Digitaler Nachlass

VIER PUNKTE ZUR VORSORGE

„Seit es das Internet gibt, sind wir alle unsterblich“, sagte einmal ein bekannter Datenschützer. Er bezog sich dabei auf die Löschungs- bzw. NICHT-Löschungspraktiken der großen Internetfirmen. Im Krankheits- oder Todesfall eines nahestehenden Menschen möchte man ungern Anwälte oder Gerichte bemühen. Muss man auch nicht, wenn man ein paar Dinge beachtet.

Was gehört zum Digitalen Nachlass? Alles, was digital ist, also alle Geräte und Dienste, die Daten elektronisch verarbeiten und speichern. Unproblematisch sind die Dinge, auf die der Bevollmächtige oder Erbe körperlich Zugriff hat, d. h. CDs, DVDs, Festplatten, eBook-Reader, Computer (obwohl dabei das Zugangspasswort eine Rolle spielen kann). Sie sind zu behandeln wie Bücher.

DIE KONTENLISTE: Probleme können auftauchen, wenn man keinen Zugriff mehr hat auf Online-Dienste wie E-Mail, Soziale Medien, Online-Kaufhäuser, Online-Banken, eigene Internetseiten, Blogs u. ä. Hier hilft eine Übersicht: Wo habe ich mich im Internet schon einmal angemeldet? Wo habe ich ein „Konto“ (account) angelegt? Dazu zählt auch das Konto, mit dem ich mein Smartphone aktiviert, d. h. beim Anbieter des Betriebssystems (meist Google/Android oder Apple) registriert habe.

DER DIGITALE BEVOLLMÄCHTIGTE: Alleine schon, wenn man sich „nur“ die Hände bricht, ist es gut, wenn man jemanden hat, dem man vertraut, und der dann zum Beispiel einen Blick in die E-Mails werfen kann. Sind Rechnungen eingetroffen? Habe ich eine Einladung erhalten? Ein „digitaler Bevollmächtigter“ kann nachschauen und sich ggf. kümmern.

PASSWORTMANAGER ODER LISTEN: Damit der digitale Bevollmächtigte handeln kann, muss er für den Notfall wissen, wie die Zugangsdaten lauten, also Nutzername und Passwort. Gegebenenfalls benötigt er auch den „2-Faktor-Authentifizierung“ also z. B. Zugriff auf das Handy oder Smartphone. Wegen der strengen Empfehlungen für ein sicheres Passwort – viele Zeichen (mindestens 8), viele Zeichenarten, für jeden Dienst ein anderes – empfehlen sich Passwortmanager oder gesicherte Listen. Wenn der Bevollmächtigte darauf Zugriff hat, kann ggf. er*sie handeln.

TESTAMENT UND VORSORGEVOLLMACHT: Nicht jeder Bevollmächtigte weiß auf Anhieb, wie mit den Online-Diensten verfahren werden soll. Facebook-Seiten können zum Beispiel in einen Gedenkzustand versetzt werden. E-Mail-Konten werden besser nicht sofort gelöscht. Es können da weiterhin wichtige Mails eingehen wie z. B. Rechnungen, die Hinweise auf andere Konten geben. Auch erfolgen die Funktionen „Passwort vergessen“ und „Konto wiederherstellen“ meist über das E-Mail-Konto (oder/und das Smartphone). Hier empfiehlt sich ein kurzer Hinweis in der Kontenliste, Vorsorgevollmacht oder im Testament.

Kontakt und Text: Kirsten Kemna, ZWAR e. V., Steinhammerstr. 3, 44379 Dortmund, Tel. 0231/96 13 17-0, k.kemna@zwar.org und Guido Steinke, VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, guido.steinke@verbraucher.org

IMPRESSUM: Handreichung zum Projekt „Train the Trainer – Qualifizierung digitaler Themenchampions für ältere Menschen in NRW“; Fördermittelgeber: Staatskanzlei des Landes Nordrhein-Westfalen; Projektleitung: Georg Abel (V.i.S.d.P.), VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, mail@verbraucher.org, August 2020

Seriöse Gesundheitsinformation

SIEBEN PUNKTE FÜR DIE INFORMATIONSSUCHE

Wer hat bei Symptomen oder nach einem Arztbesuch nicht schon einmal „Dr. Google" konsultiert? Gute von schlechten Gesundheitsinformationen zu unterscheiden, ist nicht einfach. Wenn Sie ein paar Tipps beachten, kommen Sie gut durch den Informationsdschungel.

