Rat & Recht | Wir machen Sie stark.

Medien

verbraucherzentrale
Nordrhein-Westfalen

LEITFADEN ZUM DATENSCHUTZ

Ich habe doch nichts zu verbergen –
Datensparsamkeit lohnt sich trotzdem

www.vz-nrw.de/datenschutz

INHALT

Foto: Shutterstock / Twin Design

LEITFADEN ZUM DATENSCHUTZ

Ich habe doch nichts zu verbergen – und warum sich Datensparsamkeit trotzdem lohnt

Immer wieder lesen Sie von Chancen und Risiken sozialer Netzwerke oder neuer mobiler Endgeräte, aber auch von Datenlecks, von Passwortklau … Sie werden aufgefordert, mit Ihren Daten sorgsam umzugehen. Sie fragen sich, warum Ihre Daten so interessant sein sollen und ob sich der Aufwand lohnt, da Sie doch nichts zu verbergen haben?

Es geht um Ihre personenbezogenen Daten, das sind nicht nur Informationen wie Wohnort, Geburtstag oder sonstige Kontaktdaten. Es sind vor allem auch Informationen über Ihre Lebensgewohnheiten, Ihre gesundheitliche Situation, Ihre finanziellen Hintergründe, über Ihr soziales Netzwerk, Ihre Freunde und Ihr Wohlbefinden. Was passiert mit dieser Flut von Daten?

Immer wieder lesen Sie von den Herausforderungen beim Thema „BIG DATA“. Beim Thema Datenschutz fühlen sich viele Internetnutzer noch unzureichend informiert. Welche Aspekte spielen im Alltag eine Rolle, worauf sollten Sie achten und was können Sie tun, um Ihre Daten zu schützen und damit auch Ihre Privatsphäre zu erhalten?

Dieser Leitfaden will Ihnen die einzelnen Aspekte, die es bei der Nutzung der Angebote der digitalen Welt gibt, näherbringen. Er soll ein Grundverständnis dafür vermitteln, dass Sie selbst entscheiden können, welche und wie viele Daten Sie von sich preisgeben und wie Sie sich vor allzu neugierigen Webseiten oder gar Schadprogrammen schützen können.

Weitere und aktuelle Informationen finden Sie auf der Webseite der Verbraucherzentrale NRW [1].

[1] *www.vz-nrw.de/datenschutz*

PASSWÖRTER

Auch wenn es lästig und aufwendig ist – um ein sicheres Passwort kommt man nicht herum!

Oft liest man in der Presse vom „Passwortklau“ bei bekannten und viel genutzten Anbietern und Unternehmen und dennoch denken viele, dass es sie schon nicht trifft. Was aber, wenn doch?

Wenn beispielsweise das Passwort z.B. für den Ebay-Account geklaut wurde, das zugleich vielleicht auch das Passwort für PayPal, den Facebook-Account, diverse Online-Shops und den persönlichen E-Mail-Account ist? Dann besteht die Gefahr, dass Dritte sich einloggen und mit diesen Daten unter der falschen Identität Bestellungen im Internet tätigen, Verträge abschließen, Nachrichten verschicken, Profile verändern und vieles mehr. So sind beispielsweise weltweit 145 Millionen Ebay-Nutzer registriert, hiervon sind 16,5 Millionen Deutsche als Käufer unterwegs und haben nicht nur ihre Stammdaten wie Namen, Adressen und Kontaktdaten, sondern vor allem auch Kontodaten hinterlegt. Darüber hinaus geben sie mit jedem Besuch im Internet auch ihre Interessen, ihr finanzielles Budget und die eine oder andere wertvolle Information über ihre

Foto: Shutterstock / Maksim Kabakou

Lebensumstände preis, wenn sie sich nach Kindersachen, Autoreifen, Möbelstücken etc. umsehen und mitsteigern. Wird ein Passwort geknackt, sind alle diese Informationen frei verfügbar und laden zum Missbrauch ein.

Ein schlecht gewähltes Passwort ist noch immer die meistgenutzte Sicherheitslücke im Internet, denn mittels vollautomatischer Programme, die ganze Wörterbücher und Zahlenkombinationen in Sekundenschnelle durchtesten, können Hacker zu schlecht gewählte und damit unsichere Passwörter schnell entschlüsseln.

Dieser Gefahr kann jeder Verbraucher mithilfe eines guten Passwortes und mit der Verwendung unterschiedlicher Passwörter in unterschiedlichen Lebens- und Themenbereichen entgegenwirken.

Beim Erstellen eines sicheren Passwortes sollten Sie Folgendes beachten:

Notieren Sie sich das Passwort an einem geschützten Ort, nicht auf einem Zettel am PC oder gar gesammelt in Ihrem Kalender, den Sie überall dabeihaben und leicht verlieren können. Heben Sie Ihre Passwörter an einem sicheren Ort zu Hause auf und geben Sie sie auch nicht per E-Mail, SMS etc. weiter. Achten Sie darauf, dass Sie niemals dasselbe Passwort für alle Portale nutzen. Legen Sie wenigstens für die wichtigsten und meistgenutzten Dienste eigene Passwörter, ggf. nach Lebensbereichen sortiert (Zugang zum Rechner, E-Mail, soziale Netzwerke, Shopping-Portale, Apps etc.) an. Sonst besteht die Gefahr, dass bei einem Passwortklau auch alle anderen Dienste mit Ihrem Passwort genutzt und missbraucht werden können. Je sensibler ein Zugang ist (z.B. beim Online-Banking), umso mehr Sorgfalt sollten Sie auf die Qualität des Passworts und die Sicherheit der Verschlüsselung bei der Übermittlung legen.

Bei der Gestaltung des Passwortes bauen Sie sich Eselsbrücken, indem Sie beispielsweise einen Reim oder ein Kinderlied nutzen, das Ihnen immer wieder einfallen wird und von dem Sie jeweils nur den ersten Buchstaben der einzelnen Wörter nutzen. Oder nehmen Sie zum Beispiel einen für Sie gängigen Liedtext: „99 Luftballons fliegen hoch am Horizont, 99 Luftballons.“ Als Passwort: 99LfhaH,99L.

Ändern Sie Ihre Passwörter regelmäßig; hier reicht dann auch eine kleine Umstellung oder Ergänzung um Sonderzeichen o.Ä. Je nach Umfang der von Ihnen benötigten Passwörter macht auch die Zuhilfenahme eines

Passwortmanagers wie beispielsweise „Keepass“ Sinn; so behalten Sie zum einen den Überblick und werden auch an die regelmäßige Änderung der einzelnen Passwörter erinnert. Neben der Sicherheit des Passwortes ist es besonders wichtig, dass Sie sich nach der Nutzung einzelner Dienste, wie beispielsweise der sozialen Netzwerke, Online-Shops etc. bewusst ausloggen. Die Buttons „Logout“ sind oftmals auf den Webseiten schwer zu finden; zur Sicherheit Ihrer Daten lohnt es sich, genau hinzuschauen.

UNSERE TIPPS ZUM SICHEREN PASSWORT:

- Je sensibler ein Zugang, z.B. zum Online-Banking ist, desto wichtiger sind Qualität und Sicherheit des Passwortes.
- Ein sicheres Passwort sollte mindestens 10 Zeichen lang sein.
- Ein sicheres Passwort besteht aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z.B. § & ? * !); es ist nicht im Wörterbuch zu finden oder steht in keinem Zusammenhang mit Ihnen oder Ihrer Familie. Nutzen Sie also auch keine Namen, Geburtsdaten, Telefonnummern von Verwandten, Freunden etc.
- Ein sicheres Passwort darf keine bloße Zahlenfolge (12345...) oder alphabetische Buchstabenfolge (ABCDEF...) darstellen.
- Bauen Sie sich Eselsbrücken beim Passwortbau, z.B. mit einem Liedtext.
- Notieren Sie sich Ihre Passwörter an einem geschützten Ort und geben Sie sie nicht weiter.
- Ändern Sie Ihre Passwörter regelmäßig.
- Loggen Sie sich nach jeder Nutzung eines Dienstes aus.

Ausführliche Tipps für sichere Passwörter finden Sie bei der VZ NRW [2] und auf den Seiten des Bundesamtes für Sicherheit und Informationstechnik [3] oder als Kurzfilm des Landespräventionsrates NRW [4].

[2] ***www.checked4you.de/passwortschutz***
[3] ***www.bsi-fuer-buerger.de***
[4] ***www.justiz.nrw.de/BS/praevention/zwischentext_internet_praevention/vl_passwort_phishing***

ONLINE-BANKING

Die Banken und Sparkassen bieten kostengünstige – oftmals auch kostenlose – Kontomodelle bei der Nutzung der Online-Banking-Funktionen an. Die Kunden werden aufgefordert, sich für diese Kontomodelle zu entscheiden, da sie für die Institute weniger Aufwand und entsprechend weniger Kosten bedeuten.

