Schieb Report

Ausgabe 2022-43

Schieb Report

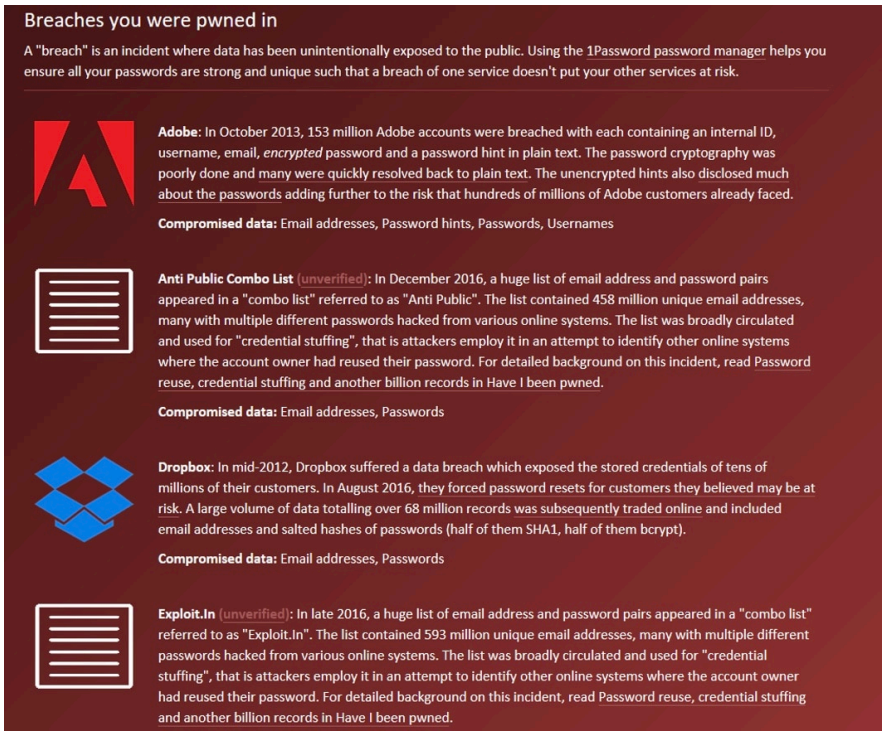
Ausgabe 2022-43

Wichtig: Regelmäßiges Überprüfen von Passwörtern

Passwörter sind der Schlüssel zu Euren schützenswerten Daten. Einmal vergeben, ändert Ihr sie nicht mehr so häufig, das sagt auch das BSI mittlerweile. Trotzdem solltet Ihr sie regelmäßig überprüfen!

Ist es schon zu spät?

Immer wieder kommen Datenlecks und -pannen in die Nachrichten: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen und im Internet verkauft. Der Käufer hat dann so lange theoretisch Zugriff auf all Eure Benutzerkonten, wie Ihr das Passwort nicht geändert habt.



Die bekanntesten Sicherheitsvorfälle (zumindest die, die bekannt geworden sind), sind auf der Seite https://haveibeenpwned.com/ zusammengefasst. Dort könnt Ihr nach Eingabe Eures Passwortes sehen, ob und bei welchem Hack Eure Zugangsdaten erbeutet wurden.

Wenn Ihr betroffen seid, dann ändert so schnell wie möglich das Passwort, und wiederholt dies häufiger.

Wie gut ist mein (neues) Passwort?

Wenn Ihr ein neues Passwort vergeben wollt, dann könnt Ihr dieses auf der Webseite https://checkdeinpasswort.de überprüfen lassen. Die berechnet, wie lange ein herkömmlicher PC brauchen würde, um dieses durch Berechnungen und stumpfes Ausprobieren zu erraten.

Probiert hier mit verschiedenen Arten von Passwörtern herum, die Ergebnisse sind teilweise verblüffend: So ist ein langes Passwort, das sich aus echten Wörtern zusammensetzt, deutlich schneller zu knacken, als ein kurzes, das sich beispielsweise aus den Anfangsbuchstaben eines leicht zu merkenden Satzes zusammensetzt (z.B. "Passwörter sind 2022leicht zu merken!" = *Ps2022lzm!*), aber rein technisch aus einer scheinbar zusammenhangslosen Zeichenkombination bestehen!

Phishing-Erkennung trainieren

Phishing-Attacken sind vielfältig und immer anders. Es gibt keinen wirklichen Schutz, außer Euch immer und immer wieder damit zu beschäftigen, Euch zu trainieren, solche Mails und Nachrichten zu erkennen und gar nicht erst darauf zu reagieren.

Google Jigsaw-Puzzle

Google als Anbieter verschiedenster Webdienste ist natürlich hoch interessiert daran, Phishing-Seiten zu identifizieren und auf der anderen Seite Euch als Benutzer davon abzuhalten, auf sie reinzufallen. Schließlich könnten die ja auch im Suchergebnisse einer Google-Suche auftauchen und Anwender auf den Link klicken!

