Schieb Report

Ausgabe 2021.32

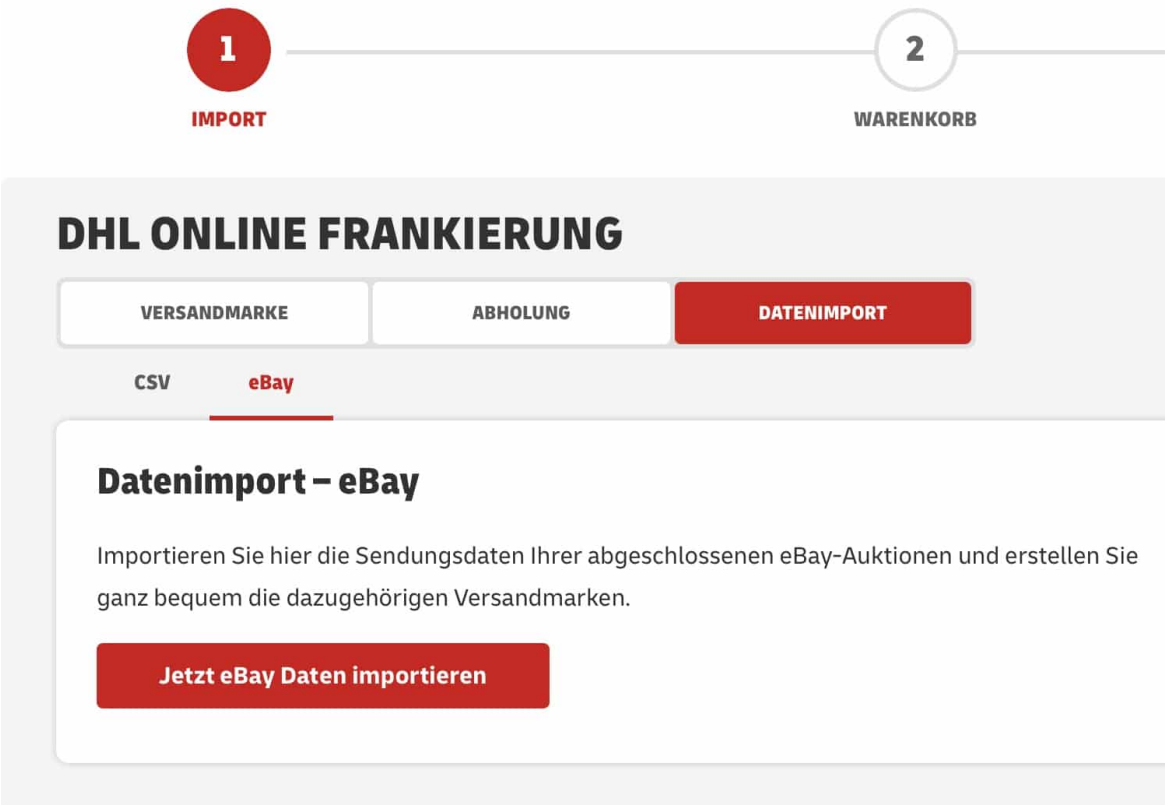
Frankieren einer eBay-Sendung per DHL

Verkaufen von Sachen über eBay ist relativ leicht, und durch die Übernahme des kompletten Zahlungsverkehrs durch ebay selbst ist auch die Abwicklung unkompliziert. Bis Sie dann die verkaufte Ware verschicken wollen. Wenn Sie bisher die Adressen Ihrer Käufer manuell eingegeben haben, machen Sie sich zu viel Arbeit!

Die manuelle Übertragung der Adressen ist nicht nur Aufwand, sondern auch ein Risiko: eBay schaut bei einer Reklamation sehr genau nach, ob der Versand tatsächlich auch exakt an die angegebene Adresse stattgefunden hat. Werden hier Abweichungen identifiziert, dann kann das schnell zu einer Entscheidung gegen den Verkäufer führen. Aus diesem Grund bietet eBay die Möglichkeit, die

Etiketten direkt aus dem System zu erstellen.

Dazu klicken Sie in Ihrem eBay-Konto auf **Verkauft**, dann auf **Versandetikett erstellen**. eBay bietet Ihnen nun eine Vielzahl von Paketdiensten und Produkten, aus denen Sie auswählen können und überträgt die Absender- und Empfängerdaten automatisch in den Paketschein. Über diesen Weg wird auch die Paketnummer in die Sendungsverfolgung der Auktion eingetragen und der Käufer informiert.

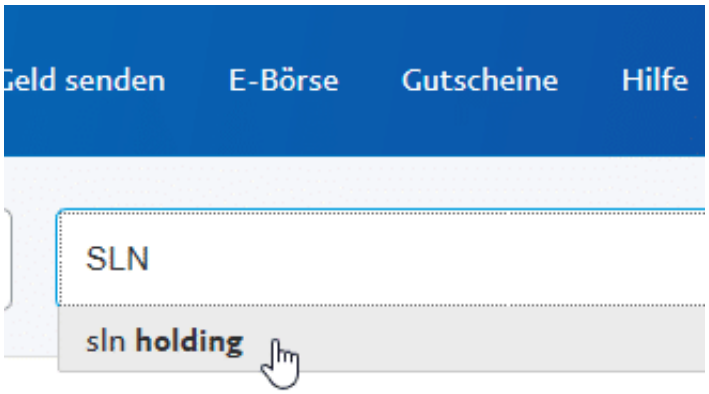


Dieser Weg hat einen Nachteil: Sie kommen nicht ganz so einfach an eine Rechnung für den Paketschein. Eine Alternative bietet DHL: Wenn Sie auf der DHL-Seite auf **Pakete versenden** > **Versandmarke kaufen klicken**, dann können Sie über **Datenimport** > **eBay** eine Verbindung zur eBay-Seite her und können die letzten Auktionen und deren Empfängeradressen importieren. Der Vorteil: Sie können eine Rechnung anfordern und haben die Pakete direkt in Ihrer Paketübersicht. Allerdings müssen Sie die Paketnummern manuell in die Auktionen eintragen.

