

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

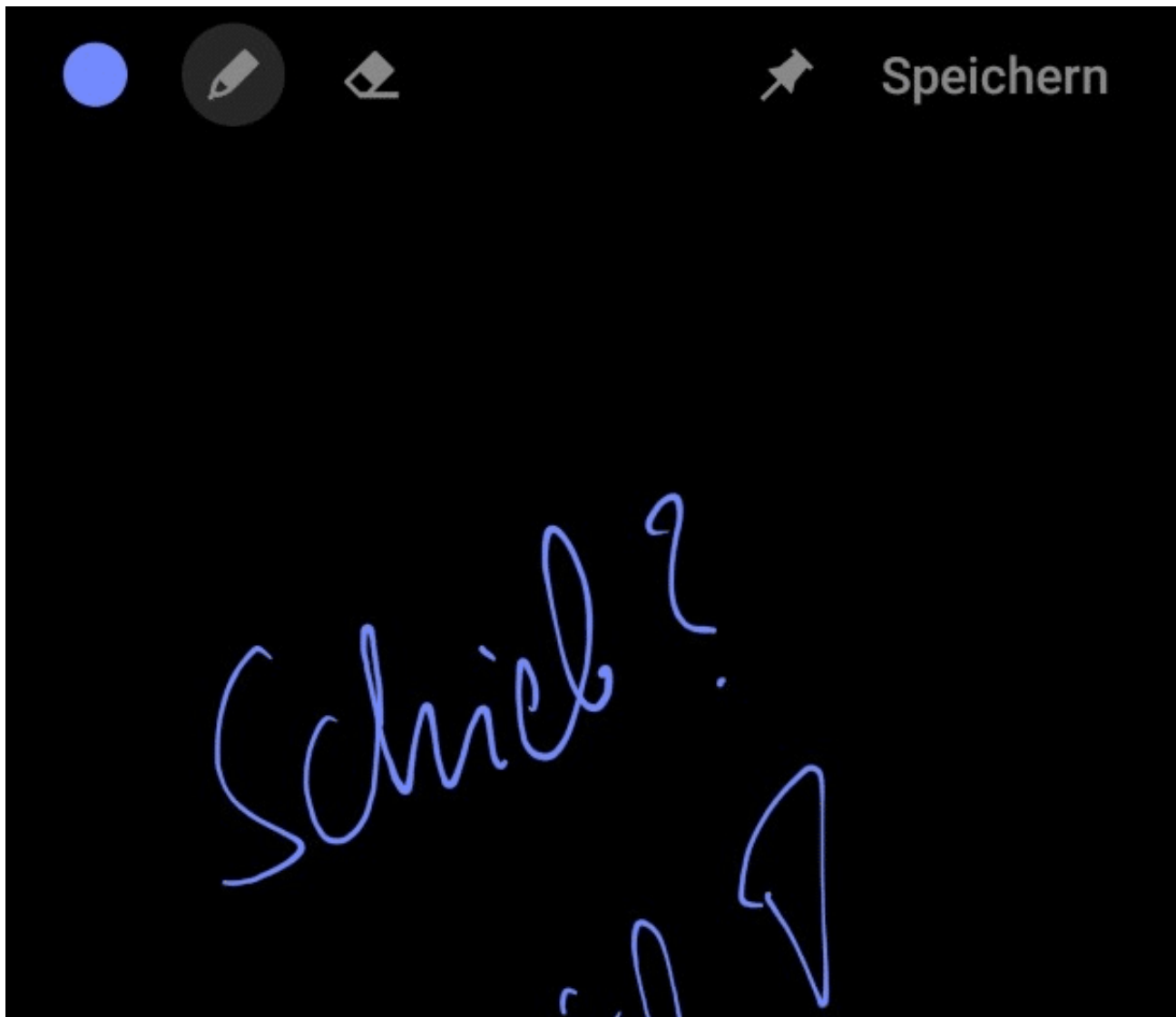
Schieb Report

Ausgabe 2019.36

Kurznotizen direkt auf dem Startbildschirm platzieren

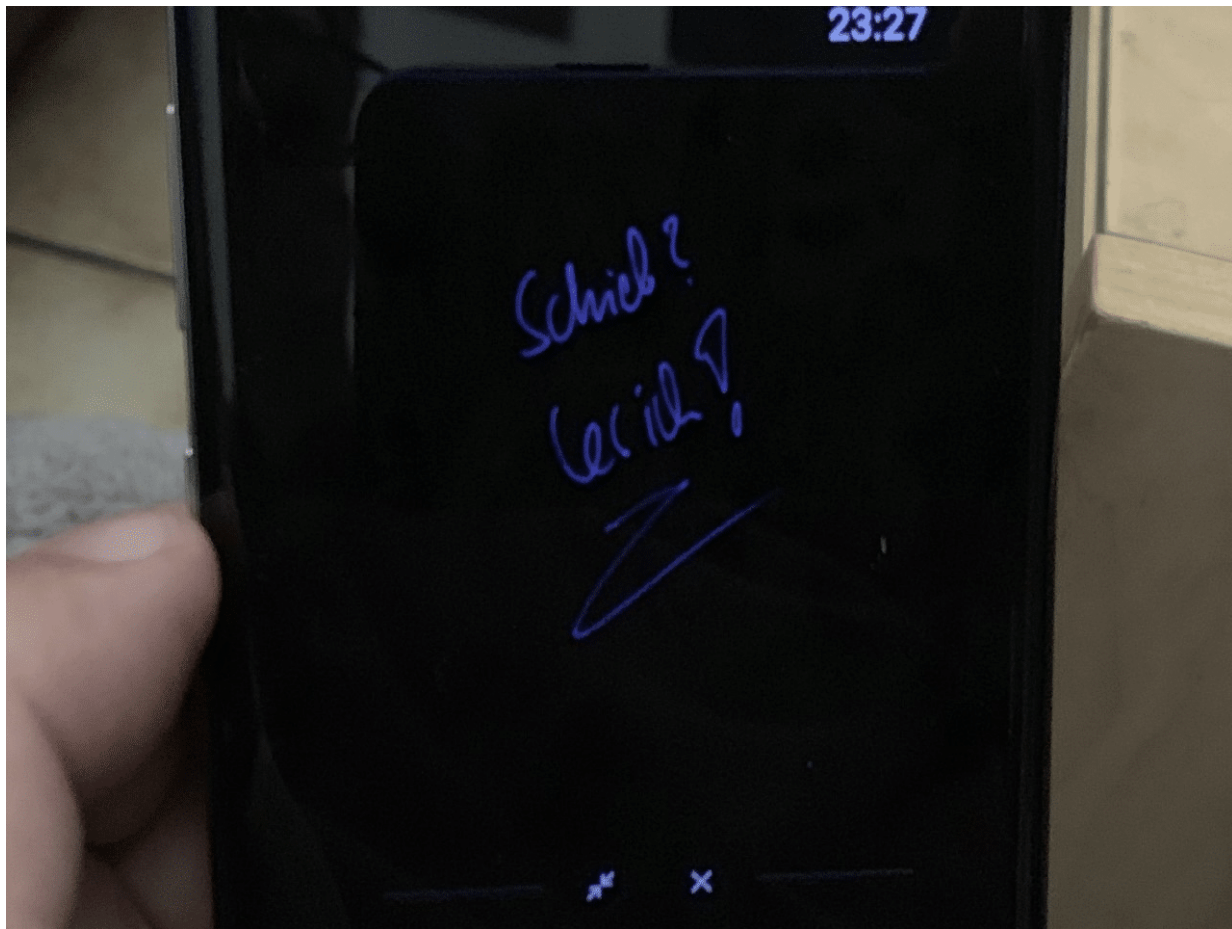
Der alte Notizzettel hat ausgedient. So schön er war, der Zeitaufwand der Suche, wenn Sie eine bestimmte Notiz dann mal brauchten, hat ihn aufs Altenteil geschickt. Nur ist das Notieren auf einem Smartphone normalerweise mit mehr Aufwand verbunden. Wenn Sie ein Smartphone mit einem Stift besitzen, dann können Sie allerdings fast so komfortabel wie mit dem Notizzettel arbeiten!

Das Samsung Galaxy Note hat den Stift direkt integriert. Wenn Sie ihn aus dem Gehäuse entfernen, dann startet direkt die Notizapp. Malen Sie auf dem Display, und Ihr Geschreibsel wird als Notiz abgespeichert und lässt sich schnell von dort wieder aufrufen. Allerdings ist das nur der halbe Komfort: Sie notieren sich oft Dinge, die Sie direkt wieder brauchen. Statt jetzt die Notiz wieder herauszusuchen, platzieren Sie sie doch direkt auf dem Always On-Display (AOD)!



Dazu tippen Sie in der Notiz oben auf die kleine Reißzwecke. Die sorgt dafür, dass die Notiz über den Benachrichtigungen im Always On-Display angezeigt wird. Dazu muss das Gerät nicht

mal entsperrt werden. So kann beispielsweise auch ein Kollege Ihre "Notizzettel" in Form Ihres Smartphones nutzen, wenn Sie gerade nicht da sind.



Wird das Always On-Display nicht direkt angezeigt, dann tippen Sie einmal auf den Bildschirm. Alternativ schalten Sie es unter **Einstellungen > Sperrbildschirm > Always On Display > Immer anzeigen** ein.

Deutsche Verlage senden auf Facebook Watch

Facebook: Wer die Massen erreichen will, kommt um das Soziale Netzwerk nicht herum. 2,8 Milliarden Nutzer weltweit. Das ist einfach attraktiv. Und deshalb versuchen auch Verlage und Sender, im Netzwerk präsent zu sein – wohl wissend, dass das auch eine Menge Nachteile mit sich bringt. Jetzt haben führende Verlage aus Europa eine Kooperation mit Facebook bekanntgegeben: Sie stellen exklusive Video-Inhalte auf Facebook Watch zur Verfügung. Ob das eine gute Idee ist?

Mark Zuckerbergs Soziales Netzwerk Facebook macht gemeinsame Sache mit großen Verlagshäusern aus Europa. Darunter Springer, Burda sowie Gruner+Jahr aus Deutschland.