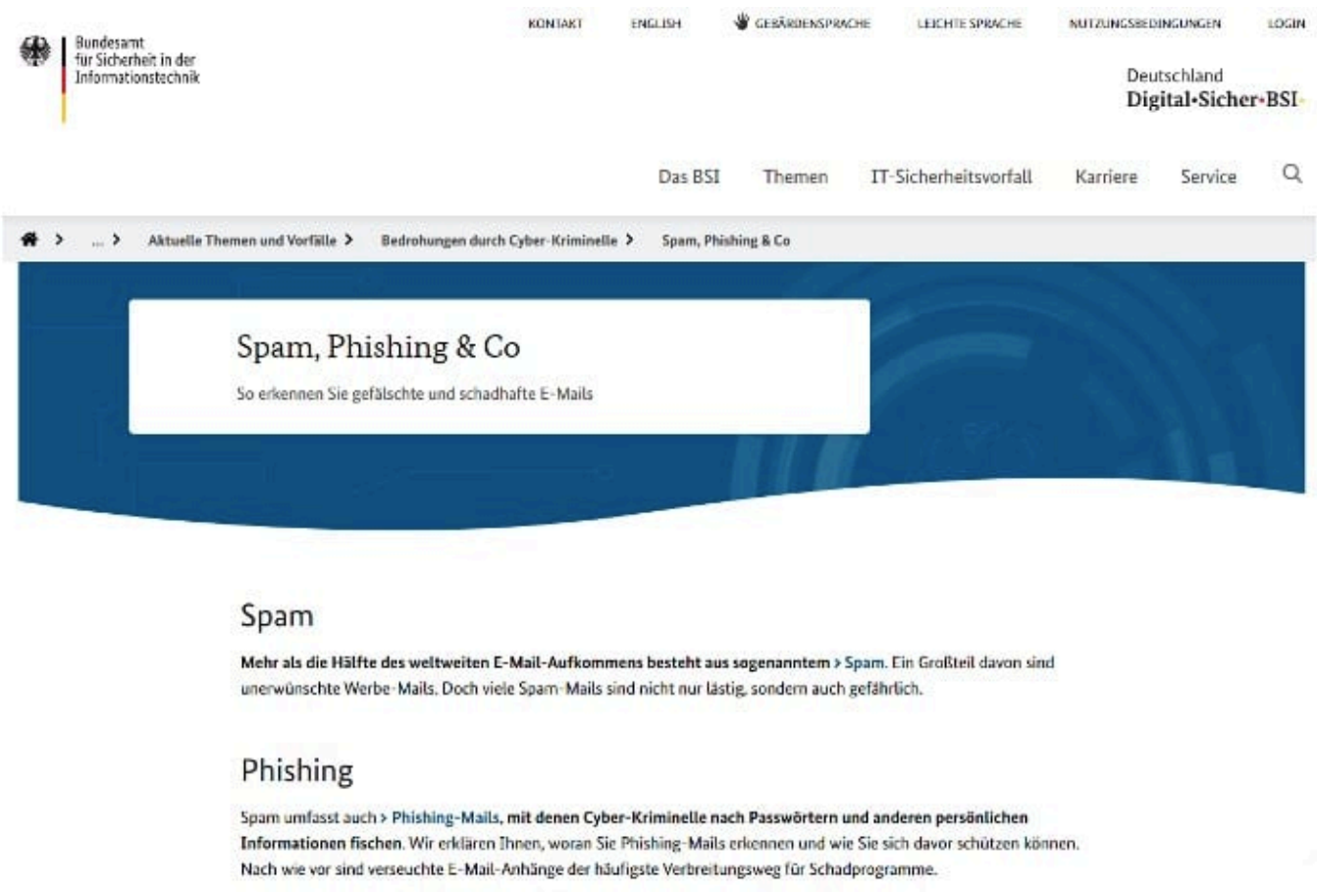
Unter diesem Link findet Ihr das Quiz. Ihr gebt Euren Namen und Eure E-Mail-Adresse an, dann zeigt Euch das Quiz verschiedene E-Mails und fordert Euch auf, diese zu bewerten: Phishing oder nicht?

Keine Sorge: Weder werden Eure eingegebenen Informationen verwendet (die dienen nur dazu, die angezeigten E-Mails noch ein wenig realistischer zu machen), noch sind die Links in den Beispielen klickbar. Google will Euch ja schließlich nicht gefährden!

Die Beispiel-E-Mails ändern sich immer mal wieder, es macht also Sinn, das Quiz regelmäßig zu machen!

Der E-Mail-Sicherheitscheck des BSI

Das Bundesamt für Sicherheit in der Informationstechnik, kurz: BSI, ist die Behörde, die sich intensiv mit Sicherheitslücken beschäftigt. Die Aufklärung der Bürger ist dabei ein wichtiges Thema.

