Schieb Report

Ausgabe 2022.33

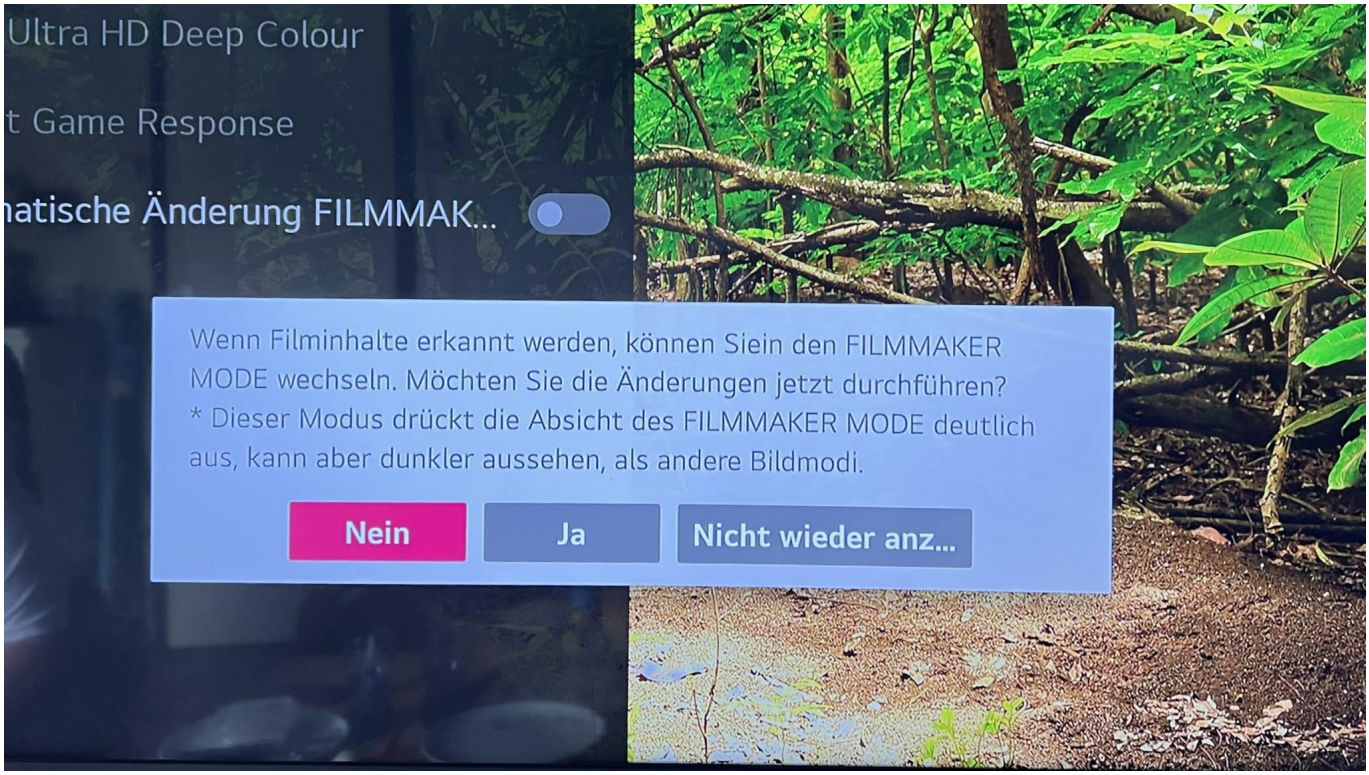
Wenn Amazon Prime Video im Filmmaker-Mode dargestellt wird

Die optimale Bilddarstellung eines Videos liegt stark im Auge des Betrachters. Wenn das Wiedergabegerät hier eingreift, ist das oft nicht im Sinne des Benutzers. Der Filmmaker Mode von Amazon Prime Video ist ein solcher Fall.

Videos so schauen, wie der Produzent sie für das Kino gedacht hatte? Das ist das Versprechen, das der Filmmaker Mode für verschiedene Endgeräte macht. Viele verschiedene Werte des Bildes wie Helligkeit, Kontrast, Farbtemperatur, Schärfe werden so eingestellt, dass das Bild dem in einem Kino entspricht. Nun ist aber nicht jeder Smart-TV oder jedes Display gleich, und die vom Benutzer gewählten Standardeinstellungen können durchaus nicht dem vermeintlichen Optimum entsprechen, aber trotzdem gewünscht sein.

Amazon Prime Video gibt aktuell aber den Filmmaker Mode vor: Sobald ein Inhalt

wiedergegeben wird, schaltet Amazon ohne Nachfrage die Darstellung um, unter anderem auch bei LG Smart TVs. Das könnt Ihr aber deaktivieren, allerdings ein wenig versteckt!



Die Deaktivierung der automatischen Umschaltung findet Ihr in den Einstellungen der App/des Smart TVs:

- Klickt auf Einstellungen - Bild - Zusätzliche Einstellungen
- Neben Automatische Änderung FILMMAKER deaktiviert den Schalter, um die automatische Umschaltung auszuschalten.
- Ihr könnt diese auf dem selben Weg immer wieder aktivieren.

Unabhängig davon lässt sich der Filmmaker Mode auf Smart TVs auch separat für einen Kanal aktivieren oder deaktivieren.

Sicherheitslücke bei Apple: Fast alle Geräte betroffen

Gewöhnlich gelten Apple-Geräte als vergleichsweise sicher. Doch aktuell warnt Apple selbst vor einer gravierenden Sicherheitslücke bei iPhones, iPads und Macs. Sicherheitsexperten empfehlen ein umgehendes Update – das bereits vorliegt.

Dass bei einer Sicherheitslücke gleich mehrere Gerätetypen betroffen sind, ist selten. Schließlich verwenden Macs, iPhones und iPads völlig unterschiedliche Betriebssysteme. Doch eine Schwachstelle in Apples eigenen Browser Safari – genauer: im Webkit, das für die Darstellung von HTML-Webseiten genutzt wird –, macht den Unterschied: Alle Geräte verwenden Safari – deshalb sind auch nahezu alle Gerätetypen betroffen.

Unverzügliches Update empfohlen

Das Sicherheitsleck ist nach einhelliger Meinung so gravierend, dass ein unverzügliches Update empfohlen wird. Auf iPhones auf iOS 15.6.1, auf iPads auf iPadOS 15.6.1 und auf Macs auf MacOS 12.5.1.

Hacker und Angreifer könnten die nun bereits allgemein bekannte Sicherheitslücke ausnutzen – und so Kontrolle über das komplette Gerät erhalten. Ein GAU, da intern praktisch alle Rechte zur Verfügung stehen. Dadurch stehen Angreifern alle Möglichkeiten zur Verfügung: Daten abgreifen, Daten manipulieren, Spionage-Software installieren oder Nutzer abhören, zum Beispiel.

Sicherheitslücke wird bereits ausgenutzt

Man wisse auch um einen "Bericht, wonach dieses Problem aktiv ausgenutzt worden sein könnte", teilte der US-Konzern mit. Ein Hinweis darauf, dass eine Bedrohung nicht nur denkbar und damit potenziell gefährlich ist, sondern bereits konkret ausgenutzt wird. Das macht ein Update zwingend erforderlich.

Sicherheitsexperten raten Nutzern, bei betroffenen Geräte sofort ein Udate vorzunehmen: Die meisten Geräte bieten das Update automatisch bereits an oder führen es sogar selbständig aus, je nach Einstellung. Betroffen sind das iPhones 6s und alle späteren Modelle, etliche iPad-Modelle, darunter jene der 5. Generation und spätere, alle iPad-Pro-Modelle und das iPad Air 2, sowie Mac-Computer mit MacOS Monterey (die aktuellste Version). Betroffen seien auch einige iPod-Modelle, aber hier ist das Risiko gering.

Im sogenannten „Changelog“ der Updates nennt Hersteller Apple einige Details. Eine Schwachstelle befindet sich im „Kernel“, das ist quasi die Schnittstelle zwischen Hardware und Software innerhalb des Betriebssystems. Genau hier ist es möglich, dass Angreifer -obwohl unbefugt – beliebigen Programmcode einspielen und ausführen.

Auch Browser Safari mit Sicherheitsleck

Eine weitere Sicherheitslücke betrifft das „Webkit“: Eine Programm-Bibliothek, die in Apples Browser Safari zum Einsatz kommt – und der wird auf praktisch allen Apple-Geräten benutzt, deswegen sind auch unterschiedliche Gerätetypen gleichzeitig betroffen.

Das Webkit sorgt dafür, dass in HTML programmierte Webseiten ansprechend aussehen. Eine hier entdeckte Sicherheitslücke, die auch andere Browser wie Chrome und Edge betrifft, bietet Angreifern ebenfalls weitreichende

Möglichkeiten. Sie erlaubt insbesondere die Verarbeitung von Webinhalten, die zur Ausführung von beliebigem Code führen kann.

Das Update unter iOS installieren

In den iPhone-Einstellungen unter dem Reiter "Allgemein" findet sich der Bereich "Softwareupdate". Mit einem Klick öffnet sich nun der Update-Bildschirm des iPhones.