Eine solche Headline liest man selten. Denn normalerweise sind Facebook und die großen Zeitungsverlage wie Hund und Katze. Sie verstehen sich nicht. Kommen aus anderen Welten. Und können fast unmöglich ein und dasselbe Herrchen haben...



Eigene Sendeformate auf Facebook Watch

Doch jetzt haben [Facebook](#) und einige Großverlage doch tatsächlich ein gemeinsames Projekt gestartet: Springer, Burda und Gruner+Jahr werden auf der Video-Plattform **Facebook Watch** mit eigenen Video-Formaten vertreten sein. Mit eigenen täglichen "Sendungen", könnte man sagen. Aber eben nicht fürs lineare Fernsehen, sondern für die Video-Ecke bei Facebook.

"Bild Daily", "Welt News", "Focus Life Hacks": So heißen die täglichen Sendungen, die künftig auf Facebook zu sehen sein sollen. "Bild daily" gibt es sowieso schon und kommt jetzt auch auf Facebook Watch. "Welt News" soll relevante Nachrichten aus der Welt präsentieren. Und "Focus Life Hacks" eine Art Ratgebersendung sein: Die Zuschauer können sich mit Fragen an die Redaktion wenden und Feedback geben.

Facebook unterstützt die Verlage. Nicht nur bei der Konzeption und Erstellung der Formate, sondern auch finanziell. Laut Branchenmeldungen zahlt Facebook einen zweistelligen Millionenbetrag an die Verlagshäuser, um ihnen den Start in die Videowelt bei Facebook zu versüßen. Facebook hat keine eigenen Inhalte und ist auf namhafte Lieferanten angewiesen.

Man könnte es wohl auch als **Köder** bezeichnen.



Processed with VSCO with a8 preset[/caption]

Unheilvolle Liäson eingegangen

Die Verlagshäuser haben angebissen – und hängen jetzt am Haken. Sie werden die Zusammenarbeit vertiefen und haben künftig ein starkes Interesse daran, dass es Facebook gut geht. Denn geht es Facebook gut, dann schauen auch mehr Menschen die Online-Sendungen der Verlage auf Mark Zuckerbergs Plattform. Gut für die Verlage. Noch besser für Facebook.

Die Werbeeinnahmen teilen sich Facebook und die Verlagshäuser. Es soll also ein eigenes Ökosystem entstehen. Klingt nach Win-Win.

Doch die Verlagshäuser gehen damit eine gefährliche Koexistenz ein. Denn wenn sie erst einmal angewiesen sind auf den Ausspielweg Facebook – und später vielleicht auch Instagram -, wie sich dann wieder trennen? Das ist fast unmöglich.

Gefährlich auch deswegen, weil Mark Zuckerberg unberechenbar ist. Sein Wort gilt nichts. Er macht, was er will – und schlägt gerne Haken. Mal werden die Verlage umgarnt. Mal abserviert.

[caption id="attachment_764891" align="alignnone" width="1030"]



Ein geschickter Schachzug von Facebook

Für die Verlage ist es schwierig. Facebook stellt eine riesige Zielgruppe zur Verfügung. 2,8 Milliarden Nutzer weltweit. Allerdings bestimmte Facebook die Spielregeln: Mal sind die Verlage willkommen – da werden ihnen Ausspielwege für Artikel versprochen. Dann wieder werden Artikel und Links darauf weniger sichtbar gemacht in den Timelines der User. Alle Verlage haben nach diesem Schritt erhebliche Einbußen in der Sichtbarkeit gehabt.

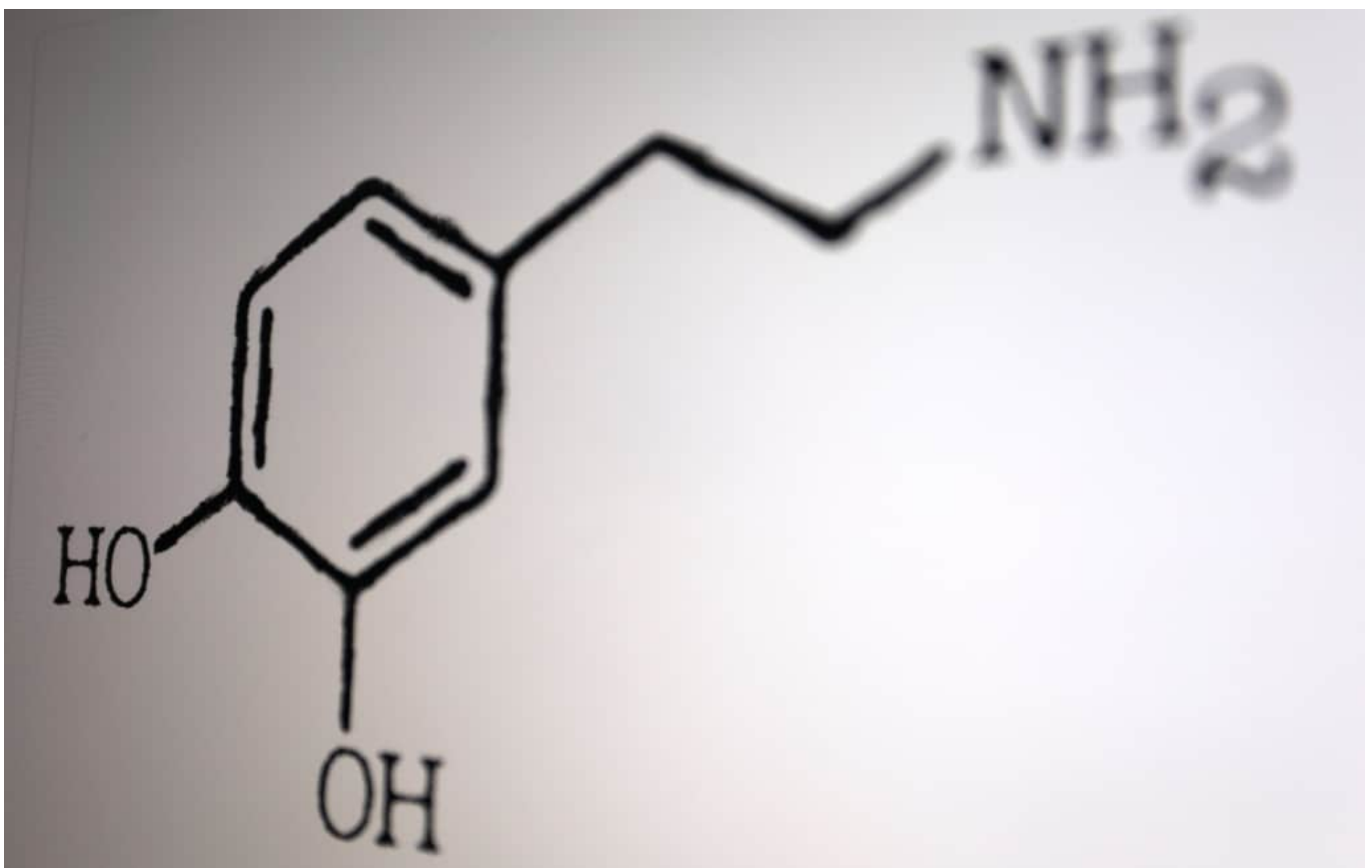
Das wird durch die Kooperation bei Facebook Watch nicht besser. Es wird schlimmer. Denn haben die Verlage erst mal einiges investiert in ihre Facebook-Watch-Sendungen, können sie auf den Ausspielweg kaum noch verzichten. Und müssen vielleicht noch größere Kröten schlucken, die Mark Zuckerberg ihnen künftig präsentiert. "Dann gehen wir halt zu Google", wird als Drohung verpuffen.

Ein geschickter Schachzug von Facebook. Ein vermutlich unheilvolle Entscheidung der Verlage.

Dopamin, das aus dem Smartphone kommt

Im Grunde wissen wir es alle: Smartphone, Soziale Netzwerke und Apps haben eine unerklärliche Sogwirkung, die durchaus Suchtcharakter haben kann. Aber wieso ist das eigentlich so? Es ist gut zu wissen, dass App-Entwickler bewusst süchtig-machende Faktoren einsetzen, um uns am Smartphone zu halten. Diese Tricks sollte man kennen - und seinen Smartphone-"Konsum" ebenso.

Der erste Griff nach dem Aufwachen? Bei den meisten neben das Bett. Zum Smartphone. Was hat sich getan in der Nacht? Irgendwelche wichtigen Nachrichten? E-Mails? Neue Fotos? Breaking News? Noch bevor wir unser Spiegelbild begrüßen, haben die meisten von uns einen Blick in die Online-Welt geworfen. Die einen mehr, die anderen weniger intensiv. Und so geht es den ganzen Tag weiter: Smartphone hier, Smartphone da.



3¼ Stunden am Tag am Smartphone - Tendenz: Steigend

80 Mal am Tag zum [Smartphone](#) zu greifen - das ist gar keine Seltenheit. Im Schnitt bekommt das Smartphone in Deutschland bereits 3¼ Stunden Aufmerksamkeit von seinem Besitzer. Im Schnitt! Das bedeutet: Es gibt viele Menschen, die auch vier, fünf, sechs Stunden mit dem Smartphone verbringen. Natürlich nicht nur daddelnd und chattend - aber auf das Display schauend. Nur: Wo beginnt es problematisch zu werden - eine Abhängigkeit?

Darüber haben [Dennis Horn](#) und ich uns in unserer neuesten Ausgabe des [CosmoTech-Podcast](#) mit der Neurowissenschaftlerin Maren Urner unterhalten, die unter anderem die

[Onlineplattform Perspective Daily](#) gegründet hat.

Sie hat uns bestätigt: Wenn Gewohnheiten unseren Alltag bestimmen und sogar unser Leben beherrschen, kann von einer Sucht gesprochen werden. Und: App-Entwickler setzen gezielt und bewusst süchtig-machende Effekte und Tricks ein, um uns immer häufiger zum Smartphone greifen zu lassen. Ist etwas erst mal eine Gewohnheit, legen wir es nicht mehr so leicht ab.



