SICHER IM INTERNET?

ALLTAGSTIPPS FÜR HANDY UND PC

Backups
Spam-Mails
Datenschutz
Virenabwehr
Online-Shopping
Betrugsversuche
WhatsApp und Co

VKI

Backups

Spam-Mails

Datenschutz

Virenabwehr

Online-Shopping

Betrugs-versuche

WhatsApp und Co

Verein für Konsumenteninformation (Hrsg.)
Natalie Oberhollenzer und Gernot Schönfeldinger

SICHER IM INTERNET?

Alltagstipps für Handy und PC

Impressum

Herausgeber
Verein für Konsumenteninformation (VKI)
Mariahilfer Straße 81, 1060 Wien
ZVR-Zahl 389759993
Tel. 01 588 77-0, Fax 01 588 77-73, E-Mail: konsument@vki.at
www.vki.at I www.konsument.at

Geschäftsführung
Mag.(FH) Wolfgang Hermann

Autor:innen
Mag.ª Natalie Oberhollenzer
Mag. Gernot Schönfeldinger

Grafik/Produktion
Günter Hoy

Foto Umschlag
Thitichaya Yajampa/Shutterstock.com

Druck
Gerin Druck GmbH,
2120 Wolkersdorf

Bestellungen
KONSUMENT Kundenservice
Mariahilfer Straße 81, 1060 Wien
Tel. 01 588 774, Fax 01 588 77-72
E-Mail: kundenservice@konsument.at

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Verein für Konsumenteninformation
ISBN 978-3-99013-121-3

€ 25,–

Zu diesem Buch

Für viele ist es kaum mehr vorstellbar, ohne sie auszukommen: Tablets, Laptops, und vor allem Smartphones sind zu einem oft unverzichtbaren Bestandteil unseres täglichen Lebens geworden. Die Technologien haben uns unzählige Möglichkeiten eröffnet. Wir können nahtlos über Ozeane hinweg kommunizieren und mit einem Klick auf nahezu unbegrenztes Wissen zugreifen. Die Anwendungen unterstützen uns bei Entscheidungen jeglicher Art, sie informieren und navigieren uns, und sie dienen der Unterhaltung. Mit jedem Geräte-Upgrade werden noch mehr Funktionen integriert, die früher separate Geräte erforderten.

Wir können das Licht in der Wohnung per Sprachbefehl einschalten, erfassen unsere Gesundheitsdaten via App, und Algorithmen bestimmen über unsere Kreditwürdigkeit. Die Systeme besitzen mittlerweile sogar die Fähigkeit, selbstständig zu denken und zu lernen – Stichwort KI, also Künstliche Intelligenz.

So komfortabel die Digitalisierung sein mag, manchmal kann sie auch nerven, überfordern und Angst machen, denn sie bringt neue Gefahren mit sich – von Betrugsversuchen über Datenlecks bis hin zu Fake News, sprich manipulierten Nachrichten.

Das vorliegende Buch wurde mit der Absicht verfasst, einen Leitfaden im digitalen Dschungel zu bieten. Einen Ratgeber, bestehend aus einer Sammlung von klaren, einfach zu befolgenden Tipps. Es soll Ihnen dabei behilflich sein, sich vor den häufigsten Gefahren im Netz zu schützen. Es gibt Anleitungen, wie Sie Ihre Daten und Ihre Privatsphäre zu einem höchstmöglichen Maß bewahren können, immer mit Rücksicht auf die praktische Umsetzbarkeit für technische Laien.

Ob Sie nun mit Ihrem Computer mit Windows-Betriebssystem im Internet surfen, mit Ihrem Android-Smartphone Bankgeschäfte erledigen, Fotos in die Cloud speichern, sich mit Ihren Freunden über einen Messenger austauschen oder Filme streamen – das Buch beantwortet Fragen zur Handhabung von verschiedenen Anwendungen, zeigt Einstellungsmöglichkeiten und - empfehlungen auf, löst Probleme oder verhindert, dass sie überhaupt auftreten. So können Sie mit der laufenden Weiterentwicklung der digitalen Landschaft Schritt halten.

Wir wünschen viel Vergnügen beim Schmökern und Erfolg beim Umsetzen des einen oder anderen Tipps in die Praxis!

Ihr KONSUMENT-Team

LIEBE LESER:INNEN!

Inhalt

Computer

Sicherung (Back-up) einrichten

Zum umsichtigen Umgang mit dem Computer gehört auch die Sicherung, also die regelmäßige Durchführung eines Back-ups. Nur so können Sie im Fall des Falles (Geräte- oder Festplattendefekt, Schadsoftwarebefall) Ihre Daten wiederherstellen.

Cloud oder Festplatte(n)

Unter „Start > Einstellungen > Update und Sicherheit > Sicherung" gelangen Sie zur Aktivierung des **automatischen Back-ups** auf Microsofts Cloudspeicher OneDrive. Trauen Sie der „Wolke" im Internet nicht, dann sollten Sie das Back-up auf einem externen Datenträger durchführen. Dabei stellen tragbare Festplatten im Hinblick auf das Preis-Leistungs-Verhältnis, die Lebensdauer und (im Vergleich zur Cloud) auch den Datenschutz die beste Lösung dar. Möchten Sie auf Nummer sicher gehen, sollten Sie sich zwei Stück davon zulegen. Warum, das erklären wir weiter unten. Achten Sie darauf, dass das verfügbare Speichervolumen keinesfalls geringer ist als jenes Ihrer Computerfestplatte.