Käuferschutz bei PayPal nutzen

Der Online-Kauf ist auf dem Weg, den klassischen Handel abzulösen. Sie sparen Zeit, Geld und haben dazu oft noch eine größere Auswahl. Die Kehrseite der Medaille: Sie haben oft keinen Ansprechpartner aus Fleisch und Blut. Kommt dann die Ware nicht, die Sie vorab bezahlt haben, dann geht der Stress los. Wenn Sie als Zahlungsmittel PayPal einsetzen, dann können Sie mit wenig Aufwand Käuferschutz beantragen.

Melden Sie sich dazu bei Ihrem PayPal-Konto an und klicken Sie auf **Letzte Aktivitäten**. Wenn Sie den betroffenen Einkauf nicht direkt sehen, dann klicken Sie in das Suchfeld und geben Sie den Namen des Händlers ein. Damit können Sie die Liste der Transaktionen filtern.

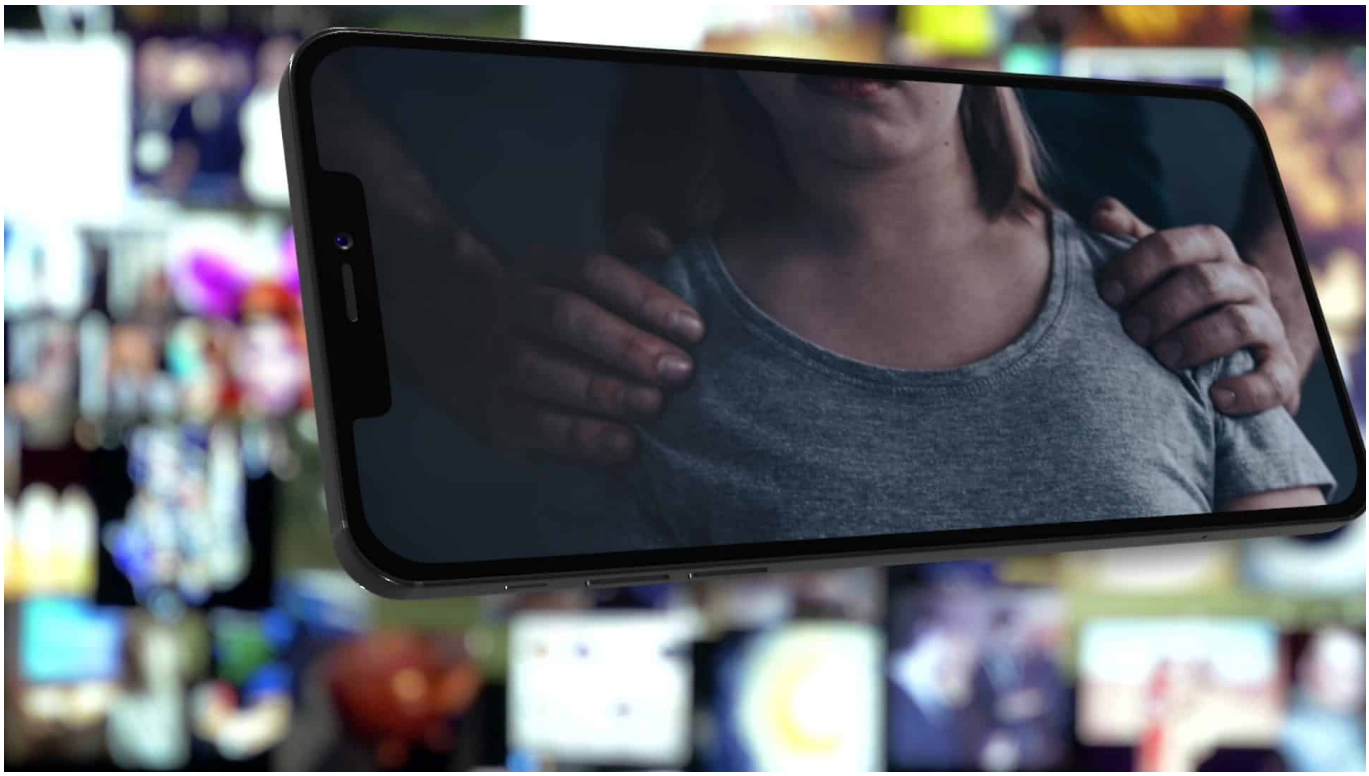


Öffnen Sie die Transaktion, dann finden Sie unten den Link zu **Problem melden**. Geben Sie die angeforderten Informationen an, dann wird automatisch ein Fall bei PayPal geöffnet. Das ist allerdings noch kein Antrag auf Käuferschutz, der zu einer Gutschrift führt!

PayPal empfiehlt nun, einige Tage auf eine Reaktion des Verkäufers zu warten. Wenn Sie das schon getan haben (oder ungeduldig sind): Klicken Sie in der PayPal-Übersicht auf **Konflikte**, dann öffnen Sie den gerade geöffneten Fall. Klicken Sie ganz unten auf **Paypal zur Klärung einschalten**. Sie müssen noch einige Informationen eingeben, dann wird PayPal offiziell mit der Lösung des Konflikts beauftragt. Wenn der Händler eine Zustellung der Bestellung nicht

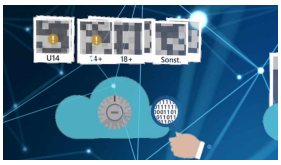
nachweisen kann, dann haben Sie gute Chancen, eine Gutschrift zu bekommen.

Warum es keine gute Idee ist, wenn Apple unsere Geräte durchsucht



Apple legt normalerweise großen Wert auf Datenschutz und Privatsphäre. Deshalb überrascht es, was Apple vor hat: In künftigen Betriebssystem-Versionen sollen die Geräte der User nach Fotos durchsucht werden, die Bilder sexualisierter Gewalt zeigen. Die Motivation ist verständlich - die Idee trotzdem schlecht.