App-Entwickler setzen gezielt süchtig-machende Tricks ein

Tricks wie das endlose Scrollen: Die Facebook oder Twitter Timeline geht nicht zu Ende. Selbst das dickste Buch ist irgendwann ausgelesen. Eine Timeline nicht. Damit kommt das Gehirn nicht klar: Es will immer mehr. Push-Nachrichten und Vibrieren fordert unsere Aufmerksamkeit. Knallbunte Farben sprechen unser Hirn an. Und dann wäre da noch das Glückshormon Dopamin: Das wird immer dann ausgeschüttet, wenn wir belohnt werden - mit Likes, Retweets, Antworten, Kommentaren, Freundschaftsanfragen, Auszeichnungen.

Es ist regelrecht pervers, wie ungeniert App-Entwickler - nicht nur bei Facebook, Snapchat und Instagram, sondern fast überall - diese Tricks anwenden. Mittlerweile haben sich einige Ex-Gründer und Ex-Entwickler angewidert von ihren (ehemaligen) Arbeitgebern abgewandt und das [Center for Humane Technology](#) gegründet. Hier informieren sie über die Tricks - und warnen davor.

In unserem CosmoTech-Podcast haben wir intensiv darüber gesprochen. Unser Vorschlag: Nicht unbedingt gesetzliche Vorschriften für jedes Detail. Aber die Vorschrift für das Einrichten von Ethik-Kommissionen, die klären, was ethisch vertretbar ist in einer Plattform, in einer Benutzeroberfläche. Damit Gewohnheiten nicht zur Sucht werden.

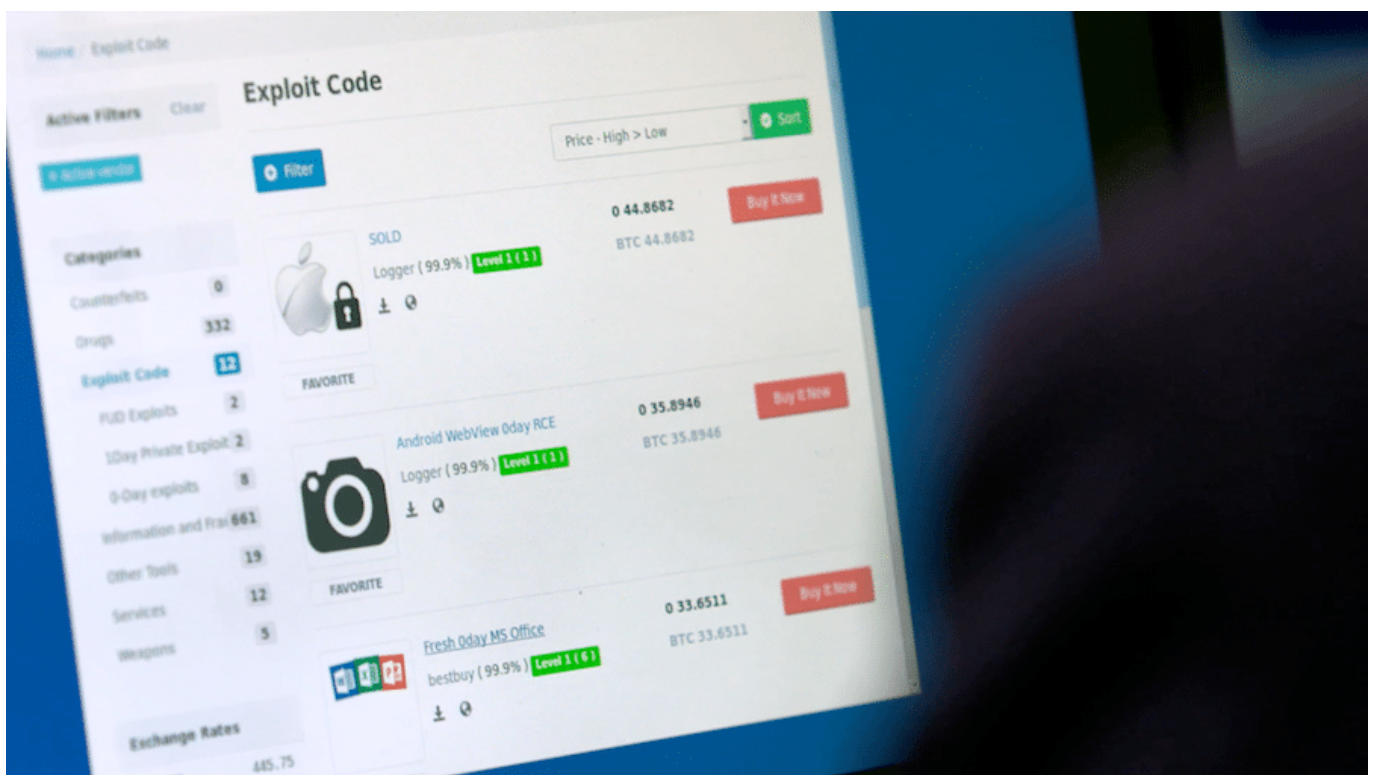
Denn das ist ein sehr schmaler Grat!



Lecks in iOS, Android und Windows ausgenutzt

Jahrelang war eine Lücke in iOS offen - die von der chinesischen Regierung ungeniert ausgenutzt wurde. Um eigene Bürger auszuspionieren. Mittlerweile ist klar: Auch Android und Windows haben riskante Sicherheitslücken. Das Ansteuern einer entsprechend präparierten Webseite reicht aus, um zum Opfer zu werden. Und nun?

Lücken können ganz schön teuer sein. Vor allem Sicherheitslücken. Wer findig genug ist, einen sogenannten "[Zero Day Exploit](#)" in einem Betriebssystem wie [iOS](#) zu entdecken - also eine bis dato selbst den Herstellern unbekannte Sicherheitslücke -, der bekommt bis zu eine Million Dollar Prämie. Zum Beispiel von Apple (im [Bug Bounty Program](#))! Oder locker die zwei- bis dreifache Summe auf dem Schwarzmarkt.



Google hat Sicherheitsleck bei Apple entdeckt

Zero Day Exploits sind daher besonders begehrt, da sie eine Art Generalschlüssel in fremde Maschinen (ob PCs, Tablets, Smartphones) sind. Käufer für solche Lecks finden sich immer. Nicht nur Kriminelle greifen zu, sondern immer öfter auch Regierungen. Wie gerade erst: Wie es aussieht, hat die chinesische Regierung im großen Stil Dissidenten ausspioniert. Durch Ausnutzen einer Zero-Day-Exploit-Sicherheitslücke in iOS.

Google hat das Problem [ans Tageslicht gezerrt](#). Der Onlinedienst hat ein spezielles Team aus Experten, die nichts anderes machen als solche Sicherheitslecks auszukundschaften. Die

Chinesen aber haben das Leck vorher entdeckt (oder entdecken lassen) und auf ihre Weise genutzt: Sie konnten auf infizierten Geräten [unbemerkt Passwörter auslesen](#), Chats mitlesen, E-Mails abgreifen, Apps fernsteuern und auch auf Fotos und Videos zugreifen. Unbemerkt. Aus der Ferne.

Kurz: Der Traum für jeden Geheimdienst - der Albtraum für jeden User.



China freut sich übers Internet

Dass ein derart schwerer Eingriff ins iPhone möglich ist - allein durch Ansurfen einer entsprechend präparierten Webseite -, zeigt deutlich: Auch Apples Betriebssysteme haben erhebliche Macken, sind nicht hundertprozentig sicher. Lücken sind bei Apple zwar eher selten, aber definitiv existent. Mittlerweile ist bekannt: Auch [Android und Windows sind/waren von dem aktuellen Problem betroffen](#). Was die Sache nun wirklich nicht besser macht.

Doch was bedenklicher ist: Wie sich Regierungen immer öfter ungeniert solcher Möglichkeiten bedienen. Die Hinweise verdichten sich, dass China die Sicherheitslecks ausgenutzt hat. Erneut

gegen die eigene Bevölkerung (in diesem Fall, um Dissidenten auszuspionieren). Erst vor wenigen Wochen ist die chinesische Regierung damit aufgefallen, [auf YouTube gezielt Desinformation zu verbreiten](#).

Das Internet: In China selbst zwar extrem reglementiert. Aber wenn es den Herrschenden zu Diensten sein kann, wird es nur zu gerne (aus)genutzt.

Wer kann angesichts solcher Ungeheuerlichkeiten noch davon ausgehen, dass China nicht auch [Sicherheitslecks in 5G](#) ausnutzen würde - oder in China hergestellten Geräten irgendwas "implantiert" wird, was dem Land dient? Einfach davon auszugehen, dass sich China nicht traut, wäre wohl eine äußerst naive Fehleinschätzung.

<https://vimeo.com/325319749>

GPS-Tracking im Auto: Wenn Arbeitgeber zu viel wissen wollen

GPS: Unter diesen drei Buchstaben kann sich heute jeder etwas vorstellen. Satellitenortung. Immer genau wissen, wo man gerade ist. Das geht mit dem Smartphone. Das geht in vielen Autos. Und kann praktisch sein. Oder auch bedrohlich: Etwa, wenn der Arbeitgeber seine Arbeitnehmer überwacht – und immer weiß, wo sie gerade sind. Aber ist das in Ordnung?

Vertrauen Arbeitgeber ihren Mitarbeiterinnen und Mitarbeitern? Oft ja, manchmal nein - umgekehrt ist es wohl genau so.

Allerdings gibt es ein erhebliches Machtgefälle: Arbeitgeber könnten auf die Idee kommen, ihre Mitarbeiter mit modernen Werkzeugen und Geräten zu kontrollieren - und/oder zu überwachen. Offensichtlich kommt das immer häufiger vor. Bei dem [Landesbeauftragten für Datenschutz NRW](#) (LDI NRW) gehen jedenfalls immer häufiger Anfragen besorgter Arbeitnehmer ein, die befürchten, Ortungssysteme in Firmenwagen würden zu einer gezielten und teilweise sogar vollständigen Kontrolle missbraucht.