Besser automatisch

Die simpelste Back-up-Methode ist das **händische Kopieren** aller wichtigen Daten (Dokumente, Fotos, Videos, Musikdateien etc.) vom Computer auf die externe Festplatte. Sinnvoller ist die Nutzung der mit Windows mitgelieferten (automatisierten) Möglichkeiten. Geben Sie ins Suchfeld der Taskleiste am unteren Bildschirmrand den Begriff „Systemsteuerung" ein. Dann scheint dieser in der Trefferliste auf. Klicken Sie ihn an sowie in der folgenden Auflistung (Anzeigeoption „Große Symbole") auf den Punkt „Sichern und Wiederherstellen (Windows 7)". Der Hinweis auf Windows 7 findet sich gleichlautend in allen aktuellen Windows-Betriebssystemen und bestätigt die Kompatibilität mit den Vorgängerversionen bis hinunter zu Windows 7.

Sicherung einrichten

Schließen Sie die externe Festplatte an, vergewissern Sie sich, dass sie vom Computer erkannt wurde, und klicken Sie auf „Sicherung ein-

richten". Bestätigen Sie die Sicherheitsabfrage mit „Ja" und wählen Sie nun die externe Festplatte als Sicherungsziel aus. Nach Klick auf „Weiter" stehen Sie vor der Frage, welche Daten Sie sichern möchten. Beschränken Sie sich auf eine einzelne externe Festplatte, dann ist die „Auswahl durch Windows" die bessere Option. Hier werden regelmäßig alle relevanten Daten gesichert und zusätzlich wird ein „Image", ein **Systemabbild** angelegt, sprich: eine 1:1-Kopie der gesamten Computerfestplatte. Klicken Sie auf „Zeitplan ändern" und wählen Sie die tägliche Sicherung sowie eine Uhrzeit, zu der Sie Ihren Computer am häufigsten einschalten. Bestätigen Sie mit „OK" und danach mit „Einstellungen speichern und Sicherung ausführen".

Restrisiko minimieren

Was bleibt, ist ein gewisses Restrisiko. Manche Schadprogramme, wie etwa Ransomware (siehe ► Seite 118), können auch angeschlossene externe Datenträger befallen und deren Inhalt verschlüsseln. Im schlimmsten Fall kann es also passieren, dass gemeinsam mit den Daten auf Ihrer Computerfestplatte auch das Back-up verloren ist. Die sicherere Methode ist daher, **zwei externe Festplatten** zu verwenden. Eine davon lassen Sie ständig am Computer angeschlossen, wählen unter „Sicherung einrichten" die Option „Auswahl durch Benutzer" und sichern die vorgeschlagenen Elemente unter der Bezeichnung „Datendateien". Unterhalb des Fensters entfernen Sie das Häkchen vor „Systemabbild von Laufwerken einschließen". Nun klicken Sie auf „Weiter" und danach auf „Zeitplan ändern". Wählen Sie die tägliche Sicherung und eine Uhrzeit, zu der Sie Ihren Computer am häufigsten einschalten. Bestätigen Sie mit „OK" und danach mit „Einstellungen speichern und Sicherung ausführen".

Systemabbild

Zusätzlich schließen Sie regelmäßig (z. B. einmal im Monat) die zweite externe Festplatte an und führen unter „Systemabbild erstellen" eine manuelle Sicherung durch. Ist diese abgeschlossen, entfernen Sie die externe Festplatte wieder von Ihrem Computer.

Smartphones

Datensicherung mit Tücken

Bei Android-Smartphones ist die Datensicherung nicht so einfach. Versierte Nutzer:innen greifen zum „Root". Das ist ein gezielter Eingriff ins System, der Funktionen freischaltet, die der Hersteller für die technische Weiterentwicklung vorgesehen hat. Ein vollständiges Back-up des Smartphones wird erst dadurch möglich, entsprechende Apps findet man im Play Store. Da ein Root den Verlust der Herstellergarantie bedeutet und zu technischen Problemen führen kann, empfehlen wir diese Vorgangsweise aber nicht für Laien.

Google-Back-up

Eine einfache Alternative ist die Aktivierung des Google-Back-ups in den Einstellungen (unter „System", „Sicherung") Ihres Smartphones. Es handelt sich um eine **Online-Sicherung** in der Cloud (siehe ► Seite 19), die Bestandteil jedes Google-Kontos ist (siehe ► Seite 47). Gesichert werden laut Google folgende Daten: App-Daten (z. B. individuelle Einstellungen, Spielstände), Anrufliste, Kontakte, individuelle Handy-Einstellungen, SMS und MMS, Fotos und Videos. Die Apps selbst werden nicht gesichert. In Ihrem Google-Konto ist nachvollziehbar, welche Apps aus dem Play Store Sie auf Ihrem Smartphone installiert hatten. Im Falle eines Gerätewechsels werden diese neu heruntergeladen. Sollte der kostenlose Speicherplatz in der Cloud knapp werden, können Sie zusätzlichen abonnieren, oder Sie übertragen z. B. Ihre Fotos und Videos auf Ihren Computer (per Kabel oder alternativ per WLAN, etwa mithilfe der App „PhotoSync" von touchbyte). **Achtung!** In den folgenden Fällen werden Ihre Daten laut Google gelöscht: Wenn Sie Ihr Handy 57 Tage lang nicht verwenden und/oder wenn Sie das Back-up in den Geräteeinstellungen deaktivieren.

Hersteller-Alternativen

Einige Gerätehersteller bieten ihr eigenes Cloud-Back-up an, die Apps sind vorinstalliert. Die funktionieren im Großen und Ganzen gut, der entscheidende Nachteil ist aber, dass das Rücküberspielen des Back-ups in

der Regel nur auf ein Gerät desselben Herstellers erfolgen kann. So wird versucht, die Nutzer:innen längerfristig an eine Marke zu binden.