Der Kunde loggt sich dann mit seinem Benutzernamen und einer PIN in das Online-Banking-Programm seiner Bank oder Sparkasse ein und gibt Zahlungen mit einer Transaktionsnummer (TAN-Nummer) frei. Aber geht dies auf Kosten der Sicherheit? Missbrauchsfälle werden immer wieder publik.

Möglichst verzichten sollten Sie auf Papierlisten, die die Transaktionsnummer enthalten und vom Programm abgefragt werden. Hier kam es in der Vergangenheit vor, dass Kunden auf Zuruf mehrere Transaktionsnummern eingaben und einen Schaden erlitten. Aber auch das sog. mTAN oder smsTAN-Verfahren wurde bereits Ziel von Angriffen. Hier schleusten die Täter einen Virus auf den PC des Kunden und spionierten neben den Bankdaten dessen Mobilfunkdaten aus. Sie erhielten eine Ersatzkarte für das Handy und fingen die per SMS gesandte

Transaktionsnummer ab. Das gängigste Verfahren, das zurzeit die meiste Sicherheit bietet, ist das chipTAN-Verfahren. Hier erwirbt der Kunde einen TAN-Generator, den er gemeinsam mit seiner Girokarte zur Erzeugung einer Transaktionsnummer nutzt.

Im Umgang mit dem Online-Banking sind einige grundsätzliche Regeln zu beachten:

Seien Sie im Umgang mit Ihren Zugangsdaten vorsichtig, bewahren Sie sie wie Ihre Passwörter an einem geschützten Ort auf und verbreiten Sie die Daten nicht per E-Mail, SMS etc. Kontoinformationen haben grundsätzlich nichts in öffentlichen Portalen, sozialen Netzwerken etc. zu suchen.

Darüber hinaus ist ein sicheres Passwort für den Zugang zu Ihrem Online-Banking-Konto besonders wichtig, beachten Sie hier die Regeln zur Erstellung eines sicheren Passwortes. Wenn Sie noch mit TAN-Listen auf Papier arbeiten, bewahren Sie diese Listen sicher auf, um sie vor Diebstahl oder missbräuchlicher Verwendung durch unberechtigte Dritte zu schützen; die Kombination Ihrer Zugangsdaten mit den TAN-Nummern ermöglichen Dritten erhebliche Möglichkeiten der missbräuchlichen Verwendung.

Grundsätzlich sollten Sie Online-Banking nur aus dem heimischen Netzwerk betreiben; verzichten Sie auf ein Einloggen an öffentlichen Orten und insbesondere mittels öffentlichem WLAN, beispielsweise in Cafés und Bahnhöfen. Ihre WLAN-Verbindung sollte im heimischen Netzwerk verschlüsselt sein; standardmäßig ist dies heute per WPA 2 (Wi-Fi Protected Access 2) der Fall. Auch die Übertragung der Daten sollte beim Online-Banking immer verschlüsselt erfolgen, d.h. am Anfang der Browserzeile sollte das Schlosssymbol oder „https://“ und nicht „http://“ angezeigt werden.

Vergewissern Sie sich, dass Sie sich tatsächlich auf der Seite Ihrer Bank und nicht auf einer namensähnlichen Webseite einloggen. Hierzu sollten Sie die Internetadresse am besten jedes Mal manuell eintippen. Beim Einloggen darf noch keine TAN-Nummer abgefragt werden; erst bei Transaktionen wie Überweisungen oder der Änderung eines Dauerauftrages o.Ä. kommen diese zum Einsatz.

Einen weiteren Schutz bietet die regelmäßige Kontrolle der Kontobewegungen, vor allem auch bzgl. kleinerer Beträge. Vereinbaren Sie mit der Bank ein Tageshöchstlimit für Online-Banking-Transaktionen, um im Falle eines Datenmissbrauchs oder

Datenklaus den Schaden einzugrenzen. Beim Online-Banking ist es besonders wichtig, dass Sie sich nach der Sitzung selbstständig ausloggen.

UNSERE TIPPS ZUR SICHEREN NUTZUNG VON ONLINE-BANKING:

- Seien Sie im Umgang mit Ihren Zugangsdaten vorsichtig, bewahren Sie sie an einem geschützten Ort auf und verbreiten Sie die Daten nicht per E-Mail, SMS etc.
- Sichern Sie Ihren Computer mit einer Antivirensoftware, die stets aktuell gehalten werden sollte.
- Bewahren Sie die Listen mit Ihren TANs sicher auf, um sie vor Diebstahl oder missbräuchlicher Verwendung zu schützen.
- Schützen Sie Ihre Kontodaten und geben Sie sie nicht in öffentlichen Portalen, sozialen Netzwerken etc. preis.
- Wählen Sie ein sicheres Passwort für den Zugang zu Ihrem Online-Banking-Konto.
- Achten Sie bei der Übertragung der Daten auf die Verschlüsselung durch „https://“ oder das Schlosssymbol.
- Achten Sie auf die Verschlüsselung Ihrer WLAN-Verbindung per WPA 2 (Wi-Fi Protected Access 2).
- Nutzen Sie das Online-Banking nur im heimischen Netzwerk und nicht im offenen WLAN-Netz in Cafés, Bahnhöfen etc.
- Geben Sie die Internetadresse zu Ihrer Bank immer per Hand ein und verzichten Sie auf die Nutzung von Links per Suchmaschine o.Ä.
- Kontrollieren Sie regelmäßig Ihre Kontobewegungen und vereinbaren Sie mit der Bank ein Tageshöchstlimit für Online-Banking-Transaktionen.
- Loggen Sie sich nach einer Online-Banking-Sitzung immer aus.

RECHT AUF VERGESSEN-WERDEN – RECHT AUF LÖSCHUNG IM NETZ

Nach dem wegweisenden Urteil des EuGH im Mai 2014 zum Thema „Recht auf Vergessenwerden“ haben die Verbraucher seither das Recht, veraltete Links, die auf ihre Person verweisen, löschen zu lassen. Das Urteil bezieht sich jedoch nur auf konkrete Links und Verweise in Suchmaschinen, nicht auf die Inhalte der Seiten selbst, wie beispielsweise konkrete Zeitungsartikel, Veröffentlichungen etc. In diesem Urteil wird das Recht des Einzelnen auf Privatsphäre und Selbstbestimmtheit unter bestimmten Umständen höher bewertet als das allgemeine Interesse und Recht auf Information.

Sie haben ein Recht auf Löschung von Links mit darin enthaltenen personenbezogenen Daten zu Ihrer Person, wenn diese Informationen veraltet sind und kein öffentliches Interesse an der Information besteht. Hierzu muss eine Abwägung zwischen Ihrem Recht auf Privatheit und dem Interesse der Öffentlichkeit an umfassender Information stattfinden. So wird beispielsweise das Recht auf die Löschung von Links zu Schul- oder Abiturfotos immer höher wiegen als das öffentliche Interesse an diesen Fotos. Hingegen wird das öffentliche Interesse bei Personen

Foto: Shutterstock / Ioan Panaite

des öffentlichen Lebens aus Politik, Unterhaltung etc. grundsätzlich höher als das Recht auf Privatheit eingestuft. Personen des öffentlichen Lebens sind neben Personen der Zeitgeschichte Prominente im Allgemeinen und solche Personen, die ein öffentliches Amt bekleiden.

Es macht Sinn, regelmäßig nach dem eigenen Namen im Netz zu suchen, ggf. auch in Kombination mit passenden Schlagworten, die Sie oder Ihre Tätigkeit beschreiben (sogenanntes „Egosurfing"/„Self-Googling"). Finden Sie entsprechende Links, die auf Ihre Person verweisen und deren Inhalt veraltet ist, können Sie einen Löschantrag stellen.

Den Antrag auf Löschung einer Verlinkung müssen Sie formlos gegenüber dem jeweiligen Suchmaschinenbetreiber stellen; richtiger Adressat ist hier jeweils die deutsche Niederlassung. Im Fall von Google ist es die Niederlassung in Hamburg (Google Germany GmbH, ABC-Straße 19, 20354 Hamburg, Fax: 040-4921-9194).

Im Schreiben müssen Sie Ihre Stammdaten (Name, Adresse, Geburtsdatum) und den zu löschenden Link nennen. Darüber hinaus ist eine kurze Begründung sinnvoll, warum eben kein öffentliches Interesse an diesem Link, z.B. wegen hier enthaltener veralteter Informationen, besteht.