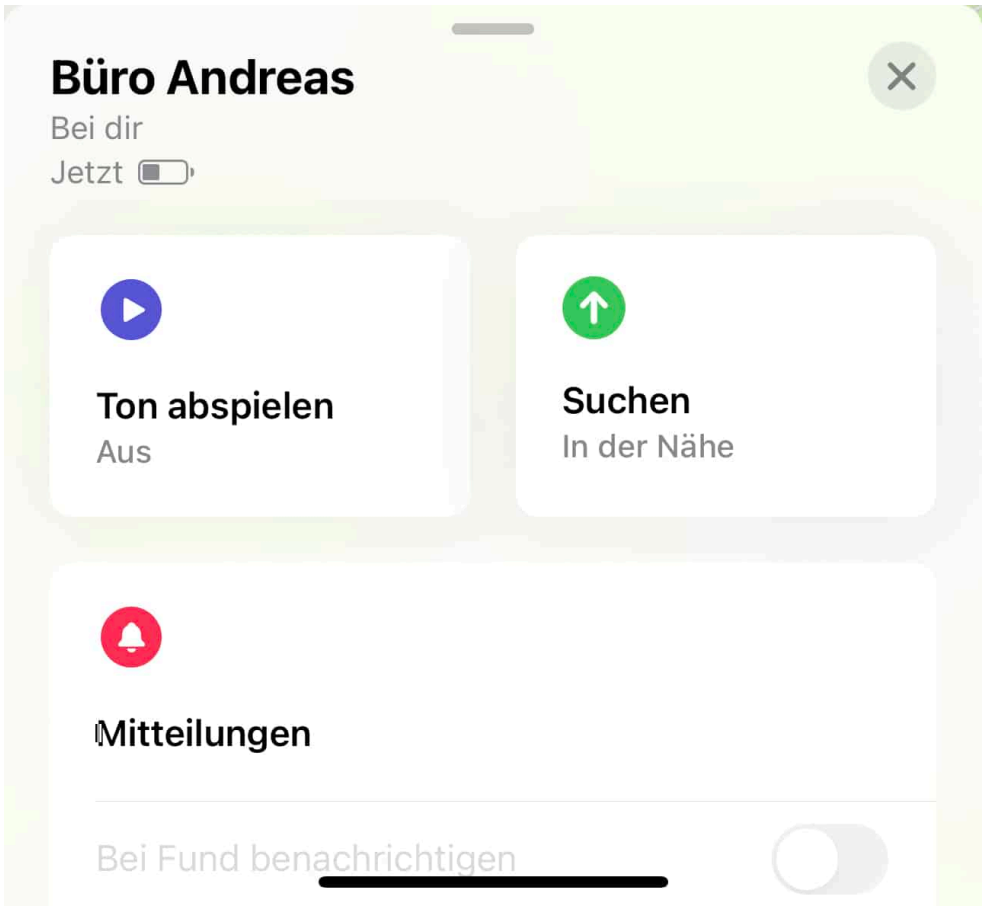
Ganz unten gibt es die Option, die aktuelle Version herunterzuladen. Mit einem Klick auf "Laden und installieren" startet der Vorgang.

Zudem findet sich dort eine kleine Beschreibung zu den Verbesserungen, die das Versions-Update mit sich bringt.

AirTags: Vorsicht bei Update und Batteriewechsel!

Die Apple AirTags sind vor allem wegen Ihrer verlässlichen Positionsübermittlung beliebt. Dumm, wenn eine leere Batterie dazwischen kommt. Apple hilft den Anwendern hier nicht wirklich.

WennIhr einen Gegenstand mit einem AirTag ausgestattet habt, dann verlasst Ihr Euch darauf, dass Ihr den auch orten könnt. Die Voraussetzung dafür: Die Batterie hat noch genug Saft übrig. Da hilft die Batteriestatus-Anzeige, wie Ihr sie in der Wo Ist-App für jedes AirTag sehen könnt:

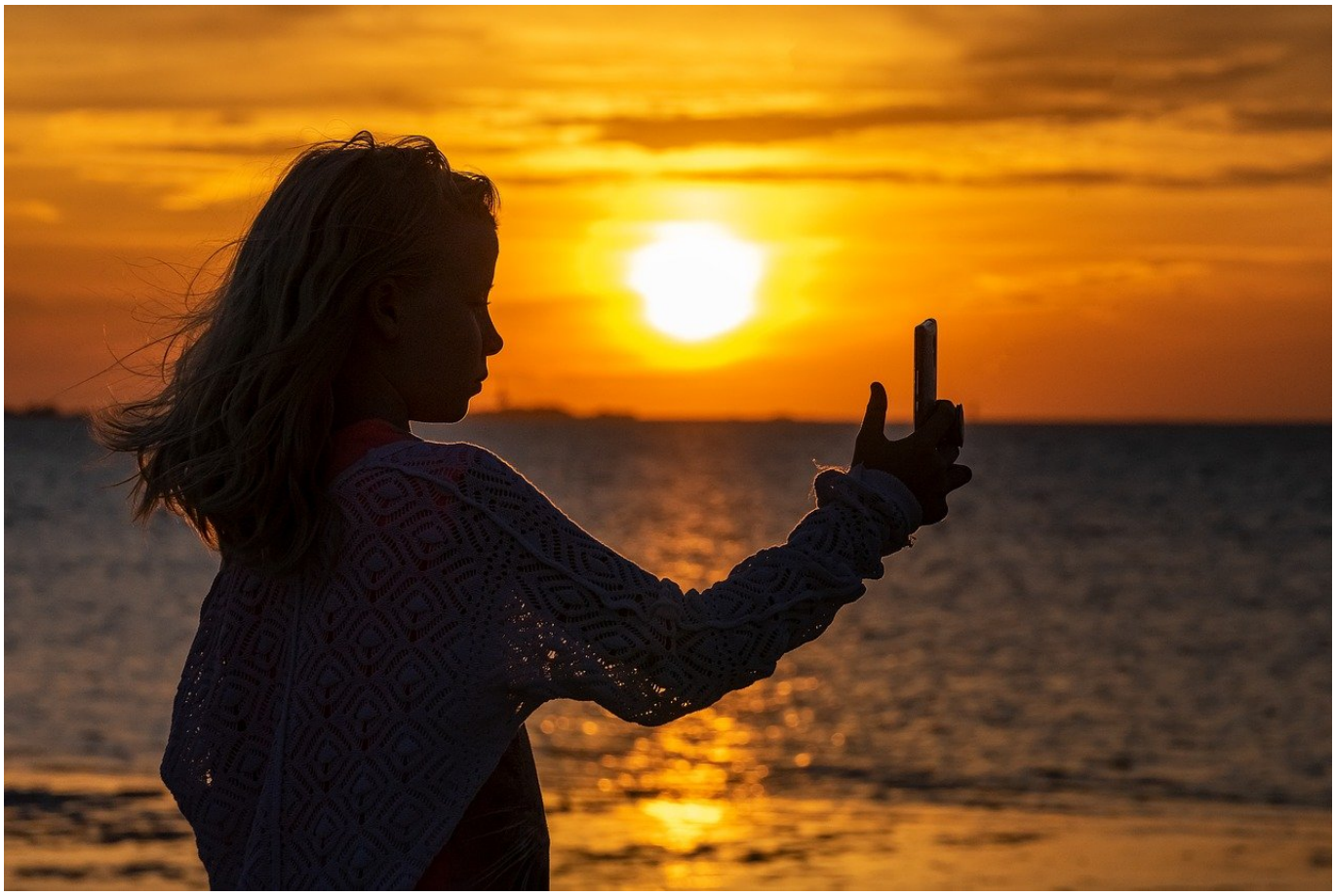


Oder besser: "Sehen konntet", denn mit dem Update auf iOS 15.6 ht Apple diese Anzeige ersatzlos gestrichen. Ein Airtag warnt immer noch, wenn die Batterie schwach ist. Habt Ihr es aber nicht direkt im Zugriff (weil es beispielsweise am Fahrrad im Ferienhaus ist), dann könnt Ihr nach dem Update nicht mehr proaktiv prüfen. ob Ihr beim nächsten Mal die Batterie wechseln wollt.

Der Batteriewechsel an sich ist technisch einfach, aber trotzdem knifflig: Ihr dreht den Metalldeckel ab, dann liegt darunter eine CR2032-Knopfzelle, eine Standardbatterie also. Im Idealfall tauscht Ihr die einfach gegen ein identische Modell aus. Nicht selten verweigert das AirTag dann aber den Betrieb. Statt mit einem Ton seine Bereitschaft zu signalisieren, bleibt es still.

Das leibt daran, dass beschichtete Batterien nicht funktionieren. Viele Hersteller beschichten Ihre Knopfzellen mit Bitterstoffen wie Bitrex, damit Kinder diese - sollten sie sie in den Mund genommen haben - direkt wieder ausspucken. Diese Beschichtung behindert den Kontakt zum AirTag. Die meisten Duracell-Batterien, aber auch Modelle von Varta funktionieren nicht. Hier bleibt Euch nur das Ausprobieren aus, denn die Hersteller ändern ihre Fertigung immer wieder, eine länger gültige Empfehlung gibt es also nicht.