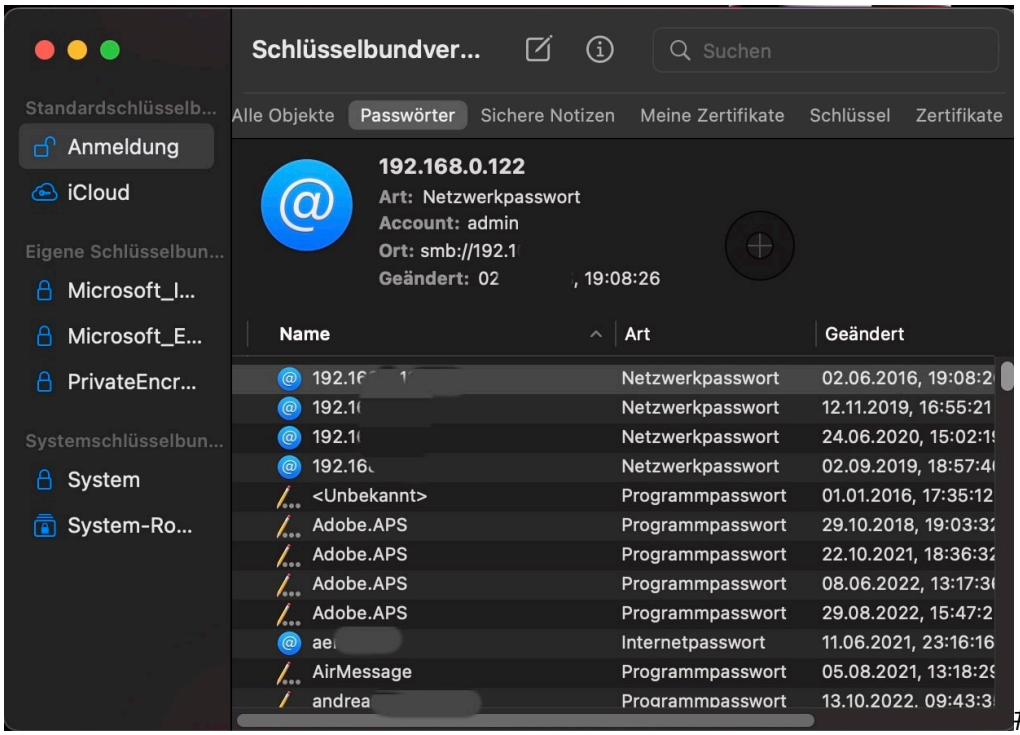


Hier findet Ihr den Bereich zum Thema SPAM und Phishing. Darin findet Ihr ein Video, in dem anschaulich dargestellt wird, woran Ihr gefälschte E-Mails erkennen könnt. Auch auf der BSI-Seite werden die Inhalte immer wieder angepasst und verändert, regelmäßiger Besuch lohnt sich also.

Herausfinden gespeicherter Passwörter bei macOS/iOS

MacOS, iOS- und iPad-OS-Geräte speichern die Passwörter ab und füllen sie bei der nächsten Verwendung komfortabel vor. Einen Nachteil hat das allerdings: Ihr merkt Euch immer weniger Passwörter. Wir zeigen Euch, wie Ihr die Passwörter auslesen könnt!

Der Kern der beschriebenen Funktionalität ist der Schlüsselbund. Der nimmt im Apple-Universum alle Passwörter auf, speichert sie verschlüsselt und macht sie bei Bedarf Anwendungen wie Browsern wieder verfügbar. Der Schlüsselbund wird zusätzlich noch mit iCloud synchronisiert, wenn Ihr das aktiviert habt. Jedes Gerät, das mit derselben Apple ID angemeldet ist, kann dann alle Passwörter nutzen, als wären sie auf dem Gerät eingegeben worden.


#

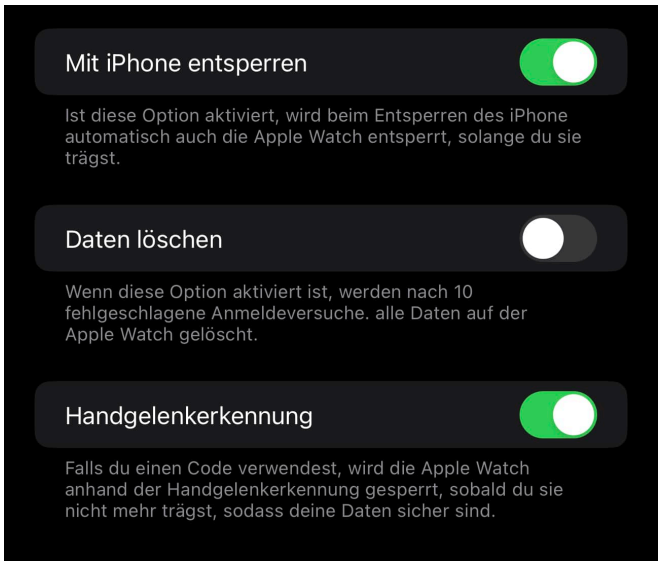
Um ein Passwort wieder auszulesen, geht wie folgt vor:

- Auf dem Mac such in Spotlight nach Schlüsselbund und startet die **schlüsselbundverwaltung.app**.
- Auf einem iPad oder iPhone klickt in den Einstellungen auf **Passwörter**.
- Klickt/tippt in das Suchfeld, dann gebt den Namen der Webseite oder des Dienstes an, für den Ihr das Passwort auslesen wollt.
- Auf dem Mac müsst Ihr zum Anzeigen des Passwortes noch das Kennwort des aktuellen Geräts eingeben.
- Ihr seht das Kennwort jetzt in Klageschrift, auf dem iPad könnt Ihr es durch Halten des Fingers auf dem Passwort-Eintrag in die Zwischenablage kopieren und dann direkt in eine Anmeldemaske eintragen.

