Medien.Wissen

IHR KOMPASS IN DER DIGITALEN WELT

AUSGABE 01/2022

WEITERBILDUNG WIRKT
Matthias Jax (im Bild) kennt die Challenges der Digitalisierung und weiß: Bildung lohnt sich.

SEITE 06

BEQUEMES BEZAHLEN
Kontaktlos statt Cash – das ist beim Mobile Payment die Devise. Die Trends im Überblick.

SEITE 18

SURFEN, ABER SICHER
Schadsoftware und Viren gehören zu den Risiken im Internet. Wissen schützt.

SEITE 22

Das Medium oder der Vorgang unserer Zeit – **die elektrische Technik** – formt und strukturiert die Muster gesellschaftlicher Beziehungen und alle Aspekte unseres Privatlebens um.

Marshall McLuhan in „Understanding Media: The Extension of Man" (1964)

LIEBE LESERINNEN UND LESER!

Haben Sie das Gefühl, dass die Welt immer komplexer wird und es zunehmend schwierig ist, den Überblick zu behalten? Dann sind Sie nicht allein – auch mir geht es oft so. Falsche Informationen und Verschwörungsmythen rund um die Coronavirus-Pandemie oder eine scheinbar ungefilterte Online-Nachrichtenflut mit Kriegsbildern aus der Ukraine: Für viele sind diese Entwicklungen und Berichte überwältigend. Unsere Gehirne laufen auf Hochtouren, um mit dieser Überforderung umzugehen. Hilfreich ist dabei zu verstehen, wie das Internet funktioniert und wie Medien arbeiten. Schauen wir deshalb gemeinsam neugierig und mutig hin!

Die Wiener Zeitung Mediengruppe will Bürgerinnen und Bürger beim richtigen Umgang mit Medien und Informationen unterstützen. Wir möchten allen, die das Internet nutzen, Hintergrundwissen und damit Sicherheit geben. Ob Nachrichtenkonsum, Online-Shopping oder die digitale Beantragung eines Reisepasses – wer versteht, wie Services funktionieren, nutzt diese auch risikobewusster.

In der ersten Ausgabe des Magazins „Medien.Wissen", die Sie in Händen halten, richten wir unseren Fokus auf die Funktionsweise sowie den Nutzen des „Digitalen Amts". Ich wünsche Ihnen spannende Einblicke!

MARKUS GRAF

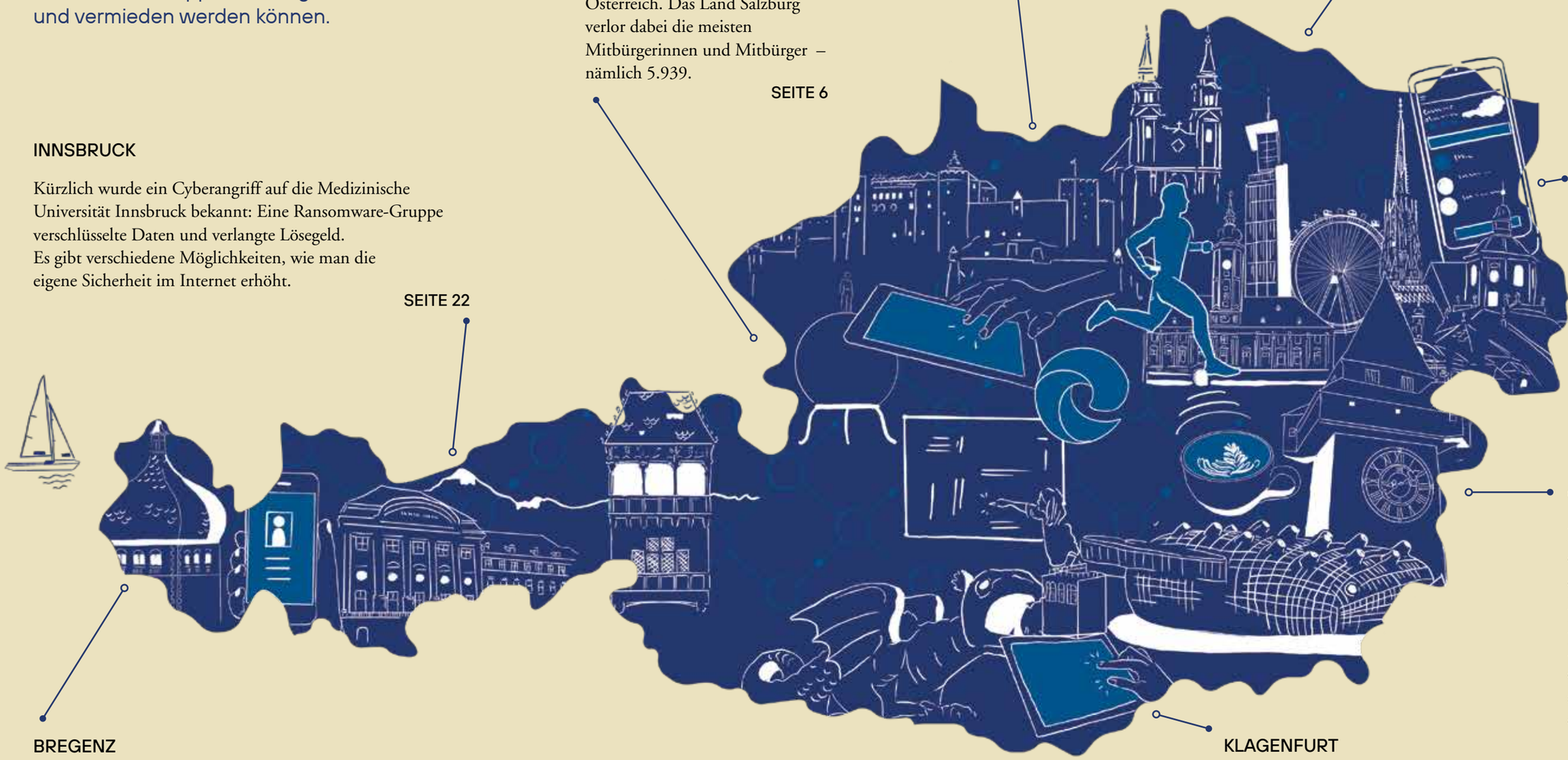
Chief Commercial Officer,
Wiener Zeitung Mediengruppe

COVERFOTO: Franziska Liehl, FOTO: WZMG/Pertschy

IMPRESSUM
Herausgeber und Medieninhaber: Wiener Zeitung GmbH, Konzept und Gesamtumsetzung: Wiener Zeitung GmbH, Verlagsort, Redaktions- und Verwaltungsadresse: Media Quarter Marx 3.3, Maria-Jacobi-Gasse 1, 1030 Wien, Tel.: +43 1 20699-0 **Geschäftsführung:** Martin Fleischhacker **Chief Commercial Officer:** Markus Graf **Leitung Content Production:** Nadja James **Koordination und Abwicklung:** Cornelia Ritzer **Autorinnen und Autoren:** Kim Kopacka, Teseo La Marca, Raimund Lang, Marion Pertschy, Cornelia Ritzer **Lektorat:** Oliver Poschner **Art Direction und Fotoredaktion:** Judit Fortelný **Druck:** Druckerei Ferdinand Berger & Söhne GmbH, 3580 Horn. Stand: 30. August 2022.

INHALT

Die Digitalisierung hat durch die Pandemie, durch Homeoffice und hybrides Arbeiten an Aktualität gewonnen. Die Digitalisierung begleitet uns aber bereits länger im Alltag. Ob bei wichtigen Behördengängen oder beim privaten Shoppen und Entertainment – Services verlagern sich ins Internet. Wir geben einen Überblick und Tipps, wie mögliche Gefahren erkannt und vermieden werden können.



SALZBURG

Wer umzieht, kann das online machen. 2021 wechselten 782.995 Menschen ihren Wohnort in Österreich. Das Land Salzburg verlor dabei die meisten Mitbürgerinnen und Mitbürger – nämlich 5.939.

SEITE 6

LINZ

Eine der ersten Fitness-Apps im deutschsprachigen Raum war „Runtastic“, die ab 2009 in Pasching entwickelt wurde. Seit 2015 gehört das Unternehmen zu Adidas.

SEITE 14

ST. PÖLTEN

Microsoft Edge zählt zu den beliebtesten Browsern weltweit. In Österreich ist der US-Technologiekonzern in Wien vertreten, in Niederösterreich ist der Bau von drei Rechenzentren geplant.