Wir empfehlen eine Fristsetzung von ein bis zwei Wochen zur Umsetzung des Löschantrages. Kommt der Suchmaschinenbetreiber Ihrem Wunsch nicht innerhalb der gesetzten Frist nach, wenden Sie sich an die zuständige Datenschutzaufsichtsbehörde, die für das Unternehmen im jeweiligen Bundesland zuständig ist und fordern Sie diese zum weiteren Tätigwerden auf. Einen entsprechenden Musterbrief mit den Adressen der gängigsten Suchmaschinenbetreiber finden Sie auf der Homepage der Verbraucherzentrale NRW [5].

[5] *www.vz.nrw.de/datenschutz*

UNSERE TIPPS ZUM RECHT AUF VERGESSENWERDEN:

- Begeben Sie sich im Internet auf die Suche nach sich selbst: „Egosurfing/ Self-Googling“.
- Bei veralteten Ergebnissen und Links, die Sie nicht mehr veröffentlicht wissen wollen und an denen kein öffentliches Interesse besteht, wenden Sie sich schriftlich an den jeweiligen Suchmaschinenanbieter und fordern ihn zur Löschung des entsprechenden Links auf.
- Bei Nichttätigwerden der Suchmaschinenbetreiber wenden Sie sich an die zuständigen Datenschutzbehörden (in NRW: Landesbeauftragter für Datenschutz und Informationsfreiheit).

Nordrhein-Westfalen
Kavalleriestr. 2 und 4
44013 Düsseldorf
poststelle@ldi.nrw.de

APPS

In Zeiten vom Smartphone und Tablet sind „Apps“ (englisch: Application Software = Anwendungssoftware im Bereich mobiler Betriebssysteme) als Helfer des Alltags nicht mehr wegzudenken, sei es im öffentlichen Nah- und Fernverkehr, bei der Nutzung von Messaging-Diensten, Einkaufs-, Haushalts- oder Fitnessberatern, sozialen Netzwerken und auch vielen anderen Lebensbereichen.

Apps können Sie in den verschiedenen App-Stores, wie z.B. iTunes, Google Play, Windows Phone-Store herunterladen; die Kosten hierfür sind sehr unterschiedlich. Auch wenn das Herunterladen einer App zunächst kostenlos sein sollte, bedeutet es nicht, dass der angebotene Dienst tatsächlich auch umsonst ist. Kostenlose Apps finanzieren sich in der Regel über die Verwendung Ihrer personenbezogenen Daten, die über Sie erhoben werden, und über die Auswertung Ihres Nutzungsverhaltens auf dem jeweiligen Gerät. Mit dem Herunterladen einer App werden dem Anbieter zumeist diverse Zugriffe auf bestimmte Dienste und gespeicherte Daten des Geräts, wie z.B. das Adressbuch mit allen Kontaktdaten, E-Mails oder Fotos erlaubt. Ihnen als Nutzer bleibt verborgen, zu welchem Zweck dies geschieht und was mit den abge-

griffenen Daten von Ihrem Smartphone oder Tablet passiert. Bei der Nutzung von Apps werden beispielsweise die Standort- und Bewegungsdaten des Nutzers an die App-Anbieter übertragen, wenn die Ortungsfunktion des Geräts zugleich eingeschaltet ist. In manchen Fällen, wie z.B. bei einer Navigations-App oder einer Auskunft für öffentliche Verkehrsmittel, kann die automatische Übertragung des Standorts notwendig oder praktisch sein; bei anderen, wie z.B. einer App der Hausbank, bei Spiele-Apps, Kochbuch-Apps etc. gibt es hierfür aber keinen sinnvollen Grund. Die ständige Übermittlung von Standortdaten ermöglicht detaillierte Bewegungsprofile.

Aus den Daten lässt sich erkennen, wo eine Person lebt, wo und wann sie regelmäßig arbeitet, einkauft, ihre Freizeit verbringt oder wo sie übernachtet. Es entstehen umfangreiche Nutzerprofile, die professionell vermarktet und verkauft werden und Sie und auch Ihre Kontakte zu Adressaten gezielter Werbeattacken machen.

Auf Ihrem Gerät haben Sie die Möglichkeit, die Zugriffe der Apps auf Ihre Daten zu steuern, indem Sie die Berechtigungen beschränken. Diese Funktion finden Sie je nach Betriebssystem (z.B. Android, iOS/Apple, Windows Phone) im Menü unter „Anwendungsmanager“ oder unter „Einstellungen/Apps/Berechtigungen“. Bei Apple-Geräten können Sie hier festlegen, wer sich bei Standortdaten, Fotos und weiteren Daten bedienen darf. Bei Android-Geräten finden Sie unter dem Anwendungsmanager nur die Information, auf welche Daten und Funktionen zugegriffen wird. Manuelles Einstellen ist hier nicht möglich.

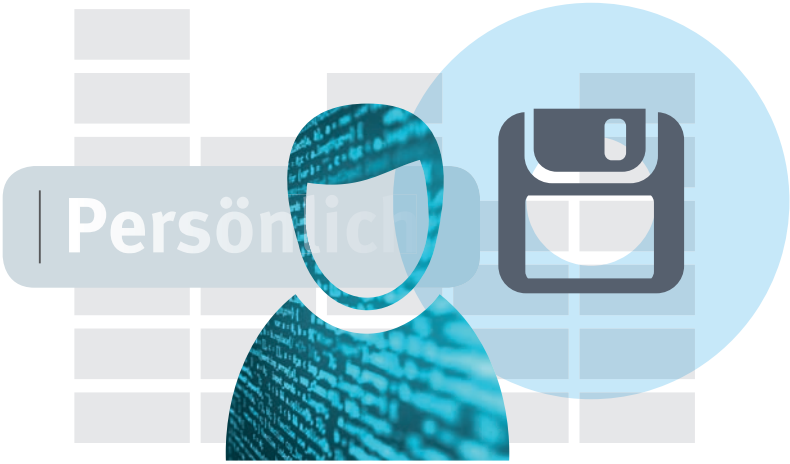
Wir raten dringend dazu, diese Einschränkungen vorzunehmen und nur dann einen Zugriff auf andere Dienste zu erlauben, wenn dies für die Funktionalität unerlässlich ist, wie beispielsweise bei einer Navigations-App und der dann notwendigen Ortungsfunktion.

UNSERE TIPPS ZUR SICHEREN NUTZUNG VON APPS:

- Nutzen Sie zum Download von Apps nur die offiziellen Stores, wie z.B. den App-Store oder den Google Play Store.
- Erhöhen Sie Ihre Privatsphäre und beschränken Sie die Berechtigungen zum Zugriff der Apps auf die Daten Ihrer Geräte unter dem Anwendungsmanager oder in den Einstellungen. Erlauben Sie nur den Zugriff auf Informationen, die für die Nutzung eines Dienstes erforderlich sind, wie die Ortungsfunktion bei Navigations-Apps.
- Schalten Sie die allgemeine Ortungsfunktion Ihrer mobilen Geräte grundsätzlich aus.

Eine anschauliche Darstellung zu diesem Thema finden Sie auf dem Portal des Jugendmagazins der Verbraucherzentrale NRW [6] sowie im Kurzfilm des Landespräventionsrates NRW [7].

[6] *www.checked4you.de/was_apps_ueber_mich_wissen_wollen*
www.checked4you.de/was_sind_eigentlich_app_berechtigungen
[7] *www.justiz.nrw.de/BS/praevention/zwischentext_internet_praevention/vl_smartphone_app*



DATENSPARSAMKEIT

Auf vielen Webseiten werden Sie aufgefordert, persönliche Daten anzugeben. Dies fängt häufig beim Namen, der Adresse und dem Geburtsdatum an, geht oftmals aber darüber hinaus und erstreckt sich dann auf Familienstand, Anzahl der Kinder, Bildungs- und Berufsabschluss und nicht zuletzt Einkommensspanne oder ähnliche sehr persönliche Angaben. Überdenken Sie in jedem einzelnen Fall, ob die abgefragten Daten an dieser Stelle wirklich erforderlich sind. Fragen Sie sich, ob es unbedingt nötig ist, in jedem Online-Shop ein Kundenkonto anzulegen oder ob es nicht auch möglich ist, als „Gast“ einzukaufen? Müssen wirklich alle Felder ausgefüllt werden oder reichen bestimmte Pflichtfelder (in der Regel mit einem Stern versehen) aus? Gibt es einen gleichen Anbieter, der weniger Daten von mir fordert und dasselbe Angebot macht? Grundsätzlich gilt: Einmal ins Netz gestellte Daten sind nahezu nicht mehr zu löschen. Viele Unternehmen lassen sich in den Allgemeinen Geschäftsbedingungen die Genehmigung ihrer Kunden geben, die einmal angegebenen Daten auch an andere Unternehmen weiterzugeben und zu verkaufen. Dieses Prozedere zeigt: Ihre Daten haben einen echten monetären Wert. Und dieser Wert Ihrer persönlichen Daten ist nicht nur für

Foto: Shutterstock / Mclek

die gezielte Werbeansprache äußerst attraktiv, sondern lädt auch zum Missbrauch durch Kriminelle ein.