Eigentlich gehört Apple in Sachen Datenschutz und Privatsphäre zu den Guten. Der Apfel-Konzern schränkt die Möglichkeiten von Trackern ein - und macht sie besser sichtbar. Das sorgt für deutlich mehr Privatsphäre. Auch weigert sich Apple immer wieder, verschlüsselte iPhones zu knacken und gibt sich auch viel Mühe, die iCloud sicher zu machen. Deshalb kam die jüngste Ankündigung etwas überraschend - auch für mich.



Apple verwendet bewährte Mechanismen zum Dateanabgleich[/caption]

Apple lässt auf den Geräten selbst suchen

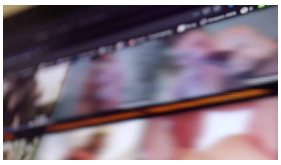
Denn Apple hat angekündigt, auf iPhones, iPads und PCs aktiv nach CSAM-Material zu suchen (Child Sexual Abuse Material). Die genaue Vorgehensweise wird in diesem White Paper beschrieben: Danach schaut sich der Konzern nicht etwa alle in der iCloud gespeicherten Fotos und Videos an, sondern wendet eine - wenn man so will - "elegantere" Methode an.

Apples Betriebssysteme werden wohl ab Herbst, wenn die neuen Betriebssystem-Versionen herauskommen - zunächst aber nur in den USA - auf den Geräten(!) nachsehen, ob dort bereits bekanntes und in entsprechenden Datenbanken gespeichertes Material vorhanden ist. Etwa Fotos, die sexualisierte Gewalt an Kindern zeigen. Schon im Gerät! Das ist das Besondere.

Inkriminierte Fotos vor dem Upload gekennzeichnet

Werden bei diesem Check auffällige Fotos entdeckt, erzeugt das Betriebssystem ein besonderes Zertifikat. Erst nach dem Upload in die iCloud schauen sich Mitarbeiter das Material möglicherweise an - sofern mehrere solche Aufnahmen entdeckt wurden (wie viele genau, verrät Apple nicht).
[caption id="attachment_775756" align="alignnone" width="1030"]
Technisch gesehen ist das eine elegante Methode, da die Vorabkontrolle im Smartphone, iPad oder PC erfolgt - und nicht etwa ohne begründeten Verdacht alle Fotos in der Cloud durchforstet werden.

Von einer "Totalüberwachung durch die Hintertür" kann meiner Ansicht nach keine Rede sein. Schon allein deswegen, weil es keine Totalüberwachung gibt.



Es weren "nur" bereits bekannte Bilder entdeckt[/caption]

Missbrauch nicht nur möglich, sondern fast sicher

Allerdings hinterlässt es einen nicht nur merkwürdigen Eindruck, wenn ein US-Konzern jedes einzelne Gerät aktiv - wenn auch softwaregesteuert - untersucht. Zwar für eine gute Sache - aber dennoch. Hier öffnet Apple die Büchse der Pandora: Es besteht die begründete Sorge, dass solche Technologien missbraucht werden.

Durch Hacker: Sie könnten arglosen Usern inkriminiertes Material unterjubeln (und so Alarm auslösen). Durch Regierungen, die Apple auffordern könnten, ihre Scan-Technologie für andere Zwecke einzusetzen. Und durch die NSA, die sowieso für alles zu haben ist, was dabei hilft, die Kommunikation zu überwachen.

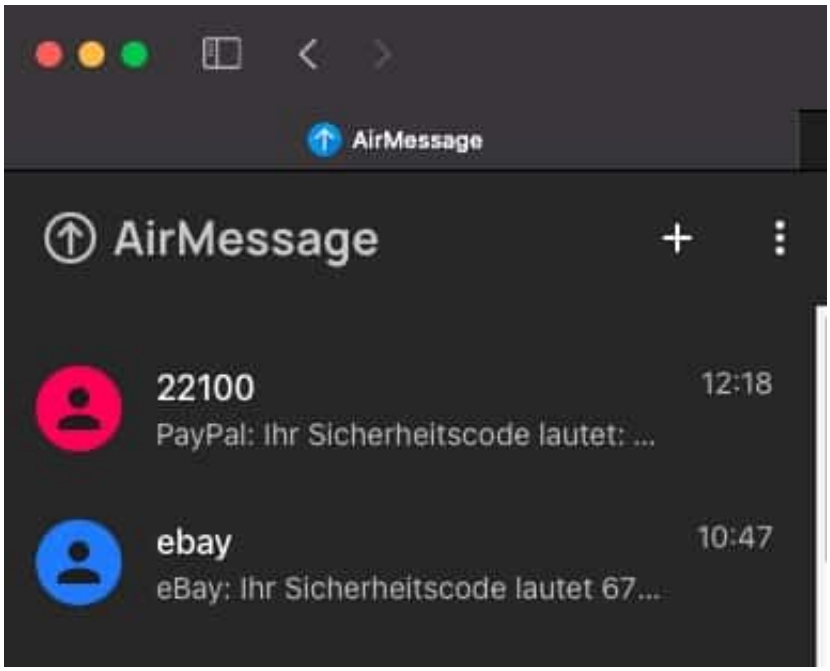
Auch wenn Apple eine vergleichsweise elegante technische Lösung wählt und zweifellos einen guten Zweck verfolgen möchte: Die Risiken sind einfach viel zu hoch. Zwar werden nicht alle Befürchtungen eintreten, aber einige gewiss - und das kann niemanden gefallen. Es ist nie eine gute Idee, ein Problem lösen zu wollen - und Dutzende neue zu schaffen.