Lokales Back-up

Mit Rücksicht auf den Datenschutz besteht vielfach der Wunsch nach lokalen Back-ups, um die Cloudspeicherung zu vermeiden. Es gibt im Play Store etliche **Back-up-Apps**, die aber bei genauerem Hinsehen fast alle unbrauchbar sind. Entweder ist auch hier eine Cloud im Spiel und/oder es gibt massive Datenschutzbedenken, oder der versprochene Funktionsumfang ist nur nach dem eingangs erwähnten Root möglich. Abraten müssen wir von der dauerhaften Datenaufbewahrung auf einer SD-Speicherkarte, hier ist die Gefahr eines technisch bedingten Datenverlustes wesentlich höher als bei internen oder externen Festplatten am Computer. Zum Überspielen gesicherter Handydaten auf den Computer können Sie die SD-Karte verwenden. Wenn Sie keine App nutzen, dann können Sie – wie gesagt – Fotos und Videos manuell überspielen. Kontakte und SMS lassen sich oftmals über die Einstellungen der jeweiligen App exportieren bzw. (per Mail oder Messenger) senden und somit auf ein anderes Gerät oder ein Speichermedium übertragen (die Kontakte in Form einer VCF-Datei). Auch andere Apps haben oft eine integrierte Sicherungsfunktion, allen voran WhatsApp (siehe ► Seite 83), dessen Inhalte nur auf diese Weise vollständig gesichert werden können. Hier ist man beim vollständigen Back-up allerdings auf die Cloud angewiesen („Einstellungen", „Chats", „Chat-Backup"). Die Option „Chat exportieren" ist kein Back-up im eigentlichen Sinn. Man kann damit aber einzelne Chatverläufe in Form einer Textdatei plus den dazugehörigen Bilder und Videos abspeichern sowie an andere Personen senden.

MyPhone Explorer

Tatsächlich gibt es eine einzige bewährte, vielseitige und noch dazu kostenlose Möglichkeit der Handy-Datensicherung lokal am Computer. Sie heißt **MyPhoneExplorer** (fjsoft.at) und stammt vom österreichischen Entwickler Franz Josef Wechselberger.

Cloudspeicher

Daten auslagern

Hinter dem englischen Begriff „Cloud" (Wolke) stecken Online-Speicherdienste von teils sehr großen, namhaften Anbietern, bei denen Unmengen an Daten gespeichert werden.

Datenschutzbedenken

Unweigerlich mit dem Begriff verbunden sind freilich auch Datenschutzbedenken, die nicht völlig von der Hand zu weisen sind. Das Risiko, dass von außen unbefugt auf Daten zugegriffen wird, besteht grundsätzlich immer. Hinzu kommt, dass ausgerechnet die gängigsten Anbieter ihren Sitz in den **USA** haben, wo in Sachen Datenschutz nicht dasselbe Niveau herrscht wie in Europa. So werden die Daten auf den Online-Speichern automatisch auf Viren, aber auch auf verbotene Inhalte gescannt, und der Zugriff von Behörden auf diese Inhalte ist gemäß der US-amerikanischen Gesetzgebung wesentlich einfacher als bei uns. Auch wenn etwa Microsoft mittlerweile eigene Speicherstandorte in Europa hat, ist es bisher nicht gelungen, alle Zweifel restlos zu beseitigen, dass nicht doch Daten nach Amerika übermittelt werden.

Fernzugriff und Back-up

Andererseits bietet eine Cloudlösung auch Vorteile: Der Zugriff auf die Daten kann von überall auf der Welt und von unterschiedlichen Geräten aus erfolgen (auf Wunsch auch gleichzeitig von verschiedenen Personen). Zudem kann man die Cloud als Back-up-Speicher nutzen, also zur zusätzlichen Sicherung von Daten für den Fall, dass ein Gerät oder eine Festplatte beschädigt wird oder abhandenkommt. Zuletzt muss man auch noch die Möglichkeit der nahtlosen Nutzung mehrerer Geräte gleichzeitig nennen. Egal ob Laptop, Tablet oder Smartphone – dank Synchronisierung über die Cloud sind die Daten immer aktuell.

Die bekanntesten Anbieter

Mit jedem Microsoft-Konto mitgeliefert wird **OneDrive**, bei Google ist es **Google Drive**. Beide bieten ein gewisses Ausmaß an kostenlosem Speicherplatz (zusätzlicher Platz kann jederzeit abonniert werden), was

sie zu den meistgenutzten Cloud-Anbietern im Privatbereich macht. Als „traditionsreicher" Anbieter nennenswert ist außerdem **Dropbox** (dropbox.com).

Tipps für mehr Sicherheit

Abseits der erwähnten Datenschutzvorbehalte sprechen die lange Tradition und die weite Verbreitung schon für die Nutzung der genannten Dienste. Auch die grundsätzliche Anforderung an die Sicherheit der Daten, also ihre **Verschlüsselung** auf dem Online-Speicher, ist bei OneDrive, Google Drive und Dropbox gewährleistet. Was Sie sonst noch beachten sollten:

- Überprüfen Sie die Einstellungen dahingehend, welche Daten genau synchronisiert werden und welche Geräte auf sie zugreifen können.
- Checken Sie Ihre Cloud-Konten regelmäßig. Wenn Sie verdächtige Aktivitäten bemerken, ändern Sie am besten gleich Ihr Passwort und kontaktieren den Cloud-Anbieter.
- Speichern Sie keine hochsensiblen Daten wie Kreditkarteninformationen oder Passwörter in der Cloud.