SEITE 16

INNSBRUCK

Kürzlich wurde ein Cyberangriff auf die Medizinische Universität Innsbruck bekannt: Eine Ransomware-Gruppe verschlüsselte Daten und verlangte Lösegeld.
Es gibt verschiedene Möglichkeiten, wie man die eigene Sicherheit im Internet erhöht.

SEITE 22

WIEN

Am 19. März 2019 ging die App „Digitales Amt“ des damaligen Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW) online.

SEITE 10

GRAZ

Den Kaffee mit dem Smartphone oder der Smartwatch bezahlen – das ist unter anderem im Grazer Kunsthauscafé möglich. Das Kunsthaus wurde im Rahmen des Kulturhauptstadtjahres 2003 errichtet und gilt als neues architektonisches Wahrzeichen der Stadt.

SEITE 18

BREGENZ

Um die Vollversion der ID Austria mit ihren neuen Funktionen – wie etwa der Möglichkeit, Ausweise am Smartphone vorzuweisen – zu erhalten, ist die persönliche Registrierung bei einer Behörde notwendig. In Vorarlberg ist die Landespolizeidirektion (LPD) Bregenz zuständig.

SEITE 12

ILLUSTRATION: Judit Fortelný

KLAGENFURT

Die Digitalisierung beschäftigt uns alle. Am A1 Campus in Klagenfurt werden kostenlose Internet-Schulungen angeboten – für Schulklassen, Eltern und Lehrkräfte sowie Seniorinnen und Senioren.

SEITE 20

Digital statt Wartesaal

So sieht das Amt der Zukunft aus

Es gibt Dinge, die muss man tun, auch wenn sie keinen Spaß machen. Hausarbeit zählt dazu, aber auch Zahnarztbesuche oder lästige Behördenwege. Letztere sollen künftig erleichtert werden und sich vorwiegend in der digitalen statt in der physischen Welt abspielen – dank der App „Digitales Amt".

FOTO: Adobe Stock/peopleimages.com

Matthias Jax, Datenschutz-Experte und Projektleiter für das EU-Projekt Saferinternet.at, erklärt im Interview, wie man sich mit der App und in der digitalen Welt am besten zurechtfindet.

Von Kim Kopacka

Warum wurde die App „Digitales Amt" entwickelt?

Die grundsätzliche Idee hinter diesem neuen digitalen Amtsservice ist, dass man in Österreich zukünftig per Smartphone Dinge erledigen kann, die man vorher physisch machen musste, indem man zu einer Behörde ging, um etwa einen Wohnsitzwechsel bekanntzugeben oder eine Wahlkarte zu beantragen.

Was muss man können, um die App „Digitales Amt" zu nutzen?

Die App ist relativ unkompliziert und selbsterklärend. Man kann sie jederzeit herunterladen, sich aktuell zum Beispiel mit der Handysignatur anmelden und die App dann sofort nutzen, um etwa digitale Verträge zu unterschreiben. Man braucht also keine Angst zu haben, dass man viel lernen muss, um sie nutzen zu können, aber man sollte schon eine halbe Stunde investieren, um sich einzulesen.

Man muss sich also bewusst damit auseinandersetzen?

Genau, es ist der Wunsch vieler, dass man die App startet und alles funktioniert automatisch. Das hat jedoch nichts mit der Realität zu tun, speziell wenn es um Amtswege geht. Die sind eben ein bisschen komplizierter. Aber in der physischen Welt nimmt man sich auch die Zeit, um zum Amt zu gehen und zum Beispiel einen neuen Reisepass zu beantragen. Ähnlich kann man das beim „Digitalen Amt" sehen. Auch da sollte man etwas Zeit einplanen, um sich mit der App vertraut zu machen.

Wenn man sich aber eingearbeitet hat, ist sie durchaus ein Gewinn. Man spart zum Beispiel Geld, weil die Gebühren für Behördenwege reduziert oder ganz erlassen werden. Und man gewinnt Zeit. Denn wenn ich mich einmal eingelesen habe und zum Beispiel weiß, wie ich einen Wohnsitzwechsel beantrage, kann ich das zukünftig mit zwei Klicks machen.

Ergeben sich durch die App Nachteile für Bürgerinnen und Bürger?

Der größte Nachteil ist, dass manche Personengruppen ausgeschlossen werden. Das heißt, wenn ich kein Smartphone besitze oder mit solchen Themen nicht vertraut bin, ist es ein durchaus komplexer Vorgang, wie ich zu dieser App komme und sie dann auch nutze. Da gibt es schon ein bisschen Lernbedarf – und vor allem Lehrbedarf. Das bedeutet, dass man jene Personengruppen abholen muss, die möglicherweise Unterstützung benötigen.

Wie kann man diese Personengruppen unterstützen? Es heißt ja oft, dass sich speziell ältere Generationen mit solchen Apps schwertun.

Das ist ein bisschen die Gefahr, dass man dabei sofort eine bestimmte Zielgruppe im Kopf hat, wie zum Beispiel Personen in der nachberuflichen Lebensphase.

Das stimmt aber oft nicht mehr. Man unterschätzt, wie digitalaffin viele von ihnen sind. Tatsächlich betrifft es alle Personenschichten in ganz Österreich. Das fängt bei jungen Erwachsenen an und hört dann eben bei den Seniorinnen und Senioren auf.

Mit der ID Austria erhalten Österreicherinnen und Österreicher eine amtlich beglaubigte elektronische Identität. Experte Matthias Jax rät, sich gründlich mit der App „Digitales Amt" auseinanderzusetzen.

Deshalb ist es wichtig, gesamtgesellschaftlich hinzuschauen. Es gibt zum Beispiel für Personen in der nachberuflichen Lebensphase Weiterbildungsangebote und Plattformen wie www.digitaleseniorinnen.at, über die man erfährt, wo man Trainerinnen und Trainer findet oder wie man zu gut aufbereiteten Informationen kommt. Aber auch die Arbeiterkammern bieten regelmäßig kostenlose Webinare zu diversen Digitalthemen an. Auf www.oesterreich.gv.at/id-austria gibt es eine Schritt-für-Schritt-Anleitung, wie man sich bei der App „Digitales Amt" mit der ID Austria anmeldet.

„Man sollte Zeit einplanen, um sich mit der App vertraut zu machen."

Welche Herausforderungen bringt die digitale Welt noch mit sich?

Eine der größten Herausforderungen ist, aus Sicht der Behörde betrachtet, dass man die Menschen dazu motiviert, die App zu nutzen, und dass man gut vorbereitet ist. Denn sobald man diese App präsentiert, muss sie auch funktionieren, weil die Frustrationsgrenze vieler Menschen vor allem in der jetzigen Zeit sehr niedrig ist. Wenn es nicht gleich beim ersten Mal klappt, habe ich möglicherweise noch eine zweite Chance, wahrscheinlich habe ich aber schon einen Großteil der Leute verloren.

Umgekehrt gilt aber auch der Appell an alle, die die App nutzen möchten, nicht zu erwarten, dass alles sofort zu 100 Prozent funktioniert. Das wäre unfair gegenüber jedem, der so etwas programmiert. Man sollte sich stattdessen mit der App auseinandersetzen und sich sagen: Wenn es nicht funktioniert, werfe ich das Handy nicht gleich aus dem Fenster, sondern lege es vielleicht kurz weg und probiere es am nächsten Tag noch einmal. Und wenn es dann nicht klappt, weiß ich, an welche Informationsstellen, von denen es in Zukunft bestimmt einige geben wird, ich mich wenden kann.

FOTO: Franziska Liehl

Was ist in näherer Zukunft noch zu erwarten?

Die größte Entwicklung wird bestimmt die ID Austria sein, die mit der App „Digitales Amt" einhergeht. Sie ist eine Weiterentwicklung von Bürgerkarte und Handysignatur und wird es Menschen ermöglichen, sich digital zu identifizieren – und das in ganz Europa. In fünf bis zehn Jahren werden wir vielleicht nur noch unser Smartphone einpacken müssen, wenn wir reisen. Denn dann ist möglicherweise auch unser Reisepass darauf gespeichert.

Das hat natürlich Vor- und Nachteile, ganz klar, darüber kann man diskutieren. Ich sehe aber einen großen Vorteil darin, dass man die Möglichkeit hat, sehr viel über das Smartphone zu machen, und dieses sozusagen in den Mittelpunkt seiner digitalen Identität stellt. Man hat ja am Grünen Pass bereits gesehen, dass der Datenaustausch innerhalb Europas funktioniert.