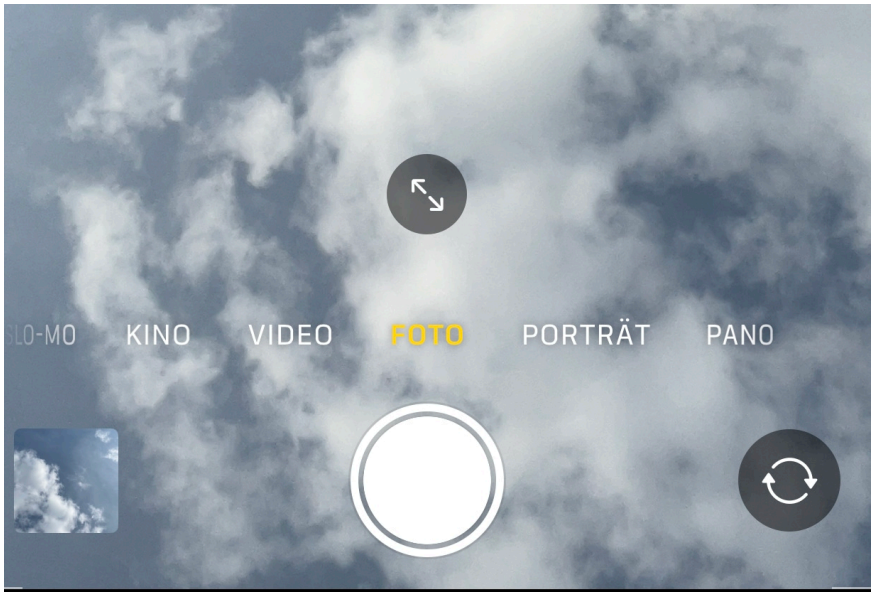
Selfies ohne Stick: Der Weitwinkel-Modus von iOS



Wollt Ihr mehr Personen auf Euren Selfies haben? Dann ist der Arm meist nicht lang genug. iOS erspart Euch den Einsatz eines Selfie-Sticks über einen tollen iOS-Hack!

Selfies sind schon länger eine der Foto-Kategorien, die jeder Anwender immer mal wieder nutzt. Eigentlich ausgerichtet darauf, dass Ihr Euch in einem Umfeld präsentiert, das die Empfänger interessieren könnte. Im Standard passt dabei dann vielleicht noch eine weitere Person darauf. Sollen es noch mehr sein, dann ist der Arm zu kurz, das Gerät muss weiter von Euch weggehalten werden. Oft nutzt Ihr vielleicht dann einen Selfie-Stick, der das Handy auf einer Teleskopstange von Euch wegbewegt. Sieht komisch aus, ist Aufwand, muss nicht sein!

Apple hat dieses Problem erkannt und die Lösung in iOS selbst umgesetzt. Allerdings so versteckt, dass Ihr es kaum findet. Wenn Ihr die Kamera Eures iPhones auf den Selfie-Modus umstellt und die Kamera das unterstützt, dann erscheint knapp über der Symbolleiste ein kleines, rundes Symbol mit zwei voneinander wegweisenden Pfeilen.



- Tippt darauf, dann wird das Bild der Selfie-Kamera weitwinkliger, Ihr seht also einen breiteren Bereich vor der Kamera und damit auch Personen -

oder andere Dinge - links und rechts von Euch. Das ist der selbe Effekt, als würdet Ihr die Kamera weiter weghalten.

- Das Symbol ändert sich daran und zeigt die beiden Pfeile aufeinander zeigend an. Tippt darauf, um die Selfie-Kamera wieder an Eúch heranzoomen zu lassen.

Sky Ticket (WOW) im Ausland nutzen

Sky Ticket, das neuerdings "WOW" heißt, ist für viele Anwender die einzige Chance, auch unterwegs die Formel 1 oder Bundesliga schauen zu können. Das geht auch im Ausland, ist aber mit Vorsicht zu genießen!

Smart TVs, Tablets, Smartphones, für de unterschiedlichsten Gerätetypen könnt Ihr das Programm on Wow anschauen. Im Ausland ist das erst einmal auch kein Problem, auch ohne VPN-Verbindung könnt Ihr in den meisten Ländern Eure abonnierten Sender anschauen. Allerdings verbirgt sich dahinter eine rechtliche Herausforderung: Die Lizenzvereinbarungen für bestimmte Inhalte sind von Land zu Land unterschiedlich. Das Programm, das Ihr in Deutschland abonniert habt, kann in den Niederlanden nicht für Sky lizensiert sein. Anschauen könnt Ihr es nur, wenn Ihr Euren Wohnsitz in Deutschland habt.

WOW

Noch 7 Tage im Ausland WOW genießen

Hey Andreas,

es ist schön zu sehen, dass du dein WOW Erlebnis auch auf deinen Reisen genießt.

Wir möchten dich nur darauf hinweisen, dass das Ende deines Roaming-Zeitraums näher rückt. Du hast jetzt noch 7 Tage Zeit, um im Ausland dein WOW Erlebnis zu genießen.

Solltest du weiterhin außerhalb von Deutschland WOW nutzen wollen, musst du dich zunächst wieder von zu Hause aus anmelden um zu bestätigen, dass du weiterhin in Deutschland wohnst.

Das macht Sky daran fest, dass Ihr den Dienst auch in Deutschland nutzen müsst und nicht nur im Ausland. Ist Wow auf dem Fernseher im Ferienhaus im Einsatz, dann erkennt Sky, dass die Nutzung nur aus dem Ausland erfolgt und schickt Euch nach kurzer Zeit eine E-Mail wie die oben.

Keine Sorge: Hier geht es nicht darum, dass das roaming abgeschaltet werden soll, wie der erste Blick befürchten lässt. Sky will nur den Nachweis, dass Ihr weiterhin (immer mal wieder) in Deutschland seid. Hier reicht es, Euch einmal mit einem Gerät in Deutschland an Wow anzumelden und etwas zu streamen. Der Zähler wird zurückgesetzt. Ärgerlich: Es hilft nicht, eine VPN-Verbindung nach Deutschland aufzubauen und dann den Stream zu starten: Wow merkt, dass Ihr immer noch im Ausland seid!

Bei Präsentationen in der Zeit bleiben: Presenter

Die Folien sind der eine Teil, der über Erfolg oder Misserfolg einer Präsentation entscheidet. Ihr als Präsentator müsst Euch aber auch mit der zur Verfügung stehenden Zeit ausrichten.

Für viele – auch erfahrene – Menschen ist das Einhalten der Zeitvorgaben eine Herausforderung: Ihr seid aufgeregt, wollt Eure Inhalte an Euer Publikum bringen, und gleichzeitig müsst Ihr die Zeitvorgaben einhalten, oft habt Ihr einen genau festgelegten Zeit-Slot, von dem Ihr nicht abweichen könnt.

Eine gute technische Hilfe stellen so genannte Presenter dar.

Einmal an den PC oder das Notebook angeschlossen geben sie Euch viel Freiheit:

- Über die Tasten könnt Ihr zwischen den Folien wechseln, statt fest an der Tastatur des Rechners stehen zu müssen oder immer wieder dorthin gehen zu müssen. Das gibt Euch Bewegungsfreiheit, die für viele Anwender gleichzusetzen ist mit Stressabbau.
- Die Presenter haben meist einen Laserpointer integriert. Mit dem könnt Ihr an der Leinwand oder Wand die Stellen der Präsentation markieren, über die Ihr gerade redet. Das macht bei Texten relativ wenig Sinn, bei der Erklärung einer Abbildung hilft es dagegen sehr.
- Bei vielen Presentern könnt Ihr einstellen, wie lange Ihr für eine Folie brauchen dürft. Das berechnet Ihr einfach aus der Anzahl der Folien und der Zeit, die Ihr zur Verfügung habt (am Beispiel oben: 60 Minuten und 20

Folien ergibt 3 Minuten pro Folie). Wenn Ihr diesen Wert in den Presenter eintippt, dann vibriert dieser, wenn Ihr zur nächsten Folie übergehen solltet. Das ist viel unauffälliger und effektiver als der regelmäßige Blick auf die Uhr!

Gesichtserkennung und ihre Risiken

Gesichtserkennung: Kann praktisch sein, um das eigene Smartphone zu entsperren - oder wenn das iPhone die Fotos automatisch nach Personen sortiert. Leider hat Gesichtserkennung aber auch ein Missbrauchspotenzial - und das nimmt immer weiter zu.