[caption id="attachment_77557" align="alignnone" width="1030"]Microsoft beteiligt sich am Internationalen Jahr[/caption]

iMessage unter Android nutzen

Die Zahl der mobilen Geräte, sie Sie parallel nutzen, ist meist größer als Eins. Solange Sie mit allen Geräten innerhalb eines mobilen Betriebssystems bleiben, haben Sie wenig Probleme. Wenn Sie aber zwei Smartphones nutzen und eines mit iOS und das andere mit Android läuft, dann haben Sie ein Problem: iMessage, der Apple-eigene Kurznachrichtenservice, läuft nicht auf Android. Wie zeigen Ihnen eine Lösung!

iMessage soll ein Problem lösen, das viele Anwender kennen: SMS kommen nur am Smartphone an. Wenn Sie das nicht neben sich liegen haben, dann gehen wichtige Meldungen an Ihnen vorbei. iMessage nutzt iCloud, um die Nachrichten zeitnah auf iPhone, iPad, MacBook und iMac zu bringen. Die Geräte müssen nur mit der selben Apple ID angemeldet sein. Das funktioniert bei Android-Geräten natürlich nicht.

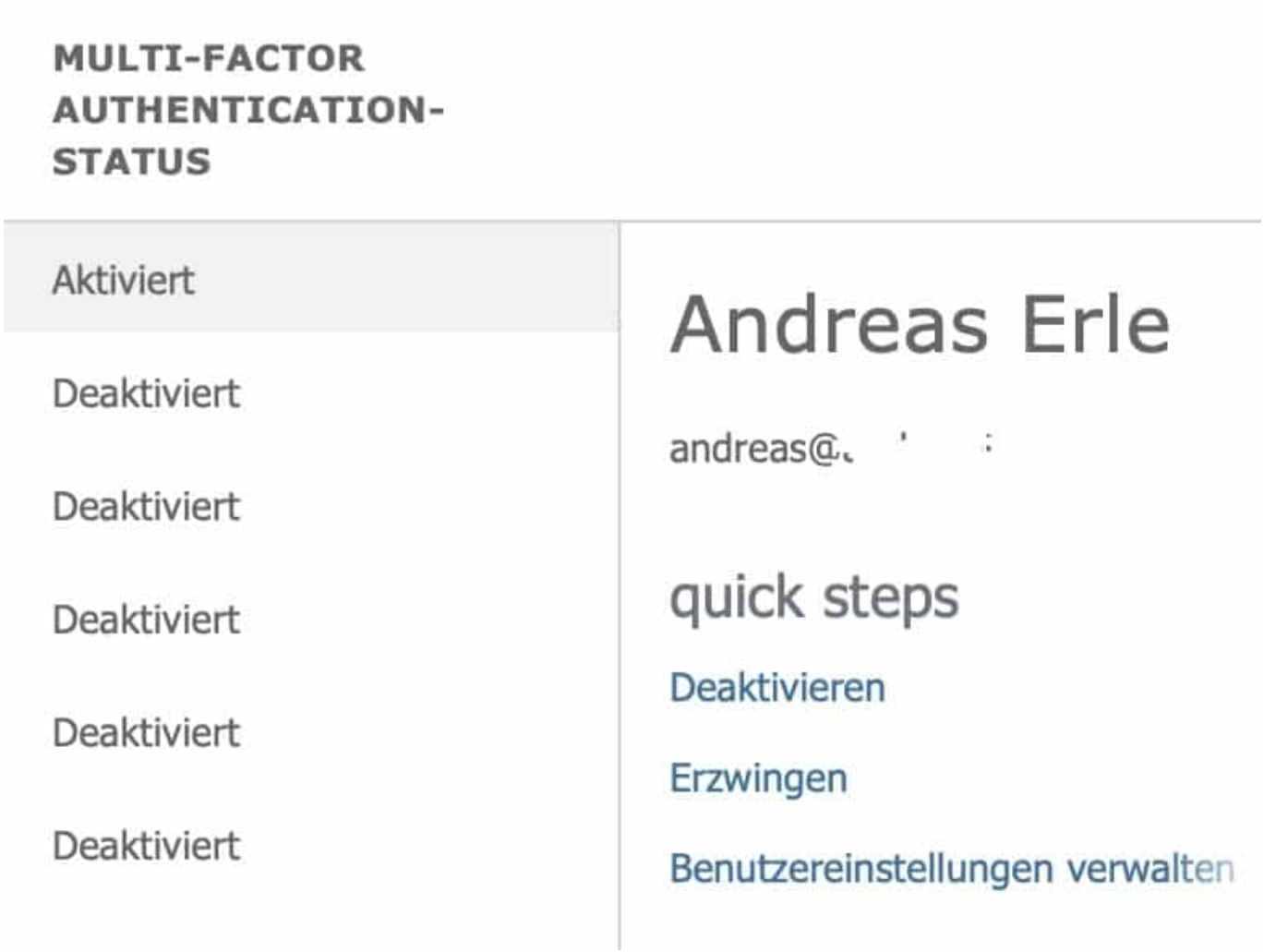


Die Alternative: AirMessage für den Mac. Dazu müssen Sie den Mac, auf dem die Software läuft, zum AirMessage-Server machen und laufen lassen, damit dieser die eingehenden iMessages dann weiterleitet. PArallel dazu müssen Sie auf Ihrem Android-Gerät die AirMessage-App installieren und können dann sowohl eingehende iMessages lesen und beantworten wie auch neue schreiben.

Einschalten der Zwei-Faktor-Authentifizierung (2FA) bei Office 365

Der Schutz eines E-Mail-Kontos mit einem Passwort hat ein gewisses Risiko: Bringt ein Angreifer dieses in Erfahrung, dann kann er auf Ihr Konto zugreifen und es missbrauchen. Besser ist es, einen weiteren Faktor in die Authentifizierung mit aufzunehmen, beispielsweise eine SMS an Ihr Mobiltelefon. Wir zeigen Ihnen, wie das bei Office 365 geht.

Der Sinn dieses zweiten Faktors ist die Trennung von Wissen und Besitz. Ein Kennwort wissen Sie, wenn jemand anderes in Erfahrung bringt, dann weiß der es auch und kann es verwenden. Wenn Sie zusätzlich einen Code per SMS bekommen und diesen als zweiten Teil der Anmeldung nutzen müssen, dann muss der Angreifer zusätzlich noch Ihr Handy unter Kontrolle bekommen.