In Zukunft wird sich also noch viel mehr in der digitalen Welt abspielen. Was braucht es, um sich darin sicher bewegen zu können?

Es wird wichtig sein, das Smartphone wie eine Brieftasche zu bewerten und dementsprechend abzusichern. Wenn ich zum Beispiel aktuell eine PIN habe, die 1111 lautet, dann wäre es jetzt an der Zeit, mir eine sicherere PIN zu überlegen beziehungsweise die Gesichtserkennung oder den Fingerprint zu aktivieren.

FOTO: Franziska Liehl

Verlieren sollte man das Smartphone künftig also nicht, oder?

Das stimmt, und die Frage, wie wir damit umgehen, dass alles auf einem Smartphone gespeichert ist, wird uns begleiten. Man wird sich Gedanken darüber machen müssen, ob man die Möglichkeit eines (Offline-)Backups hat oder wie man zu Daten kommt, wenn man sein Smartphone nicht mithat, aber das wäre einen eigenen Artikel wert. ♦

MATTHIAS JAX

ist Social-Media-Experte mit Spezialisierungen in den Bereichen Datenschutz und Online-Sicherheit.

Als Projektleiter bei Saferinternet.at setzt er sich für die verständliche Vermittlung eines sicheren Umgangs mit digitalen Medien ein.

www.saferinternet.at

Österreichs Verwaltung in der Hosentasche

Durch die App „Digitales Amt“ haben Bürgerinnen und Bürger alle notwendigen Informationen zu Themen der österreichischen Verwaltung rund um die Uhr griffbereit. Die Basis dafür bildet die Website oesterreich.gv.at, die sämtliche behördlichen Dienste und Bürgerservices vereint.

Von Marion Pertschy

FOTO: Adobe Stock/insta_photos

Der langersehnte Urlaub steht vor der Tür, doch der Reisepass ist beinahe abgelaufen. Bald wird gewählt, es fehlt jedoch die Zeit, eine Wahlkarte zu beantragen. Und die offizielle Wohnsitzänderung nimmt einfach nur unnötig viel Zeit in Anspruch. Um all dies zu vereinfachen, ging am 19. März 2019 die App „Digitales Amt“ des damaligen Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW) online.

Smartphones sind als ständige Begleiter aus dem Alltag nicht mehr wegzudenken. In Österreich liegt ihre Marktdurchdringung bei über 90 Prozent. Es war also naheliegend, mit einer App auf dem Smartphone auch Behördengänge und das Bürgerservice flächendeckend auf eine digitale und mobile Ebene zu heben, sodass die Basis-Website oesterreich.gv.at über das Smartphone genutzt werden kann.

HILFREICHE FUNKTIONEN UND SERVICES

Laut Zahlen des Finanzministeriums verzeichnet Österreich jährlich 800.000 Wohnsitzänderungen, in Wahljahren etwa ebenso viele Wahlkartenanträge sowie 80.000 Geburten. Die im Vorfeld des App-Launches 2018 von der Unternehmensberatungsfirma EY durchgeführte Studie „Smart Country Österreich“ sowie drei Bürgerkonferenzen machten den Wunsch in der Bevölkerung deutlich, entsprechende Behördenwege online erledigen zu können.

Im Jahr 2021 zählten die Website oesterreich.gv.at und die App „Digitales Amt“ 54,7 Millionen Besucherinnen und Besucher. Heute nutzen monatlich rund drei Millionen Menschen die App. Und das mit gutem Grund: Neben dem Aus von ausgewählten physischen Amtswegen inklusive Wartezeiten stellt die zeitlich und örtlich uneingeschränkte Nutzung der App via Smartphone einen erheblichen Vorteil für Bürgerinnen und Bürger dar.

Ursprünglich war eine gültige Handy-Signatur als digitaler Schlüssel für die Anmeldung notwendig. Seit Mitte Juli 2022 können sich Userinnen und User über die neue ID Austria anmelden. Wurde die digitale Identität bei einer behördlichen Stelle aktiviert, können mit der App etwa offizielle Schreiben über den Postkorb abgerufen und digital unterzeichnet werden. Dadurch ersparen sich Userinnen und User auch für die Beantragung einer Wahlkarte oder die An- und Abmeldung des Hauptwohnsitzes den Weg zur Meldebehörde. Und das Angebot der Amtsservices wird laufend erweitert. In Planung ist zum Beispiel die Integration zusätzlicher Meldewesenfunktionen (Nebenwohnsitz, Umzug ins Ausland) sowie eines Online-Führerscheins und -Zulassungsscheins.

Mithilfe einer plattformübergreifenden Suche, die unter anderem das Rechtsinformationssystem (RIS), die österreichische Datenbank data.gv.at und das Unternehmensserviceportal (USP) inkludiert, erleichtert die Smartphone-App zudem die Informationsbeschaffung zu rund 200 Lebenslagen und für die Bevölkerung relevanten Verwaltungsthemen. Single-Sign-on-Verbindungen ermöglichen den Zugang zu weiteren Portalen wie JustizOnline, zur App FinanzOnline [+] und Anwendungen wie der Online-Diebstahlsanzeige. Darüber hinaus beantwortet der Chatbot Mona administrative Fragen, Neuigkeiten kommen per Push-Mitteilung und ein Erinnerungsservice meldet Userinnen und Usern, wenn es Zeit für die Beantragung eines neuen Reisepasses ist.

WAS IST OESTERREICH.GV.AT?

Oesterreich.gv.at soll als behördenübergreifende Plattform das Leben aller Menschen in Österreich vereinfachen, indem Fragen zu konkreten Lebenssituationen wie einer Geburt oder der Wohnsitzänderung auf der Website im Vordergrund stehen. Gleichzeitig soll gewährleistet werden, dass Österreich auch in Zeiten voranschreitender Digitalisierung ein konkurrenzfähiger Wirtschaftsstandort bleibt. Die Entwicklung des „mGovernment“ (Mobile Government mit oesterreich.gv.at und der App „Digitales Amt“) spielt dabei eine zentrale Rolle.

BIOMETRISCHE IDENTIFIZIERUNGEN NÖTIG

Die App „Digitales Amt“ kann für iOS und Android in den jeweiligen App-Stores kostenfrei heruntergeladen werden. Aus Sicherheitsgründen sind für ihre Aktivierung bei iOS eine Touch- oder Face-ID sowie ein Betriebssystem der Version 11 oder höher notwendig. Android-Smartphones müssen die biometrische Authentifizierungssoftware Android BiometricPrompt API und zumindest die Betriebssystemversion 10 unterstützen. Nach Anmeldung über ID Austria sind alle Services der App uneingeschränkt verfügbar. ♦

Digitaler Ausweis löst Handy-Signatur ab

ID Austria

Mit Herbst 2022 wird die digitale Unterschrift der Handy-Signatur durch die digitale Identität ID Austria abgelöst. Gegenüber ihrer Vorgängerin wartet diese mit einer Reihe neuer Funktionen auf.

Von Marion Pertschy

Digital, direkt und kostenlos – das Erledigen von Behördengängen verlagert sich zunehmend von der physischen in die digitale Welt. Dabei erlauben es digitale Identitätsnachweise wie die im Jahr 2009 eingeführte Handy-Signatur, behördliche Services online zu nutzen. Nun ist die Pionier-Version aber bald passé. Im Herbst 2022 wird sie von der weitaus umfangreicheren ID Austria abgelöst. Diese wird neben sämtlichen Funktionen von Handy-Signatur und Bürgerkarte eine Reihe neuer Anwendungen beinhalten und EU-weit gültig sein.