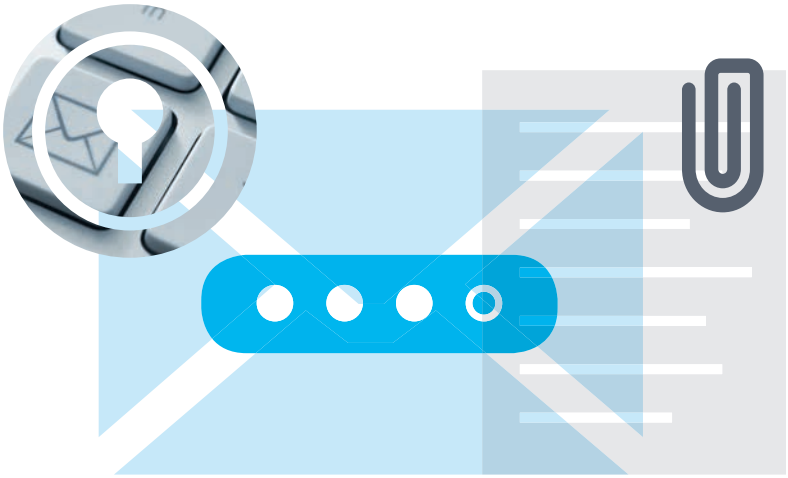
Die anhand der vielen Daten entstandenen Nutzungsprofile verändern sich stetig mit jeder Information, die neu hinzukommt. Daher ist es auch nie zu spät, datenschutzbewusst im Internet unterwegs zu sein und immer dann zu geizen, wenn es um das Preisgeben von persönlichen Informationen geht. Entsprechende Musterbriefe, mit denen Sie Auskunft über die von Ihnen gespeicherten Daten erhalten, der weiteren Erhebung und Verwendung Ihrer Daten durch ein Unternehmen widersprechen und Datensätze löschen lassen können, finden Sie auf der Homepage der Verbraucherzentrale NRW [8].

UNSERE TIPPS ZUR DATENSPARSAMKEIT:

- Was nicht da ist, kann nicht gespeichert werden. Einmal im Netz verbreitete Informationen können nicht mehr gelöscht oder zurückgeholt werden. Das Recht auf Vergessen bezieht sich nur auf das Löschen von Links.
- Beschränken Sie Ihre Angaben im Internet auf das Notwendigste. Geizen Sie bei Informationen zu Ihrem Privatleben, Interessen und finanziellem Spielraum und geben Sie niemals Passwörter und Kontoinformationen an Dritte im Netz weiter.
- Nutzungsprofile verändern sich mit jeder neuen Information. Für datensparsames Verhalten im Netz ist es daher nie zu spät; fangen Sie heute damit an.
- Das Veröffentlichen von Bildern anderer Personen ist nur mit deren Einwilligung zulässig.

Einen weiteren Überblick zum Thema Datensparsamkeit finden Sie auch beim Online-Jugendmagazin der Verbraucherzentrale NRW [9].

[8] *www.vz-nrw.de/datenschutz*
[9] *www.checked4you.de/datenschutz*



E-MAIL-DIENSTE

Die Bezeichnung E-Mail (= Electronic Mail) deckt begrifflich die elektronische Post via Internet ab. Sie bietet die Möglichkeit, Nachrichten mit Anlagen verschicken. Wichtig ist zu wissen, dass eine E-Mail einer Postkarte im realen Leben entspricht. Das heißt, ähnlich wie bei der Postkarte, kann jeder, dem sie auf dem Weg durchs Netz begegnet, sie auch lesen. Der Zustellweg einer E-Mail ist nicht immer der physikalisch kürzeste Weg; das elektronische Netz sucht sich seinen Weg selber und kann durch eine Vielzahl anderer Länder führen, auch wenn es sich um eine E-Mail innerhalb Deutschlands handelt. Dies hängt u.a. von den gewählten E-Mail-Anbietern und dem Standort der Server ab. Es gibt eine Vielzahl von Anbietern solcher „Post"-Dienstleistungen. Hier bietet sich grundsätzlich ein Leistungsvergleich an: Zahlreiche Anbieter bieten ihre Dienste kostenlos, wiederum andere gegen eine monatliche Gebühr an. Kostenlose Dienste finanzieren sich in der Regel über die Verwendung der Daten ihrer Nutzer und beispielsweise entsprechende Werbeanzeigen, jedoch auch über den Weiterverkauf der mit den Daten erstellten Nutzerprofile. Dies spricht für die Nutzung eines kostenpflichtigen Dienstes, der sich nicht mit der Vermarktung oder Verwendung

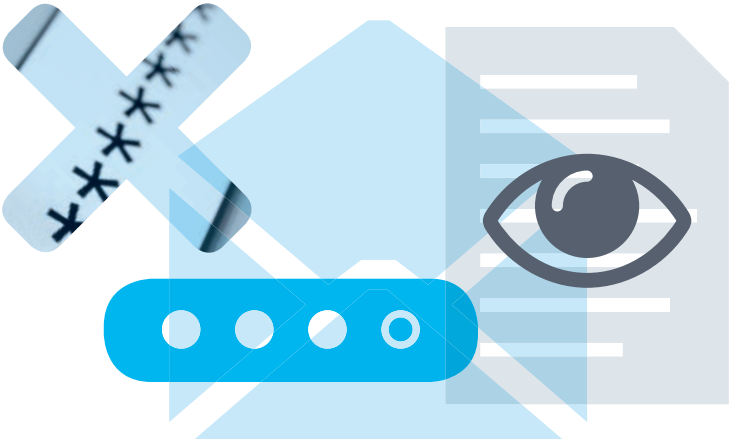
Ihrer Daten zu Werbezwecken finanziert. Hier kann von einem höheren Datenschutzniveau ausgegangen werden. So können Sie bei den infrage kommenden Anbietern prüfen, ob er in den Geschäftsbedingungen oder den Datenschutzbestimmungen zusichert, dass weder Daten erhoben noch weitergegeben oder zur Profilbildung verarbeitet werden. Achten Sie außerdem darauf, dass Ihr E-Mail-Anbieter seine Dienste verschlüsselt anbietet; dies erkennen Sie an der verschlüsselten Anmeldeprozedur („ssl“ oder Schlosssymbol). Wenn Sie ganz sicher sein wollen, dass nur der Empfänger, nicht aber beispielsweise der E-Mail-Anbieter Ihre E-Mail lesen kann, müssen Sie diese mit einem gesonderten Programm verschlüsseln. Dazu bietet sich das Programm OpenPGP an. Hier ist es jedoch notwendig, dass auch der Empfänger Ihrer Mail mit diesem Programm arbeitet, um die Mail entschlüsseln zu können.

Weitere Informationen und praktische Hilfe zum Thema „Verschlüsselung von E-Mails“ bekommen Sie im Rahmen von sog. „Crypto-Partys“. Termine unterschiedlicher Veranstalter finden Sie unter dem Stichwort „Crypto-Party“ im Internet. Der Unternehmenssitz Ihres E-Mail-Anbieters spielt ebenfalls eine entscheidende Rolle, wenn es um die Sicherheit Ihrer Daten geht. Beim Unternehmenssitz in Deutschland ist deutsches Recht anwendbar; damit können Sie von einem höheren Datenschutzniveau und damit verbunden auch von mehr Sicherheit für den ordnungsgemäßen Umgang mit ihren E-Mails ausgehen als in anderen Staaten, wie z.B. in den USA. Legen Sie entsprechend Wert auf die Auswahl Ihres E-Mail-Anbieters und dessen Unternehmenssitzes.

Ein weiteres wichtiges Phänomen beim Thema E-Mails ist das Thema Phishing-Mails.

UNSERE TIPPS ZU E-MAIL-DIENSTEN:

- Seien Sie sich der Risiken bei der Verwendung von E-Mails bewusst; verschicken Sie keine hochsensiblen Informationen wie Bankinformationen, Passwörter o.Ä. auf diesem Wege.
- Wägen Sie Kosten und Risiken eines kostenlosen mit einem kostenpflichtigen Anbieter ab. Kostenpflichtige Anbieter sollten Ihnen zusichern, dass keinerlei personenbezogene Daten erhoben und verwendet werden.
- Bedenken Sie bei der Wahl eines E-Mail-Anbieters dessen Unternehmenssitz.