Wir Menschen erkennen andere Menschen in der Regel, sobald wir ihr Gesicht sehen. Denn so ein Gesicht, das ist schon unverwechselbar... Nur manchmal denken wir: Hmm, die sieht der aber ähnlich. Auch Maschinen können Gesichter erkennen – und das kommt immer öfter zum Einsatz. Unsere Smartphones lassen sich mit dem Gesicht entsperren, Kameras ziehen die Schärfe, wenn sie ein Gesicht erkennen – und die Polizei fahndet mit Gesichtserkennung nach Menschen, zum Beispiel auf öffentlichen Plätzen. Die Technik der Gesichtserkennung wird aber auch missbraucht. Fotos aus dem Netz werden missbraucht, um Menschen zu identifizieren.

Da gibt es auch wieder einen aktuellen Fall in Russland: Mit Hilfe von Gesichtserkennung wird Frauen nachgestellt oder es werden Menschen bedroht.

Der Begriff "Gesichtserkennung"

Die Begriffe „Gesichtserkennung“ und „KI“, also Künstliche Intelligenz, werden gerne immer zusammen verwendet. Ist Gesichtserkennung wirklich nur mit KI möglich?

Wir müssen die Begriffe in der Tat richtig verwenden: Unter „Gesichtserkennung“ wird eigentlich die automatische Zuordnung eines Bildes zu einer Person verstanden. Bedeutet also: Ich zeige einem Computer ein Foto – und der sagt mir dann, wer da zu sehen ist. Das Bild kann ein Foto, aber auch ein Bewegtbild sein, also ein Video – oder die Live-Aufnahme einer Überwachungskamera. Um diese Aufgabe zeitnah zu bewältigen, braucht man heute in der Tat KI-Anwendungen.

Denn KI kann sehr effektiv Muster erkennen. Und für Computer sind Gesichter am Ende Muster: Bestehend aus Tausenden von Einzelpunkten. KI denkt nicht: Oh, diese Person sieht aber hübsch aus oder asiatisch, sondern „sieht“ nur die Tausenden Merkmale. Die werden dann erfasst und verglichen mit gespeicherten Merkmalen. KI-Systeme gehen da nicht vor wie wir Menschen: Wir vergleichen Fotos miteinander. KI-Anwendungen vergleichen Gesichtsmerkmale, markante Punkte im Gesicht – das ist etwas völlig anderes. Viele entsperren mit ihrem Gesicht ihr Smartphone. Das ist streng genommen keine Gesichtserkennung, da hier keine KI zum Einsatz kommt. Hier werden auch nicht mehrere Personen erkannt, sondern nur eine Person. Die Software überprüft lediglich: Ist das Gesicht, das ich gerade sehe, das Gesicht des Besitzers. Dein Gesicht würde mein Smartphone zum Beispiel nicht erkennen.

Wie sicher ist mein Gesicht im Smartphone?

Was sich viele fragen: Wenn ich mein Gesicht benutze, um mein Smartphone zu registrieren, freuen sich Google und Apple dann nicht riesig, weil ich ihnen meine biometrischen Daten frei Haus liefere?

Die Frage wird mir auch häufig gestellt – und das ist ein gutes Zeichen, weil es zeigt, dass die Menschen skeptischer werden. Aber in diesem Punkt braucht man

sich wirklich keine allzu großen Sorgen zu machen. Es ist so: Wenn ich mein Gesicht herzeige, wird nicht etwa mein Gesicht abfotografiert und dann später mit meinem Live-Gesicht verglichen. Stattdessen werden etliche hundert, teilweise tausend Punkte in meinem Gesicht vermessen: Wangenknochen, Augenstand, Nase, Ohren, Gesichtsform.

Bei Apple iPhones sind es 30.000 Punkte. Diese Punkte beschreiben meine Gesichtsform. Diese Daten bleiben im Gerät(!) gespeichert und werden nicht etwa online hinterlegt. Wichtig zu wissen: Mit diesen Datenpunkten lässt sich überprüfen, ob ein hergezeigtes Gesicht meins ist – doch damit lässt sich nicht etwa mein Gesicht rekonstruieren, also nachbilden oder im 3D-Drucker bauen. Das geht nicht. Es dient nur zur Überprüfung, eignet sich aber nicht zur Rekonstruktion.

Das ist beim Fingerabdruck genauso, wenn ich den zum Entsperren von PC, Smartphone oder Tablet nutze.

Missbrauch der Gesichtserkennung

Doch sprechen wir über Gesichtserkennung im großen Stil. Facebook zum Beispiel hatte lange Zeit eine Funktion, die Gesichter von Nutzern erkennt – die können das also.

Facebook hat 2010 eine Gesichtserkennung eingeführt: Dadurch konnten Personen auf hochgeladenen Fotos automatisch erkannt werden. Wenn ich also ein Partyfoto hochlade, sagt mir Facebook: Da sind Jan, Martin und Steffie drauf. Ruckzuck. Weil Facebook täglich Milliarden Fotos „sieht“ und die Profilbilder der Nutzer kennt – und damit die Zuordnung erstaunlich gut hinbekommt. 2012 wurde die Funktion in Europa nach Protesten abgeschaltet, 2018 wieder eingeschaltet – um dann 2021 weltweit abgeschaltet zu werden.

Die Proteste hatten überall auf der Welt zugenommen. Prinzipiell ist es technisch kein Problem für einen Dienst wie Facebook, eine solche Gesichtserkennung sehr zuverlässig hinzubekommen. Die Menschen laden Fotos von sich und anderen hoch, markieren die Personen in den Fotos sogar – das hilft der KI, die Menschen zu erkennen und automatisch zuzuordnen. Doch das ist spooky. Kein Wunder, dass immer mehr Datenschützer Bedenken haben.

China: Jedes Gesicht bekannt

In China, hört man immer wieder, gibt es diese Bedenken nicht: Da wird Gesichtserkennung zur Massenüberwachung eingesetzt.

In China können sich Bürger nicht wehren und Datenschutz einfordern. Da gelangt Gesichtserkennung auf ein ganz neues Niveau: Alle öffentlichen Räume sind nahezu flächendeckend mit Überwachungskameras ausgestattet. Die Gesichter der Menschen werden live erfasst und blitzschnell erkannt. Bei Fehlverhalten erfolgen Bestrafungen. „Social Scoring“ wird das genannt: Geht jemand bei rot über die Ampel, erfasst die Kamera die Person, das Gesicht wird erkannt – und Sekunden später erscheint der Name der Person auf einer übergroßen Anzeigetafel. Und der Verstoß wird verbucht und hat Konsequenzen. Das ist ein Beispiel dafür, was mit Gesichtserkennung in einem Überwachungsstaat möglich ist. Und deswegen warnen Datenschützer aus gutem Grund vor dem Einsatz von Gesichtserkennung im öffentlichen Raum.

Russland: FindClone findet jedes Gesicht

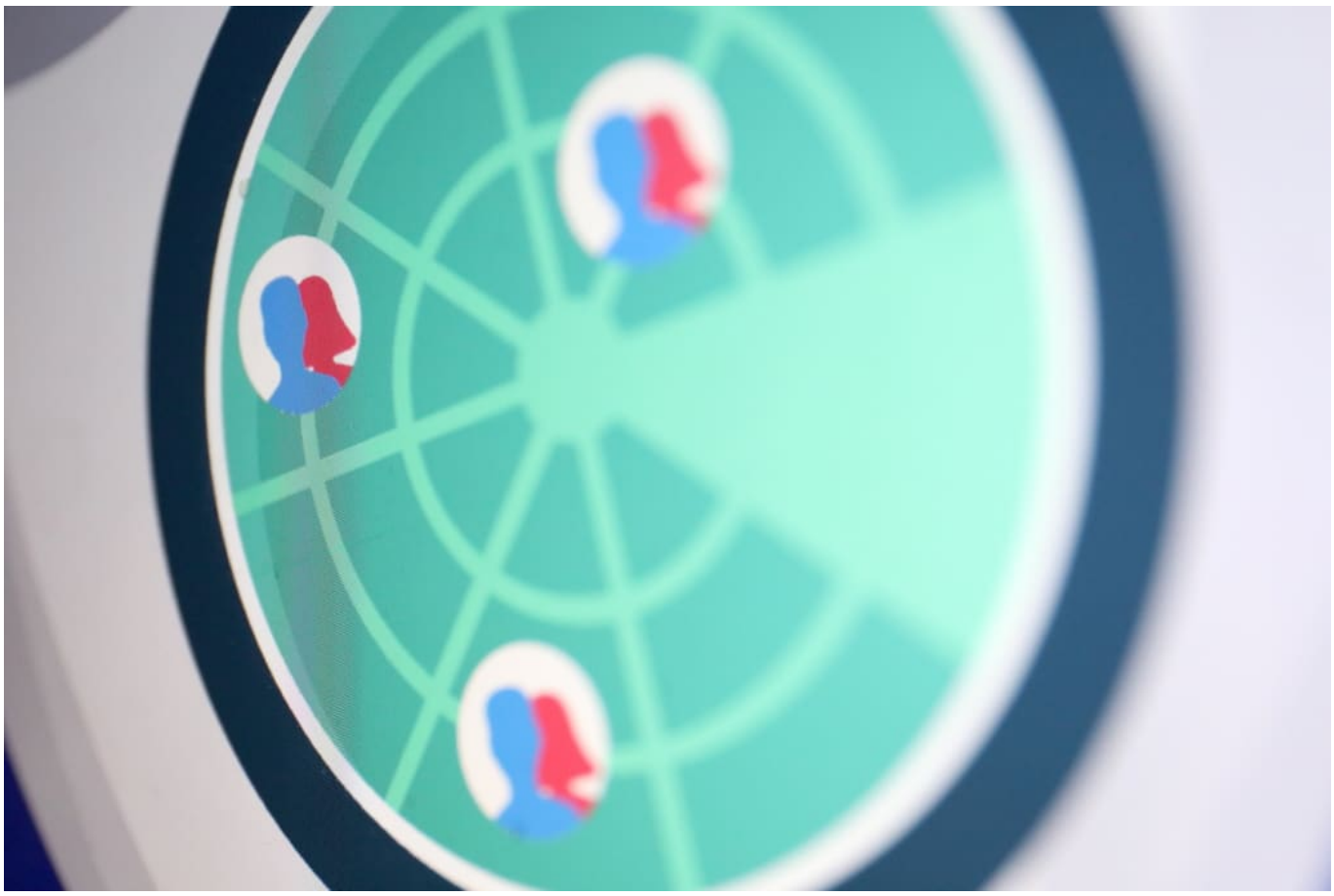
Wir haben einen aktuellen Fall: In Russland kommt eine KI zum Einsatz, die sich FindClone nennt: Darüber kann mehr oder weniger jeder ein Foto hochladen und erfahren, wer das ist. Da wurde Frauen nachgestellt, Personen wurden bedroht...