Alternativen aus Europa

Neben den Anbietern aus Übersee gibt es auch welche mit Sitz in **Europa**, die sich den DSGVO-Grundsätzen verschrieben haben. Zu nennen ist etwa **Luckycloud** (luckycloud.de). Bei diesem deutschen Dienst zahlen Sie nur den Speicherplatz, den Sie nutzen. Sicherheit durch Mehrfachverschlüsselung wird großgeschrieben. Gleiches gilt für den Anbieter **Your Secure Cloud** (yoursecurecloud.de). Auch er arbeitet mit hohen Verschlüsselungs-Standards und hat Angebote ab einigen wenigen Euro pro Monat im Programm.

Zwei Schweizer Anbieter

Die **Schweiz** kommt ebenfalls als Standort für sichere Cloudlösungen infrage. Ein wahrer Musterschüler in Sachen Datenschutz ist **Infomaniak** (infomaniak.com). Er hat nun auch Angebote für Privatkunden im Programm. Schließlich ist noch **pCloud** (pcloud.com) zu empfehlen, weil das Unternehmen neben dem Abo-Modell auch Speicherplatz per Einmalzahlung anbietet und ein kostenloses Paket im Programm hat.

Windows

Umgang mit Benutzerkonten

Der richtige Umgang mit den Benutzerkonten zählt zum Basisschutz. Beim ersten Hochfahren eines neuen Computers durchlaufen Sie einen automatisierten Registrierungsprozess, bei dem Sie das Gerät individuell benennen mit einem Passwort (= Administratorkennwort) absichern. Das Ergebnis dieses Prozesses ist Ihr persönliches **Administratorkonto** mit erweiterten Zugriffsrechten auf das System.

Administratorkonto versus Standardkonto

Ergänzend dazu ist es sinnvoll, ein „normales" Benutzerkonto, also ein **Standardkonto** für den täglichen Gebrauch, einzurichten. Mit diesem können Sie alle Programme verwenden und die Einstellungen nach Belieben anpassen. Im Standardkonto haben Sie aber nicht die Möglichkeit, Änderungen vorzunehmen, die Einfluss auf das System haben, sozusagen in die Tiefe gehen (Installation und Deinstallation von Software, Vergabe von Benutzerrechten, Zugriff auf sämtliche Dateien etc.). Auch Ihr Standardkonto sollten Sie jedenfalls mit einem Passwort sichern, das nicht dasselbe sein sollte wie jenes für das Administratorkonto. Das persönliche Standardkonto ergibt noch mehr Sinn, wenn Sie oft mit Laptop unterwegs sind. Denn Diebstahl oder schlichtes Vergessen des Laptops ist ebenfalls ein Sicherheitsproblem. Und wird das Gerät innerhalb der Familie von mehreren Personen genutzt, sollte jede davon ihr eigenes Benutzerkonto haben.

Benutzerkonto anlegen

Andere Benutzerkonten oder ein aus Sicherheitsgründen verwendetes lokales Konto (siehe den nächsten Absatz) können Sie in den „Einstellungen" (zu finden nach Klick auf das Windows-Fenstersymbol und das Zahnradsymbol) im Bereich „Konten", „Familien und andere Benutzer" anlegen. Dazu wird ein Microsoft-Konto benötigt, es sei denn, Sie melden das Konto unter „Ihre Familie" an und wählen „Konto für eine(n) Minderjährige(n) erstellen" aus. Im Ausklappmenü unter „Anmeldung nicht möglich" müssen Sie dann noch „Anmeldung zulassen" aktivieren. Unter

„Andere Nutzer" können Sie ebenfalls weitere Konten hinzufügen (ein Microsoft-Konto ist hierfür obligatorisch) und unter „Kontooptionen" den Kontotyp ändern(also entweder auf „Standard" oder auf „Administrator"). Dafür müssen Sie als „Administrator" angemeldet sein. Nicht mehr benötigte Konten sollten Sie aus Sicherheitsgründen löschen, auch das können Sie hier tun.

Alternative: Lokales Konto

Alternativ gibt es die erwähnte Möglichkeit, sich mit einem **lokalen Konto** anzumelden. Wenn Sie damit arbeiten, unterbinden Sie die automatische Synchronisierung der Daten und werden nicht automatisch bei Microsoft-Diensten wie OneDrive, Teams, Outlook, im App-Store oder im Edge-Browser angemeldet. Sie reduzieren damit den Datenfluss in Richtung Microsoft deutlich, können sich aber bei Bedarf gezielt bei einem der genannten Dienste anmelden. Um ein lokales Konto anzulegen, klicken Sie wieder in den „Einstellungen" auf „Konten", „Familie und andere Benutzer" und „Diesem PC eine andere Person hinzufügen". Anstatt eine E-Mail-Adresse oder Telefonnummer einzugeben, klicken Sie auf „Ich kenne die Anmeldeinformationen für diese Person nicht". Dann wählen Sie „Benutzer ohne Microsoft-Konto hinzufügen".

Sinnvolle Kombination

Wenn Sie ohne Microsoft-Konto arbeiten, dann muss Ihnen jedoch auch klar sein, dass Sie auf ein gewisses Maß an Komfort verzichten. So erweist sich etwa der Online-Speicher OneDrive (siehe ► Seite 19) bei der Weitergabe von größeren Mengen an Bildern als praktisch. Ratsam ist daher die Kombination beider Varianten, also Microsoft- plus lokales Konto.