SPAM- UND PHISHING-MAILS

Nicht nur der heimische Briefkasten ist oft mit Werbung verstopft, auch der elektronische Briefkasten wird immer mehr zugemüllt. Unerwartete und unbestellte E-Mails werden umgangssprachlich auch als „Spam“ bezeichnet. Während Sie Werbung im heimischen Briefkasten gefahrlos öffnen und unkompliziert entsorgen können, müssen Sie sich in der digitalen Welt schützen, denn hier begegnen Ihnen Spam, Viren, trojanische Pferde, Phishing und viele andere Gefahren, die Ihre persönlichen Daten und Ihr Geld abgreifen wollen.

Spam, also unerwartete elektronische Post, gibt es in ganz verschiedenen Formen. Neben der klassischen Werbe-Spam-Mail, die zwar ärgerlich, aber ungefährlich ist, sind Varianten häufig verbreitet und mit hohen Sicherheitsrisiken verbunden:

Phishing-Mails – Phishing ist ein englischer Begriff für „Passwort-Fischen“. Das Bundesamt für Sicherheit in der Informationstechnik [10] erläutert den Begriff als Kunstwort aus „Passwort“ und „Fishing“. Er bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu werden häufig Methoden

[10] *www.bsi.de*

Foto: Shutterstock / JMiks

des Social Engineering, teilweise in Verbindung mit Identitätsdiebstahl, verwendet. Beispielsweise können die Angreifer geschickt formulierte E-Mails an die Benutzer senden. Unter „Social Engineering“ versteht man alle kriminellen Methoden, die die Verbraucher mittels zwischenmenschlicher Beeinflussung dazu bewegen, vertrauliche Informationen preiszugeben.

Den Kriminellen geht es darum, Sie dazu zu bringen, persönliche Daten wie beispielsweise PIN, Girokontonummer oder Kreditkartennummer mitzuteilen. Die Phishing-E-Mail wird so konstruiert, dass sie Vertrauen schafft und den Eindruck erweckt, von einem seriösen Absender zu stammen. Sie erkennen Phishing-Mails häufig jedoch an der Fehlerhaftigkeit der deutschen Sprache in den Texten, da die Texte aus dem Ausland mittels automatisierter Übersetzungsprogramme versendet werden. Weiteres Erkennungsmerkmal ist eine gefälschte Absenderadresse, d.h. die Adresse, die zu sehen ist, stimmt nicht mit der Adresse überein, die im Header steht. Was der Header ist und wie Sie diesen einsehen können, erläutert die Verbraucherzentrale NRW [11].

In der Praxis sehen Phishing-Mails so aus, dass sich jemand als Absender eines tatsächlich existierenden Unternehmens ausgibt – beispielsweise eine Bank, ein Kreditkartenunternehmen etc., und versucht, Sie zur Eingabe von persönlichen Daten zu bewegen. Die Liste der Unternehmen, deren Namen in Phishing-Mails missbraucht werden, reicht von Sparkassen über MasterCard bis hin zu PayPal, Telekom, Lidl und Real, von der Postbank über Commerzbank, Deutsche Bank, Visacard bis hin zu Amazon, Ebay, Tchibo etc. Die Kriminellen schreiben inzwischen auch E-Mails im Namen eines Bundes- oder Landesministeriums oder einer sonstigen nationalen oder internationalen öffentlichen Institution.

Bereits die Ansprache der Adressaten der E-Mail ist oftmals vertrauenerweckend, da sie mit vollständigem Namen angesprochen wird und ggf. noch weitere korrekte Informationen, wie Kundennummer, Bankverbindung o.Ä. in der E-Mail genannt werden. Nachdem der Grund für die Versendung der E-Mail erklärt wurde, wie z.B. die Klärung von Unstimmigkeiten auf einem Kundenkonto o.Ä., geht es jetzt darum, dass der E-Mail-Empfänger aktiv werden soll. In der Regel soll er seine Daten erneut eingeben, kontrollieren, bestätigen oder verifizieren und dies oft innerhalb einer kurzen Frist. Bei Nichthandeln werden schwere Konsequenzen angedroht, wie die Einschränkung oder gar Sperrung

[11] *www.vz-nrw.de/phishing*

des Kundenkontos. Die Dateneingabe soll zumeist über einen in der E-Mail hinterlegten Link erfolgen, der zu einer nachgebauten Internetseite des in der Mail genannten Unternehmens führt.

Eine neuerdings stark verbreitete Unterart der Spam-Mails zeichnet sich durch die Ankündigung eines lukrativen neuen Jobs, eines unerwarteten Gewinns oder einer Erbschaft aus. Diese Mails beinhalten immer ein attraktives Geldversprechen. Die Kriminellen wollen hier in der Regel an die persönlichen Daten des E-Mail-Empfängers und im Anschluss an dessen Geld kommen, indem sie zur Angabe von Bankdaten etc. auffordern. Grundsätzlich macht es immer Sinn, mehrere E-Mail-Adressen zu nutzen, damit nicht alle Bereiche Ihres Lebens betroffen sind, wenn Sie eine E-Mail-Adresse löschen müssen, weil beispielsweise der Anteil der Spam-Mails unzumutbar hoch ist.

Trojanisches Pferd („Trojaner“) – Diese E-Mails unterscheiden Sie von den Phishing-Mails dadurch, dass als Grund für die E-Mail oftmals ein erfundener Kauf, eine vermeintliche Bestellung, eine fiktive Mitgliedschaft oder eine angebliche Mahnung angegeben wird. Entsprechend sind Absender neben bekannten Unternehmen oftmals auch Anwaltskanzleien oder Inkassounternehmen. Der E-Mail-Empfänger wird beispielsweise aufgefordert, umgehend einen noch offen stehenden Betrag zu begleichen. Im Gegensatz zum Phishing wollen die Absender der E-Mail Sie hier nicht dazu bewegen, Ihre Daten auf einer vorbereiteten Seite einzutragen. Sie wollen Sie vielmehr dazu bringen, einen mitgelieferten Datei-Anhang – oft im ZIP-Format – zu öffnen. Grundsätzlich muss die Datei aber nicht zwangsweise auf „zip“ enden, Schadprogramme können sich auch hinter anderen Formaten wie zum Beispiel „rar“ verbergen.

Beim Trojaner wird der E-Mail-Empfänger aufgefordert, den Anhang zu öffnen, um die Daten zu kontrollieren. In der Regel wird bei kurzer Fristsetzung mit einem Rechtsanwalt, einer gerichtlichen Klage oder einem Inkassobüro gedroht. In diesem Anhang ist dann ein Schadprogramm enthalten, ein Virus oder ein trojanisches Pferd. Einmal installiert, verschafft sich das Programm den kriminellen Zugang zu Ihrem Computer und zu den mobilen Endgeräten. Mit der Installation eines Schadprogramms werden unterschiedliche Szenarien möglich, die letztlich zunächst Ihre persönlichen Daten wie dann auch Ihr Vermögen gefährden. Ein Schadprogramm kann den gesamten Rechner bzw. das mobile Endgerät nach Passwörtern und Zugangsdaten

absuchen und diese an die Kriminellen senden. Nach Installation eines Schadprogramms kann jede Tastatureingabe protokolliert und weitergegeben werden. Auf diese Weise wird ein sog. „Identitätsklau“, beispielsweise in sozialen Netzwerken, möglich. Dies ist nur eine kleine Auswahl dessen, was für Kriminelle möglich ist, wenn sie die Kontrolle über Ihre Geräte übernommen haben.

Es gilt daher, besondere Achtsamkeit an den Tag zu legen. Seien Sie bei der Überprüfung des Absenders einer E-Mail gewissenhaft und prüfen Sie sie auf korrekte Schreibweise. Öffnen Sie niemals Anhänge in E-Mails von Ihnen unbekannten Absendern. Grundsätzlich sollten Sie in E-Mails niemals auf Links klicken. Sollten Sie E-Mails als Spam-Mails identifizieren, antworten Sie auf diese Mails nicht. Die Verbraucherzentrale NRW führt seit Dezember 2010 das sogenannte Phishing-Radar und stellt diese E-Mails anonymisiert in das Phishing-Forum [12] ein. Zusätzlich prüft die Verbraucherzentrale bei Phishing-E-Mails, die einen Link enthalten, ob die betrügerische Seite gesperrt werden muss. Leiten Sie sie an phishing@vz-nrw.de und – wenn möglich – zusätzlich an den echten Anbieter weiter und löschen Sie sie anschließend. Denken Sie an Ihre Mitbürger, die solche E-Mails nicht als Betrug erkennen. Mit der Weiterleitung helfen Sie, vor solchen kriminellen Machenschaften zu warnen und ermöglichen zusätzlich die schnellere Sperrung betrügerischer Internetseiten.