Wenn die Apple Watch dauernd die PIN abfragt

Die Apple Watch soll Euch den Blick aufs Handy sparen und Euch damit erleichtern, informiert zu sein. Das allerdings fällt schwer, wenn sie Euch dauernd zur PIN-Eingabe auffordert und vorher keine Benachrichtigungen oder andere Informationen anzeigt! Wir zeigen Euch die Lösung dafür!

Jede Benachrichtigung birgt ein gewisses Risiko: Die Uhr liegt unbeaufsichtigt auf dem Tisch, weil Ihr gerade unter der Dusche seid, damit kann jeder, der auf die Uhr schauen kann, den Inhalt der Nachricht lesen. Um das zu vermeiden, gibt es die Handgelenkerkennung: Die Watch erkennt anhand der Sensoren auf der Unterseite, dass sie nicht am Arm des Benutzers ist und erfordert die PIN-Eingabe, bevor sie wieder bedienbar ist.



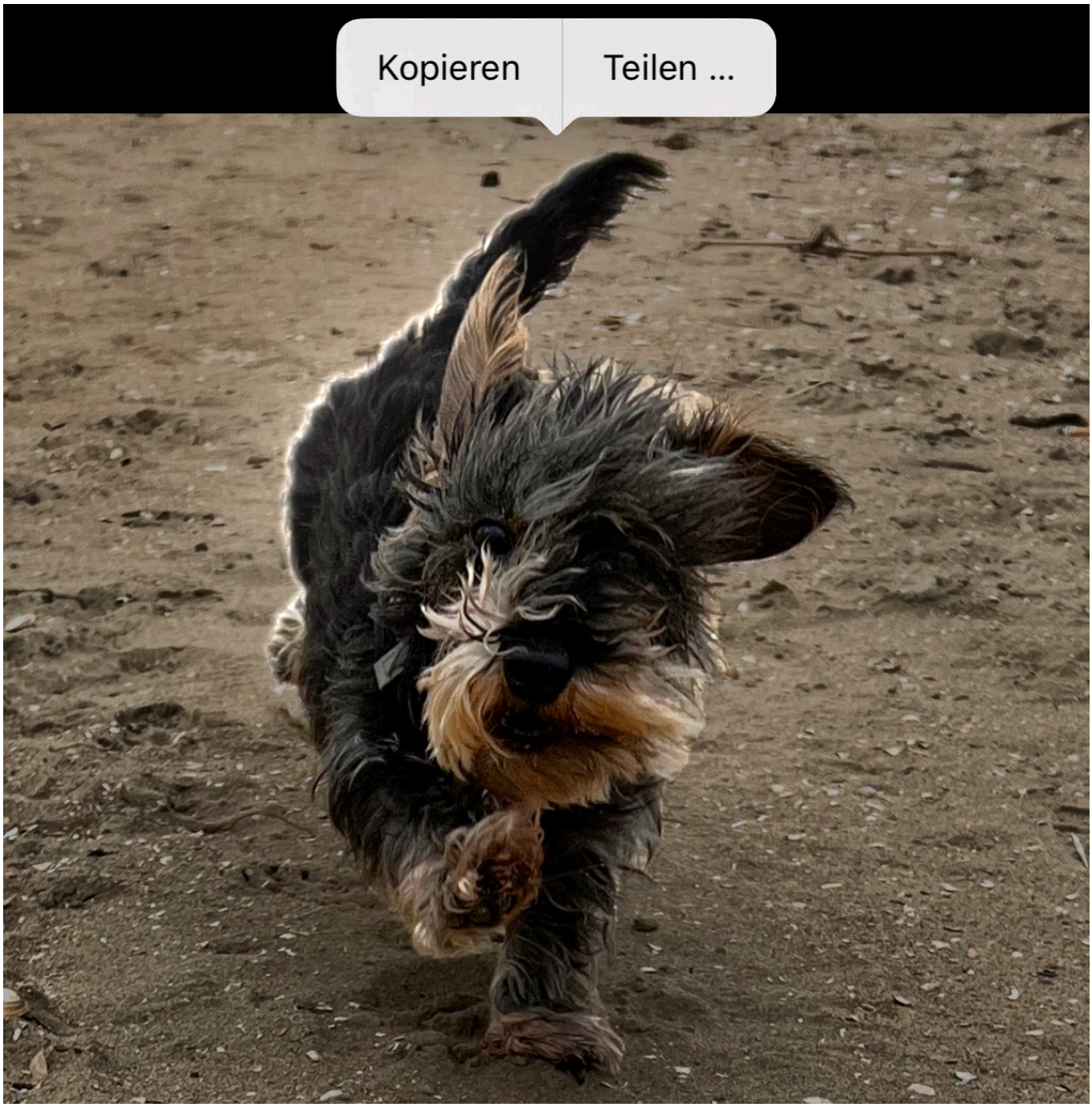
Was erst einmal toll klingt, funktioniert nicht bei jedem Anwender einwandfrei: Wenn Ihr Eure Uhr locker tragt, dann kann es schnell passieren, dass sie den "Kontakt" mit dem Arm verliert und denkt, sie sei nicht mehr an Eurem Arm. Jedes Mal die PIN einzugeben, nervt und ist unnötiger Aufwand.