Rufen Sie die Admin-Seite von Office 365 auf, dann klicken Sie auf **Benutzer**, setzen Sie einen Haken beim dem Benutzer, den Sie anpassen wollen und klicken Sie ihn an. Unten rechts klicken Sie dann auf **Mehrstufige Authentifizierung**. Office 365 öffnet den Benutzer und erlaubt Ihnen unten rechts die **Mehrstufige Authentifizierung** zu aktivieren.

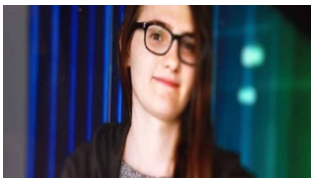
Bei jeder Anmeldung müssen Sie nun neben Ihrem Passwort einen Code eingeben. Diesen bekommen Sie entweder per SMS, per E-Mail oder über die Microsoft Authenticator-App.

Entwicklerin Lilith Wittmann will Open Data fördern

Open Data ist ein sinnvolles Konzept: Daten werden der Öffentlichkeit zuständig gemacht - und lassen sich frei für Apps oder Anwendungen verwenden. Das fördert die Kreativität und bringt im Idealfall viele gute Anwendungen hervor. Problem: In Deutschland wird OpenData nicht wirklich gefördert. Das will LIlith Wittmann ändern.

In einer idealen Welt sind alle Daten, die unter dem Einsatz von Steuermitteln ermittelt wurden oder entstanden sind, frei für die Allgemeinheit zugänglich. Ausgenommen natürlich Daten, die aus gutem Grund geheim oder unter Verschluss sind. "Open Data" wird das genannt, wenn Daten frei zugänglich sind.

Warum sollten Bürgerinnen und Bürger nicht frei über alle Daten verfügen können? Die Crowd hat oft viel bessere Ideen, wie sich Daten kreativ zusammenbringen lassen - um neue Erkenntnisse zu gewinnen oder Dienstleistungen anzubieten.



Sicherheitsexpertin Lilith Wittmann setzt sich für mehr Open Data ein[/caption]

Open Data: Offizielle Daten der Allgemeinheit zur Verfügung stellen

Eigentlich könnte man erwarten, dass die Politik genau das fördert. Schließlich redet die Politik gerne von Digitalisierung und wie wichtig es wäre, in diesem Bereich voranzukommen. Doch die Daten, die Behörden und öffentliche Institutionen erfassen und ermitteln, sind oft genug Verschlusssache.

Doch es gibt auch Daten, die stehen grundsätzlich zur Verfügung - aber niemand redet darüber. Es gibt keine öffentliche "Schnittstelle", wie Experten dazu sagen. Über eine API (Application Programming Interface) könnte sich jede App, jede Software mit den öffentlich gemachten Daten versorgen.

In Wahrheit gibt es solche Schnittstellen teilweise, doch die Behörden dokumentieren diese Schnittstellen nicht. Die Folge: Nur Insider können sie verwenden, nicht aber die Öffentlichkeit.

[caption id="attachment_775773" align="alignleft" width="1024"]

Es lagern so viele Daten in Aktenschränken – lasst sie uns förderm und nutzen[/caption]

Lilith Wittmann will Schnittstellen dokumentieren

Genau das will Lilith Wittmann ändern. Gerade erst hat die Software-Entwicklerin dadurch Aufsehen erregt, dass sie Schwachstellen in der Wahlkampf-App "CDU Connect" entdeckt hat - und wurde dafür von der CDU angezeigt.

Jetzt wirbelt Lilith wieder Staub auf: Sie hat ein Projekt gestartet, um gemeinsam mit Freiwilligen eigentlich offene Schnittstellen zu dokumentieren, damit sie jede/r nutzen kann. So gibt es beispielsweise solche Schnittstellen für die Warn-App NINA. Lilith Wittmann hat die App analysiert - und herausgefunden, wie sich relevante Daten abrufen lassen - und das dokumentiert.

Bundesstelle für Open Data

Mit der als politischen Protest gedachten und alles andere als offiziellen Bundesstelle für Open Data will Lilith Wittmann Druck machen: Sie fordert Entwickler und Aktivisten auf, frei erreichbare API von Bundesbehörden und offiziellen Stellen gemeinsam mit ihr zu dokumentieren. In einem Blogbeitrag erklärt sie die Idee.
[caption id="attachment_775774" align="alignleft" width="1030"]

Erstaunlicherweise finden nicht alle diese Idee toll: Offensichtlich wollen einigen Behörden und Verantwortliche gar nicht, dass solche Schnittstellen öffentlich werden - und von allen genutzt werden können. Das sollte sich unbedingt ändern. Denn je mehr Menschen öffentlich bereitgestellte Schnittstellen und Daten nutzen, deso höher ist die Wahrscheinlichkeit, dass die Daten - und damit auch die eingesetzten Steuergelder! - sinnvoll verwendet werden.

https://vimeo.com/156265875

Das Konzept Open Content: So profitieren alle von Inhalten

Identitätsklau im Internet: Wie Betrüger Eure Daten missbrauchen

Es kann jeden treffen: Identitätsdiebstahl. Je mehr Daten Cyberbetrüger über eine Person in die Hände bekommen, desto eher können sie im Netz die Identität einer fremden Person übernehmen - und dabei mitunter auch Schaden anrichten.

Wenn sich im Briefkasten ominöse Rechnungen häufen oder ständig Zahlungsaufforderungen von Firmen eintrudeln, die Sie nicht kennen, sind Sie möglicherweise Opfer eines Identitätsdiebstahls geworden.

Betrüger nutzen regelmäßig die Namen anderer, um online Geschäfte zu erledigen. Laut einer Statista-Umfrage waren bereits etwa 30 Prozent der Bundesbürger mindestens einmal Opfer von Identitätsklau. Kriminelle missbrauchen dabei persönliche Verbraucherdaten. Sie bestellen Waren im Internet mit den geklauten Daten, schließen Mitgliedschaften und Abonnements ab oder versenden Spam-Mails.