FindClone zieht Fotos aus dem in Russland populären Social Media Dienst VKontakte. Das ist eine Art russisches Facebook – mit unzähligen Fotos und Porträts. Wir hatten so etwas auch schon in den USA mit Clearview AI und in Europa mit Pimeyes (aus Polen).

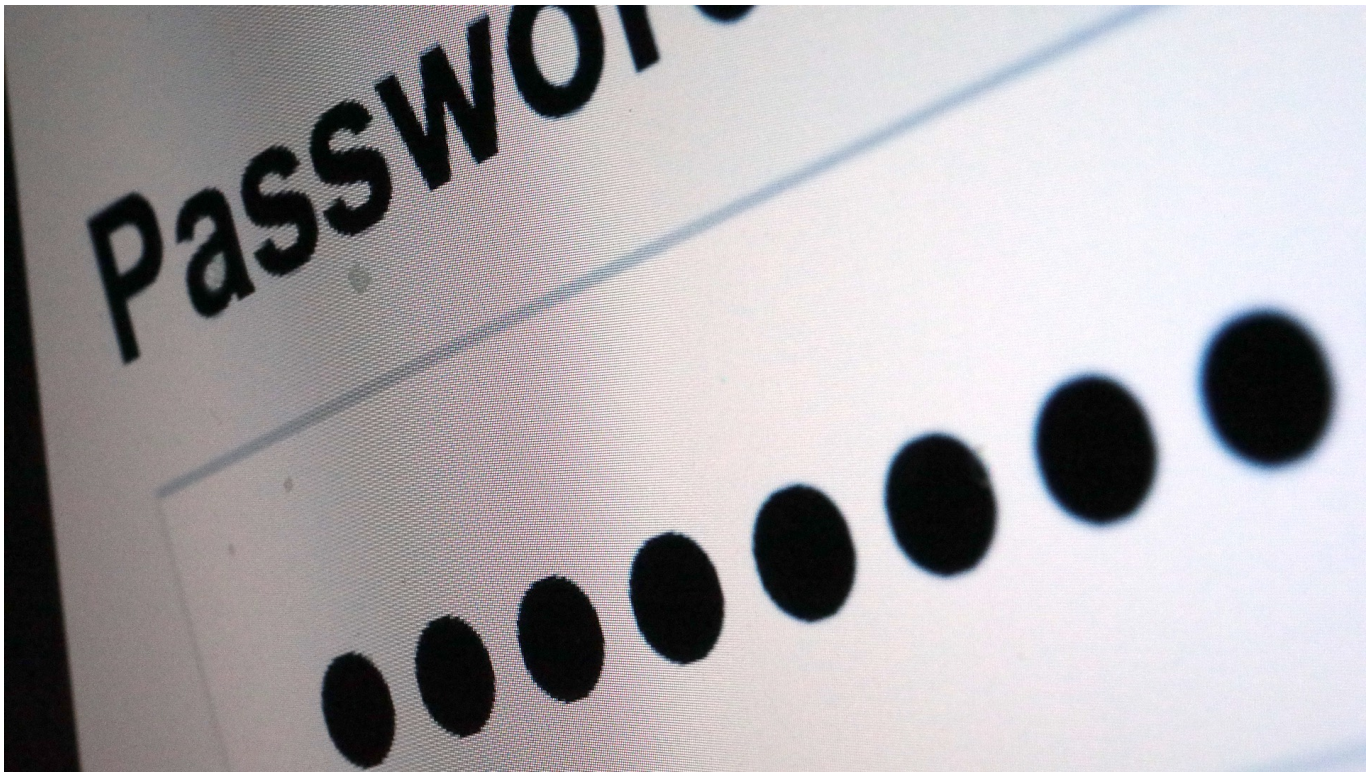
Die Vorgehensweise ist immer dieselbe: Diese „Anbieter“ ziehen Millionen, nein Milliarden von Fotos aus den Netzen, was problemlos geht, da die Fotos ja öffentlich zugänglich sind. Zusammen mit entsprechenden Daten aus den Netzwerken wie Name, Wohnort, Hobbys. Was man in Social Media so findet. Die Fotos werden biometrisch vermessen, also „gescannt“, und in einer Datenbank gespeichert. KI-Systeme können dann blitzschnell ein hochgeladenes Foto einer Person zuordnen.

Illegal, weil so etwas in Europa verboten ist mittlerweile. In den USA nutzen Polizeibehörden den privaten Dienst Clearview AI, um Personen zu identifizieren. Wir alle füttern diese Dienste, weil die Fotos aus Facebook, Instagram und Co.

kommen. Ein unhaltbarer Zustand.



Neue Regeln für Passwörter: Lieber einmalig als zu komplex



Kompliziert und möglichst lang: Das waren lange die wichtigsten Regeln für Passwörter. Doch nach den neuen Richtlinien des BSI gelten nun neue Regeln. Die wichtigste: Passwörter sollen vor allem einzigartig sein. Wir können und sollten also alle umdenken - und die eigenen Passwörter mal auf den Prüfstand stellen.

Geht es nach vielen Portalen und Arbeitgebern, können Passwörter gar nicht lang genug sein. Doch wer soll sich Passwörter wie „T0ta!Gehe1m_12$“ merken – und auch noch für jeden Onlinedienst ein anderes? In der Praxis kaum möglich, zumindest nicht ohne Hilfe wie einen Passwort-Manager.

Viele Menschen verzweifeln an so vielen Regeln – und erst recht an so vielen unterschiedlichen Passwörtern.

Beirat Digitaler Verbraucherschutz des BSI

Das ist auch der Grund, wieso der „Beirat Digitaler Verbraucherschutz“, der das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) als unabhängiges Gremium bei der Wahrnehmung seiner Aufgaben im Digitalen Verbraucherschutz berät, nun unmissverständlich zu weniger komplexen Passwörtern rät. Denn dann besteht nicht mehr das Risiko, dass User ein zwar komplexes Passwort generieren, das aber aus Bequemlichkeit überall benutzen.

Mit den veröffentlichten Handlungsempfehlungen will das BSI sichere Passwörter quasi alltagstauglich machen. Denn was nutzen Regeln, die keiner befolgt. Denn nach Ansicht des Gremiums sind die bisherigen Regeln zu undurchsichtig: „Was ein Passwort sicher macht, ist für die Verbraucherinnen und Verbraucher aufgrund der großen Anzahl unterschiedlicher Ratgeber nicht immer klar erkenntlich“, heißt es in der für jeden öffentlich zugänglichen Richtlinie.

Neue Regeln für gute Passwörter

In vielen Unternehmen wird heute zum Beispiel noch verlangt, dass Passwörter regelmäßig – etwa alle drei Monate – erneuert werden. Dadurch versprechen sich Betreiber einen höheren Schutz, weil ggf. verloren gegangene oder entwendete Passwörter dann nicht mehr funktionieren. Doch von einem turnusmäßigen Wechsel rät das BSI schon länger ab. Auch hier gilt: Lieber ein ausgefallenes, aber merkbares Passwort als ein kurzes, das sich regelmäßig ändert.

Das wichtigste Motto der neuen Empfehlungen aus dem BSI lautet daher: Lieber weniger komplex, dafür aber einmalig. Damit ist gemeint, dass User unbedingt für jeden Onlinedienst ein anderes Passwort wählen sollen. Das gelingt leichter, wenn die gewählten Passwörter nicht übertrieben komplex und kompliziert sind.