INFORMATIONEN: Starten Sie die Suche nach verlässlichen Gesundheitsinformationen auf diesen Seiten:

- Das Ärztliche Zentrum für Qualität in der Medizin: www.patienten-information.de
- Das Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen: www.gesundheitsinformation.de
- Das Deutsche Krebsforschungszentrum: www.krebsinformationsdienst.de

Eine ausführliche Liste bietet auch der Patientenwegweiser: www.sylvia-saenger.de/patientenwegweiser

SUCHMASCHINEN: Die Reihenfolge der Suchergebnisse sagt nichts über Qualität und Seriösität der Informationen aus. Schauen Sie sich mehr als die ersten fünf Treffer an. Bei den ersten Treffern handelt es sich oft um Werbeanzeigen.

INTERNETSEITEN: Wer steht hinter der Information? Welche Ziele und Interessen verfolgt er oder sie? Wie finanziert die Seite sich? Ein Blick ins Impressum hilft meist schon weiter. Schauen Sie, wie andere die Internetseite bewerten. Geben Sie in das Suchfeld des Browers z. B. den Namen der Internetseite mit dem Zusatz „Beschwerden" oder „Kritik" ein. Enthält die Internetseite Hilfsangebote, z. B. Adressensammlungen von Stellen, an die Sie sich wenden können?

INTERNETFOREN: Die Foren bieten Raum zum Austausch, sind aber keine zuverlässigen Informationsquellen. Die Angaben sind subjektiv und werden i. d. R. nicht hinsichtlich ihrer Richtigkeit und Qualität überprüft. Trotzdem kann man dort schon mal eine Anregung aus praktischer Erfahrung finden, die man dann z. B. mit dem Hausarzt diskutieren kann.

INFORMATIONSQUALITÄT: Achten Sie darauf, wer die Information geschrieben hat. Suchen Sie am Ende des Informationstextes oder im Impressum des Webangebotes nach einem Autor. Gut ist, wenn die Aussagen mit seriösen Belegen, z. B. aus Studien oder Leitlinien (www.patientenleitlinien.de/, www.patienten-information.de/patientenleitlinien#, www.awmf.org/leitlinien/aktuelle-leitlinien.html) abgesichert sind. Zur Überprüfung kann man sich auch an die Unabhängige Patientenberatung Deutschland (0800 011 77 22, www.patientenberatung.de) oder eine Beratungsstelle der Bundesarbeitsgemeinschaft der PatientInnenstellen (www.bagp.de/beratung) wenden.

GÜTESIEGEL: Es gibt Internetseiten, die ein „Qualitätssiegel" tragen. Solche Siegel sind kein Garant für die absolute Korrektheit der Information, jedoch bieten sie ein hohes Maß an Transparenz. Diese Siegel dürfen nur diejenigen tragen, die eine Qualitätsprüfung durchlaufen haben. Interessant für deutschsprachige Internetseiten sind zwei Siegel: das sogenannte AFGIS-Logo (www.afgis.de) und das HON-Logo (www.hon.ch).

FRAGEN SIE AUF JEDEN FALL ERST IHREN ARZT, BEVOR SIE SICH SELBST THERAPIEREN.

Kontakt und Text: Kirsten Kemna, ZWAR e. V., Steinhammerstr. 3, 44379 Dortmund, Tel. 0231/96 13 17-0, k.kemna@zwar.org und Guido Steinke, VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, guido.steinke@verbraucher.org

Bundesverband Die Verbraucher Initiative e.V.

ZWAR ZWISCHEN ARBEIT UND RUHESTAND

IMPRESSUM: Handreichung zum Projekt „Train the Trainer – Qualifizierung digitaler Themenchampions für ältere Menschen in NRW"; Fördermittelgeber: Staatskanzlei des Landes Nordrhein-Westfalen; Projektleitung: Georg Abel (V.i.S.d.P.), VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, mail@verbraucher.org, August 2020

Bezahlen mit dem Smartphone

SIEBEN PUNKTE FÜR DEN SICHEREN EINKAUF

Das Smartphone wird immer mehr zum Multifunktionswerkzeug. Telefonieren und fotografieren sind selbstverständlich, Bezahldienste nehmen zu. Worauf sollte man achten, wenn man diese neuen Dienste nutzen möchte?