GPS-Tracking lässt sich einfach nachrüsten

Früher waren bestenfalls Geldtransporter und andere besonders wichtige Fahrzeuge mit [GPS](#) ausgerüstet, um jederzeit geortet werden zu können. Heute sind viele Fahrzeuge serienmäßig mit einer solchen Funktion ausgerüstet. Außerdem lässt sich jedes Fahrzeug mit wenigen Handgriffen und schon für 100 bis 200 EUR nachträglich GPS-tauglich machen. Schon kann der Firmenwagen rund um die Uhr überwacht werden.

Kann. Technisch. Aber darf der Arbeitgeber das auch? Das habe ich Nils Schröder gefragt, der

bei der LDI NRW für solche Themen zuständig ist. Klare Antwort: Es gibt - natürlich! - Situationen, in denen eine GPS-Überwachung sinnvoll und auch erlaubt ist. Etwa bei Werttransportern. Oder wenn jemand in einer Flotte Getränke ausfährt und es zum Service gehört, dem Kunden den nahenden Fahrer anzukündigen. Aber eine Überwachung "einfach so", damit klar ist, wo sich Mitarbeiter aufhalten?



Kontrollen und Überwachung sind nur selten erlaubt

No way! Vor allem dürfen Arbeitgeber das nicht für eine "allgemeine Verhaltens- und Leistungskontrolle" tun. Machen aber manche - und da drohen saftige Bußgelder, wenn das rauskommt. Ähnlich verhält es sich mit der Videoüberwachung. In Zeiten winziger und erschwinglicher Cams, die blitzschnell überall installiert sind, könnten Arbeitgeberinnen und Arbeitgeber auf den Gedanken kommen, das für sich zu nutzen. Aber auch hier: dürfen sie nur unter bestimmten Voraussetzungen.

"Im Zweifel fragen", empfiehlt der Experte. Denn ein Auskunftsrecht besteht immer. Arbeitgeber dürfen nie verdeckt überwachen - auch wenn das heute mit moderner Technologie leicht möglich ist. Ein Tracken des Firmen-Handys ist in der Regel auch nicht erlaubt. Das Einschalten von Kamera oder Mikrofon sind völlig tabu. Und das Surfen am Arbeitsplatz darf auch nicht kontrolliert werden, sofern der Arbeitnehmer in der Arbeitszeit online gehen darf.

Wer also den Verdacht hat, auf irgend eine Weise überwacht und/oder kontrolliert zu werden - was leider immer wieder vorkommt! -, muss sich das also nur selten gefallen lassen.

<https://vimeo.com/356911392>

Nils Schröder (vom LDI NRW) erklärt, was Arbeitgeber dürfen - und was nicht

Das Ende der TAN-Liste auf Papier

Homebanking ohne TAN als Unterschrift? Undenkbar. Die Banken schaffen auch nicht die TAN an sich ab, sondern die ausgedruckte TAN auf Papier. Künftig müssen Homebanker andere Methoden anwenden, um eine TAN zu generieren: Am Smartphone zum Beispiel.

Wer [Online-Banking](#) betreibt, kann schon bald seine gedruckte [TAN](#)-Liste in den Schredder packen. Denn ab 14. September sind Freigaben durch iTAN nicht mehr erlaubt. Die über Jahrzehnte üblichen Papierlisten - von den Banken an die Kunden verteilt -, werden in ganz Europa abgeschafft.

Wie ich darauf aufmerksam wurde? Meine Hausbank hat beim Einloggen ins Onlinekonto die Umstellung angekündigt. So dürfte es den meisten Kunden gehen: Sie bekommen einen Hinweis auf die Umstellung - ohne jemals zuvor etwas darüber gehört zu haben. Besonders gut und ausführlich informiert haben die Banken nicht gerade.



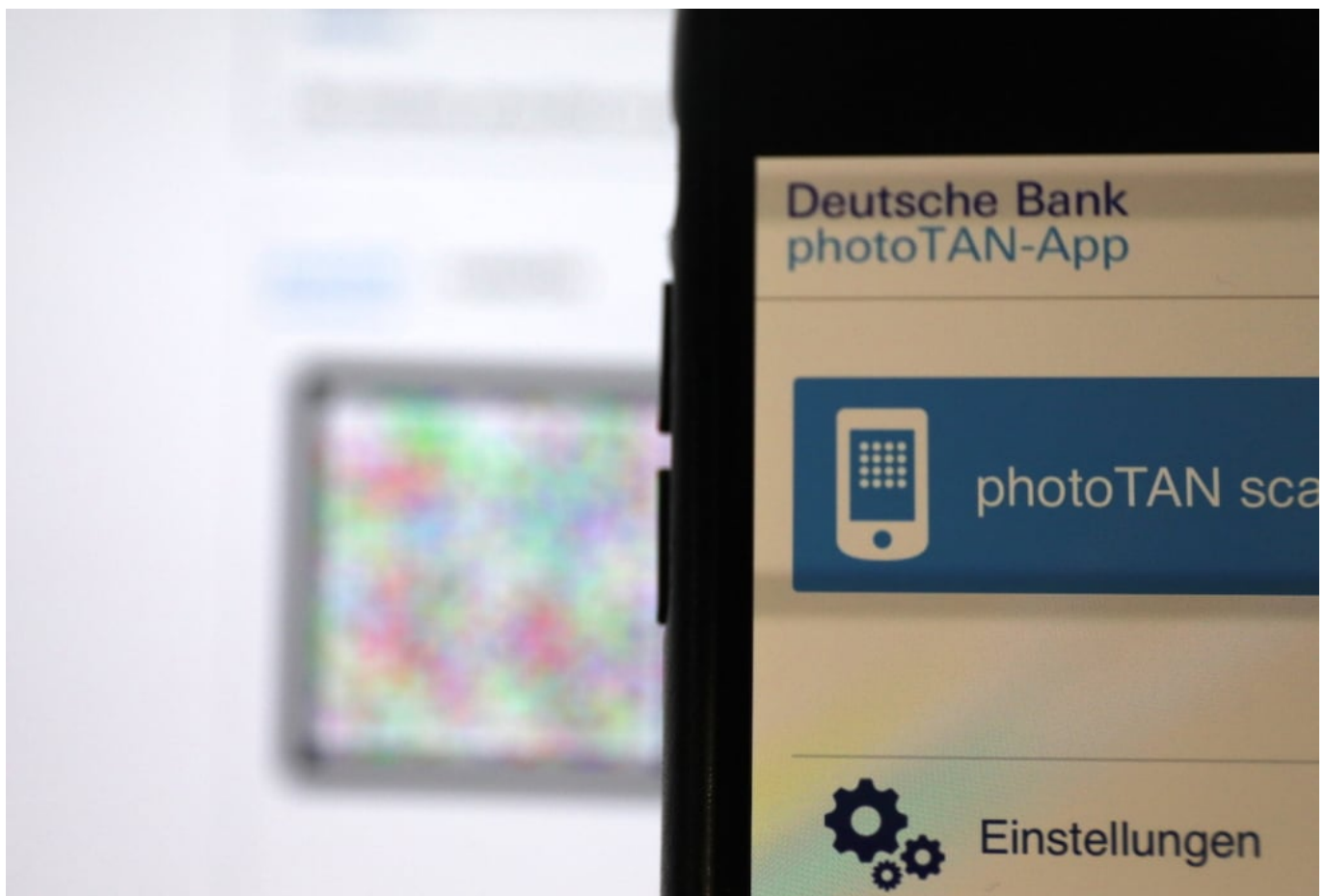
TAN-Liste geht in den Schredder

Die Fakten: Selbst beim Einloggen ins Onlinekonto ist künftig eine Zwei-Faktor-Authentifizierung erforderlich. Die stets gleiche PIN reicht nicht mehr aus. Stattdessen müssen Kunden künftig eine dynamisch erzeugte TAN eingeben. Die erzeugt ein spezielles Gerät wie ein TAN-Generator. Oder der Kunde muss mit seinem Handy eine PhotoTAN erzeugen (Pixelhaufen auf dem Bildschirm mit dem Smartphone scannen). Biometrische Verifikation ist auch erlaubt - also durch Fingerabdruck oder Gesichts-Scan.

Denkbar auch die mTAN - die TAN, die per SMS kommt. Aber die kostet die Banken Geld. Aufgepasst, dass sie die Gebühren nicht (mit saftigen Aufschlägen) weitergeben.

Wer Geld überweisen oder überhaupt irgendetwas in seinem Konto bewegen will, muss diese Prozedur wiederholen. Jede Transaktion muss jeweils durch zwei Faktoren wie **Wissen** (etwa Geheimnummer/PIN), **Besitz** (Smartphone oder Karte) oder **Sein** (biometrische Merkmale wie Fingerabdruck) bestätigt werden. Da kommt also deutlich mehr Aufwand auf uns zu: Weil wir uns schon beim Einloggen ins Konto aufwändiger ausweisen müssen.

Zumindest am PC. Am Mobilgerät geht es einfacher - durch Fingerabdruck oder Gesichts-Scan, wo möglich. In Mobilgeräten sind biometrische Login-Verfahren schon deutlich weiter verbreitet als am PC.



Homebanking und Co. werden sicherer

Aufwändiger wird mittelfristig auch das Bezahlen mit Kreditkarte im Netz, denn auch hier schreiben EU-Regeln künftig die aufwändigere Bestätigung vor. Das kommt noch nicht am 14. September, aber bald. Jede einzelne Transaktion will dann bestätigt werden. Einfach nur Kreditkarten-Nummer eingeben - das reicht nicht mehr. Besser, wir gewöhnen uns daran.

Eine Umstellung ist immer etwas mühsam. Trotzdem erscheint mir diese neue Vorgehensweise richtig: Sie macht das Online-Banking sicherer.

Außerdem gewöhnt es die Menschen an die Zwei-Faktor-Authentifizierung in einem Bereich, der sehr weit verbreitet ist: das Homebanking. Und diese Umstellung könnte die deutlich bessere Methode zum Einloggen generell auch in anderen Bereichen wie E-Mail, Online-Shops und anderen relevanten Onlinediensten beflügeln. Das wäre dringend nötig. Denn die Nutzernamen/Passwort-Methode hat sich überlebt - und ist alles andere als sicher.