Wenn Sie eine Phishing-Mail nicht als solche erkannt haben und auf die Machenschaften der Kriminellen hereingefallen sind, gilt es zu handeln: Sperren Sie sofort die betroffenen Konten und Karten. Aktualisieren Sie sofort das Antivirenprogramm Ihres Rechners, und führen Sie im Anschluss einen Virenscan durch. Schließlich bleibt Ihnen noch die Möglichkeit, sich an einen Fachmann zu wenden, der den Rechner auf Viren überprüft. Ändern Sie Ihre Passwörter und Sicherheitsfragen. Informieren Sie Freunde, Bekannte und Geschäftspartner, da die Gefahr besteht, dass kriminelle Dritte Mails in Ihrem Namen versenden. Und nicht zuletzt: Erstatten Sie Strafanzeige bei der Polizei. Löschen Sie in diesem Fall keineswegs die betreffenden E-Mails, auf die Sie hereingefallen sind, da diese als Beweismittel dienen.

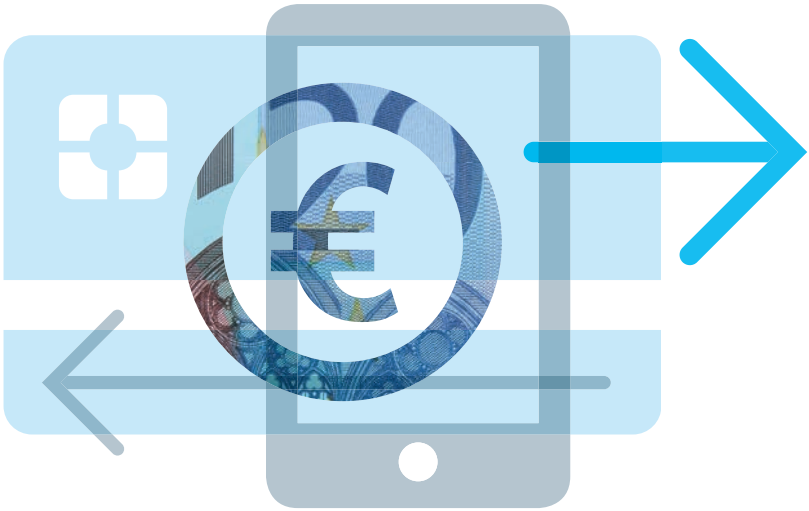
[12] *www.vz-nrw.de/phishing*

UNSERE TIPPS ZU SPAM- UND PHISHING-MAILS:

- Öffnen Sie niemals Datei-Anhänge in E-Mails unbekannter Absender.
- Klicken Sie niemals auf Links in E-Mails.
- Antworten Sie nicht auf Spam-und Phishing-Mails.
- Leiten Sie betrügerische E-Mails an phishing@vz-nrw.de und an den echten Anbieter weiter.
- Halten Sie das Virenschutzprogramm, den Internetbrowser und das Betriebssystem stets auf dem aktuellen Stand.
- Nutzen Sie mehrere E-Mail-Adressen für unterschiedliche Lebensbereiche..

Aktuelle Warnungen und allgemeine Hinweise zu Phishing-Mails erhalten Sie auf der Webseite der Verbraucherzentrale NRW [13] und in den Kurzfilmen des Landespräventionsrates NRW [14].

[13] [14] *www.justiz-nrw.de/BS/praevention/zwischentext_internet_praevention/vl_email_sicherheit*



MOBILE PAYMENT

Mittlerweile können Sie kleinere Geldtransaktionen auch mit mobilen Endgeräten, wie zum Beispiel dem Smartphone, vornehmen. Dies spielt im Alltag etwa beim Kauf von Fahrkarten im öffentlichen Nahverkehr oder beim Überweisen von kleinen Spendenbeträgen eine Rolle. Gerade bei geringen Beträgen ist die Bezahlung mit einem mobilen Gerät eine komfortable Lösung.

Für Smartphones bieten einzelne Bezahldienstleister wie etwa PayPal eigene Apps an, über die Zahlungen abgewickelt werden können. Auf diese Art und Weise lassen sich auch Zahlungen von Anwender zu Anwender auslösen. Oft können auch innerhalb einer App Käufe ausgeführt werden, die genau wie die Kosten für die App selbst über den Betreiber des App-Stores abgewickelt werden. So wird es innerhalb einer App unproblematisch möglich, z.B. in einer Tageszeitungs-App die neue Ausgabe oder sonstige zusätzliche Funktionalitäten bestimmter Apps zu kaufen.

Wir raten Ihnen generell, beim Einkaufen im Internet wie beim Online-Banking darauf zu achten, dass alle Daten über eine sichere SSL-Verbindung verschlüsselt übertragen werden – sowohl

Ihre persönlichen Angaben als auch alle Informationen zu Bankverbindungen oder Kreditkarteninformationen. Dies erkennen Sie daran, dass in der URL-Zeile Ihres Browsers statt „http“ nun „https“ bzw. ein Schlosssymbol am Anfang der Webadresse angezeigt wird. Die Zugangsdaten beim Mobile Payment sollten Sie wie beim Online-Banking nicht an Dritte weitergeben und mit höchster Vertraulichkeit behandeln. Da sich das Mobile-Payment vor allem im Alltag und bei kleineren Beträgen durchsetzt, ist eine stetige Überprüfung der Abbuchungen von Ihrem Bankkonto besonders wichtig. Bei Ihnen unbekannten Transaktionen nehmen Sie sofort Kontakt mit dem Anbieter auf. Weitere Informationen finden Sie auf der Seite des BSI [15].

UNSERE TIPPS ZU MOBILE-PAYMENT:

- Seien Sie im Umgang mit Ihren Zugangsdaten zu Ihren Konten vorsichtig, bewahren Sie sie an einem geschützten Ort auf und verbreiten Sie die Daten nicht per E-Mail, SMS etc.
- Überprüfen Sie auch bei seltener Nutzung regelmäßig die Vorgänge und Abbuchungen auf Ihrem Konto.

[15] *www.bsi-fuer-buerger.de/BSIFB/DE/MobileSicherheit/Bezahlenmobil/bezahlen_mit_mob_Geraeten_node.html*

PSEUDONYME

Ein Pseudonym ist ein fingierter Name einer Person. Dies wird im Internet vielfach genutzt, um die Privatsphäre in bestimmten Lebensbereichen zu erhalten und einen direkten Bezug zur realen Person zu erschweren. Pseudonyme sind im Internet zulässig und im Telemediengesetz gesetzlich verankert (§ 13 TMG).

Auf vielen Plattformen ist die Einrichtung eines Accounts unter einem Pseudonym möglich. Wir raten grundsätzlich zur Nutzung von Pseudonymen, sofern der jeweilige Anbieter dies erlaubt und die Angabe der Echtdaten nicht erforderlich ist, wie beispielsweise bei den Online-Spielen. Es erschwert das Erstellen von Nutzungsprofilen erheblich und stellt damit eine umsetzbare und realistische Maßnahme zum Schutz der Privatsphäre dar. Beim Online-Shopping hingegen ist die Angabe von Echtdaten unerlässlich.

UNSERE TIPPS ZUR NUTZUNG VON PSEUDONYMEN:

- Wägen Sie ab, in welchen Fällen Sie mit Ihrem Klarnamen und damit echten Daten und wann Sie unter Pseudonym im Netz unterwegs sind. Wenn keine Authentifizierung notwendig ist, reicht ein Pseudonym
- Bei manchen Anbietern werden Pseudonyme nicht akzeptiert; in diesem Fall ist der Klarname mit entsprechenden weiteren Echtdaten erforderlich.

SOZIALE NETZWERKE

Soziale Netzwerke haben in den vergangenen Jahren massiv an Bedeutung gewonnen und sind für sog. „Digital Natives“ aus der alltäglichen Kommunikation nicht mehr wegzudenken. Sie stellen eine Form von Netzgemeinschaften (Online-Communities) dar, die technisch durch Webanwendungen oder Portale abgebildet werden. Soziale Netzwerke sind unter anderem Google+, Xing, Flickr, LinkedIn und der Marktführer Facebook mit rund einer Milliarde Nutzern weltweit.