Schaltet die Handgelenkerkennung einfach aus:

- Startet die Watch App auf dem iPhone.
- Tippt auf die Option **Code**.
- Wischt ganz nach unten und deaktiviert den Schalter **Handgelenkerkennung**.

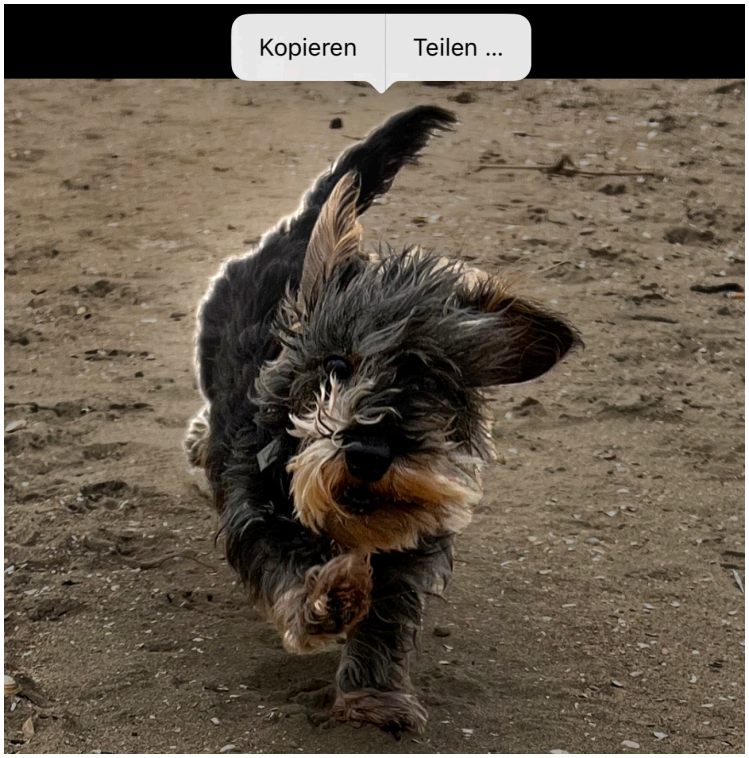
Die Watch prüft nicht mehr die Verbindung zu Eurem Handgelenk und bleibt aktiv. Seid Euch nur darüber bewusst, dass die Uhr damit keinen Schutz mehr vor unberechtigten Zugriffen bietet, wenn sie unbeaufsichtigt ist.

Versteckter Hack: Bilder in iOS 16 freistellen



Fotos mit dem Smartphone sind schnell und unkompliziert gemacht. Leider oft mit dem Nebeneffekt, dass um das Motiv störende Objekte sind. iOS 16 bietet einen tollen Hack, der ohne großen Aufwand nur das Motiv ausschneidet!

Das so genannte Freistellen von Objekten, also das trennen des Motivs von seinem Hintergrund, ist manuell nicht ganz so einfach. Zu oft verschwimmen das Motiv und der Hintergrund miteinander, und mit manuellen Bildbearbeitungswerkzeugen seid Ihr nie so exakt, dass man die Ränder nicht seht.



In iOS 16 hat Apple eine Funktion zum Freistellen von Bild-Teilen direkt in die Foto-App integriert.