<https://vimeo.com/356825842>

Soziale Medien aktiv nutzen – aber sicher

Wer bei Facebook, Twitter, YouTube, Instagram und Co. aktiv mitmacht, sollte sich der Tatsache bewusst sein, dass die Betreiber der Netzwerke eine Menge Daten sammeln. Einige Daten sind zweifellos erforderlich, um ein solches Netzwerk überhaupt sinnvoll betreiben zu können - aber die Anbieter gehen oft zu weit. Es gibt Mittel und Wege, sich zumindest etwas zu schützen.

Soziale Netzwerke sind bekanntlich eine Möglichkeit, mit Familienmitgliedern, Freunden oder Arbeitskollegen in Kontakt zu bleiben. Vor allem dann, wenn sie nicht in unserer unmittelbaren Nähe wohnen und wir sie nicht einfach mal schnell besuchen können.

Durch soziale Medien können wir unsere Erlebnisse und unseren Alltag trotz Entfernung miteinander teilen. Doch oft sind wir in sozialen Netzwerken nicht nur mit Personen befreundet, die wir gut kennen und denen wir vertrauen können, sondern fast jeder hat dort auch ein paar „Freunde“, die er nur flüchtig kennt oder möglicherweise sogar gar nicht.

Auf jeden Fall ist es gerade, wenn man in sozialen Netzwerken aktiv unterwegs ist, wichtig, sich Gedanken über den Schutz seiner Daten und seiner Privatsphäre zu machen. Es gibt durchaus einige Optionen, die Privatsphäre zu schützen und dennoch [Facebook](#), [Twitter](#) und Co. aktiv nutzen zu können. Was viele nicht wissen: Auch ein VPN kann - in Maßen! - vor Datendiebstahl schützen.



Warum so wichtig in Sozialen Netzwerken?

Der springende Punkt ist: Nutzer sozialer Medien müssen notgedrungen Einiges über sich preisgeben, um diese Dienste überhaupt sinnvoll verwenden zu können. Schließlich ist es eigentlich Sinn der Sache, dass wir hier Profile anlegen, in denen alle möglichen Informationen über uns stehen. Es ist also nur natürlich, dass hier Nutzerdaten erfasst, verarbeitet und gespeichert werden.

So können andere Nutzer, die es auf Eure Daten abgesehen haben, an diese [rankommen und schlimmstenfalls Datenmissbrauch damit betreiben](#). Aus diesem Grund ist es gerade im Bereich der sozialen Medien so wichtig, sich und seine Daten zu schützen.

-

Denkt genau darüber nach, welche Informationen ihr preisgeben wollt

Es gilt immer, dass ihr möglichst sparsam mit persönlichen Informationen umgehen solltet und euch vorher fragt, ob eine bestimmte Information wirklich für die Öffentlichkeit bestimmt ist. Es ist zum Beispiel nicht immer klug, alle darüber zu informieren, dass man gerade für zwei Wochen im Urlaub ist und in der Zeit die eigene Wohnung oder das Haus komplett leer steht.

Eine Information, die nicht nur eure Freunde interessieren dürfte, sondern eventuell auch Einbrecher, die nur auf solche „Einladungen“ warten. Ihr könnt bestimmte Daten auch nur für Freunde zugänglich machen oder für bestimmte Personengruppen sperren. Im Zweifelsfall solltet ihr das Posten bestimmter Dinge aber lieber ganz sein lassen.

Keine unbekanntem Kontakte in die Freundesliste aufnehmen

Dies dürfte eigentlich klar sein und doch sind so häufig Kontakte in Freundeslisten zu finden, die man vielleicht erst einmal im Leben gesehen hat, wenn überhaupt. Aber leider ist Euch nicht jeder wohlgesonnen, der Euch eine Freundschaftsanfrage schickt. Es kommt häufig vor, dass Fremde, die mit Euch befreundet sein wollen, es eigentlich nur auf Eure Daten abgesehen haben. Deshalb nehmt nur Kontakte, die ihr auch wirklich kennt, in Eure Freundschaftsliste auf.



Verwendet ein VPN

Ein sehr wichtiger Tipp: Nutzt ein VPN. Denn durch [die Nutzung eines VPN-Servers](#) bewegt ihr Euch weitgehend sicher und anonym in Netz.

Eure Daten werden verschlüsselt übermittelt und dadurch, dass nicht eure eigene IP-Adresse angezeigt wird, sondern die des VPN-Servers, seid ihr quasi anonym unterwegs.

Ein [VPN](#) macht nicht nur die Nutzung sozialer Medien, sondern eure ganze Internetnutzung ein ganzes Stück sicherer. Es gibt kostenlose VPN-Anbieter und kostenpflichtige. Aber warum Geld für etwas ausgeben, das Ihr auch umsonst haben könnt? Der springende Punkt ist, dass niemand einen solchen Dienst komplett kostenlos zur Verfügung stellt.

Schließlich müssen die Anbieter auch mit irgendetwas Geld verdienen. Nutzt ihr also einen kostenlosen VPN-Anbieter, müsst Ihr oft (nicht immer) mit Werbung rechnen oder sogar damit, dass der Anbieter selbst Eure Daten aufzeichnet und an Drittanbieter verkauft.

Es lohnt sich also definitiv, etwas Geld zu investieren und zur sicheren, kostenpflichtigen Variante zu greifen.



Sicherheit vor Cyber-Bedrohungen

Achtet auch auf die Rechte anderer

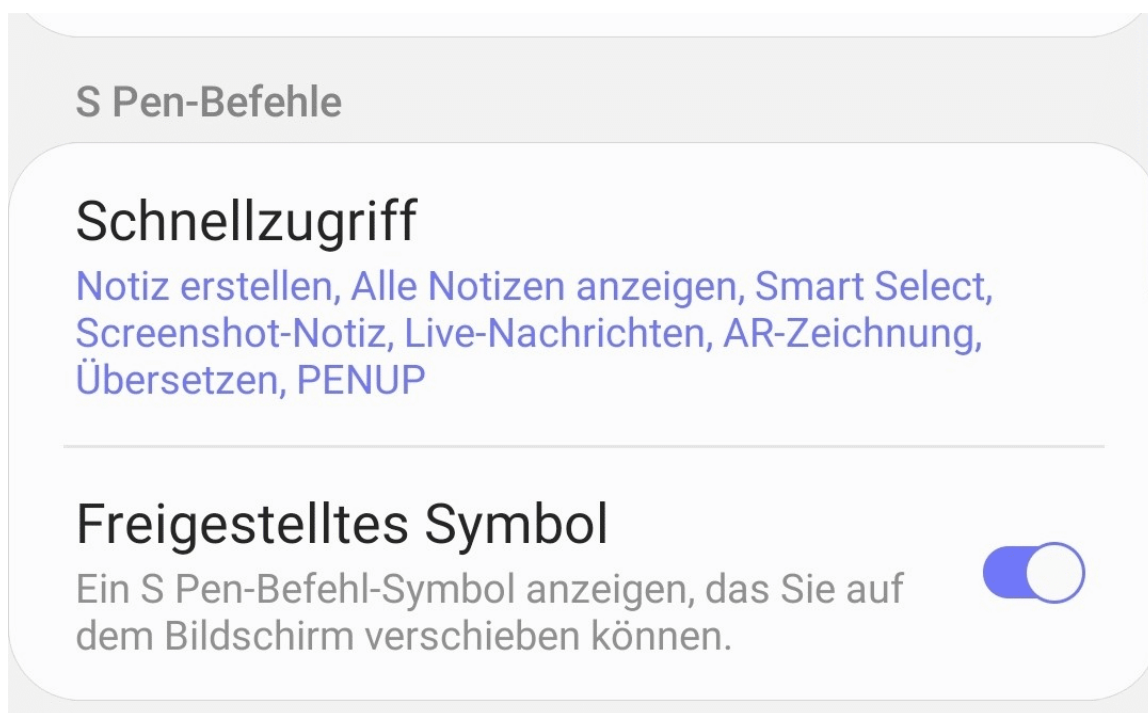
Nicht nur Euch selbst ist eure Privatsphäre wichtig, sondern auch den meisten anderen. Deshalb solltet ihr nie ein Foto oder ähnliches posten, auf dem eine andere Person zu sehen ist, ohne diese um Erlaubnis zu fragen. Erwähnt ihr andere in einem Kommentar, solltet ihr darauf achten, dies respektvoll zu tun und niemanden öffentlich bloßzustellen.

Auch auf die Urheber- und Nutzungsrechte ist zu achten. Bevor ihr beispielsweise Bilder veröffentlicht, müsst ihr sicherstellen, dass ihr auch dazu berechtigt seid und gegebenenfalls Angaben zu Urheber und Lizenz hinzufügen.

Abschließend bleibt zu erwähnen, dass man sich bei der Nutzung sozialer Medien damit abfinden muss, dass man Informationen über sich anderen zur Verfügung stellt. Wer das gar nicht möchte, sollte sich bei diesen Diensten besser gar nicht erst anmelden. Mit den oben genannten Tipps kann man seine Daten jedoch so gut wie möglich vor Missbrauch schützen.