Wichtigste Regel: Jedes Passwort nur einmal nutzen

Um einigermaßen den Überblick zu bewahren, nutzen viele Menschen in vielen Onlinediensten dasselbe Passwort – ist einfacher zu merken. Aber auch unsicher. Denn fällt einem Hacker oder Betrüger, etwa durch einen Hack auf einen Server, ein Passwort in die Hände, lassen sich damit auch alle anderen Onlinedienste „knacken“. Es macht einen Unterschied, ob man nur den Kellerschlüssel verliert – oder einen Generalschlüssel, der viele Türen öffnet.

Die zweite Empfehlung überrascht: „Überkomplexe Passwörter und beständige Passwort-Erneuerung sind wenig zielführend“, so die Richtlinie. Zum ersten Mal kommt von offizieller Seite also der Rat, weniger komplexe Passwörter zu wählen. Denn: Ein Passwort kann zu kompliziert sein. Insbesondere Anforderungen an Passwörter mit langen, oft sinnlosen Zeichenfolgen sieht das BSI mittlerweile als kontraproduktiv an. Merken unmöglich.

Gute Passwörter sind zwar lang, aber trotzdem – irgendwie – gut zu merken. Etwa, indem man die ersten Buchstaben eines Satzes zusammensetzt: „eToEimAevT!“. Steht für „Ein Tag ohne Eiscrème ist möglich, aber ein verlorener Tag!“. Oder – man macht es sich nich einfacher und kombiniert Begriffe, die sinnlos sind, und die deshalb niemals zusammen beim Knacken ausprobiert würden: „SonnenBadenImMeer“.

Test: Wie gut ist mein Passwort?

Ob ein Passwort leicht oder schwer zu knacken ist, lässt sich leicht herausfinden. Einfach das Passwort beim Onlinedienst CheckDeinPasswort eingeben, schon erscheint eine Einschätzung, wie lange Hacker zum Knacken dieses Passwortes brauchen würden. Für „SonnenBadenImMeer“ erstaunliche 471 Milliarden Jahre. Ein gutes Passwort also. Der Onlinedienst gibt aber auch praktische Tipps, wie ein gutes Passwort aussieht. Eine gute Möglichkeit, ein Gefühl für gute Passwörter zu bekommen.

Mac-User sollten dringend ihre Zoom-Software aktualisieren

In Zeiten von Home Office ist die Videokonferenz-Lösung Zoom so populär wie nie. Doch nun hat ein Sicherheitsforscher auf einer Konferenz gezeigt, dass Zoom auf Apple Mac ein erhebliches Sicherheitsproblem hat. Dringendes Update empfohlen!

Die dringende Handlungsanweisung gleich zu Anfang: Nutzer der Videokonferenzsoftware Zoom unter MacOS (Apple-Hardware) sollten so schnell wie möglich das aktuelle Update der Software installieren. Denn eine auf der Hackerkonferenz Defcon in Las Vegas jüngst vorgestellte Sicherheitslücke lässt sich dafür nutzen, Schad-Software zu installieren - und Sicherheitsmaßnahmen des Betriebsystems zu umgehen.

Ein GAU in punkto IT-Sicherheit

Es ist quasi der GAU für alle, die sich für sichere Arbeitsumgebungen in der IT-Welt einsetzen. Eine Software, die extrem weit verbreitet ist und von vielen

nahezu täglich genutzt wird, hat ein Sicherheitsleck, das so groß ist, dass Angreifer so ziemlich alles machen können.

Genau das ist der Fall bei Zoom. Allerdings nur unter MacOS, dem Betriebssystem von Apple. Der Fehler liegt aber nicht im Betriebssystem, sondern in der Art und Weise, wie Zoom Updates einspielt. Um das Laden und Installieren von Updates so einfach und bequem wie möglich zu machen, aktiviert Zoom bei automatischen Updates den Systemverwalter-Modus. Das macht es einfacher, weil Nutzer keine Passwörter eingeben müssen.

Ein Leckerbissen für Hacker

Aber es ist eben ein Risiko, denn so wird das, was da geladen wird, nicht weiter überprüft - und die Installation erfolgt unbemerkt. Ein klassisches Einfallstor, das sich Hacker und Kriminelle zunutze machen können - was angesichts der starken Verbreitung von Zoom sehr attraktiv erscheint.

Wie das Online-Magazin "The Verge" aktuell berichtet, hat der ehemalige NSA-Hacker Patrick Wardle, der als einer der bekanntesten Experten für Mac-Malware gilt, das Problem entdeckt und nun öffentlich gemacht.

Update einspielen

Angreifer können Opfern über das Auto-Update von Zoom (freilich nicht ohne weitere Manipulation) beliebige Programme unterjubeln. Der Experte hat auf der Konferenz gezeigt, dass eigentlich eingezogene Sicherheitsnetze nicht funktionieren. Für Nutzer wäre eine solche Attacke nicht zu bemerken - und auch nicht zu verhindern.

Das Traurige daran: Experte Wardle hatte den Hersteller vom Zoo,m nach eigenen Angaben bereits vor Monaten über eine ganze Reihe solcher Schwachstellen informiert. Doch das Sicherheitsleck im Auto-Updater wurde nicht geschlossen.

Jetzt hat der Hersteller reagiert. Es wurde ein Update veröffentlicht. Damit sollte das Problem ein Ende haben.

Eine PDF-Datei mit SwifDoo PDF elektronisch signieren

Dokumente tauscht man heute in der Regel als PDF-Datei aus - damit kommt fast jeder klar. Manchmal ist es aber erforderlich, ein solches Dokument zu "signieren", also mit einer Art digitalen Unterschrift zu versehen. Dazu sind spezielle Werkzeuge nötig.

Das Unterschreiben auf Papier kennen wir alle: Ob Vertrag, Quittung, Kreditkartenbeleg oder auf dem Amt. Unten unterschreiben, bitte. Allerdings wird es schwieriger mit dem Unterschreiben, wenn digitale Dokumente ausgetauscht werden.

Die gute Nachricht: Das Erstellen und Hinzufügen von Signaturen in PDF-Dokumenten ist recht einfach und bequem. In diesem Artikel wird beschrieben, wie man mit Hilfe SwifDoo PDF - einem einfach zu handhabenden PDF-Editor - ein PDF-Dokument elektronisch signiert.

Warum ein PDF elektronisch signieren?

Einem PDF-Dokument eine elektronische Signatur hinzuzufügen ist der einfachste Weg, ein digitales Dokument zu signieren, ohne es ausdrucken und nach erfolgter Unterschrift wieder einscannen zu müssen (was zweifellos viele machen, aber denkbar unpraktisch ist).

Eine elektronische Unterschrift ist heutzuage genauso rechtsverbindlich wie eine handschriftliche Unterschrift - und zudem umweltfreundlicher. Egal, welches Dokument Sie erhalten: Sie können es schnell mit einer elektronischen Signatur versehen und per E-Mail versenden.

Allerdings lassen sich PDF-Dokumente nur schwer bearbeiten. Deshalb brauchen Sie einen geeigneten "PDF-Signierer", wenn es darum geht, ein PDF elektronisch zu unterschreiben.

Wie man eine PDF-Datei an einer bestimmten Stelle elektronisch signiert

SwifDoo PDF ist ein professionelles PDF-Softwarepaket, mit dem Sie eine elektronische Signatur erstellen und in ein beliebiges PDF-Dokument einfügen können. Mit dieser Desktop-Software können Sie:

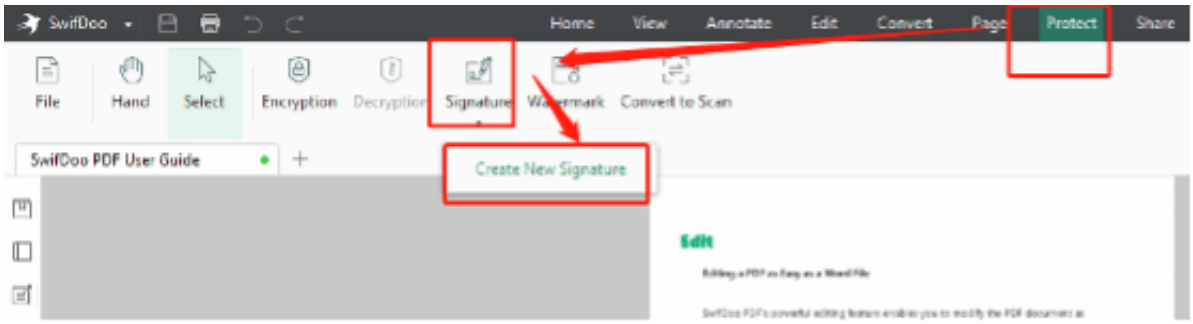
- Ihre eigene elektronische Signatur erstellen;
- Ihr Dokument mit einem Passwort verschlüsseln, um Informationsverluste zu vermeiden;
- Ihr elektronisch signiertes PDF-Dokument per E-Mail, Dropbox und Google Drive mit Mitarbeitern teilen;
- Ein PDF-Formular ausfüllbar machen, um das Formular auszufüllen.

Um ein PDF in einer bestimmten Position elektronisch zu signieren, folgen Sie bitte diesen einfachen Schritten.