Was genau ist Identitätsdiebstahl?

Es gibt viele verschiedene Formen von Identitätsklau im Internet. In erster Linie schließen die Betrüger kostenpflichtige Verträge und Abonnements ab, richten Nutzerkonten ein oder shoppen nach Herzenslust auf Kosten des Opfers. Nachfolgend ein paar ganz konkrete Beispiele für Schäden durch Identitätsklau:

- Abonnements für Premium-E-Mail-Konten
- Abonnements für Online-Dating-Portale
- Verträge mit kostenpflichtigen Streaming-Diensten
- Erwerb von Hörbüchern
- Erwerb von Software-Lizenzschlüsseln
- Abschluss von Mobilfunkverträgen
- Abbuchungen über die Handy-Rechnung mit PIN-Freigabe
- Missbrauch von Payback

Wenn der Schaden passiert ist

Im schlimmsten Fall merkt ein User zunächst gar nicht, dass er Opfer von Identitätsdiebstahl geworden ist und ignoriert die Zahlungsaufforderungen. Da auch der Händler oder Dienstleister nichts von dem Betrug weiß, leitet er weitere Schritte ein, um sein Geld zu bekommen.

Im schlimmsten Fall meldet er die Zahlungsverweigerung an die Schufa, wo sich das negative Merkmal direkt auswirkt, wenn der Betroffene Geld von seiner Bank braucht.

Mit einem negativen Schufa-Eintrag ist es sehr schwierig, einen günstigen Kredit zu bekommen. Hier bleibt häufig nur noch die Möglichkeit, einen schufafreien Kredit aufzunehmen. Langfristig muss sich der Betroffene unbedingt darum kümmern, den Sachverhalt aufzuklären, damit der Schufa-Eintrag wieder gelöscht werden kann.

Wie kommen die Diebe an die Daten?

[caption id="attachment_775769" align="alignleft" width="440"]


Mit einer sogenannten Phishing-Mail kommen die Betrüger häufig ganz einfach an die Daten der User. Hier ist es wichtig, ein paar Vorsichtsmaßnahmen zu treffen.[/caption]

Phishing ist eine sehr beliebte Methode, um an die Daten anderer Nutzer im Internet zu gelangen. Der Datendiebstahl kann auch über den Provider erfolgen oder über Social Media. Große Unternehmen von E-Mail-Providern oder Onlineshops sind hier besonders anfällig. Smartphone, E-Mail-Konto und Onlineshopping werden hier sehr leicht zur Falle.

Natürlich sind die User hier teilweise selbst schuld, weil sie Allerwelts-Passwörter verwenden. Sehr beliebt ist 12345678. Hier ist es tatsächlich notwendig, sich entsprechend zu schützen und sichere Passwörter zu verwenden.

Wer haftet für den entstandenen Schaden?

Grundsätzlich muss der Geschädigte nichts bezahlen, was er nicht selbst bestellt hat. Der Verkäufer ist hier in der Beweispflicht und muss beweisen, dass der Geschädigte tatsächlich selbst den Kauf getätigt hat. Wer nachweisen kann, dass er von der Bestellung nichts wusste, muss auch nicht bezahlen. Der Geschädigte muss hier nicht haften.

Das gilt allerdings nur, wenn Sie gewisse Sicherheitsmaßnahmen ergriffen haben und der Umgang mit den eigenen Daten nicht grob fahrlässig erfolgt ist. Wer Kennwörter, sensible Daten oder PINs im Internet preisgibt, darf sich nicht wundern, wenn Unbefugte diese Daten benutzen. Die Rechtslage ist hier allerdings nicht eindeutig. Denn es ist noch unklar, welche

Sicherheitsvorkehrungen Verbraucher treffen müssen.

Was tun, wenn’s passiert ist?

Wer feststellt, dass er Opfer eines Identitätsklaus geworden ist, sollte unbedingt schnell handeln. Am besten ist es, direkt Anzeige bei der Polizei zu erstatten. Der nächste Schritt ist eine Information an den Online-Shop oder die Stelle, die das Geld verlangt, dass keine Bestellung erfolgt ist. Das sollte in jedem Fall schriftlich geschehen, dabei auch das Aktenzeichen der polizeilichen Anzeige mit angeben. Wenn das Geld bereits vom Konto abgebucht ist, sofort die Karte sperren lassen. So lässt sich weiterer Missbrauch verhindern.

Was können User tun, um sich zu schützen?

Das Bundeskriminalamt empfiehlt ein paar Maßnahmen, um sich vor Datenmissbrauch zu schützen.

- Die Software von Betriebssystem, Anti-Virenprogramm und Browser sollte immer auf dem neusten Stand sein. Das heißt, sie sind regelmäßig zu aktualisieren.
- Datensicherungen auf externen Datenträgern sollten regelmäßig erfolgen.
- Programmdownloads sollten nur über die Originalquellen erfolgen.
- E-Mail-Anhänge oder Links von unbekannten Absendern oder von nicht vertrauenswürdigen Absendern niemals öffnen.
- Unseriöse Internetseiten sind zu meiden.
- User sollten keine Werbebanner anklicken.
- Sensible persönliche Daten dürfen User nicht überall im Internet oder in den sozialen Medien preisgeben.
- Passwörter sollten immer effektiv und sicher sein.
- Bei der Verwendung öffentlicher WLAN-Hotspots ist immer Vorsicht geboten.
- Bei Bank-Transaktionen sollte immer die Zwei-Faktoren-Authentifikation zum Einsatz kommen.
- User sollten nicht an Online-Gewinnspielen teilnehmen.
- Wer Schriftstücke entsorgt, sollte immer dafür sorgen, dass persönliche Daten unkenntlich sind.

Einen 100-prozentigen Schutz vor Identitätsklau gibt es nicht. Doch durch bestimmte Verhaltensweisen ist es möglich, das Risiko gering zu halten.

