuellen IT-Themen mit Expert:innen und Gleichgesinnten deutschlandweit. Bundesweit existieren 100 Digital-Kompass-Standorte. Dort schaffen Internetlotsinnen und -lotsen eine vertrauensvolle (Lern)Umgebung für ältere Menschen und unterstützen sie dabei, digitale Dienste auszuprobieren und einen souveränen Umgang mit dem Internet zu erlernen. Die Digital-Kompass-Standorte sind zugleich Anlaufstellen für Internetlotsinnen und -lotsen, die sich weiterbilden oder in das Projekt einbringen möchten.

Sie möchten mehr rund um den Digital-Kompass erfahren? Dann abonnieren Sie unseren Newsletter:

www.digital-kompass.de/newsletter-abonnieren

Digital Kompass

info@digital-kompass.de
www.digital-kompass.de

DsiN Deutschland sicher im Netz

bagso