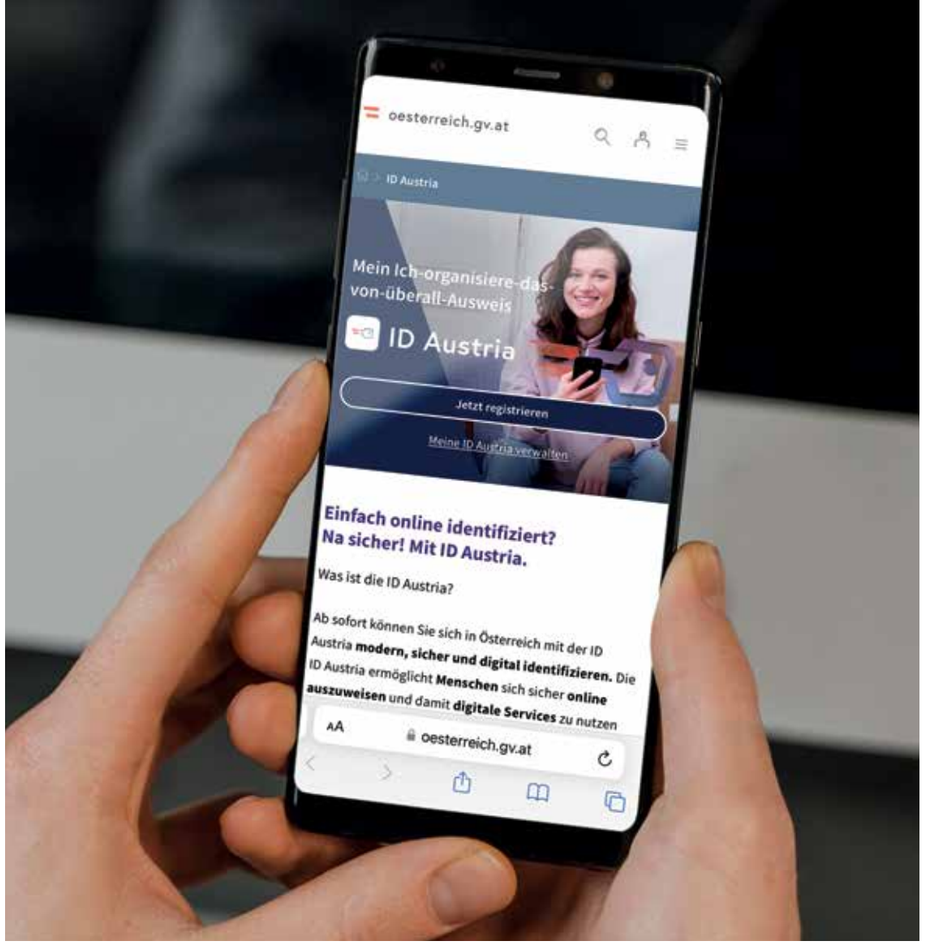
VIELE NEUE MÖGLICHKEITEN

Die ID Austria ist Teil des „Digitalen Aktionsplans Austria" des Finanzministeriums (BMF) gemeinsam mit dem Bundesministerium für Inneres (BMI). Sie beinhaltet neben den Funktionen der Handy-Signatur etwa die hochsichere digitale Abwicklung von Verwaltungs- und Geschäftsprozessen. Dabei folgt die ID Austria neuesten datenschutzrechtlichen Standards und erfüllt somit auch die höchsten Sicherheitsanforderungen der Europäischen Union. Userinnen und User bestimmen, welche ihrer Daten aus bestehenden elektronischen Verzeichnissen (etwa dem Zentralen Melderegister) abgefragt und an Dritte weitergegeben werden.

Unautorisierte Abfragen werden blockiert. Überdies bildet die ID Austria die Grundlage für die in Umsetzung befindliche digitale Plattform „eAusweis" und zahlreiche weitere Anwendungen. Das bedeutet, dass Nutzerinnen und Nutzer der ID Austria künftig via Smartphone auch auf Personalausweise oder Führerscheine zugreifen können.

ID AUSTRIA IN DER EUROPÄISCHEN UNION

Im Gegensatz zur Handy-Signatur kann die ID Austria ab 2023 auch für Online-Services von Behörden in anderen EU-Staaten verwendet werden.



Um eine ID Austria zu erhalten, braucht man ein Smartphone mit Face- oder Touch-ID, außerdem muss das 14. Lebensjahr vollendet sein.

FOTO: Freepik, VISUALISIERUNG: Content Agentur Austria

Die gesetzlichen Rahmenbedingungen des gesamteuropäischen Projekts sind in der von allen Mitgliedstaaten unterzeichneten Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung) des Europäischen Parlaments und des Rates festgelegt.

Um ihre ID Austria registrieren zu können, müssen Nutzerinnen und Nutzer das 14. Lebensjahr vollendet haben und ein Smartphone mit Face- oder Touch-ID besitzen. Um Missbrauch vorzubeugen, erfolgt die Beantragung für im Inland wohnhafte Österreicherinnen und Österreicher durch den einmaligen Gang zur lokalen Passbehörde, einer ermächtigten Gemeinde oder der zuständigen Landespolizeidirektion. Existiert bereits eine Handy-Signatur, kann die ID Austria ab Herbst 2022 auch online über die App „Digitales Amt" angefordert werden. In Zukunft sollen alle Bürgerinnen und Bürger die digitale Identität beim Beantragen eines neuen Reisepasses automatisch erhalten, wenn sie dies nicht ausdrücklich ablehnen. Ausländische Staatsangehörige, die im Inland einen Wohnsitz, ein Beschäftigungsverhältnis oder einen anderen Bezug zu Österreich nachweisen können, erhalten die ID Austria bei der jeweiligen Landespolizeidirektion. Im Ausland aufhältige Österreicherinnen und Österreicher können sie bei den zuständigen Vertretungsbehörden (Botschaften, Konsulate) beantragen.

FUNKTIONEN IN VOLLEM UMFANG

Derzeit befindet sich der neue digitale Identitätsnachweis noch im Pilotstadium und ist vorerst nur im Ausmaß der Handy-Signatur-Anwendungen verfügbar. Die Testphase endet jedoch mit 31. Oktober 2022. Danach soll die ID Austria allen Bürgerinnen und Bürgern in vollem Umfang zur Verfügung stehen. Sämtliche bisherigen Anwendungen der Handy-Signatur werden automatisch auf die ID Austria umgestellt. ♦

DIGITALE WERKZEUGE

Bunte Buttons als Türöffner

DIE WUNDERBARE WELT DER APPS: EIN ÜBERBLICK

Viele von uns haben sie auf dem Smartphone oder dem Laptop und benutzen sie ganz intuitiv und vor allem täglich: Apps.

Die Kurzform von Applikation bezeichnet eine Anwendungssoftware auf dem Gerät, mit der wir kommunizieren, arbeiten oder uns auch einfach die Zeit vertreiben können.

Zu den beliebtesten bunten Buttons, die sich auf den Endgeräten finden, zählt die App der Social Media Plattform Facebook samt dem dazugehörigen Messenger für Textnachrichten. Außerdem der Instant-Messaging-Dienst WhatsApp, der das Verschicken von Textnachrichten, Fotos, Videos oder Audiodateien ganz einfach macht. Oft und gerne genutzt werden auch Spotify, Soundcloud oder andere Musik-Streaming-Apps.

HINTER DEN BUNTEN BUTTONS STECKEN:

- SOZIALE NETZWERKE
- SPIELE
- INTERNET
- KOMMUNIKATION
- PAYMENT
- NACHRICHTEN, WETTER & CO
- SHOPPING

FOTO: Adobe Stock/Andreas Prott

BROWSER FÜR UNTERWEGS

Mit einem Browser kann man auch am Handy oder Tablet verschiedene Webseiten aufrufen und im Internet surfen. Je nach Betriebssystem des Smartphones – Android oder iOS – sind manche Browser bereits vorinstalliert. Ansonsten ist die Auswahl groß, die bekanntesten sind Google Chrome und Safari von Apple. Aber auch Alternativen wie Microsoft Edge und Mozilla Firefox überzeugen mit praktischen Funktionen.

NUTZEN, ABER RICHTIG!

Browser sammeln Daten über das persönliche Surfverhalten und speichern dabei automatisch Cookies und auf Wunsch auch Anmeldedaten. Es ist wichtig, sich dieser Praxis bewusst zu sein, weil persönliche Daten betroffen sind. Deshalb sollte man stets auf die Datenschutz- und Sicherheits-Einstellungen achten.

Manche Apps greifen auf zahlreiche am Handy gespeicherte Daten zu. Diese Berechtigungen sollten regelmäßig überprüft werden, denn der Zugriff einer Anwendung auf Anruflisten, private Nachrichten, Standort, Kamera oder das Mikrofon könnte von unberechtigten Dritten missbraucht werden.

SO STÖBERN SIE IN SICHERHEIT

Beim Surfen im Internet ist der Internet-Browser so etwas wie Ihr Surfbrett. Ein Überblick der beliebtesten Anbieter und der wichtigsten Sicherheitstipps.