Tipps für die Erstellung eines sicheren Passworts

Viele User tendieren dazu, ein Passwort für alle möglichen Nutzerkonten zu verwenden. Sie scheuen den Mehraufwand, den es bedeutet, sich für jeden Dienst ein neues Kennwort auszudenken. Zudem haben sie Angst, das Kennwort wieder zu vergessen.

Es ist allerdings so, dass ein Hacker, der Zugriff auf das E-Mail-Konto hat, sich mit dem Passwort dann auch Zugriff auf viele andere Dienste verschaffen kann, wenn das Passwort überall das gleiche ist.

Ein sicheres Passwort ist komplex aufgebaut. Das soll den Zugang zu den damit gesicherten Daten erschweren. Länge der gewählten Zeichenfolge und die Struktur tragen zur Sicherheit bei.

- **die Länge des Passworts**

Ein sicheres Passwort ist mindestens acht bis zehn, besser sogar zwölf oder mehr

Zeichen lang. Je länger das Passwort, umso schwieriger ist es für einen Hacker es zu knacken.

- **die Zeichenfolge**

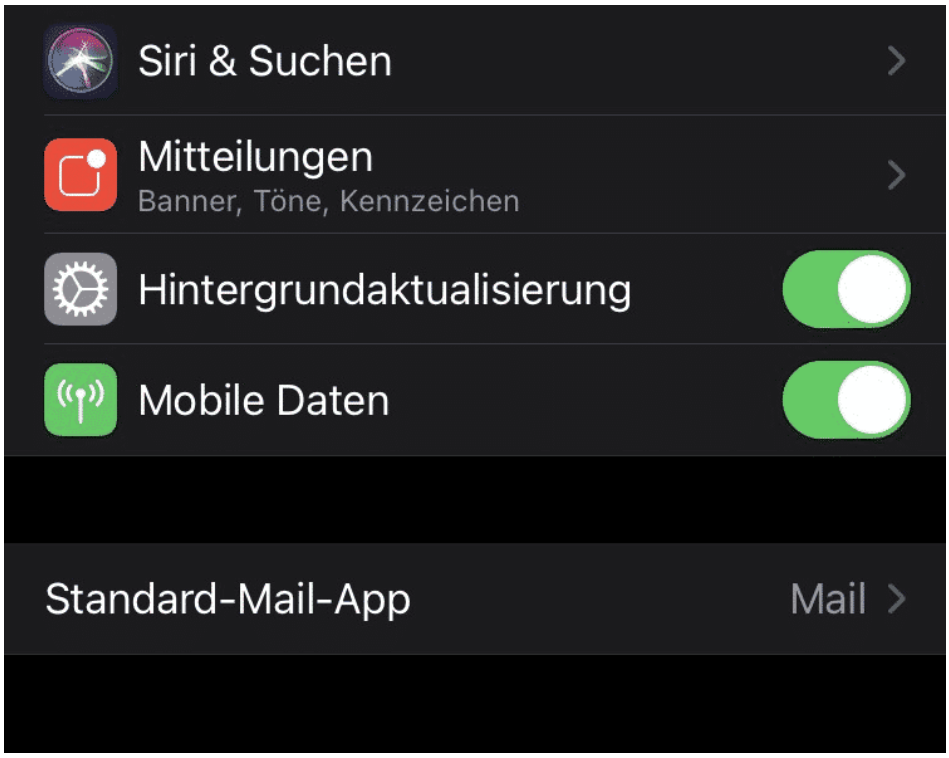
Das Passwort sollte eine Kombination aus Buchstaben, Zahlen und Sonderzeichen sein, abwechselnde Groß- und Kleinschreibung trägt ebenfalls zu mehr Sicherheit bei.

Kennwörter sollten niemals in einer Tabelle auf dem Computer gespeichert sein. Was sich allerdings speichern lässt, ist eine Tabelle, die Eselsbrücken zu den Passwörtern enthält oder Hinweise, die nur der User versteht.

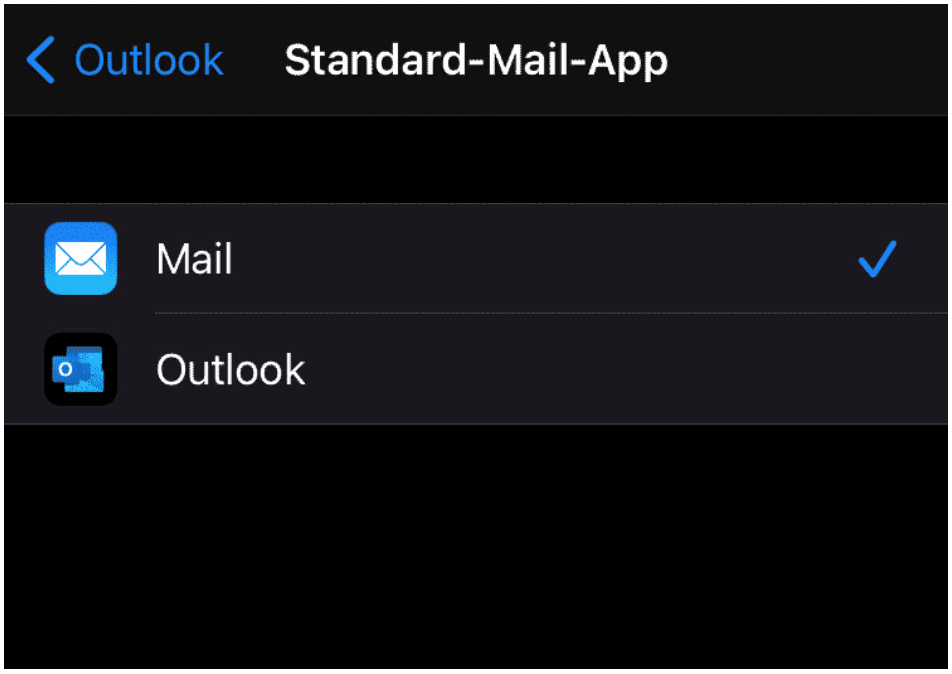
Umstellen des Standard-E-Mail-Programms bei iOS

Mail ist das Standard-Programm für E-Mails auf allen Apple-Geräten. Viele Anwender nutzen aber lieber Alternativen wie Outlook oder Boomerang. Das ist kein Problem, allerdings nimmt iOS weiterhin Mail, wenn Sie einen Link für eine neue E-Mail antippen. Das können Sie seit iOS 14 aber schnell ändern!