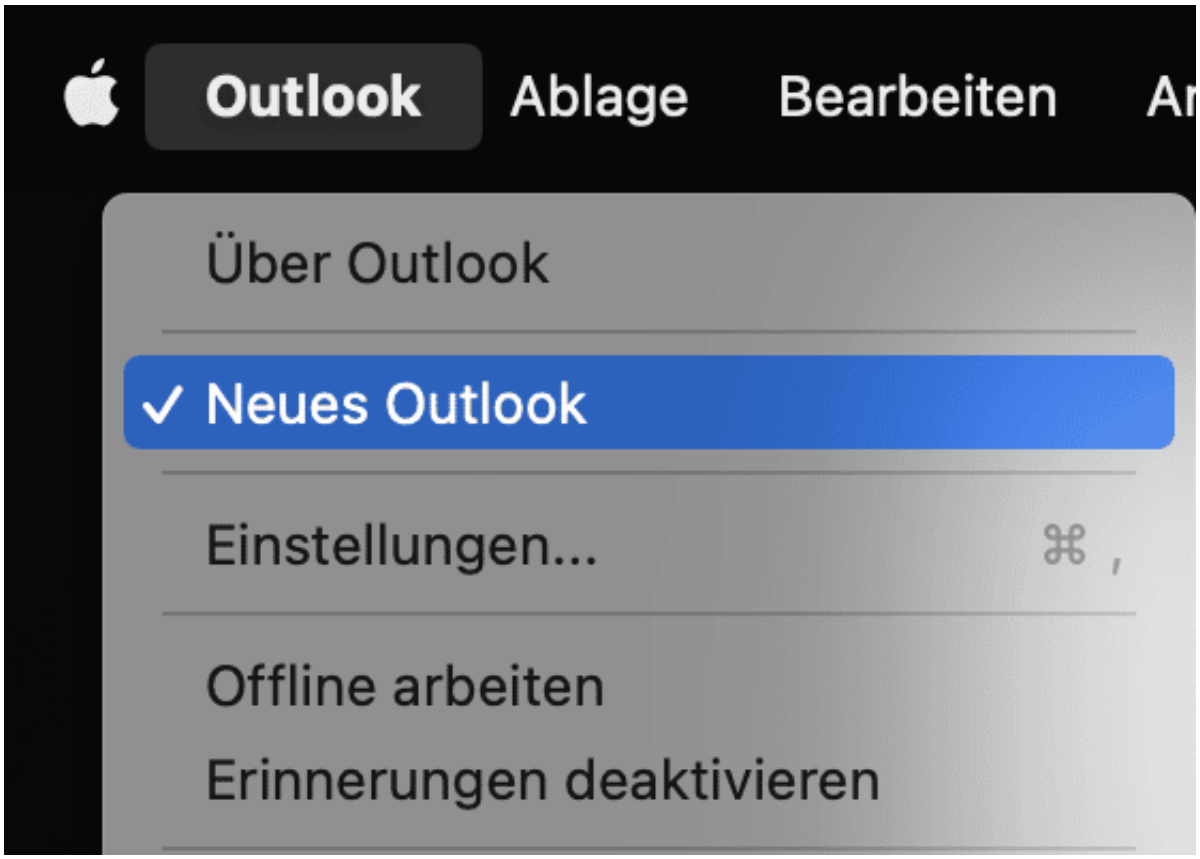
- Öffnet das Bild, in dem Ihr ein Objekt freistellen wollt, mit der Fotos-App.
- Haltet den Finger einen Moment auf das Objekt auf dem Bildschirm.
- Wenn iOS das Objekt identifizieren konnte, dann zeigt es eine laufende Lichtleiste um das Objekt an.
- Wenn Ihr den Finger jetzt bewegt, dann bewegt sich das Objekt mit dem Finger, damit könnt Ihr leicht sehen, ob die Grenzen korrekt erkannt worden sind.
- Hebt den Finger vom Display des iPhones , dann erscheint am oberen Bildschirmrand eine neue Symbolleiste.
- Tippt auf **Kopieren**, um das freigestellte Objekt in die Zwischenablage zu kopieren und damit in eine E-Mail oder eine andere App einfügen zu können.
- Tippt auf Teilen, um es direkt über iOS an Empfänger per E-Mail,

Facebook, Twitter und andere Apps und Dienste weiterzuleiten.

Wechsel zwischen neuem und alten Outlook auf dem Mac

Neue Funktionen vorab zu testen ist super. Auch bei Outlook und anderen Produktivitäts-Tools. Wenn die aber noch nicht vollends getestet sind, dann müsst Ihr manchmal zurück zur stabilen Version. Bei Outlook für Mac ist das nicht ganz so einfach. Es sei denn, Ihr nutzt unseren Hack.

Es gibt zwei Arten von Vorab-Versionen bei Microsoft-Produkten: Das Insider-Programm ist vor allem für Windows und deren Vorabversionen in verschiedenen Kanälen gedacht. Nachdem dies für Microsoft recht erfolgreich war, ist dieses Programm auch für Office ausgerollt worden. Hierbei handelt es sich aber um dauerhafte Veränderungen: Es wird eine neuere Version von Windows/Office installiert, die nur durch eine Neuinstallation wieder auf die Standardversion zurückgestellt werden kann.



Bei Outlook gibt es separat vom Insider-Programm die Funktion "Neues Outlook". Bei den ersten Versionen konntet Ihr mit einem Schalter in der Symbolleiste zwischen der aktuellen Outlook-Version und der Vorschau-Version umschalten. Eine Neuinstallation war (und ist) nicht nötig. Noch besser: Ihr könnt alte und neue Version schnell miteinander vergleichen.

Bei den neueren Versionen von Outlook für Mac fehlt allerdings dieser Schalter. Keine Sorge, die Umschaltmöglichkeit besteht weiterhin! Klickt auf Outlook in der Symbolleiste und aktiviert (oder deaktiviert) die Option **Neues Outlook**. Nach einem automatischen Neustart schaltet Outlook zwischen den beiden Versionen um.

Zugriff auf den Schlüsselbund durch Microsoft-Dienste?

Ihr seid sensibilisiert durch die verschiedenen Veröffentlichungen über Ransomware und Phishing. Meldungen über Zugriffsversuche auf Eure Passwörter machen Euch also zu Recht unruhig. Nicht jede solcher Meldungen ist aber tatsächlich Hinweis auf ein echtes Sicherheitsproblem!