Von Teseo La Marca

Auf Deutsch bedeutet „browsen“ stöbern. In der Praxis befolgt ein Browser vor allem Anweisungen aus dem Internet, wie er eine Webseite darstellen soll. Weil diese Befehle in verschiedenen Sprachen, wie zum Beispiel HTML, übermittelt werden und nicht jeder Browser alle Sprachen beherrscht, kann es vorkommen, dass verschiedene Browser dieselbe Webseite unterschiedlich anzeigen. Abgesehen von der Grafik unterscheiden sich die einzelnen Browser noch in weiteren Aspekten, die für Nutzerinnen und Nutzer relevant sind: von der Benutzerfreundlichkeit bis hin zur Datensicherheit.

FOTO: Adobe Stock/Angelov

SAFARI

Dieser Browser steht ausschließlich Userinnen und Usern von Apple-Geräten zur Verfügung, von denen er für seine Stabilität und das individuell anpassbare Surferlebnis geschätzt wird. Sicherheitsoptionen wie ein Datenschutzbericht sowie ein Tracking-Schutz gegen Werbeanzeigen zeigen, dass es dem Anbieter mit Datenschutz und Sicherheit ernst ist.

GOOGLE CHROME

Der Browser von Google punktet mit einem übersichtlichen Design, außerdem läuft er schnell und stabil. Für Sicherheit sorgt der Open-Source-Code des Programms, den Nutzerinnen und Nutzer überprüfen können. Wer jedoch auf Datenschutz großen Wert legt, sollte von Chrome Abstand nehmen, da der Anbieter in Vernetzung mit dem Google-Konto Nutzerdaten zu Werbezwecken sammelt.

MICROSOFT EDGE

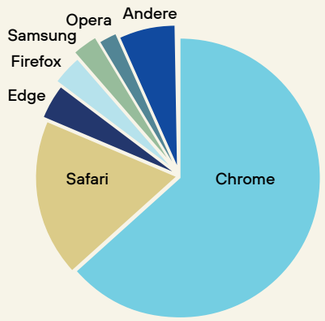
Der Nachfolger des Internet Explorer ist seit 2015 der Standardbrowser für Computer mit Windows 10. Trotz Tracking-Schutz und überarbeitetem Design konnte der Browser das breite Publikum nicht von sich überzeugen. Von der Nutzung des veralteten Vorgängers Internet Explorer sollte abgesehen werden, da dieser zahlreiche Sicherheitslücken aufweist.

MOZILLA FIREFOX

Firefox, einer der beliebtesten Browser im deutschen Sprachraum, verfügt ebenfalls über einen Open-Source-Code. Der Browser läuft stabil, hat aber wegen seines etwas sperrigen Designs zuletzt Sympathiepunkte verloren. Dafür bietet der Browser interessante Sicherheitsoptionen wie einen Passwort-Manager, ein VPN (virtuelles privates Netzwerk) sowie das Warntool Firefox Monitor, das Nutzerinnen und Nutzer informiert, falls ihre Daten durch Hacks oder Datenpannen gefährdet sind.

ILLUSTRATIONEN: Mariia Shaplova/Alamy Vektorgrafik

MARKTANTEILE DER BROWSER



Google Chrome 65,9 %
Apple Safari 18,6 %
Microsoft Edge 4,1 %
Mozilla Firefox 3,3 %
Samsung Internet 2,9 %
Opera 2,1 %
Andere 6,8 %

Quelle: gs.statcounter.com
Stand: Juni 2022

TIPPS FÜR ZUSÄTZLICHE SICHERHEIT

Wer im Internet sicher unterwegs sein will, hat mit den Browsereinstellungen ein wichtiges Instrument in der Hand. Sehr beliebt ist die Option, privat zu surfen, wodurch Browserdaten (zum Beispiel Cookies, durch die individuelle Nutzerdaten gespeichert werden, sowie temporäre Internetdateien, Verlauf und Websitedaten) auf dem verwendeten Gerät nicht mehr automatisch gespeichert werden.

Für die besuchten Webseiten, den Internet-Service-Provider und die Suchmaschinen bleiben die Browser-Aktivitäten jedoch weiter sichtbar. Einen noch besseren Schutz der Privatsphäre bieten deshalb Browser, die einen kostenlosen VPN-Zugang anbieten. Eine besondere Empfehlung in dieser Hinsicht ist der Browser „Brave“, der optisch im Chrome-Gewand daherkommt, im Gegensatz zum Google-Produkt aber auch auf Datenschutz setzt und in mehreren Tests einschlägiger Magazine sogar schneller performte als Chrome.

Ansonsten verfügen moderne Internetbrowser über zahlreiche, von Haus aus aktivierte Sicherheitsmechanismen. Wenn Sie darüber hinaus das automatische Speichern von Passwörtern deaktivieren, sind Sie auf der sicheren Seite.

Zusätzliche Plug-ins wie Werbeblocker – also optionale Programmkomponenten, die den Datenschutz und die Sicherheit erhöhen sollen – beziehen Sie am besten nur aus offiziellen, vertrauenswürdigen Quellen. Das ist zum Beispiel der Anbieter des Browsers oder der jeweilige Hersteller des Plug-ins. Andere Quellen sollten Sie jedenfalls einer kritischen Prüfung unterziehen. ♦

SMARTE GERÄTE STATT GELDBÖRSE

Mit Smartphone oder Smartwatch zu bezahlen ist praktisch – und wenn man bestimmte Vorkehrungen trifft, auch sicher.

Von Teseo La Marca

FOTO: Adobe Stock/Mariia Korneeva

Die schwere Geldbörse einfach mal zu Hause lassen und den Cappuccino im Café, das Benzin an der Tankstelle und die Milch im Supermarkt bequem mit dem Smartphone, der Quartz-Uhr oder der Smartwatch bezahlen: Das ist der praktische Gedanke hinter dem mobilen Bezahlen (Mobile Payment).

WIE FUNKTIONIERT MOBILES BEZAHLEN?

Der Unterschied zu anderen digitalen Bezahldiensten besteht darin, dass beim mobilen Bezahlen nicht im Internet, sondern direkt am sogenannten Point of Sale, dem physischen Verkaufsort, mithilfe eines Smartphones oder eines anderen mobilen Endgeräts, etwa einer Smartwatch, bezahlt wird. Es handelt sich im Grunde um die digitale Variante des kontaktlosen Bezahlens mit Plastikkarten. Damit dies möglich ist, muss Ihr Smartphone die NFC-Funktion (Nahfeldkommunikation; eine Funktechnik für kontaktlose Datenübertragung) unterstützen und über eine aktive Mobile-Payment-App verfügen. Mobile-Payment-Lösungen wie Apple Pay oder Google Pay lassen sich auch über den jeweiligen Internetbrowser (Safari oder Google Chrome) verwenden.

DIE WICHTIGSTEN ANBIETER UND AKTUELLE TRENDS IM ÜBERBLICK

Weltweit gibt es mehr als 300 Anbieter für Mobile Payment. Zu den beliebtesten Apps in Österreich gehören Bluecode, Apple Pay und Google Pay sowie Fitbit Pay und Garmin Pay (beide für Smartwatch). Laut einer von der Österreichischen Nationalbank 2020 durchgeführten Zahlungsmittelumfrage wurden im Einzelhandel im Jahr 2020 nur 0,7 Prozent der Transaktionen mit dem Mobiltelefon getätigt. Das klingt zunächst nach wenig, doch der Trend zeigt, gemessen an früheren Befragungen, klar nach oben und dürfte sich mit der Pandemie noch verstärkt haben. Neun Prozent der Befragten haben sich jedenfalls schon ausgerüstet und gaben in derselben Studie an, über ein NFC-fähiges Smartphone mit einer entsprechenden Bezahl-App zu verfügen.

Viele Unternehmen erkennen das Potenzial von Mobile Payment: von Supermärkten, die an der Kassa die Bezahlung via Supermarkt-App einrichten, bis hin zu Banken, die eine Digitalisierung ihrer Debit- und Kreditkarten anbieten. Auch die Europäische Zentralbank erwägt aktuell die Möglichkeit, einen „digitalen Euro" einzuführen, der für Mobile Payments verwendet werden kann.

IST MOBILES BEZAHLEN SICHER?