(K)eine Alternative: die Basisvariante

Der Vollständigkeit halber möchten wir darauf hinweisen, dass es im Internet Tipps gibt, wie man Windows ausschließlich mit einem lokalen Konto nutzen kann, also ohne ein Microsoft-Konto anzulegen – indem man etwa bei Ersteinrichtung des Computers die Internetverbindung trennt oder nicht existente Nutzerdaten eingibt, was zu einer Fehlermeldung führt. Die Frage ist, wie sinnvoll dies angesichts der damit verbundenen **Nutzungseinschränkungen** ist und wie lange Microsoft dies noch zulassen wird.

Windows

Datenschutz-Einstellungen

Um den Datenfluss in Richtung Microsoft zu reduzieren, sollten Sie sich mit den Datenschutzeinstellungen von Windows befassen. Wir orientieren uns an Windows 11, wo unter anderem die Werbeeinblendungen ausgeweitet wurden. Die grundlegenden Dinge finden Sie aber genauso in Windows 10, denn schon dort hat Microsoft die Nachverfolgung deutlich ausgeweitet.

Berechtigungen

Gehen Sie in die „Einstellungen", dort in die Rubrik „Datenschutz & Sicherheit", und zwar zum Abschnitt „Windows-Berechtigungen". Unter „Allgemein" können Sie unterbinden, dass Ihnen auf Grundlage Ihrer Windows-Nutzung und Ihres Surfverhaltens **personalisierte Werbung** zugestellt wird. Stellen Sie dazu die Schalter auf „Aus".

Spracherkennung

Über eingebaute oder angeschlossene Mikrofone können Sie Windows über Sprachbefehle steuern oder Texte diktieren. Das funktioniert lokal, aber auch mit Unterstützung der Online-Spracherkennung. Letzteres bedeutet, dass Ihre Spracheingaben in die **Cloud** versendet und dort ausgewertet werden. Was genau mit diesen Informationen geschieht, ist unklar. Wir raten, diese Funktion abzuschalten.

Diagnose und Feedback

Wie nutzen Sie Ihren Computer und welche Probleme treten in Ihrem System auf? Es ist nachvollziehbar, dass Microsoft solche Daten erhebt, um künftige Windows-Versionen zu verbessern. In den versendeten Telemetriedaten und Fehlerberichten können allerdings auch Inhalte von privaten Dokumenten enthalten sein. Abschalten!

Individuelle Nutzererfahrung

Möchten Sie, dass Ihre Nutzungsdaten **zu Werbezwecken** verarbeitet werden? Nein? Abschalten! Setzen Sie dabei gleich auch die „Feedbackhäufigkeit" auf „Nie", um Nachfragen vonseiten des Konzerns zu unterbinden.

Aktivitätsverlauf

Standardmäßig speichert Windows lokal, welche Apps Sie benutzen und welche Webseiten Sie besuchen. Die Option, diese Informationen auch mit Microsoft zu teilen, sollte ausgeschaltet sein. Das lokale Speichern können Sie dagegen aktiviert lassen.

Suchberechtigungen

Die **Windows-Suche** (erreichbar über die Lupe bzw. das Suchfeld rechts neben dem Windows-Button) berücksichtigt unter anderem auch auf Ihrem Computer gespeicherte Informationen, Daten aus OneDrive, SharePoint, Outlook, Bing und anderen Diensten, bei denen Sie sich mit Ihrem Microsoft-Konto angemeldet haben, sowie von Ihnen besuchte Webseiten. Wenn Sie diese Funktionen deaktivieren, werden Ihnen natürlich weniger relevante Suchergebnisse angezeigt. Hier können Sie auch Ihren lokal gespeicherten Suchverlauf löschen, um ihn vor unbefugten Augen zu verbergen. Unter „SafeSearch" können Sie außerdem festlegen, wie stark der Jugendschutz bei der Anzeige von Suchergebnissen berücksichtigt werden soll.

Windows durchsuchen

Windows erstellt einen Index aus Ihren Festplatteninhalten, damit Sie schnellere Suchergebnisse erzielen. Da sich diese Funktion auf die lokale Ebene beschränkt, ist sie für den Datenschutz weniger relevant.

App-Berechtigungen

Für diesen Bereich lassen sich kaum allgemeine Empfehlungen geben. Hier wird insbesondere der Zugriff von bestimmten Apps und Programmen auf bestimmte Hardwarebauteile wie Kamera und Mikrofon sowie auch auf Inhalte wie Bilder, Videos und das Dateisystem geregelt. Solche Berechtigungen sind notwendig, um bestimmte Funktionen auszuführen. Es empfiehlt sich aber, die 25 Unterpunkte von Zeit zu Zeit durchzugehen, um festzustellen, welcher Dienst aktuell welche Berechtigungen hat. Oft stellt sich dabei heraus, dass man Berechtigungen unbewusst erteilt hat oder sich nicht mehr daran erinnert. Berechtigungen für Programme, die Sie gar nicht nutzen, sollten Sie auf jeden Fall zurücknehmen.

Weitere Einstellmöglichkeiten

Möchten Sie sich noch genauer in Ihre **Datenschutzeinstellungen** einarbeiten, finden Sie unter der Adresse account.microsoft.com/privacy weitere Erklärungen von Microsoft sowie die Möglichkeit, die Einstellungen nach Anmeldung mit Ihrem Microsoft-Konto online anzupassen.

Browser

Sicherer surfen

Der Browser ist das zentrale Werkzeug für das Surfen im Internet. Ob Google Chrome, Microsoft Edge oder Mozilla Firefox: Sie alle bieten vergleichbare Einstellungsmöglichkeiten und vordefinierte Sicherheitsfeatures.