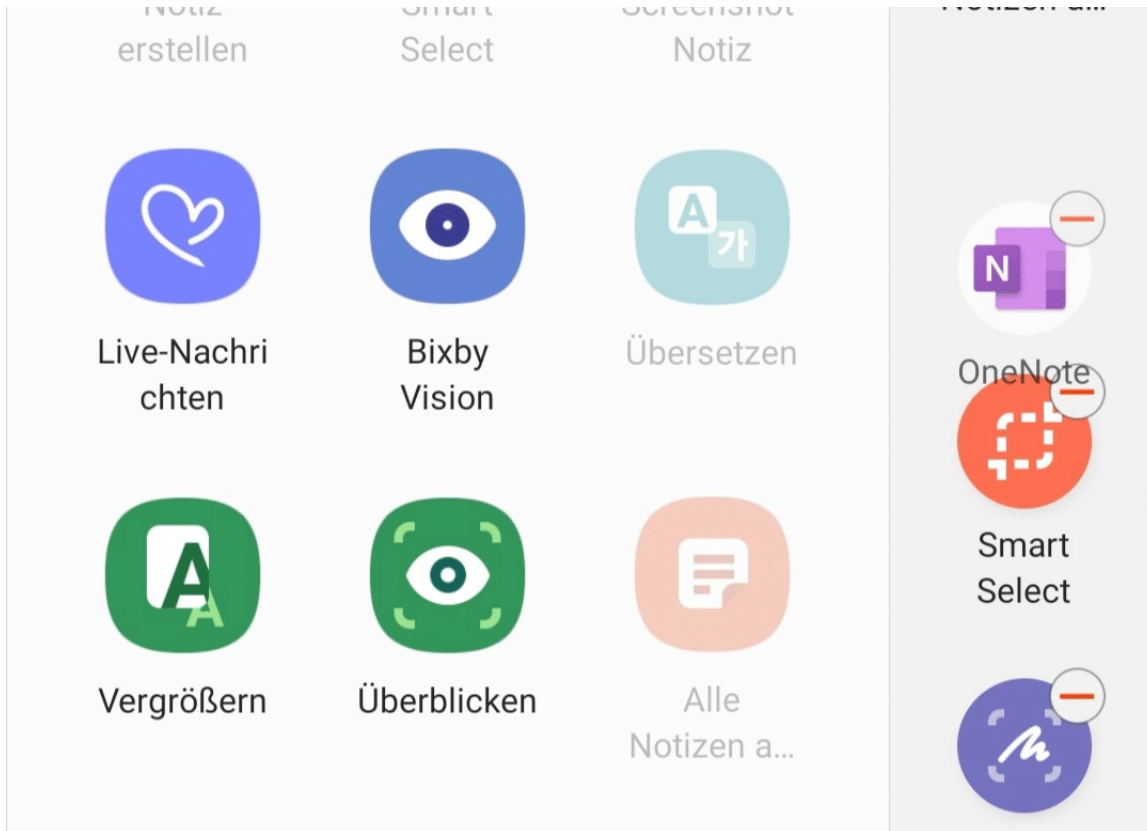
S Pen-Kurzaktionen beim Samsung Galaxy Note 10/10+ festlegen

Die Samsung Galaxy Note bewegen sich zwischen den Welten. Auf der einen Seite Smartphone, auf der anderen ein Tablet. Der Stift, den die Notes integriert hat, kann für vielerlei Dinge genutzt werden. Wenn Sie ihn aus dem Gerät nehmen, dann bekommen Sie direkt eine Liste von Aktionen angezeigt. Wenn Sie die gewünschten darin nicht finden und andere gar nicht benötigen, dann passen Sie die Liste einfach an! Unter **Einstellungen > Erweiterte Funktionen > S Pen** können Sie die Einstellungen rund um den digitalen Stift Ihres Note aufrufen. Unter **Schnellzugriff** finden Sie dann die Liste der Apps, die über die Schnellzugriffsleiste angezeigt bekommen.



Auf der linken Seite des Bildschirms werden Ihnen alle Apps angezeigt, die stiftbedienbar sind und somit in der Schnellzugriffsleiste Sinn machen. Fehlt Ihnen die gewünschte App in der Aufstellung, dann installieren Sie sie. Rufen Sie dann den Schnellzugriff wieder auf. Ziehen Sie die App dann an

Einigen freien Platz in der Leiste rechts



Ist dort kein Platz mehr frei, dann können Sie Einträge in der Liste löschen, indem Sie auf das **Minus-Zeichen** an dem jeweiligen App-Symbol tippen. Um die Position einer App in der Liste zu verändern, greifen Sie sie mit dem Stift, Nach einem kurzen Moment ziehen Sie den Stift mit dem App-Symbol an die gewünschte Position. Sobald Sie den Stift das nächste mal entnehmen, zeigt das Note Ihnen die Liste in der angepassten Form an.

Bosch E-Bikes mit dem Smartphone steuern

E-Bikes werden immer beliebter: Statt mühsam die komplette Strecke strampeln zu müssen, lassen Sie sich mit Motorunterstützung ans Ziel bringen. Das ist nicht nur weniger anstrengend, sondern macht auch noch mehr Spaß. Viele E-Bikes haben eigene Bordcomputer, die allerdings bei Weitem nicht mit den Möglichkeiten eines Smartphones vergleichbar sind. Für Bosch E-Bikes gibt es mit [COBI](#) aber eine tolle Alternative!

Voraussetzung: Ihr E-Bike ist aus dem Modelljahr 2014 oder später und hat das abnehmbare Bedienteil ("Intuvia"). Dann bekommen Sie für Android- und iOS-Smartphones einen so genannten Hub, der statt des originalen Bedienteils eingesetzt wird. In diesen Hub kann dann entweder eine gerätespezifische Hülle für diverse iOS- und Android-Smartphones gesteckt oder eine flexible fest montiert werden.



Letztere ist zugelassen für Smartphones bis 6 Zoll. Allerdings passt auch ein iPhone XS Max mit seinem 6,5 Zoll-Display hinein. Das liegt vor allem daran, dass die neueren Geräte weniger Gehäuse und mehr Display haben.

Lass uns loslegen!

Bring deinen Hub zum Laufen mit
unserer Schritt für Schritt
Anleitung.

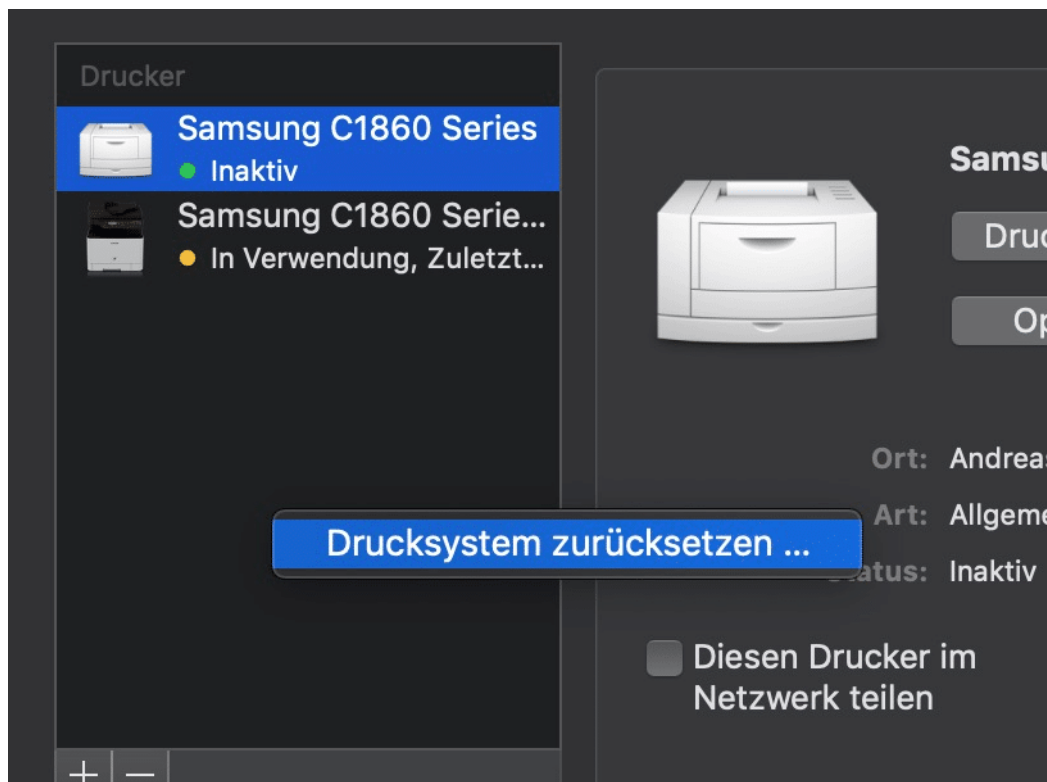


Über die COBI.bike-App für [iOS](#) und [Android](#) können Sie dann all das machen, was Sie auch mit dem Standard-Bedienteil machen können, also die Unterstützungsleistung des Motors regeln, das Licht einschalten, gefahrene Strecke, Kilometer und andere Daten anzeigen lassen. Das allerdings ist noch nicht alles: Die Anzeige und viele Datenfelder sind frei konfigurierbar. Sie können sich über das integrierte Navigationssystem bequem ans Ziel führen lassen, natürlich mit entsprechenden Sprachanweisungen und für das Fahrrad geeigneten Wegen.

Druckerprobleme beim Mac lösen

Drucken sollte doch so einfach sein: Das Dokument ist erstellt, der Drucker angeschlossen und eingeschaltet, und schon werden Nullen und Einsen in Schwarz und Weiß umgewandelt. Leider ist das nicht immer ganz so einfach, und bei einem Rechner mit macOS kann die Behebung ein wenig knifflig sein.

Zu allererst sollten Sie natürlich nachsehen, ob der Drucker ordnungsgemäß angeschlossen ist. Kontrollieren Sie die Strom- und Verbindungskabel, eventuelle Fehlermeldungen am Drucker und am Rechner. Auch der Papiervorrat sollte nicht vernachlässigt werden!



Scheint hier alles in Ordnung, dann starten Sie Rechner wie auch Drucker einmal neu. Lösen diese Schritte die Probleme beim Druck nicht, dann empfiehlt sich ein Zurücksetzen des Drucksystems. Bei macOS sind alle Informationen zu den Druckern, ihren Treibern und Einstellungen zusammengefasst in einem Einstellungs-Container. Dieser ist aber nicht frei zugreifbar.

Öffnen Sie die Einstellungen von macOS und klicken Sie auf **Drucker&Scanner**. Halten Sie dann die **Ctrl-Taste** gedrückt und klicken Sie mit der Maus in einen freien Bereich in der Druckerliste. Nur über diesen Weg erscheint die Schaltfläche **Drucksystem zurücksetzen**. Klicken Sie darauf und bestätigen Sie die Abfrage.

macOS löscht nun alle Drucker aus der Liste, deren Druckwarteschlangen und die Einstellungen. Die Druckerliste ist also nach Schluss leer. Jetzt können Sie die einzelnen Drucker neu anlegen.