Mobile Payment bietet ein hohes Sicherheitsniveau. Wenn man bedenkt, dass herkömmliche Kreditkarten leicht verloren gehen, ist das Smartphone beziehungsweise die Smartwatch sogar die sicherere Methode – vorausgesetzt, dass Sie als Userin oder User bestimmte Sicherheitsvorkehrungen treffen:

- Aktivieren Sie die Standortermittlung des Geräts für den Fall eines Verlustes.
- Deaktivieren Sie bei Verlust des Smartphones umgehend die digitalisierten Bankkarten beziehungsweise kontaktieren Sie den Handybezahldienst oder die Sperrhotline der App.
- Sichern Sie das mobile Endgerät und die App mit Sperrcode ab, vorzugsweise mit einem biometrischen Verfahren wie Fingerabdruck (Touch-ID) oder Gesichtserkennung (Face-ID).
- Aktualisieren Sie regelmäßig Betriebssystem und Software der Bezahl-App, damit notwendige Sicherheitsupdates durchgeführt werden können.
- Beziehen Sie die gewünschte Bezahl-App nur aus sicheren Quellen und nutzen Sie sichere Internetverbindungen (öffentliche WLAN-Netzwerke bergen höhere Sicherheitsrisiken und sollten gemieden werden).
- Falls Sie eine Wallet-App für digitalisierte Bank- oder Kundenkarten verwenden, fügen Sie nur die notwendigen Karten hinzu.
- Klicken Sie E-Mails und Nachrichten nur dann an, wenn sie vertrauenswürdig erscheinen. ♦

TIPP ZUM DATENSCHUTZ

Manche Anbieter speichern Kunden- und Transaktionsdaten für kommerzielle Zwecke. Informieren Sie sich deshalb, welche Daten von Ihrem Dienstleister gespeichert werden – und zu welchen Zwecken.

„Das Nutzungsverhalten auch kritisch hinterfragen“

Thomas Arnoldner ist CEO der A1 Telekom Austria Group, dem führenden Kommunikationsanbieter in Österreich, und betont die Wichtigkeit der verantwortungsvollen Nutzung digitaler Medien. „Lebenslanges Lernen ist Pflicht“, wirbt er für Schulungsangebote für Schülerinnen und Schüler, um deren Medienkompetenz und Selbstverantwortung zu stärken – und fordert dies auch für Erwachsene.

Was bedeutet Medienkompetenz für Sie? Welchen Stellenwert hat Medienkompetenz für einen Großkonzern wie A1?

Medienkompetenz hat sowohl für A1 als auch für mich als Vater einen sehr hohen Stellenwert. Digitale Medien bieten ein schier unendliches Angebot an Information und Wissen. Umso wichtiger ist es, die für einen persönlich wie auch für das Unternehmen relevanten Inhalte zu finden und entsprechend zu nutzen. Neben den vielfältigen Chancen gilt es aber auch kritische Aspekte zu berücksichtigen.

FOTO: Renée del Missier

Welche Herausforderungen stellen nicht medienkompetente Mitarbeiterinnen und Mitarbeiter dar?

Für Unternehmen ist besonders der Security-Aspekt essenziell – Stichwort Datenschutz. Daher sollten alle Unternehmen und Institutionen diesem Thema besondere Aufmerksamkeit zukommen lassen, zum Beispiel in Form von eigenen Schulungen. Auch der Umgang der Mitarbeiterinnen und Mitarbeiter mit Social Media will gelernt sein.

Welchen Nutzen sehen Sie in der Medienkompetenz – für Unternehmen, aber auch für die Gesellschaft?

Generell bietet die verantwortungsvolle Nutzung digitaler Medien immens viele Vorteile – vom Zugang zu Informationen und Wissen über die Bereicherung im Unterricht und bei der Jobsuche bis hin zu Hobbys und ehrenamtlichen Engagements. Dem Individuum verschafft Medienkompetenz also viele Chancen. In einem größeren Kontext ist sie auch ein wesentliches Element einer funktionierenden Demokratie.

Wie qualifizieren Sie Ihre Mitarbeiterinnen und Mitarbeiter zu einem kompetenten Umgang mit Medien?

Wir haben im Konzern ein umfassendes eLearning-Programm, das sie je nach Interessenlage und Jobprofil selbständig und jederzeit absolvieren können. So haben wir unter anderem eLearnings zu Security und Datenschutz, um die Sensibilisierung des Teams für diese so wichtigen Themen zu erhöhen.

„Dem Individuum verschafft Medienkompetenz viele Chancen.“

Medienkompetenz ist ja ein Teilbereich von allgemeinen digitalen Kompetenzen. Welche Rolle spielen Letztere heute in der Berufswelt?

Allein die Tatsache, dass „Digitale Grundbildung“ ab dem neuen Schuljahr 2022/23 als Pflichtfach für die Mittelschule und AHS-Unterstufe auf dem Programm steht – hier besonders auch Medien- und Anwendungskompetenz –, zeigt, wie wichtig das Thema geworden ist. Die Schülerinnen und Schüler sollen schon früh lernen, sich in der digitalen Welt zu bewegen, diese zu gestalten und Informationen daraus zu verarbeiten. Das Fach ist die Grundlage für einen kompetenten und verantwortungsvollen Umgang mit der Digitalisierung und damit für ein selbstbestimmtes Leben im privaten und beruflichen Bereich.

Welche Rolle spielt in diesem Kontext der A1 digital.campus?

Im Rahmen unserer zahlreichen Nachhaltigkeitsaktivitäten bieten wir auf unserem A1 digital.campus genau für die Erlangung dieser Medienkompetenz – jeweils an die Schulstufe der Kinder angepasst – unterschiedlichste Kurse und Workshops kostenlos an. Darüber hinaus gibt es bei uns auch eigene Formate für Kindergarten- und Schulpädagoginnen und -pädagogen zu diesen Themen.

Welche Entwicklungen sehen Sie im Feld der Medienkompetenz?

Durch die Vielfalt von digitalen Tools und deren ständige Weiterentwicklung ist lebenslanges Lernen Pflicht. Besonders die neuen Trends im Bereich Metaverse haben das Potenzial, die Mediennutzung, wie wir sie heute kennen, nachhaltig zu verändern. Langfristig sollte besonderes Augenmerk darauf gelegt werden, Kinder und Jugendliche in ihrer Selbstverantwortung zu stärken. Das Ziel muss sein, verantwortungsbewusst mit digitalen Medien umzugehen und das eigene Nutzungsverhalten auch kritisch zu hinterfragen. Eine kompetente und sichere Mediennutzung ist dafür die Basis.

Haben Sie Tipps zum kompetenten Umgang mit Medien?

Idealerweise nutzen so viele Pädagoginnen und Pädagogen wie möglich mit ihren Schülerinnen und Schülern die kostenlosen Schulungsangebote unseres A1 digital.campus. Wir arbeiten hier mit Saferinternet und dem DaVinciLab zusammen. Auch Eltern sollten sich bewusst mit dem Umgang mit sozialen Medien auseinandersetzen.

Digitale Medienkompetenz und allgemeine digitale Kompetenzen können mit fit4internet-Tools (Checks und Quizzes) evaluiert und mit dem Dig-CERT, einer Online-Wissensüberprüfung zum Nachweis der digitalen Kompetenzen, überprüft werden. ♦

fit4internet

Das Gespräch führte fit4internet. Thomas Arnoldner ist Vizepräsident des Vereins.