Allgemeine Sicherheitsmerkmale

In der Adressleiste des Internetbrowsers ist in der Regel ein graues oder grünes Vorhängeschloss-Symbol zu sehen. Das deutet darauf hin, dass der Seitenaufruf über eine **verschlüsselte Verbindung** stattfindet. Diese sollte immer gewährleistet sein. Glücklicherweise sind Seiten ohne entsprechende Verschlüsselung nur mehr ganz selten im Umlauf. Sie sollten nicht aufgerufen werden.

SSL-Verschlüsselung

Seiten mit besagtem Vorhängeschloss haben das Kürzel **https** vor ihrem eigentlichen Seitennamen stehen. Das s am Ende steht für sicher (englisch: secure), weil die Verschlüsselung der Seite über SSL-Zertifikate (Secure Socket Layer) realisiert wird. Das heißt, der Server, auf dem sich die Seite befindet, muss sich über ein solches Zertifikat ausweisen können.

Adresse im Voraus checken

Daher lohnt sich immer ein kritischer Blick in die Adressleiste des Browserfensters. Sie brauchen aber nicht einmal zu klicken: Stellen Sie in einer verdächtigen E-Mail den Mauszeiger auf den dort angeführten Link. Dann erscheint ein kleines Fenster, dem Sie in der Regel entnehmen können, zu welcher Adresse der Link führt.

Blick auf die Verschlüsselung

Klicken Sie im Browser auf das Vorhängeschloss und danach auf die verschiedenen Ebenen des sich öffnenden Fensters, dann erfahren Sie wichtige Dinge zum betreffenden Zertifikat, u. a. für wen es ausgestellt wurde, welche Stelle es vergeben hat und wie lange es gültig ist. Finger weg von abgelaufenen Zertifikaten. Interessant ist auch der Grad der Verschlüsselung. **128 Bit** sollten es mindestens sein.

Achtung! Es kommt immer wieder vor, dass man neben dem Vorhängeschloss ein Warndreieck sieht oder dass das Schloss durchgestrichen ist oder dass im Browser Meldungen auftauchen, die sinngemäß besagen, dass „nur sicherer Inhalt" angezeigt wird. Dabei handelt es sich um https-verschlüsselte Seiten, die aber unverschlüsselte Elemente enthalten (z. B. Grafiken, Bilder oder Werbebanner). Man spricht auch von gemischten Inhalten. Üblicherweise hat man die Option, die unsicheren Inhalte nachzuladen. Dies sollte man zumindest auf Seiten, auf denen man persönliche Daten eingibt, keinesfalls tun, denn man weiß nicht, mit wem die unsicheren Elemente kommunizieren.

Privates Fenster: Nicht anonym

Eine spezielle Option führt oft zu Missverständnissen, nämlich das „Private Fenster" bzw. „InPrivate-Browsen" oder auch „Inkognito-Fenster" genannt. Viele Nutzer:innen nehmen an, die Aktivierung dieser Funktion ermögliche nach außen hin anonymes Surfen. Tatsache ist, dass lediglich keine lokalen Aufzeichnungen über den Surfverlauf auf dem Computer selbst erfolgen (Chronik/Verlauf, Suchanfragen, Cookies, temporäre Dateien). Das ist z. B. von Vorteil, wenn Sie an einem fremden Computer arbeiten. Nur Firefox hat mit dem Tracking-Schutz mehr zu bieten. Dieser Schutz vor Aktivitäten-Nachverfolgung ist mit dem privaten Fenster verknüpft bzw. kann er gesondert aktiviert werden. Dies ist zumindest als Basisschutz akzeptabel. **Aber Vorsicht!** Vollständige Anonymität ist trotzdem nicht gegeben, Ihr Internetanbieter kann jedenfalls nachvollziehen, welche Seiten Sie aufgerufen haben.

„Do Not Track" nützt wenig

Nicht verwechseln darf man den Tracking-Schutz bei Firefox mit der in den Browsern aktivierbaren „Do Not Track"-Aufforderung, die darauf hinausläuft, dass jeder aufgerufenen Website signalisiert wird, dass die Nutzer:innen keine Nachverfolgung wünschen. Die Betreiber der Website können sich daran halten oder auch nicht. Aufgrund dieser Freiwilligkeit kann diese Option ruhig deaktiviert bleiben. Sinnvoller ist es, einen Werbeblocker zu installieren (siehe ► Seite 37).

Zusammenfassung und Checkliste

Für Ihre Sicherheit

Abschließend geben wir Ihnen einen Überblick über jene Vorkehrungen, welche die **Grundlage** für die sichere Nutzung des Internets und der damit verbundenen Geräte darstellen. Es handelt sich zugleich um eine Checkliste jener Punkte, die Sie bevorzugt umsetzen sollten. Die Seitenverweise beziehen sich auf Beiträge in diesem Buch, die weiterführende Informationen enthalten.

Allgemeines

- Sichern Sie Ihre Geräte mit einem Schutzprogramm („Virenschutz") gegen Schadsoftware ab (► Seite 136).
- Halten Sie Betriebssystem, Programme, Apps und Virenschutz mit automatischen Updates auf dem aktuellen Stand (► Seite 14).
- Legen Sie für die alltägliche Arbeit am Computer ein Benutzerkonto mit eingeschränkten Zugriffsrechten an (► Seite 21).
- Nehmen Sie in den Browsereinstellungen diverse manuelle Anpassungen vor, um den Datenschutz zu verbessern (► Seite 27ff).
- Vermeiden Sie das (automatische) Speichern von Passwörtern im Browser, so praktisch es auch sein mag, und überlegen Sie die Verwendung eines Passwortmanagers (► Seite 138).
- Vermeiden Sie die Mehrfachverwendung von Passwörtern und gestalten Sie diese möglichst sicher (► Seite 140).
- Ändern Sie werksseitig vergebene Passwörter, nicht zuletzt in Ihrem WLAN-Router.
- Installieren Sie Browsererweiterungen (► Seite 37) zum Blockieren von Werbung und Tracking (Nachverfolgung Ihrer Internet-Aktivitäten).
- Verwenden Sie statt Google eine alternative Suchmaschine, damit Sie im Netz anonymer unterwegs sind (► Seite 34).
- Schränken Sie auf Ihrem Smartphone oder Tablet die Zugriffsberechtigungen von Google (► Seite 47) sowie der installierten Apps ein (► Seite 147).