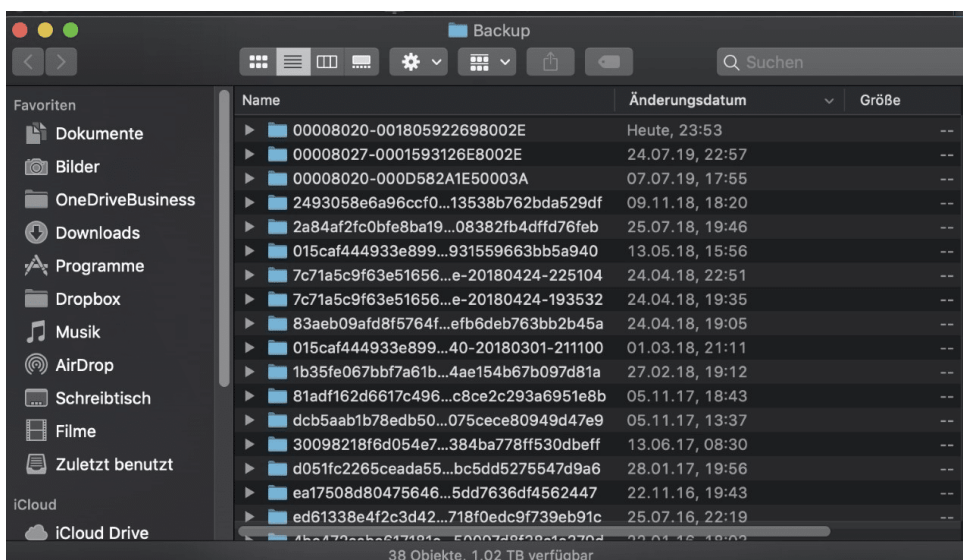
Probleme bei iPhone-Backups lösen

Der Wechsel von einem iOS-Gerät zu einem anderen ist denkbar einfach: Sie schließen das neue Gerät an, iTunes erkennt es und bietet Ihnen direkt an, ein vorher gemachtes Backup wieder einzuspielen. Sie sollten also in den Einstellungen Ihres iPhones das Backup aktiviert halten. Dumm nur, wenn das gar nicht erstellt werden will!

Im Standard möchte iTunes das Backup auf dem Rechner anlegen, auf dem es läuft. Die Durchführung ist der zweite Schritt der Synchronisation. Leider kommt es immer mal wieder vor, dass genau dieser Schritt endlos lange läuft und nicht zum Ende kommen will.

In einem solchen Fall prüfen Sie die folgenden Dinge:

Ist das Backup-Verzeichnis verfügbar? Unter Windows finden Sie es unter %appdata%\Apple Computer\MobileSync\Backup, unter macOS sind die Backups unter Library/Application Support/MobileSync/Backup/ zu finden. Wenn dieses vom System schreibgeschützt ist, dann kann das Backup nicht geschrieben werden. Oft hilft es, wenn Sie den Rechner neu starten.



Auch ein Neustart von iOS-Gerät und Rechner kann Wunder wirken.

Wenn das aber alles nichts hilft, dann stellen Sie einfach das Backup auf ein iCloud-Backup um. In den Einstellungen auf dem Gerät tippen Sie auf Ihre Apple ID ganz oben, dann auf iCloud > iCloud Backup und aktivieren Sie es. Das iOS-Gerät führt jetzt regelmäßig ein Backup durch, wenn es am Strom hängt und eine WLAN-Verbindung hat. Der zweite Schritt der iTunes-Synchronisation fällt damit ersatzlos weg und das Gerät kann synchronisiert werden.


Wenn SMS nicht ankommen

Kennen Sie die Situation: Sie warten dringen auf eine SMS, und die will und will nicht auf Ihrem Telefon ankommen? Oder Sie bekommen dauernd zu hören "Habe ich Dir doch geSMSt?", aber die Nachrichten kennen Sie gar nicht? Das Problem liegt oft ein Kleinigkeiten, lässt sich aber einfach lösen.

Vorausgesetzt, dass Ihr Telefon funktioniert und eine Verbindung mit dem Mobilfunknetz hat, gibt es eigentlich nur zwei Möglichkeiten, warum eine SMS nicht ankommt.

Das Alter der SMS

Jeder Netzbetreiber setzt eine eigene maximale Aufbewahrungszeit für Kurznachrichten. Ist die SMS für Ihre Telefonnummer empfangen worden, kann aber nicht zugestellt werden, dann wird sie nur eine gewisse Zeitz gespeichert. Meist zwischen 3 Tagen und einer Woche. Ist Ihr Gerät nach dieser Frist erst wieder erreichbar, ist die Nachricht verschollen. Eine Lösung dafür gibt es nicht.



Dieses Telefon ist nun zur Nutzung der SMS- und MMS-Dienste aktiviert. This mobile phone is now activated for the SMS- and MMS-services.

Die Empfangsberechtigung

Wenn Sie mehrere SIM-Karten mit der selben Rufnummer verwenden (so genannte Multi-SIMs), dann ist immer nur eine der SIMs für den SMS-Empfang freigeschaltet. Über Netzbetreiber-Codes (z.B. *222# bei der Telekom, *133# bei vodafone) können Sie den SMS-Empfang aktivieren. Geben Sie den entsprechenden Code einfach auf der Tastatur des Telefons ein. Wenn Si ihn für Ihren Netzbetreiber nicht kennen, fragen Sie einfach bei der Hotline an!

Amazon Music mit Garmin Smartwatches

Klassische Smartwatches wie die [Apple Watch](#) oder Uhren mit [Android Wear](#) haben es einfach: In den jeweiligen AppStores der Uhren gibt es eine Vielzahl von Apps, die auf der Uhr installiert werden können. Diese laufen dort autark. Bei kleineren Herstellern wie [Garmin](#), bei denen das Gerät zuerst Fitnessstracker und erst dann Smartwatch ist, ist das anders: Da bekommen Sie kleine Apps von Anwendern, nicht aber die großen Blockbuster-Apps. Garmin hat hier nachgelegt!

Der hauseigene [Gamin Connect Store](#) kann als App für iOS und Android heruntergeladen werden. Darin können Sie nach Apps suchen. Neben Zifferblättern und Datenfeldern finden sich darin vermehrt auch größere Apps. Dazu gehört auch Amazon Music.



Installieren Sie die Connect-App auf Ihrem Smartphone. Dann suchen Sie die entsprechende App heraus. Klicken Sie dann auf **Herunterladen**.



Amazon Music

Amazon_Mobile_LLC >

↓ 7457 | ☆ 2.9(30) | 🎵 Musik

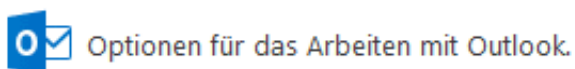
↓ Herunterladen

Die Installation der App findet erst bei der nächsten Synchronisation der Uhr mit Ihrem Smartphone statt. Das Programmpaket wird heruntergeladen und dann installiert. Danach können Sie Amazon Music auf der Uhr unter den Programmen starten. Die Voraussetzung ist natürlich eine Verbindung zu einem Telefon mit bestehender Datenverbindung. Nach Abmeldung mit Ihrem Amazon-Konto können Sie dann Musik aus dem Angebot von Amazon Music über die Uhr streamen.

Nachrichten in Outlook nicht als gelesen markieren

Wenn sie mit mehreren Kollegen zusammenarbeiten und sich vertreten müssen, dann ist [Outlook](#) das Programm der Wahl. Sie können Anderen Zugriff auf Ihre E-Mails geben. Die können dann - je nach erteilten Berechtigungen - auf die E-Mails zugreifen, sie beantworten und neue schreiben. Oft wollen Sie allerdings nur mal eben durch die E-Mails schauen, um einen Überblick zu bekommen. Da ist es ungünstig, wenn die automatisch als gelesen markiert werden. Das können Sie aber leicht ausschalten!

In Outlook 2010 und neueren Versionen klicken Sie auf **Datei > Optionen > Erweitert**. Ganz oben finden Sie die Einstellungen für die **Outlook-Bereiche**. Klicken Sie auf **Lesebereich**.



Optionen für das Arbeiten mit Outlook.

Outlook-Bereiche



Passen Sie Outlook-Bereiche an.

Navigation...

Lesebereich...

Starten und Beenden von Outlook



Outlook in diesem Ordner starten:

Suche...

Beim Beenden von Outlook die Ordner "Gelöschte Elemente" leeren

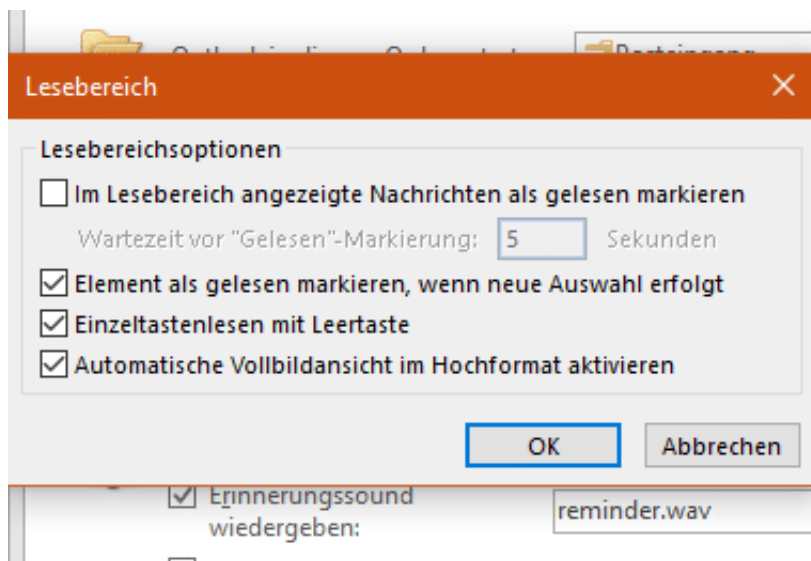
AutoArchivierung



Verringern Sie die Postfachgröße, indem Sie alte Elemente löschen oder in eine Archivdatendatei verschieben.