Viele Anwender von Office auf dem Mac werden mit einer Meldung konfrontiert, dass ein Office Produkt (SharePoint, Word, Excel und andere) Zugriff auf den Schlüsselbund erfordert. Der Schlüsselbund ist der zentrale Speicher, in dem macOS und iOS die verwendeten Passwörter ablegen und auch zwischen den Geräten über iCloud synchronisieren.

Um diesen Zugriff freizugeben, sollt Ihr das Anmelde-Kennwort Eures Macs eingeben. Potenziell ein Risiko, eine Schadsoftware hätte damit weitgehende Zugriffsrechte auf Euren Mac.

Auslöser der Meldung oben ist meist die Neuinstallation oder ein durchgeführtes Update von Office, bei dem Rechte zurückgesetzt wurden, die eine Office-App benötigt. Auch die Installation in einem anderen als dem Standard-Ordner kann dieseMeldung auslösen.

Um die betroffenen Programme weiterhin nutzen zu können, müsst Ihr hier das Kennwort eingeben und dann auf **Immer erlauben** klicken. Klickt Ihr nur auf **Erlauben**, dann kommt die Nachfrage regelmäßig wieder, wenn Office auf die entsprechenden Einträge im Schlüsselbund zugreifen will.

Pro7-Entertainer Joko und Klaas „spenden“ ihre Accounts

Das nenne ich mal einen Medien-Coup: Joko und Klaas von Pro7 räumen iranischen Aktivistinnen nicht nur Sendezeit auf Pro7 ein, sondern "spenden" auch ihre erfolgreichen Instagram-Accounts. Was bedeutet das eigentlich konkret?

Joko Winterscheit und Klaas Heufer-Umlauf sind die Gute-Laune-Clowns bei Pro7. Immer gut drauf. Alles ist eine Pointe wert. Sie sind aber auch erfahrene Medienprofis. Sie wissen ganz genau, was sie tun. Knallharte Geschäftsleute.

Und deshalb dürfen wir beim jüngsten Move Kalkül unterstellen.

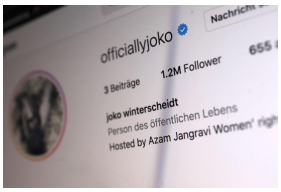
Der eine 1 Mio., der andere 1,2 Mio. Follower

Jetzt haben sie den Aktivistinnen und Aktivisten im Iran nicht nur viel Sendezeit geschenkt, sondern nur einen weiteren Kniff angewandt: Die beiden haben ihre Instagram-Accounts gespendet. Der eine (Joko) hat 1,2 Mio. Follower, der andere

(Klaas) knapp eine Mio. Follower.

Das ist für deutsche Verhältnisse wirklich extrem viel. Mit so vielen Followern lässt sich eine Menge Geld verdienen. Die beiden Accounts zu spenden – und das auch noch „für immer“, wie die beiden Moderatoren betonen –, ist also ein Commitment, das die beiden zum einen Reichweite kostet – aber auch ganz konkret Geld.

Deshalb ist es ehrenwert, den Aktivistinnen aus Iran den Kanal auf Instagram zur Verfügung zu stellen. Ein starkes Sprachrohr. Auch wenn so etwas schon andere Prominente gemacht haben. Die Idee ist also nicht neu.



Instagram Accounts gespendet[/caption]

Im Iran gibt es kein Instagram

Wie viel es den Aktivistinnen am Ende allerdings bringt, über 1 Mio. Menschen in Deutschland zu erreichen, ist fraglich. Wichtig wäre es ja, Menschen im Iran zu erreichen. Aber die sind nicht auf den Follower-Listen von Klaas und Winterscheit. Außerdem ist Instagram im Iran gesperrt.

Der Impact der Aktion dürfte also überschaubar sein. Hier in Deutschland sind doch sowieso fast alle auf der Seite der Aktivistinnen.

Winterscheit und Heufer-Umlauf machen bald neue Accounts auf und haben ihrer 1 Mio. Follower in kürzester Zeit wieder. Jede Wette.

Das ist nicht als Kritik zu verstehen. Es ist nur eine Einordnung. ;-)

https://www.youtube.com/watch?v=YMaf_7AyBRw&t=95s

[caption id="attachment_782491" align="alignnone" width="1030"]

BSI warnt vor einer bedrohlichen Cybersicherheitslage

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt in seinem verspätet veröffentlichten Jahresbericht vor einer erheblich gestiegenen Gefahr vor Cyber-Attacken auch in Deutschland.

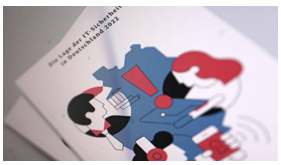
Aufgrund der öffentlichen Debatte um den bisherigen Leiter des BSI Arne Schönbohm ist der „Lagebericht zur Cybersicherheit in Deutschland“ erst mit rund zwei Wochen Verspätung veröffentlicht worden. Der Bericht deckt den Zeitraum vom 1. Juni 2021 bis 31. Mai 2022 ab.