Schritt 1: Laden Sie dieses Programm herunter (derzeit nur für Windows-Rechner zu haben) und installieren Sie es. Klicken Sie mit der rechten Maustaste auf das Symbol, gehen Sie zu **Öffnen mit** und wählen Sie **SwifDoo PDF**, um Ihre PDF-Datei zu öffnen;

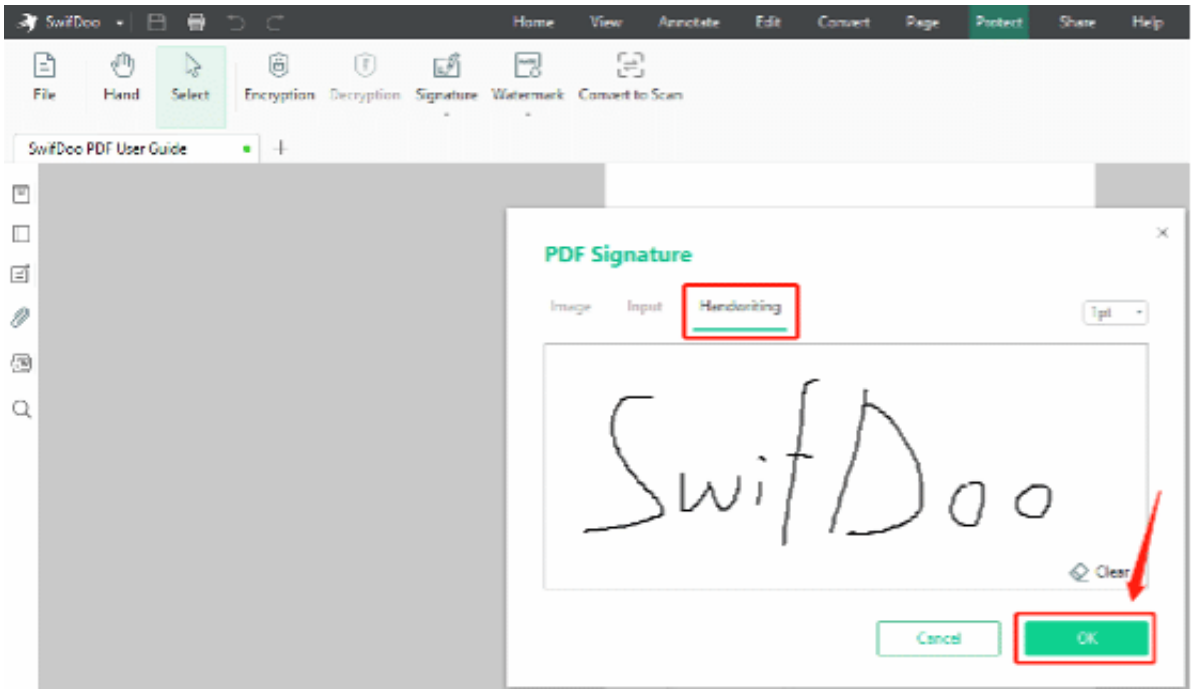
Schritt 2: Nachdem die Datei angezeigt wurde, wählen Sie Schützen in der oberen Symbolleiste;

Schritt 3: In der Multifunktionsleiste werden verschiedene Werkzeuge zum Schutz der Datei angezeigt. Klicken Sie auf die Registerkarte "**Signatur**" und dann auf "**Neue Signatur erstellen**";



Schritt 4: Klicken Sie im Fenster PDF-Signatur auf **Handschrift**, um die Schreibtafel zum Unterschreiben Ihres Namens zu verwenden;

Schritt 5: Tippen Sie auf **OK**, navigieren Sie zu der Stelle, an der Sie Ihre elektronische Signatur hinzufügen möchten, und klicken Sie darauf.



Das ist die schrittweise Anleitung, wie man eine PDF-Datei an einer bestimmten Stelle elektronisch signiert. Sie können Ihren Namen nicht nur auf die Schreibtafel schreiben, sondern haben auch zwei andere Möglichkeiten, Ihre elektronische

Unterschrift zu erfassen. Sie können Ihren Namen in verschiedenen Schriftarten eingeben oder ein Bild Ihrer handschriftlichen Unterschrift hochladen, indem Sie es fotografieren oder scannen.

Elektronisches Signieren einer PDF-Datei auf mehreren Seiten

Wenn Sie Schwierigkeiten haben, eine PDF-Datei auf mehreren Seiten zu unterschreiben, bietet SwifDoo PDF den Service, eine elektronische Unterschrift an der gleichen Stelle auf verschiedenen Seiten einzufügen.

Schauen Sie sich die einfachen Schritte an, um eine PDF-Datei auf mehreren Seiten elektronisch zu signieren:

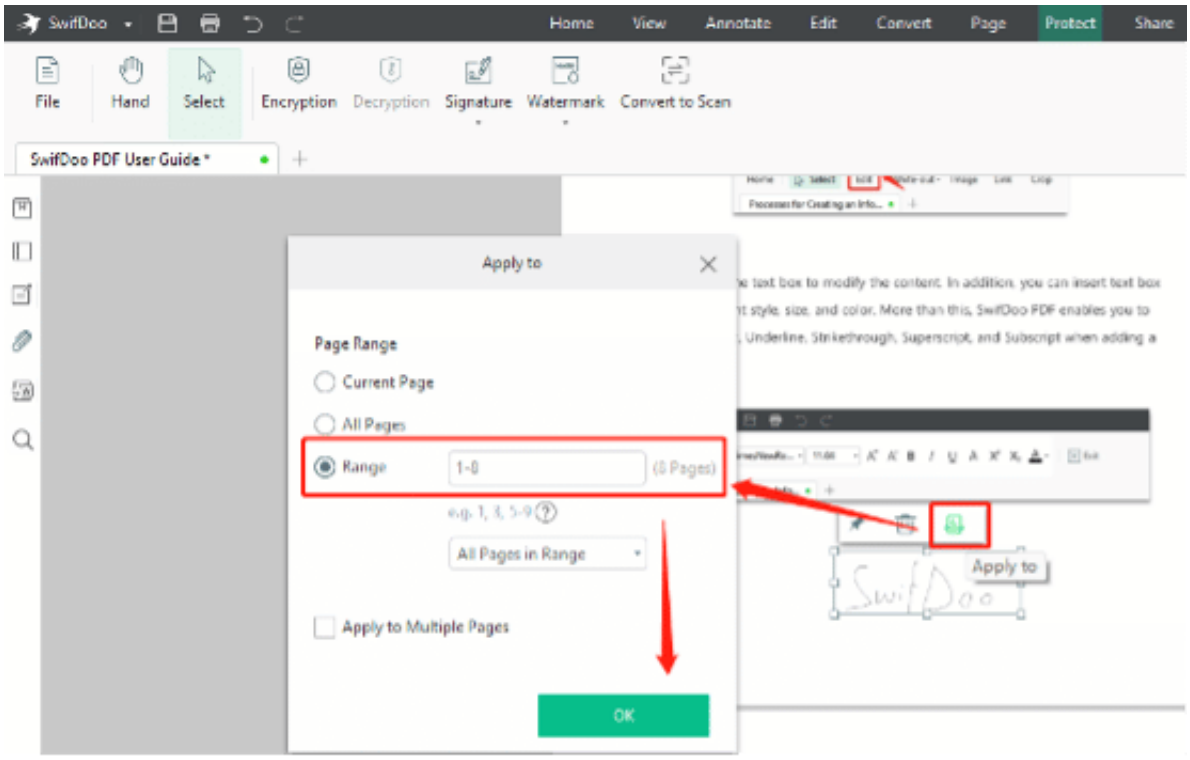
Schritt 1: Starten Sie diese Anwendung. Klicken Sie auf die Schaltfläche **Öffnen** auf der linken Seite, um Ihre Datei zu importieren;

Schritt 2: Klicken Sie auf **Schützen**, wählen Sie unten **Signatur** und wählen Sie **Neue Signatur erstellen**;

Schritt 3: Wählen Sie im Pop-up-Fenster **Schreiben** und ziehen Sie die Maus, um Ihren Namen in das leere Feld zu schreiben;

Schritt 4: Tippen Sie auf **OK** und klicken Sie auf die Stelle, an der Sie die e-Signatur gerne hinzufügen möchten;

Schritt 5: Klicken Sie auf die Unterschrift und dann auf das Symbol **Anwenden auf**. Im Fenster **Anwenden auf** drücken Sie auf **Bereich**, legen Sie den Seitenbereich fest und wählen Sie **OK**, um das zu übernehmen.



So ist das also, wie man eine PDF-Datei auf mehreren Seiten elektronisch signiert! Mit der E-Signierfunktion von SwifDoo PDF können Sie Ihre PDF-Datei im Handumdrehen elektronisch signieren und alle erstellten Signaturen speichern, was Ihre Arbeitseffizienz erheblich verbessert. Darüber hinaus können die anderen Schutzfunktionen des Programms den unbefugten Zugriff auf Ihre sensiblen Informationen verhindern und Ihre Rechte und Interessen schützen.