SICHERHEIT: Zu einem sicheren Smartphone gehören SIM-Karten-PIN und Bildschirmsperre, ein aktuelles Betriebssystem, regelmäßige Updates der Apps, ggf. Virenschutz, Firewall.

UNSICHERHEIT: Wenn Sie etwas nicht verstehen, fragen Sie erst einmal Ihre Bank oder eine Person Ihres Vertrauens. Lieber einmal zu früh abbrechen (und fragen) als einmal zu spät.

LINKS: Ihr Smartphone ist ein kleiner Computer. Als solcher ist er Ziel von Hackern und sonstigen Gaunern, die auf Ihr Gerät zugreifen möchten, um Ihnen z. B. beim Online-Banking „über die Schulter zu schauen". Dies ist u.a. durch Viren und Trojaner möglich, die über einen Link auf Ihr Telefon gelangen. Klicken Sie keine Links an in Nachrichten (z. B. bei WhatsApp), die Sie nicht kennen.

APPS: Ihr App-Shop-Betreiber prüft zwar die meisten Apps, bevor sie zum Download bereit gestellt werden, aber oft nur in technischer Hinsicht. Er prüft nicht, wo Ihre Daten hingelangen und was damit passiert. Eine gefälschte oder gehackte Banking-App kann zum Beispiel Ihre Online-Banking-Daten an jemanden weitergeben, der dann an Ihrer Stelle von Ihrem Konto Überweisungen tätigt. Sensible Daten wie Ihre Bankverbindung sollten nie unverschlüsselt übertragen werden. Nutzen Sie nur zertifizierte und sichere Apps aus seriösen Quellen.

ANBIETER: Lesen Sie sich die Vertragsbedingungen genau durch. Stellen Sie sich dabei vor allem folgende Fragen: Fallen zusätzliche Kosten an? Kann ich den Vertrag problemlos kündigen? Was passiert mit meinen Daten? Wie ist die App geschützt, z. B. Verschlüsselung, Zertifizierung? Prüfen Sie den Anbieter durch eigene Recherchen im Internet (Testportale und unabhängige Vergleichsseiten).

AUFBEWAHRUNG: Smartphone und TAN-Generator sind die neue Generation der EC-Karte mit PIN. Wenn beides zusammen abhanden kommt, kann der Finder an Ihr Geld, sofern Sie Ihr Smartphone nicht gesperrt haben. Bewahren Sie mobile Endgeräte und den „2-Faktor", also PIN, TAN-Generator u. ä., sicher auf.

VORSORGE: Es ist technisch möglich, dass jemand ein WLAN aufspannt, das Ihrem Gerät bekannt vorkommt, z. B. „Telekom" oder „Bahn". Verbindet sich Ihr Gerät dann mit diesem gefälschten WLAN, kann der Betreiber Ihren Datenverkehr mitschneiden. Wenn diese Daten dann nicht verschlüsselt sind, liest er mit. Schließen Sie alle Kanäle, durch die auf Ihr Smartphone zugegriffen werden kann, wie WLAN, Bluetooth, NFC („near field communication", ein Funkstandard für kurze Distanzen), wenn Sie sie nicht brauchen.

Kontakt und Text: Kirsten Kemna, ZWAR e. V., Steinhammerstr. 3, 44379 Dortmund, Tel. 0231/96 13 17-0, k.kemna@zwar.org und Guido Steinke, VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, guido.steinke@verbraucher.org

IMPRESSUM: Handreichung zum Projekt „Train the Trainer – Qualifizierung digitaler Themenchampions für ältere Menschen in NRW"; Fördermittelgeber: Staatskanzlei des Landes Nordrhein-Westfalen; Projektleitung: Georg Abel (V.i.S.d.P.), VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, mail@verbraucher.org, August 2020

Sicheres Smartphone

SIEBEN PUNKTE FÜR EINE BEWUSSTE NUTZUNG

Das Smartphone ist zum ständigen Begleiter geworden und ersetzt inzwischen den Wecker, die Kamera oder den Gang zur Bank. Eine Erleichterung gerade für ältere Menschen, die vermehrt die Vorzüge der mobilen Technik zu schätzen wissen. Neben Fotos und Kontakten verbleiben auch Kontodaten und Zugangscodes auf dem Handy. Das macht das Smartphone zur ganz persönlichen Datensammelstelle und zum begehrten Ziel für Hackerangriffe und Datenklau.