Die Funktionen dieser Portale sind vielfältig. Sie bieten neben dem üblichen persönlichen Profil die Möglichkeit, zahlreiche persönliche Informationen und auch Fotos und Dokumente, wie Lebenslauf, Zeugnisse etc. zu hinterlegen. Beliebt sind vor allem die unterschiedlichen Arten des Austauschs per Nachricht, Chat, Blog oder via Statusmeldungen, Timeline etc.

Auch eine Vernetzung der Online-Spiel-Aktivitäten ist möglich. Für alle diese Funktionalitäten kann ein Netzwerk von Kontakten mit entsprechenden Kontaktinformationen angelegt und gepflegt werden.

Sie selbst können über die Einstellungen die Adressaten Ihrer Aktivitäten

bestimmen und auch den Grad der Öffentlichkeit Ihres Profils festzulegen. Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen und nutzen Sie in den Einstellungen die Möglichkeit, der Verwendung und Weitergabe Ihrer Daten zu widersprechen. Dies bezieht sich auch auf die Verwendung Ihrer Daten gegenüber Ihren „Freunden“ im jeweiligen Netzwerk.

In den sozialen Netzwerken ändern sich die Allgemeinen Geschäftsbedingungen häufig; hier lohnt sich daher ein Blick auf die Webseite der Verbraucherzentrale NRW und ins Online-Magazin Checked4you, die über die Änderungen aufklären und konkrete Praxistipps geben.

Grundsätzlich gilt es bei der Aktivität in sozialen Netzwerken, jede eingestellte Information inklusive veröffentlichter Bilder zu hinterfragen. Will ich diese Information, dieses Bild dauerhaft, für immer im Netz gespeichert und abrufbar wissen?

Und nicht nur beim Einstellen von Informationen zahlt sich Besonnenheit aus; auch bei der Bestätigung von Kontaktanfragen seien Sie aufmerksam, denn Kriminelle „sammeln“ Freunde, um diesen Personen mit den gewonnenen Informationen zu schaden. Wenn Sie „zweifelhafte“ Anfragen im sozialen Netzwerk erhalten, erkundigen Sie sich außerhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachricht bzw. Anfrage. Eine anschauliche Darstellung der Nutzen und Gefahren sozialer Netzwerke finden Sie im Kurzfilm des Landespräventionsrates NRW [16], weitere Tipps auf der Homepage des BSI [17]. Praxistipps zu den Einstellungen bei Facebook finden Sie auf den Seiten des Checked4You-Magazins der Verbraucherzentrale NRW [18].

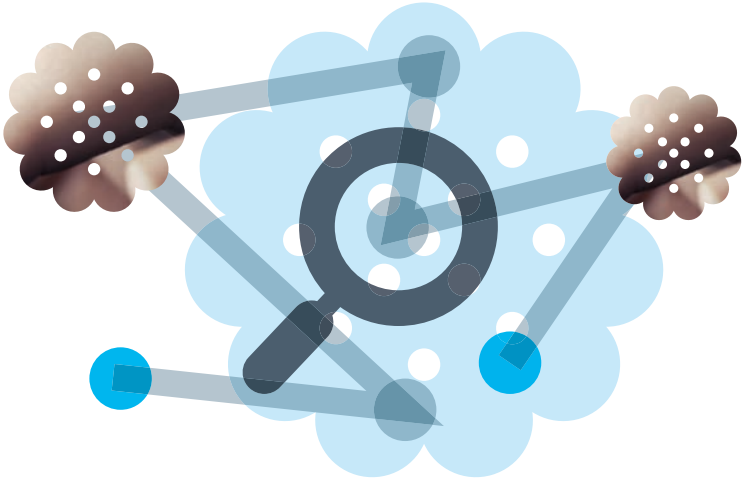
[16] *www.justiz.nrw.de/BS/praevention/zwischentext_internet_praevention/vl_account_takeover*
[17] *www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/SozialeNetze/sozialeNetze_node.html*
[18] *www.checked4you.de/werbung auf facebook*
www.vz-nrw.de/datenschutz

UNSERE TIPPS ZU SOZIALEN NETZWERKEN:

- Seien Sie zurückhaltend mit der Preisgabe persönlicher Informationen!
- Erkundigen Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Netzwerks und nutzen Sie die Möglichkeiten in den Einstellungen, Ihre Daten zu schützen.
- Prüfen Sie Kontaktanfragen auf Echtheit des Absenders und Seriosität.
- Melden Sie „Cyberstalker“, die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren, an das jeweilige soziale Netzwerk.
- Verwenden Sie für verschiedene soziale Netzwerke unterschiedliche und sichere Passwörter.
- Sprechen Sie mit Ihren Kindern über deren Aktivitäten in sozialen Netzwerken und klären Sie sie über die Gefahren auf.
- Klicken Sie nicht wahllos auf Links – soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben!

Aktuelle Mitteilungen und Praxistipps finden Sie regelmäßig im Online-Magazin Checked4you und auf der Homepage der Verbraucherzentrale NRW [19].

[19] *www.checked4you.de/werbung auf facebook*
www.vz-nrw.de/datenschutz



COOKIES

„Unsere Seite nutzt Cookies, um Ihnen ein optimales Surferlebnis zu bieten“, mit diesen oder vergleichbaren Worten weisen viele Internetseiten auf den Einsatz von sog. „Cookies“ hin.

Unter „Cookies“ versteht man kleine Textdateien, die beim Besuch einer Webseite auf Ihrem Gerät platziert werden und beim nächsten Besuch ebendieser Webseite Informationen zu Ihnen an die entsprechenden Unternehmen übermitteln. Innerhalb dieser Textdatei können Daten wie Nutzereingaben, E-Mail, Passwort, IP-Adresse, Spracheinstellungen, Warenkorbinhalte usw. gespeichert und später ausgelesen werden. So werden Sie bei wiederholtem Besuch einer Seite wiedererkannt und diese Internetseite kann sich an getroffene Eingaben, wie z.B. Waren im Warenkorb, „erinnern“.

Cookies werden zum einen von den Unternehmen, deren Seiten Sie besuchen, zeitgleich jedoch auch von einer Vielzahl anderer Unternehmen, sog. Drittanbieter, platziert. Der Umfang der übertragenen Daten und insbesondere der Vielzahl der Unternehmen, die diese Daten automatisch erhalten, bleibt dem Nutzer verborgen. Mithilfe von Cookies wird es so möglich, das Surfverhalten jedes Nutzers über Jahre

Foto: Shutterstock / wrangler

zu verfolgen (sog. Tracking). Sowohl die besuchten Seiten als auch die konkreten Inhalte und somit Interessenschwerpunkte, Bildungsstatus, finanzielle Hintergründe, wie auch Häufigkeit und Dauer von Internetbesuchen des einzelnen Nutzers werden hier transparent. Mittels „Web Analytics“ werden diese Informationen über das Verhalten des Nutzers ausgewertet. Werden diese Informationen zusammengefügt und u.a. zu Werbezwecken professionell vermarktet, spricht man von Profilbildung (engl.: Profiling). Je detaillierter sich ein solches Profil darstellt, umso höher ist der monetäre Wert des jeweiligen Nutzerprofils.

Beim Surfen im Internet gibt es jedoch mehrere Möglichkeiten, einem solchem „Tracking“ vorzubeugen bzw. es deutlich zu reduzieren:

In den Einstellungen Ihrer Geräte können Sie diverse Einschränkungen vornehmen, mit denen Sie Cookies verwalten und reduzieren können. Löschen Sie regelmäßig die Cookies auf allen Ihren Geräten in den Browsereinstellungen unter „Datenschutz“ oder „Inhaltseinstellungen“, d.h. bestenfalls nach jedem Surfen im Netz, mindestens jedoch einmal monatlich. Alternativ zum manuellen Löschen können Sie in Ihrem Browser unter „Einstellungen/Datenschutz“ einstellen, dass die Cookies nach jeder Sitzung automatisch gelöscht werden. Wer nach jeder Internetsitzung seine Cookies löscht, sorgt dafür, dass die Drittanbieter bei jeder neuen Sitzung einen neuen Cookie setzen müssen. Eine dauerhaftes Tracking und die Analyse Ihrer Daten kann somit nicht mehr erfolgen. Einziger Nachteil zulasten der Bequemlichkeit ist, dass ein Eingeloggt-Bleiben in den unterschiedlichen Diensten, wie den sozialen Netzwerken, Online-Shops o.Ä. über eine Sitzung hinaus nicht mehr möglich ist und Sie sich jedes Mal neu einloggen müssen. Hierzu raten wir ohnehin, um einen Missbrauch Ihrer Online-Zugänge durch unbefugte Dritte zu vermeiden.