Was Sie wissen sollten, bevor Sie eine PDF-Datei unterschreiben

1. Lesen Sie das Dokument, das Sie erhalten, sorgfältig durch, bevor Sie es unterschreiben

Eine elektronische Unterschrift ist genauso rechtsgültig wie eine herkömmliche Unterschrift mit Tinte. Sie müssen sich vergewissern, dass mit dem Inhalt der Datei nichts schräg ist, um Probleme zu vermeiden.

2. Verschlüsseln Sie sensible Dateien richtig

Es besteht ein Risiko, wenn Sie Ihre elektronische Signatur und Ihre Dateien falsch handhaben. Daher ist es besser, Ihre sensiblen PDF-Dokumente mit Passwörtern zu verschlüsseln, um zu verhindern, dass Unbefugte auf die Datei

zugreifen und Sie finanzielle Verluste erleiden können.

3. Verwenden Sie eine digitale Signatur

Eine digitale Signatur ist eine Art elektronische Unterschrift mit höherem Sicherheitsniveau. Sie kann das Risiko der unbefugten Unterzeichnung und der Manipulation von Dateien erheblich verringern. Allerdings kann eine seriöse Anwendung für digitale Signaturen einen hohen Preis verlangen.

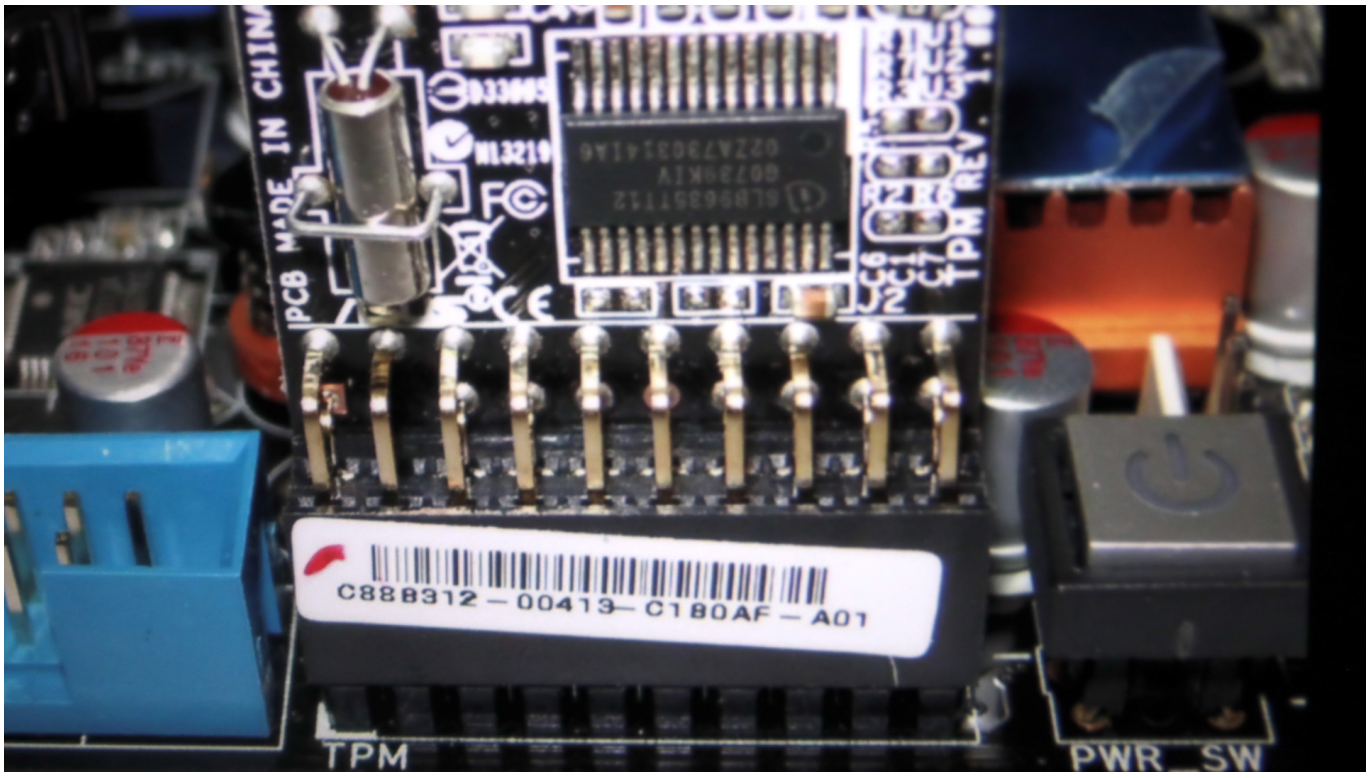
Über SwifDoo PDF

SwifDoo PDF ist aber mehr als nur ein PDF-Signierer. Als PDF-Einstiegsprodukt ist dieses Programm vollgepackt mit leicht verständlichen Funktionen, die Sie bei Ihren täglichen Aufgaben unterstützen. Neben der Erstellung von PDF-Signaturen können Sie damit auch PDF-Dateien zusammenführen, teilen, bearbeiten und konvertieren. Sie können die PDF-Tools optimal nutzen, um Ihre Produktivität zu steigern. Spoiler-Alarm: Diese Windows-Desktop-Anwendung ist im August auf Englisch, Deutsch und Französisch erhältlich.

Schlussfolgerung

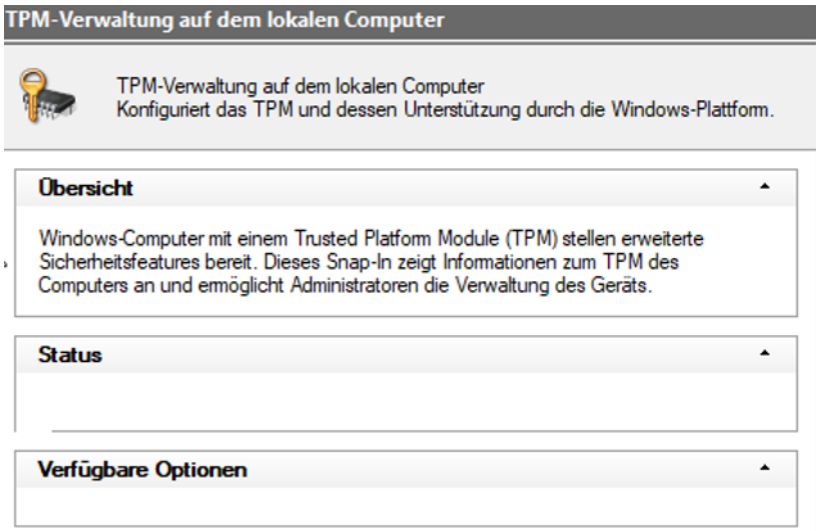
Mit den obigen Anleitungen ist klar, wie man eine PDF-Datei mit SwifDoo PDF elektronisch signieren kann. Diese funktionelle PDF-Softwarelösung ermöglicht es Ihnen, Ihr PDF-Dokument mit wenigen Klicks zu signieren, und alle Ihre Signaturen können für eine spätere Verwendung geordnet gespeichert werden. Sie können die 15-tägige kostenlose Testversion nutzen, um sie auszuprobieren.

Hat mein PC ein Trusted Platform Module?



Viele Sicherheitsfunktionen eines PC basieren auf einem TPM, dem Trusted Platform Module oder Sicherheitschip. Wir zeigen Euch, wie Ihr herausfindet, ob in Eurem Rechner einer verbaut ist.

Sicherheit ist ein wichtiges Thema, auch bei Windows 10 und 11. Da gibt es diverse organisatorische Dingen, die Euch als Benutzern obliegen: Sinnvolle Passwörter, Sperren des PCs, Vorsicht bei der Kommunikation mit Fremden, Virenschutz, all das wirkt schon viel. Was aber, wenn Euer Gerät nicht mehr in Euren Händen ist? Dazu hilft die Verschlüsselung, und die braucht für die wirkliche Wirksamkeit eine Hardware, eben den TPM-Chip.



Ohne diesen ist beispielsweise eine Installation von Windows 11 gar nicht - oder nur mit massiven manuellen Eingriffen - möglich. Wie aber findet Ihr nun raus, ob Euer Rechner einen solchen Chip hat? Dazu gibt es zwei Möglichkeiten:

- Tippt in der Suchleiste **tpm.msc** ein. Windows startet die TPM-Verwaltung, die Euch Informationen zum Chip anzeigt, wenn dieser vorhanden ist. Vorsicht: Bei verwalteten Rechnern (beispielsweise in einem Büro-Umfeld) kann hier eine Fehlermeldung erscheinen, weil die Funktion von den Administratoren gesperrt ist. Dann ist die zweite Möglichkeit eine Alternative:
- Unter **Einstellungen** > **Update &Sicherheit** > **Windows-Sicherheit** > **Gerätesicherheit** > **Sicherheitschip** zeigt Windows Euch den TPM-Chip an oder meldet, dass es keinen Chip findet. Da es sich hier um eine Windows-Standardfunktion handelt, ist diese immer verfügbar.