- Vergewissern Sie sich, dass manuell eingegebene Internetadressen vollständig und fehlerlos sind.
- Sollte eine Adresse ins Leere führen, dann geben Sie den Namen der gesuchten Seite am besten in Ihre gewohnte Suchmaschine ein.
- Sollte die Adresse zu einer Seite führen, deren Inhalt offensichtlich nichts mit dem eigentlich Gewünschten zu tun hat oder die lediglich eine Reihe von Links zum Thema enthält, dann vermeiden Sie es, darauf zu klicken, und versuchen Sie es stattdessen mit Ihrer gewohnten Suchmaschine.
- Beachten Sie, dass in vielen Suchmaschinen die Toptreffer bezahlte Werbeanzeigen sind, die meist nur unauffällig als solche gekennzeichnet sind. Klicken Sie bevorzugt auf die weiter unten in der Liste angeführten Treffer.
- Bedenken Sie, dass Sie den Anbietern die Nachverfolgung Ihrer Aktivitäten im Internet erleichtern, wenn Sie dauerhaft mit Ihrem Benutzerkonto angemeldet bleiben (z. B. bei Facebook oder Amazon). Sinnvoller ist das Anmelden bei Bedarf sowie das bewusste Abmelden danach. Deaktivieren Sie daher auch Anmeldeoptionen wie „Auf diesem Computer angemeldet bleiben".
- Sofern Sie keinen Werbeblocker verwenden (► Seite 37), der einen Großteil der Anzeigen ausblendet, finden Sie auch auf vielen Internetseiten massenhaft Werbung – zum Teil sehr auffällig, zum Teil kaum als werbliche Einschaltung wahrnehmbar mitten im Text. Schauen Sie besser zweimal, bevor Sie auf einen (Download-)Link klicken, denn es könnte der falsche sein.
- Stellen Sie den Mauszeiger, ohne zu klicken, auf einen Link, dann zeigt der Browser üblicherweise in einem Feld links unten an, wohin der Link tatsächlich führt.
- In der Adresszeile des Browsers wird die Domain, also der Hauptbestandteil einer Internetadresse, schwarz hervorgehoben (Domain-Highlighting, z. B. https://**konsument.at**/handytest). Sollte die aufgerufene Adresse nicht die erwartete Seite zeigen, dann löschen Sie alle auf den Hauptbestandteil folgenden Bestandteile und versuchen Sie es mit der Haupt-

adresse, um dann über die Links auf der Startseite oder die Suchfunktion doch noch das Gewünschte zu finden.
- Wenn Sie sich auf einer Seite persönlich registrieren müssen, dann lesen Sie vorher die Nutzungsbedingungen zumindest dahin gehend, ob Sie eine zeitliche Bindung und/oder eine finanzielle Verpflichtung eingehen.
- Achten Sie – nicht nur bei der Registrierung, sondern bei jeder Eingabe Ihrer Nutzerdaten – auf die Verschlüsselung der Seite, erkennbar am Kürzel „https" (entscheidend ist das „s" am Ende!) und am Vorhängeschloss-Symbol.

E-Mails

- Öffnen Sie keinesfalls Dateianhänge in E-Mails unbekannter Herkunft und klicken Sie auf keinen darin angegebenen Link.
- Seien Sie auch bei E-Mails scheinbar bekannter Herkunft vorsichtig, falls Sie dort zur Bekanntgabe heikler Daten oder zur Begleichung offener Forderungen, die Sie nicht nachvollziehen können, aufgefordert werden.
- Steigen Sie nicht über einen in der E-Mail enthaltenen Link, sondern direkt im Browser über Ihr persönliches Konto in die Internetseite ein und klären Sie notfalls durch Rückfrage die Echtheit der E-Mail.
- Für alle Details zum sicheren Umgang mit E-Mails sowie zum Thema Spam-Mails beachten Sie bitte die Beiträge auf den ► Seiten 122 sowie 120.
- Verwenden Sie für die Anmeldung zu Newslettern oder auf Internetseiten nicht Ihre Haupt-Mailadresse, sondern eine weitere Adresse, die Sie ausschließlich für solche Zwecke einsetzen.
- Und denken Sie immer daran: Aus welchem vernünftig erklärbaren Grund sollte Ihnen eine wildfremde Person Geld schenken oder sollten Sie bei einer ausländischen Lotterie Geld gewonnen haben (davon abgesehen, dass die Teilnahme an ausländischen Lotterien von Österreich aus verboten ist)? Zum Thema Internetkriminalität ► Seite 116ff, zum Thema Online-Glücksspiel ► Seite 128.

Online-Shopping

- Beachten Sie die Einhaltung der gesetzlichen Regelungen für sicheres Online-Shopping durch den Händler sowie Ihre Rechte (► Seite 71).