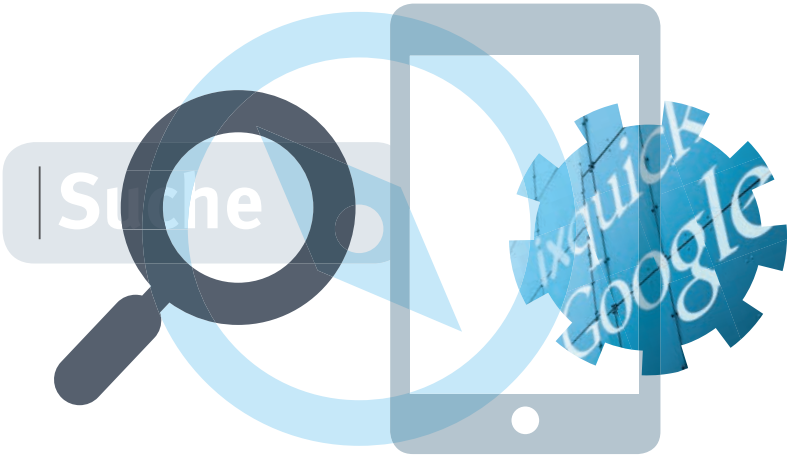
Wir empfehlen außerdem in den Einstellungen unter dem Menüpunkt „Datenschutz“/„Cookies von Drittanbietern akzeptieren“ die Optionen „nie akzeptieren“ zu wählen bzw. für Safari-Nutzer unter dem Menüpunkt „Cookies blockieren“ die Option „Von aktueller Website erlauben“ auszuwählen. Die Wahl der Optionen „Cookies akzeptieren“ und „Immer blockieren“ macht keinen Sinn, da beispielsweise die Funktion eines Warenkorbs beim klassischen Online-Shopping über einen Cookie funktioniert und damit dann auch ausgeschaltet ist.

Um einen Eindruck über die Vielzahl der Unternehmen zu bekommen, die beim Besuch jeder einzelnen Webseite Cookies platzieren, empfehlen wir die Installation eines kostenlosen Anti-Tracking-Programms, wie z.B. „no-script“. Ein solches Programm zeigt beim Öffnen einer Seite zum einen die Vielzahl der Unternehmen an, die einen Cookie setzen wollen. Darüber hinaus verhindert es aber auch, dass diese Unternehmen ihre Cookies setzen können; stattdessen haben Sie hier die Wahl zu entscheiden, welche Unternehmen die Daten über Ihr Surfverhalten erhalten sollen.

In der Kombination der oben dargestellten Verwaltung Ihrer Einstellungen zu den Cookies und der Installation eines Anti-Tracking-Programms können Sie den maximalen Schutz Ihrer Nutzerdaten erreichen. Sofern Ihr Browser die Option des anonymen Modus, auch „Inkognito-Modus“ genannt, anbietet, ist eine Nutzung dieser Option empfehlenswert. Die in einigen Browsern befindliche Option „Do Not Track“ bietet leider nur begrenzten Schutz, da es sich hierbei bisher um eine unverbindliche Empfehlung an die Unternehmen, die Nutzer nicht zu „tracken“ und keine Daten zu erheben, handelt.

UNSERE TIPPS ZU COOKIES:

- Löschen Sie regelmäßig über die Browsereinstellungen die gespeicherten Cookies auf Ihren Geräten oder stellen Sie Ihren Browser so ein, dass die Cookies nach jeder Sitzung automatisch gelöscht werden.
- Verwalten Sie Ihre Cookies in den Einstellungen Ihrer Geräte und schränken Sie die zum Cookie-Setzen berechtigten Webseiten ein.
- Installieren Sie ein Anti-Tracking-Programm, wie z.B. no-script.



SUCHMASCHINEN

Die Nutzung von Suchmaschinen ist sowohl bei der beruflichen Recherche als auch im privaten Leben nicht mehr wegzudenken. Suchmaschinen dienen der ersten Information, dem Vergleich von Preisen und Angeboten, der Suche nach Ansprechpartnern zu Themen aller Art. Der Konkurrenzkampf zwischen den Suchmaschinenbetreibern nimmt stetig zu; Marktführer ist weltweit derzeit das US-Unternehmen Google, das auch den Begriff des „googelns“ geprägt hat.

Bei der Nutzung von Suchmaschinen ist genaues Hinsehen wichtig: Die Suchmaschinen zeigen Ihnen neben den klassischen Suchergebnissen auch Werbung, die oftmals nur schwer zu erkennen ist. So werden hier Links angezeigt, die entweder als Anzeigen durch entsprechende farbliche Hinterlegung kenntlich gemacht werden oder an der Seite als Werbeanzeigen aufgeführt werden. Hierfür zahlen die jeweiligen Unternehmen an die Suchmaschinenbetreiber, es handelt sich also um Werbung im klassischen Sinne. Durch die Verwendung von Cookies sind diese Anzeigen oder Verlinkungen in der Regel auf den jeweiligen Adressaten und sein Nutzerprofil zugeschnitten, d.h. Sie bekommen entsprechend den letzten Internetrecherchen passende

Angebote präsentiert. Daher haben die Suchmaschinenbetreiber großes Interesse an der Speicherung und Verwendung möglichst vieler Informationen über ihre Nutzer, um sehr zielgerichtete und damit finanziell interessantere Werbeanzeigen schalten zu können. Die angezeigten Ergebnisse bei der Nutzung einer Suchmaschine stellen also keine neutralen Ergebnisse dar, sondern ergeben sich aus der Auswertung Ihres bisherigen Internetverhaltens. Wir raten daher zur Nutzung unterschiedlicher Suchmaschinen wie Startpage, Ixquick etc. Wir empfehlen vor allem die Nutzung von sog. Metasuchmaschinen, wie „Ixquick“, die keinerlei Nutzerdaten generiert und verarbeitet, oder „Startpage“, die zwar auf die Ergebnisse der Suchmaschine Google zurückgreift, sich zugleich aber technisch vor der Google-Webseite platziert und ohne die Übermittlung von Nutzerdaten Suchergebnisse generiert.

Das regelmäßige Löschen der Cookies auf Ihren Geräten verhindert ebenfalls, dass nur noch auf Ihr Nutzerprofil gefilterte Ergebnisse angezeigt werden, da ohne die Cookies weniger detaillierte Profile von Ihnen und Ihrem Surfverhalten angelegt werden können.

Ein weiterer Gesichtspunkt ist der Unternehmenssitz des von Ihnen favorisierten Suchmaschinenbetreibers. Bei einem Unternehmenssitz im Deutschland/Europa ist deutsches/europäisches Recht anwendbar; damit wird Ihnen mit dem in Deutschland geltenden hohen Datenschutzniveau ein hohes Sicherheitsniveau bzgl. des ordnungsgemäßen Umgangs mit Ihren Daten zugesichert. Bei einem außereuropäischen Unternehmenssitz z.B. in den USA ist eine Durchsetzung von Datenschutzrechten bei Missbrauch etc. faktisch unmöglich.

UNSERE TIPPS ZUR SICHEREN NUTZUNG VON SUCHMASCHINEN:

- Nutzen Sie nicht nur eine Suchmaschine, wie z.B. Google, sondern nutzen Sie unterschiedliche Anbieter, wie z.B. Startpage, Ixquick, Metager.
- Überdenken Sie die Wahl Ihres favorisierten Suchmaschinenbetreibers. Bedenken Sie dabei auch den Unternehmenssitz des Anbieters.
- Löschen Sie regelmäßig die Cookies auf allen Ihren Geräten.

WEITERE AKTUELLE INFORMATIONEN FINDEN SIE AUF DEN SEITEN DER VERBRAUCHERZENTRALE NRW [20].

Hier gibt es auch Musterbriefe zu folgenden Themen:

- Auskunft über meine gespeicherten Daten
- Widerspruch gegen die Verwendung meiner personenbezogenen Daten
- Aufforderung zur Löschung gespeicherter personenbezogener Daten
- Antrag auf Löschen eines Links bei einem Suchmaschinenbetreiber

[20] *www.vz-nrw.de/datenschutz*
www.checked4you.de

IMPRESSUM

Herausgeber
Verbraucherzentrale NRW e.V.
Mintropstr. 27
40215 Düsseldorf

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Für den Inhalt verantwortlich:
Sabine Petri, Bereich 1, Markt und Recht
Verbraucherzentrale NRW e.V.,
Polizei NRW Landeskriminalamt

Gestaltung: neues gestalten
Druck: Druck & Verlag Kettler

Stand: Januar 2016, 2. Auflage
Gedruckt auf 100 Prozent Recyclingpapier

verbraucherzentrale
Nordrhein-Westfalen