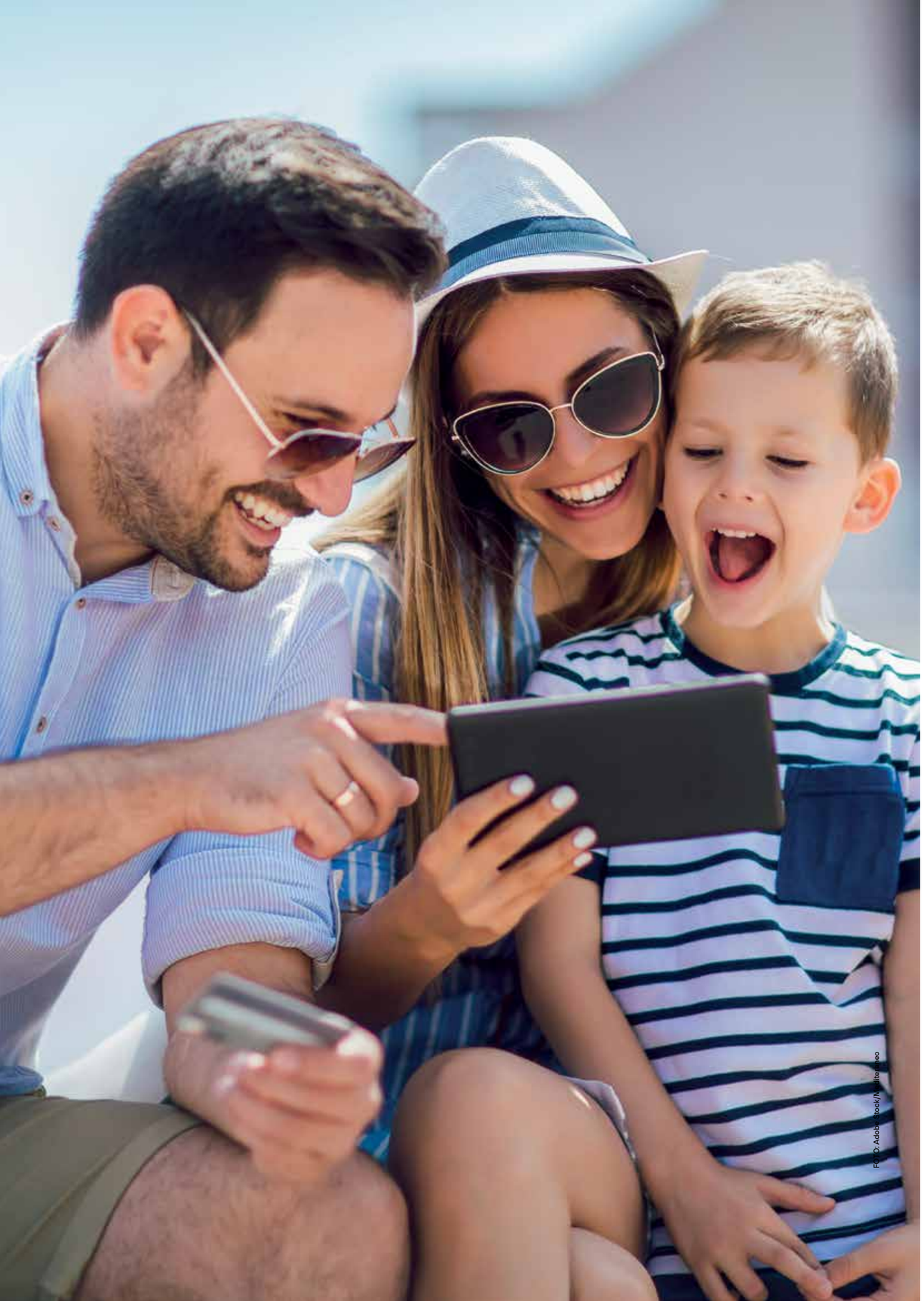


FOTO: Adobe Stock/Mauritius Images

Surfen ohne Wermutstropfen

**Phishing, Viren, Ransomware und Co.:
Das Internet kann manchmal ein hartes Pflaster sein.
Doch wer ein paar Grundsätze beachtet und die Augen offen hält,
hat wenig zu befürchten.**

Von Raimund Lang

Es ist keine Übertreibung, dass das Internet unsere Welt nachhaltig verändert hat. Das den Erdball umspannende „Netz der Netze“ hat neue Kommunikationsmöglichkeiten und Technologien sowie neue Geschäftsmodelle mit sich gebracht. Wir können jederzeit und von nahezu jedem Ort der Welt aus Nachrichten austauschen, einkaufen oder multimediale Inhalte konsumieren. In einem Sekundenbruchteil können wir Informationen teilen oder abrufen. Und dann gibt es auch noch den „Katzen-Content“ – Fotos und Videos von flauschigen Miezen in allen möglichen Lebenslagen. Ein zuverlässiger Stimmungsaufheller.

Allerdings, wie schon Goethe seinen Götz von Berlichingen verkünden ließ: „Wo viel Licht ist, ist starker Schatten.“ So ist auch das Internet ein Ort, an dem Gefahren lauern. Kriminelle nutzen die Anonymität im Netz, um ahnungslose Nutzerinnen und Nutzer zu erleichtern – im harmlosesten Fall um ihre persönlichen Daten, im schlimmsten um ihr schwer verdientes Geld. Doch zum Glück ist es recht einfach, sich vor einem Großteil der virtuellen Risiken zu schützen. Wer ein paar praktische Ratschläge beherzigt und zusätzlich den gesunden Menschenverstand walten lässt, kann sich sicher durch die Sphären des Internets bewegen.

UP TO DATE BLEIBEN GEGEN COMPUTERVIREN

Computerviren sind gleichsam die Grandseigneurs des digitalen Übels. Tatsächlich gibt es sie bereits länger als das Internet. Doch erst mit diesem konnten sie sich rasant verbreiten und so ihr Schadenspotenzial voll entfalten. Welches Unheil Computerviren anrichten können, ist der Fantasie ihrer Programmiererinnen und Programmierer überlassen. Manche tun gar nichts, andere blenden humorige Meldungen auf dem infizierten Rechner ein. Die einen verschicken automatisiert Spam-E-Mails an alle Kontakte des Opfers und andere löschen Daten oder sogar die komplette Festplatte.

Das Teuflische an Viren ist ihr Mechanismus zur Vervielfältigung: Analog zu den biologischen Vorbil-

dern schreiben sie ihren eigenen Quellcode in infizierte Dateien und vermehren sich dadurch exponentiell. Zum Glück muss man sich heute nicht mehr allzu viele Gedanken über Computerviren machen. Gängige Betriebssysteme wie Windows, iOS oder Linux bringen den Schutz dagegen bereits von Haus aus mit. Für die meisten Anwenderinnen und Anwender ist dieser auch völlig ausreichend. Kostenpflichtige Antivirensoftware von Kaspersky, McAfee, Avira oder Bitdefender beinhalten über die reine Virenerkennung hinausgehende Funktionen sowie mehr Bedienkomfort.

Achtung: Vollen Schutz bietet ein Virenscanner nur, wenn er auf dem neuesten Stand ist! Man sollte deshalb die automatische Aktualisierung des Antivirenprogramms zulassen. Dadurch werden die Signaturen der neusten Viren sofort nach ihrem Bekanntwerden in die Datenbank des Virenscanners geladen. Auf dem jeweils aktuellen Stand sollten übrigens auch Betriebssystem, Webbrowser und E-Mail-Client sein – wie jedes Programm, das sich mit einem Netzwerk verbinden kann.

ERPRESSUNG IM DIGITALEN ZEITALTER

Neben den klassischen Viren kursiert heute eine Vielzahl weiterer cyberkrimineller Bedrohungen mit oft übel klingenden Namen im Netz: Trojaner, Würmer, Spyware, Rootkits und noch etliche andere (siehe Glossar auf Seite 26). Die gute Nachricht: Virenscanner erkennen auch viele dieser Gefahren. Allerdings bei weitem nicht alle (übrigens auch nicht 100 Prozent aller Viren).

Herkömmliche Betriebssysteme haben deshalb Firewalls integriert. Das sind Programme, die den ein- und ausgehenden Datenverkehr eines Computers auf Verdächtiges überprüfen. Wie bei den Virenscannern gilt auch für Firewalls, dass die Bordmittel der Betriebssysteme in der Regel völlig ausreichend sind.

Immer öfter stößt man außerdem auf den Begriff Ransomware. Dabei handelt es sich um fiese Software, die einzelne Dateien eines Computers verschlüsselt oder sogar den Zugang zum Rechner selbst verhindert. Erst gegen Bezahlung von Lösegeld (meist in Kryptowährung) wird der Zugang wieder entschlüsselt. Das uralte „Geschäftsmodell“ dahinter ist ganz banale Erpressung, und man sollte sich gut überlegen, ob man zahlen will. Denn natürlich gibt es keine Garantie, dass die Kriminellen nach Erhalt des Lösegeldes den Computer auch wirklich wieder freigeben. Empfehlenswerter ist es, im Fall einer Infektion mit Ransomware die Festplatte komplett zu formatieren und das System neu zu installieren. Dies setzt freilich voraus, dass man regelmäßig Sicherheitskopien seiner Daten anlegt.