- Lesen Sie bitte alle Artikel zum Thema Internetkriminalität ab ► Seite 39 sowie zu den Fake-Shops (► Seite 130) und den Dark Patterns, die einen zum vorschnellen Kaufabschluss verleiten sollen (► Seite 132).
- Leisten Sie keine Vorauszahlungen per Überweisung, außer Sie selbst oder Ihnen bekannte Personen haben bereits eindeutig positive Erfahrungen mit dem Verkäufer gemacht. Alle Informationen zum sicheren Bezahlen im Internet finden Sie ab ► Seite 64.
- Vermeiden Sie es, die auf Verkaufsplattformen vorgesehenen internen Kommunikations- und Zahlungswege zu umgehen, nur weil Sie von einem Anbieter dazu aufgefordert werden.
- Wenn Sie selbst auf einer Verkaufsplattform inserieren: Misstrauen Sie (ausländischen) Interessenten, die unter allen Umständen das von Ihnen angebotene Produkt kaufen wollen und auf Mittelsmänner, Transportfirmen etc. verweisen, weil sie angeblich persönlich verhindert sind. Der nächste Schritt ist, dass Sie eine Zahlung leisten sollen.
- Achten Sie auch hier bei der Eingabe heikler Daten und Passwörter auf die Verschlüsselung der Seite, erkennbar am Kürzel „https" und am Vorhängeschloss-Symbol.

Benutzerkonten absichern

- Wählen Sie, wo es möglich ist, die Zwei-Faktor-Authentifizierung zur Absicherung Ihrer Online-Accounts, also die zweistufige Anmeldung mit Passwort und Code (► Seite 142).
- Hinterlegen Sie unbedingt eine Telefonnummer und/oder eine alternative E-Mail-Adresse (angelegt bei einem anderen Anbieter bzw. alternativ die Adresse einer Person aus Ihrem näheren Umfeld), damit Sie im Notfall von Ihrem Anbieter über verdächtige Vorgänge auf Ihrem Konto benachrichtigt werden können. Anbieter wie Google, Microsoft oder Facebook verständigen einen mittlerweile über jede Anmeldung, die über einen „unbekannten" Browser erfolgt, auch wenn man sie selbst vorgenommen hat. Sie sollten diese Benachrichtigungen keinesfalls deaktivieren, denn nur so behalten Sie den Überblick. Bei allen diesen Anbietern können Sie online auch überprüfen, welche Geräte gerade aktiv angemeldet sind bzw. es in der Vergangenheit waren. Beachten Sie auch die

weiterführenden Beiträge zu Google (► Seite 29ff), Microsoft (► Seite 21ff) und Facebook (► Seite 43) in diesem Buch.

- Verwenden Sie keinesfalls identische oder sehr ähnliche Passwörter für verschiedene Benutzerkonten (mehr zum Thema sichere Passwörter ► Seite 140).
- Sollte eines Ihrer Konten gehackt werden, dann unternehmen Sie folgende Schritte: Ändern Sie sofort das Passwort und auch allfällige Sicherheitsfragen (bzw. die Antworten darauf), die Sie dort hinterlegt haben (z. B. Mädchenname der Mutter, Haustier, Automarke). Falls Sie dasselbe Passwort für ein anderes Konto verwenden, dann ändern Sie es auch in diesem, nehmen Sie aber keinesfalls wieder ein identisches. Tauschen Sie dort gleichfalls die Sicherheitsfragen aus. Falls es sich um ein E-Mail-Konto handelt, dann verständigen Sie Ihre Kontakte und warnen Sie sie vor eventuellen Spam-Mails, die in Ihrem Namen verschickt werden könnten. Sie selbst sollten mit erhöhtem Aufkommen von Spam- und Phishing-Mails rechnen, denn vielleicht versuchen die Datendiebe ja, noch mehr von Ihnen zu erfahren. Haben Sie auf dem gehackten Konto Ihre Bank- oder Kreditkartendaten hinterlegt, dann seien Sie sehr aufmerksam und kontrollieren Sie regelmäßig Ihre Kontoauszüge und Kreditkartenabrechnungen. Notfalls müssen Sie Ihre Kreditkarte sperren lassen und eine neue beantragen. Möglich ist auch, dass Ihr Name für betrügerische Geschäfte missbraucht wird (Identitätsdiebstahl), etwa um andere Personen über Fake-Angebote auf Amazon und Co. um ihr Geld zu bringen oder um Waren zu bestellen, die dann nicht bezahlt werden. Natürlich werden Sie dafür nicht zur Rechenschaft gezogen, doch angenehm ist eine solche Situation in keinem Fall. Sollten Sie selbst von solchen Betrügereien in Ihrem Namen Kenntnis erlangen, dann melden Sie dies dem betroffenen Anbieter und erstatten Sie bei der Polizei Anzeige gegen unbekannt.

Ob Spam- oder Phishing-Mails, ob Virenattacken, Betrugsversuche, Cookies oder das übermäßige Sammeln persönlicher Daten – wir alle sind mit den Schattenseiten des Internets und der sozialen Medien konfrontiert. War vieles davon früher auf den PC beschränkt, hat die weite Verbreitung der Smartphones auch in negativer Hinsicht neue Möglichkeiten eröffnet. Sobald man den Computer aufdreht oder das Handy zur Hand nimmt, ist es mit der Anonymität vorbei. Trotzdem gibt es Mittel und Wege, um die persönlichen Dokumente und Daten besser zu schützen. Dieses Buch deckt die wichtigsten Bereiche ab. Es hilft, die Hintergründe besser zu verstehen, zeigt, worauf man im Umgang mit Internet und Co achten sollte, und liefert leicht umsetzbare Handlungsanleitungen zur Absicherung von Geräten und Privatsphäre. So kann man sich mit einem besseren Gefühl ins Internet begeben und sich dessen nützlichen Seiten zuwenden.

Verein für Konsumenteninformation, Wien
www.vki.at | www.konsument.at

ISBN 978-3-99013-121-3

€ 25.–