SIM: Wer hat nicht schon einmal sein Smartphone irgendwo liegen gelassen? Der Finder hat dann ein Gerät, das er nicht für unbefugte Zwecke nutzen kann, wenn beim Start eine SIM-Karten-PIN eingestellt ist und der Bildschirm ebenfalls gesperrt ist, z. B. durch PIN, Muster oder Fingerabdruck. Dabei ist eine lange PIN, z. B. aus sechs Ziffern, die sicherste Variante.

SCHNITTSTELLEN: Das Smartphone hat verschiedene „Tore", d.h. Schnittstellen, durch die es mit der Umwelt kommuniziert: das Mobilfunknetz, aber auch WLAN, Bluetooth oder NFC („near field communication", ein Funkstandard für kurze Distanzen). Über diese Schnittstellen kann es sich mit anderen Geräten verbinden und Daten austauschen. Wer das nicht möchte, schaltet am besten die Schnittstellen nur dann an, wenn sie benötigt werden.

APPS: Apps sind kleine Anwendungen oder Programme, die das Smartphone so praktisch machen. Als Programme können sie aber auch Unfug anstellen und zum Beispiel Bezahlvorgänge auslösen („In-App-Käufe") oder Daten weiter geben. Wer das nicht möchte, sollte auf Apps aus seriösen Quellen, von seriösen Herstellern und mit seriösen Finanzierungsmodellen achten. Im regulären „Store" werden die Hersteller der App genannt. Diesen (Firmen-)Namen kann man dann in eine Suchmaschine seines Vertrauens eingeben, z. B. zusammen mit dem Wort „Beschwerde". Das Finanzierungsmodell ergibt sich meist aus dem Hersteller: Die „Nina-App" wird z. B. vom Bundesamt für Bevölkerungsschutz herausgegeben. Dieses erfüllt seine Aufgaben aus Steuermitteln, sollte also keine Werbung und In-App-Käufe enthalten und sich an die einschlägigen Datenschutzbestimmungen und die Datensparsamkeit halten.

BEZAHLDATEN: Im Zweifel wollen Ganoven an Ihr Geld. Im Smartphone geht das über zwei Kanäle: Bezahldaten wie z. B. Ihre Bank- oder Kreditkartenverbindung, die Sie im „App-Store" oder direkt in einer App hinterlegt haben, oder die Mobilfunkrechnung. Verschließen Sie diese Kanäle, indem Sie z. B. nur mit Guthabenkarten bezahlen und bei Ihrem Mobilfunkanbieter eine Drittanbietersperre einrichten. In Apps, mit denen man direkt Bestellungen und Bezahlvorgänge auslösen kann (wie Amazon) niemals das Passwort hinterlegen.

UP-TO-DATE: Nur ein aktuelles System ist sicher. Dies gilt sowohl für das Betriebssystem als auch für installierte Apps.

DATENSPARSAMKEIT: Anbieter (z. B. Google) möchten bei der Registrierung und der Nutzung viel wissen. Alter, Geschlecht, Adresse – für die Nutzung eines Telefons eher irrelevante Daten. Auch manche Apps sind neugierig. Hier gilt: Daten nur preisgeben, wenn unbedingt erforderlich, sonst lügen. Aber aufgepasst: Bei der Wiederherstellung eines Nutzerkontos könnte von Ihnen verlangt werden, Ihre Identität nachzuweisen.

BACKUPS: Wer wichtige Daten auf seinem Smartphone hat, möchte sie nicht verlieren. Hier bietet sich ein Backup an, entweder auf dem lokalen Rechner oder in der Cloud.

Kontakt und Text: Kirsten Kemna, ZWAR e. V., Steinhammerstr. 3, 44379 Dortmund, Tel. 0231/96 13 17-0, k.kemna@zwar.org und Guido Steinke, VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, guido.steinke@verbraucher.org

Bundesverband Die Verbraucher Initiative e.V.

ZWAR ZWISCHEN ARBEIT UND RUHESTAND

IMPRESSUM: Handreichung zum Projekt „Train the Trainer – Qualifizierung digitaler Themenchampions für ältere Menschen in NRW"; Fördermittelgeber: Staatskanzlei des Landes Nordrhein-Westfalen; Projektleitung: Georg Abel (V.i.S.d.P.), VERBRAUCHER INITIATIVE e. V. (Bundesverband), Berliner Allee 105, 13088 Berlin, Tel. 030/53 60 73 3, mail@verbraucher.org, August 2020