DIE EINFALLSTORE KENNEN

Doch wie gelangt Schadsoftware überhaupt auf den Rechner? Ein altes Informatiker-Sprichwort besagt, dass sich 95 Prozent aller Computerprobleme zwischen Tastatur und Stuhl befinden – also der Mensch verantwortlich ist. Das ist wenig schmeichelhaft, doch leider steckt ein Funken Wahrheit darin. Denn oft ist Fahrlässigkeit die Ursache für Ungemach im Web. Das lässt sich anhand des Themas Phishing besonders deutlich belegen. Darunter versteht man die Versuche Krimineller, durch Täuschung Daten aus ihren ahnungslosen Opfern herauszulocken oder diese zum Anklicken von Links zu bewegen, hinter denen sich gefährliche Schadsoftware verbirgt. Bereits ein Klassiker sind die Anwaltsbriefe,

FOTO: Adobe Stock/JenkoAtaman

bei denen der Rechtsvertreter eines unlängst verstorbenen Millionärs dessen Nachlass mit dem Adressaten des E-Mails teilen möchte. Aus dubiosen Gründen benötigt er aber von diesem zunächst ein Vorabzahlung.

Der gesunde Menschenverstand sollte hier Alarm schlagen. Denn niemand verschenkt Millionen an Unbekannte. Auch suchen nigerianische oder saudische Prinzen sicher nicht via E-Mail nach einer Braut, mit der sie ihr Vermögen teilen können. Leider ist Phishing nicht immer so eindeutig erkennbar. Oft nutzen Kriminelle täuschend echt aussehende Webseiten, um ihre Opfer in die Irre zu führen. Nicht selten holt man sich

Updates sind wichtig!
Auf dem jeweils aktuellsten Stand sollten der Virenscanner, das Betriebssystem, der Webbrowser und der E-Mail-Client sein.

BEACHTEN SIE STETS FOLGENDE SICHERHEITSMASSNAHMEN:

* Öffnen Sie keine Anhänge von E-Mails Ihnen unbekannter Absender und klicken Sie auch keine Links in solchen Mails an.
* Banken fragen NIEMALS per E-Mail nach Ihren Daten.
* Eine große Gefahrenquelle sind öffentliche WLAN-Netzwerke, etwa im Zug oder in Lokalen. Stellen Sie hier sensible Verbindungen (zum Online-Banking oder zur Anmeldung in Social-Media-Accounts) nur via VPN (virtuelles privates Netzwerk) her.
* Prüfen Sie, ob Webshops Gütezeichen haben (etwa Österreichisches E-Commerce-Gütezeichen, Trustmark Austria oder Trusted Shops). Unseriöse Anbieter erhalten kein Gütezeichen.
* Um sich vor Infektionen über Werbebanner oder andere Seitenelemente zu schützen, sollten Sie Flash deaktivieren. Browser-Plug-ins wie NoScript unterstützen Sie dabei.
* Achten Sie darauf, ob Webseiten das sichere Protokoll HTTPS (Hypertext Transfer Protocol Secure) verwenden – erkennbar am „https://“ in der Adresszeile des Browsers (statt nur „http://“).

Malware über gefälschte Onlineshops („Fake-Shops“) auf den Rechner. Gefälschte Bank-Webseiten sind häufig der Ort, an dem man seine Kontodaten unwissentlich Verbrechern anvertraut.

PASSWÖRTER

Passwörter sind ein probates Mittel, um den Zugang zu sensiblen Daten, Social-Media-Accounts, Rechnern oder einzelnen Dateien zu schützen. Kaum zu glauben, aber wahr: Noch immer sind „123456“ und „passwort“ die beliebtesten Kennwörter. Das wissen natürlich auch Kriminelle. Userinnen und User sollten deshalb solche Muster („Trivialpasswörter“) unbedingt vermeiden. Auch Namen, Geburtsdaten und sonstige persönliche Informationen, die Hacker herausfinden könnten, sind tabu. Generell sollten Passwörter mindestens 15 Zeichen lang sein und Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen beinhalten.

Gibt es Grund zu der Annahme, dass das Passwort geknackt wurde, sollte es sofort (!) geändert werden. Ein Hinweis darauf sind ungewöhnliche Anmeldungen bei einem Dienst, die man definitiv nicht selbst getätigt hat. Auch Online-Einkäufe, an die man sich nicht mehr erinnern kann, sind meist ein untrügliches Zeichen. Auf Webseiten wie „haveibeenpwned.com“ lässt sich außerdem prüfen, ob die eigene E-Mail-Adresse oder Telefonnummer in irgendwelchen gestohlenen Datensätzen aufgetaucht ist.

Zu vermeiden gilt es, ein und dasselbe Passwort für verschiedene Dienste zu verwenden, beispielsweise das E-Mail-Konto, Facebook, Instagram, den Zugriff aufs Firmennetzwerk und womöglich noch fürs Online-Banking. Eine gute Lösung sind Passwort-Tresore. Das sind Programme, die Passwörter verwalten und auch selbst erstellen können. Anwenderinnen und Anwender brauchen sich somit nur noch ein einziges Master-Passwort zu merken, das Zugriff auf den Tresor gewährt. Dieses sollte man allerdings auf keinen Fall vergessen oder verlieren. Denn sonst hat man keine Möglichkeit mehr, auf seine Passwörter zuzugreifen. ♦

GLOSSAR DER SCHADSOFTWARE

- **MALWARE**: Allgemeiner Begriff für schädliche Software
- **VIRUS:** Software, die sich selbst repliziert, indem sie ihren eigenen Code in infizierte Dateien schreibt
- **TROJANER:** Schadsoftware, die als ungefährliches Programm getarnt im Hintergrund unerwünschte Funktionen ausführt
- **WÜRMER:** Vervielfältigen sich wie Viren selbst und verteilen sich dann über ganze Computernetze
- **RANSOMWARE:** Software, die den Rechner oder einzelne Dateien verschlüsselt
- **ADWARE:** Software, die unerwünschte Werbung anzeigt
- **ROOTKITS:** Programme, die sich auf dem infizierten Rechner verbergen, um einem Angreifer später unbemerkten Zugriff auf das System zu ermöglichen
- **SPYWARE:** Überbegriff für Software, die unbemerkt Informationen vom infizierten Rechner versendet
- **PHISHING:** Betrügerische Versuche, Daten von Opfern herauszufinden oder diese zum Anklicken gefährlicher Links zu bewegen
- **BRUTE-FORCE-ATTACKE:** Angriff (zum Beispiel auf Passwörter), der auf dem Durchprobieren aller Möglichkeiten basiert
- **ZERO-DAY-ANGRIFF:** Ausnützen einer Software-Sicherheitslücke, die dem Softwareentwickler unbekannt war

”

Wissen ist Macht.

Francis Bacon, Philosoph, Jurist und Staatsmann (1561–1626)

Zentrum für Medienwissen

Info.Sicher – Kostenloses Bildungsangebot für digitale Medienkompetenz

Digitale Medienkompetenz ist eine Schlüsselqualifikation des 21. Jahrhunderts, die den sicheren Umgang mit digitalen Informationen und Inhalten voraussetzt. Angesichts aktueller Phänomene wie „Fake News", Filterblasen, Verschwörungstheorien oder Phishing-Mails ist die Förderung einer fundierten Medienkompetenz von wesentlicher Bedeutung.

Info.Sicher ist ein von Expert*innen der Wiener Zeitung Mediengruppe zusammengestelltes Kursangebot, das sich an **Mitarbeiter*innen der öffentlichen Verwaltung, Lehrlinge sowie Senior*innen** richtet.

Vorteile und Nutzen für Interessierte:

✔ Basiswissen im sicheren und kritischen Umgang mit Informationen und digitalen Inhalten

- Erkennen von Fake News, Filterblasen und Verschwörungstheorien
- Sicherheit im Internet – Antivirenschutz, Passwörter, Umgang mit Phishing-Mails, Datenschutz
- eGovernment – Verwaltungsdienste digital nutzen

✔ Standortbestimmung und Orientierung der individuellen digitalen Medienkompetenz

✔ DigComp-2.2-AT-konform

✔ **Abschluss mit dem „Info.Sicher-Zertifikat"**

Das Kursangebot gilt **bis Dezember 2022** sowie **ausschließlich für Gruppenanmeldungen** von zehn bis maximal 25 Personen. Die Kurse setzen sich
aus 4 kurzweiligen Modulen à 3 Stunden zusammen.

JETZT ANMELDEN:

➜ telefonisch unter **0732 / 78 80 78 808** (Mo–Fr 9:00–13:00 Uhr) oder

➜ online unter **www.medienwissen.at/infosicher**

medienwissen.at

Zentrum für Medienwissen

Eine Initiative der Wiener Zeitung Mediengruppe