Einstellungen für AutoArchivierung...

Sie können nun für den Lesebereich festlegen, ob und wann E-Mails als gelesen markiert werden. Die "richtige" Einstellung gibt es hier nicht. Sprechen Sie sich mit demjenigen ab, mit dem Sie die Mailbox teilen. Die Option **Im Lesebereich angezeigte Nachrichten als gelesen markieren** sollten Sie im Normalfall deaktivieren.



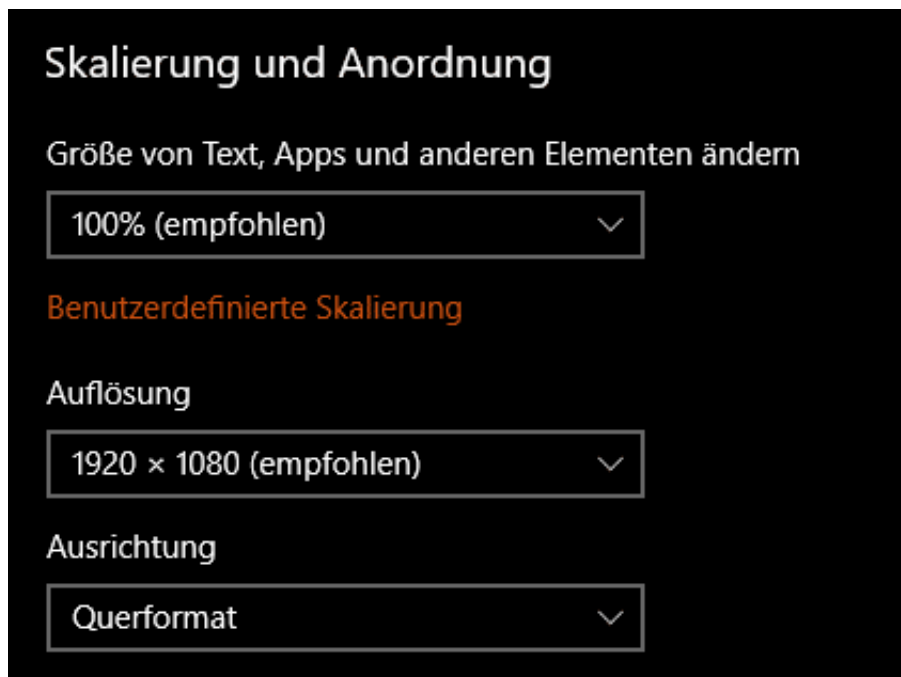
Auch **Element als gelesen markieren, wenn neue Auswahl erfolgt** ist eher störend. Damit wird eine Mail als gelesen markiert, wenn Sie eine andere anklicken. **Einzeltastenlesen mit Leertaste** dagegen gibt Ihnen die Möglichkeit, manuell durch Drücken der Leertaste eine Mail als gelesen zu markieren. Hier wird also der Automatismus ersetzt durch eine manuelle Tätigkeit.

Wenn der Monitor flackert

Der Monitor ist das Stück Hardware, ohne das die Arbeit nun gar nicht möglich ist. Es kann immer vorkommen, dass dieser ganz plötzlich nicht mehr funktionieren will. Ist er aus, dann sind die möglichen Ursachen eher begrenzt. Schlimmer ist es, wenn er flackert und so kaum nutzbar ist. Wir zeigen Ihnen die häufigsten Ursachen und ihre Lösungen.

Oft liegt das Flackern eines Monitors tatsächlich an der Verbindung zum Rechner. Ob nun das Kabel in Monitor oder PC locker ist oder eine Ader gebrochen ist: Ändert sich das Flackern durch Bewegen des Kabels, dann tauschen Sie dieses aus.

Wenn Sie ein Notebook mit flackerndem Display haben, dann kann die Ursache eine Überhitzung sein. Haben Sie das Gerät gerade aus der Tasche geholt, und es war an (statt im Standby zu sein)? Dann lassen Sie es abkühlen. In einem solchen Fall ist der Grafikchip überhitzt und sorgt für das Flackern.



Eine weitere Ursache kann die Auflösung sein: Wenn die Grafikkarte eine höhere Bildauflösung produziert als der Monitor sie darstellen kann, dann kommt es zu Verzerrungen und Flackern. Unter **Einstellungen** > **System** > **Anzeigen** können Sie die Auflösung heruntersetzen und schauen, ob das weiterhilft.

Zu guter Letzt kann es auch sein, dass die Ursache eine App ist, die die Darstellung durcheinander bringt. Das können Sie einfach prüfen. Drücken Sie auf der Tastatur parallel die Tasten **Alt**, **Strg** und **Entf**. Dann starten Sie den **Task-Manager**. Flackert dessen Fenster nicht, dann sind weder Grafikkarte noch Monitor, sondern eine App die Ursache. Beenden Sie nach und nach die laufenden Programme. Hilft das nichts, dann starten Sie den Rechner neu. Bleibt das Problem, dann müssen Sie [im Autostart suchen](#) und dort Programme entfernen.

Task-Manager

Datei Optionen Ansicht

Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste

Name	15% CPU	75% Arbeitss...	0% Datenträ...	0% Netzwe...
Apps (7)				
> Einstellungen	0%	0,1 MB	0 MB/s	0 M
> Internet Explorer (2)	0,2%	115,9 MB	0,1 MB/s	0 M
> Microsoft Edge (13)	1,5%	1.297,5 MB	0,1 MB/s	0,1 M
> Microsoft Excel (32 Bit)	0%	43,2 MB	0 MB/s	0 M
> Microsoft Outlook (32 Bit) (6)	0%	131,1 MB	0 MB/s	0 M
> Task-Manager	0,1%	40,5 MB	0,1 MB/s	0 M
> Windows-Explorer	0%	51,2 MB	0 MB/s	0 M
Hintergrundprozesse (99)				
> Antimalware Service Executable	0,2%	129,6 MB	0,1 MB/s	0 M
> Application Frame Host	0%	9,8 MB	0 MB/s	0 M

Weniger Details Task beenden

Live-Fotos beim iPhone als Endlosschleife darstellen

iOS bietet für die auf einem iPhone oder iPad geschossenen Bilder die Möglichkeit der [Live-Fotos](#). Vor und nach dem Drücken des Auslösers werden jeweils 1,5 Sekunden lang Bilder aufgenommen. Wenn Sie in der Fotoansicht den Finger auf ein so aufgenommenes Bild gedrückt halten, zeigt Ihnen iOS diese zusätzlichen Bilder als Filmchen an. Diese dann aber animiert weiterzugeben, funktioniert so einfach nicht. Das ist aber auch kein großer Aufwand!

Öffnen Sie die Fotoansicht und tippen Sie ein Live-Foto an. Das erkennen Sie durch den kleinen Kreis oben links im Bild und den Text "Live". Wischen Sie nun das Foto nach oben. iOS zeigt Ihnen eine Vielzahl von Optionen unter dem Bild an. Unter **Effekte** finden Sie neben der normalen **Live**-Darstellung zwei weitere Anzeigarten.



Effekte



Live



Endlosschleife

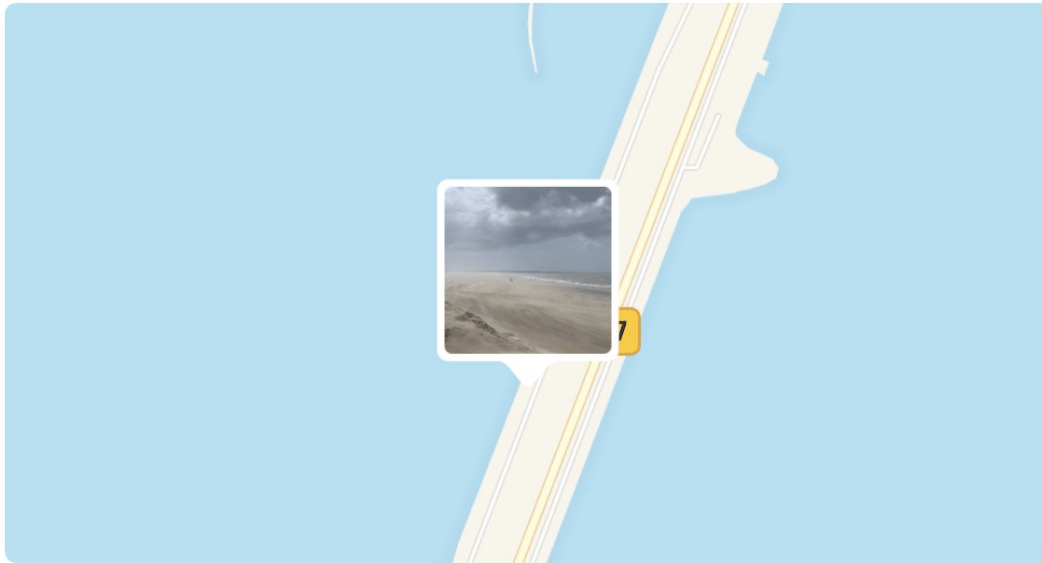


Abpraller

Endlosschleife spielt die animierte Sequenz (die jeweils 1,5 Sekunden vor und nach dem Auslösen) als Endlosfilm dar. **Abpraller** funktioniert ähnlich, spielt die Sequenz aber hin und her. Der Film läuft also vom Anfang bis zum Ende, dann vom Ende bis zum Anfang, dann wieder zum Ende. Und so weiter. Wenn Sie den Effekt auf das Bild anwenden, dann können Sie es auch als Animation Teilen, auch auf Facebook.

Orte

[Fotos in der Nähe einblenden](#)



[Brouwersdam Buitenzijde, Ouddorp, Niederlande](#)

Ganz nebenbei finden Sie darunter noch auf einer Karte den Ort, an dem das Bild gemacht wurde. Ein Tippen auf [Fotos in der Nähe einblenden](#) zeigt Ihnen dann alle Bilder, bei denen die Position in der Nähe des Ortes war, an.