Mit iOS 14 hat eine Funktion Einzug gehalten, die auf Desktops schon lange Standard ist: Die Möglichkeit, den Standard-Mailprogramm festzulegen. Damit dies möglich ist, müssen Sie Ihr natürlich erst einmal aus dem App Store installieren. Dann wechseln Sie in die Einstellungen von iOS und rollen nach unten, bis Sie den Eintrag für einen das installierte E-Mail-Programm sehen. Tippen Sie dieses an.



Als nächstes suchen Sie den Eintrag **Standard-Mail-App**. Wenn Sie diesen antippen, dann zeigt Ihnen iOS alle installierten Mail-Apps an. Markieren Sie die, die der Standard werden soll.

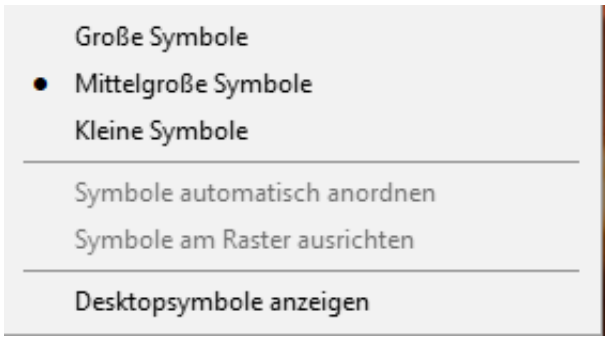


Beim nächsten Klick auf einen Link wird die neue Standard-App geöffnet.

Tricks zu Desktopsymbolen bei Windows 10

Ihr Desktop hat seinen Namen zu Recht: Er fungiert als Schreibtischfläche, auf der Sie Ihre wichtigsten Programme und deren Symbole frei anordnen können. Und genau wie bei Ihrem Schreibtisch zuhause werden Sie irgendwann einmal aufräumen wollen, Ordnung schaffen oder einfach den Blick freibekommen. Windows 10 bietet Ihnen dafür schnelle Hilfe direkt auf dem Desktop!

Klicken Sie auf einen freien Bereich auf dem Desktop, dann auf **Ansicht**. Im sich öffnenden Menü können Sie dann auswählen, in welche Größe die Desktopsymbole dargestellt werden sollen. Vermissen Sie alle Ihre Desktopsymbole? Dann kontrollieren Sie hier, ob **Desktopsymbole anzeigen** aktiviert ist. Der Haken neben dieser Option kann auch Chaos beseitigen: Entfernen Sie ihn, dann blendet Windows 10 alle Desktopsymbole aus.



Automatische Ordnung schaffen Sie mit dem zweiten Block an Optionen: **Symbole automatisch anordnen** schiebt quasi alle Symbole zueinander. **Symbole am Raster ausrichten** stattdessen ordnet die Desktopsymbole automatisch an einem Raster ausgerichtet an. Sie müssen also nicht manuell tätig werden. Der Nachteil: Wenn Sie Ihre Symbole manuell genau um ein Hintergrundbild herumdrapiert haben, dann machen Sie damit all Ihre Mühe zunichte. Diese beiden Einstellungen sind also mit Vorsicht zu genießen.

Eine weitere Sortiermethode ist die nach einem Merkmal der Dateien: mit einem Rechtsklick auf eine freie Stelle des Desktop und **Sortieren nach** können Sie dies festlegen.

Anpassen von Bildern unter Windows

Ein Foto auf dem Smartphone entsteht meist aus der Situation heraus und ohne große Vorbereitung. Nicht unbedingt immer als Schnappschuss, aber ohne die Stabilität, die eine normale Kamera mit sich bringt. Neben dem Beschneiden von Bildern können Sie in der Microsoft Fotos-App auch diverse Korrekturen in den Bildern vornehmen.

Unter **Filter** können Sie das Bild durch vorgefertigte Anpassungen anders wirken lassen. Der eine Filter macht die Farben kälter, der andere wärmer, es gibt Sepia und Schwarz-Weiß-Filter.

Bevor Sie aber einen Filter anwählen, klicken Sie auf die Voransicht auf **Foto verbessern**, damit passt die Fotos-App Helligkeit, Kontrast und Sättigung des Bildes automatisch an, damit das Bild optimal aussieht. Diese Anpassungen können Sie durch den Regler im Voransichtsbild von der Wirkung her verstärken oder abschwächen. Probieren Sie es einfach aus!

Wenn sie einen Filter ausgewählt haben, dann können Sie diesen mit dem Regler Filterintensität von der Stärke her verändern. Probieren Sie mit den verschiedenen Einstellungen herum, aber vermeiden Sie zu starke Effekte. Diese lassen ein Bild schnell künstlich aussehen – was aber durchaus auch gewünscht sein kann!

Unter **Anpassungen** können Sie die Belichtung, die Farbe, Schärfe und die Vignette (die Randbereiche des Bildes) anpassen. Zusätzlich finden Sie dort auch noch zwei wichtige Schnellkorrekturen, die Sie immer wieder brauchen werden:

Über **Rote Augen** können Sie durch einen Klick auf ein durch den Blitz rot dargestelltes Auge im Bild diesen Fehler korrigieren.

Über **Fleckenkorrektur** können Sie Flecken auf einem Objekt ausgleichen. Die Fotos-App verwenden dann die Randbereiche des angeklickten Bereiches und versucht, diese natürlich weiterzuentwickeln und den Flecken damit unsichtbar zu machen.