Verschärfte Sicherheitslage auch in Deutschland

Klarer Tenor: Durch den Angriffskrieg auf die Ukraine hat sich auch die Sicherheitslage in Deutschland erkennbar verschärft. Laut Bericht ist es seit Kriegsbeginn auch in Deutschland zu vermehrt relevanten Vorfällen gekommen.

Gezielte Angriffe auf kritische Infrastruktur nehme ebenso zu wie Hackangriffe auf Unternehmen und politische Einrichtungen. Und das sind nur die Cyber-Angriffe, die registriert und gemeldet werden.

Längst nicht alle Angriffe werden bemerkt und entdeckt – und erst recht nicht gemeldet. Denn welches Unternehmen weiß es schon zu schätzen, wenn in der Öffentlichkeit über relevante Sicherheitslecks diskutiert wird, die von Cyberangreifern erfolgreich ausgenutzt werden. Daher deckt auch der aktuelle Sicherheitsbericht längst nicht alle stattgefundenen Angriffe ab. Nur Angriffe auf Kritische Infrastruktur sind meldepflichtig.



Der neue Lagebericht zur IT-Sicherheitslage[/caption]

Angriffe nehmen deutlich zu

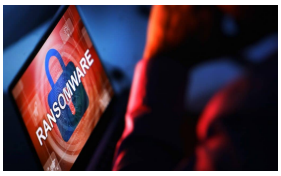
Als Beispiel für jüngste Angriffe erwähnt der BSI-Bericht den Ausfall der satellitengestützten Kommunikation zur Fernwartung von Windenergieanlagen, direkt zu Anfang des Kriegs. Ein Kollateralschaden in Teilen Europas, der durch Angriffe auf Satellitenanlagen entstanden ist – also kein direkter, gezielter Angriff. Aber einen Schaden gab es trotzdem.

Im Februar ist es zu Cyberangriffen auf einen Tankstellenzulieferer gekommen. Der Mineralöllieferant Oiltanking Deutschland GmbH kämpfte tagelang mit den Folgen eines Hackangriffs. Dadurch war das Abfüllen von Tankwagen gestört – und die Lieferkette gefährdet. Die Beispiele zeigen, wie vulnerabel heutige Systeme sind. Wenn die IT-Infrastruktur ausfällt oder gestört ist, kommt es nicht selten zu Totalausfall.

Die Vorsitzende des Verteidigungsausschusses Marie-Agnes Strack-Zimmermann (FDP) erklärte mir am Rand einer Veranstaltung in Düsseldorf: „Wir sind in Deutschland erheblich gefährdet – und müssen uns unbedingt viel besser schützen.“
[caption id="attachment_782482" align="alignnone" width="1030"]

Ziel der Angreifer: Verunsicherung der Bevölkerung

Das ist zweifellos auch der Tenor des BSI-Berichts. Auch wenn es laut Erkenntnissen des BSI bislang nicht zu einer flächendeckenden Kampagne gegen deutsche Ziele gekommen ist, so nehmen die Angriffe erkennbar zu – und eben nicht nur auf erwartbare Ziele. Es trifft auch Ziele, mit denen niemand gerechnet hätte, etwa Windanlagen oder Benzin-Zulieferer. Es geht bei vielen solcher Angriffe in erster Linie um die Verunsicherung der Bevölkerung.



Ransomware: Eine zunehmende Bedrohung[/caption]

Ransomware erpresst Lösegeld

Eins der aktuell größten Probleme für Staat, Wirtschaft und sogar Privatleute sind Ransomware-Angriffe. Durch Ausnutzen von Sicherheitslücken dringen Angreifer in PCs oder ganze Netzwerke ein, verschlüsseln alle Daten und legen somit den Betrieb lahm. Zuletzt wurden Verlagshäuser angegriffen, aber auch Behörden. Da nach der Verschlüsselung eine Lösegeldforderung (englisch: „Ransom“) gestellt wird, nennt sich diese Methode Ransomware.

Die Anzahl der Opfer sei im Berichtszeitraum erheblich gestiegen, erklärt das BSI. Aber auch die Höhe der gezahlten Lösegeldforderungen. Oft sehen angegriffene Unternehmen oder Institutionen keinen anderen Ausweg, als das Lösegeld zu zahlen. Davon raten Kriminologen aber ab: Denn die Zahlung eines Lösegelds garantiert keineswegs, dass die Daten danach wieder zur Verfügung stehen. Es erhöht er das Risiko – weil Zahlungsbereitschaft besteht –, erneut zum Ziel zu werden. Außerdem machen erst die Lösegeldzahlungen die Angriffe lukrativ. Würde keiner zahlen, gäbe es auch keine Angriffe.

[caption id="attachment_782483" align="alignnone" width="1030"]

Tricks zum Startmenü in Windows 11 22H2

Das nächste große Funktionsupdate von Windows 11 ist da: 22H2 bringt eine Menge Neuerungen mit sich. Viele davon nicht direkt ersichtlich, so wie die im Startmenü, die wir Euch heute zeigen.

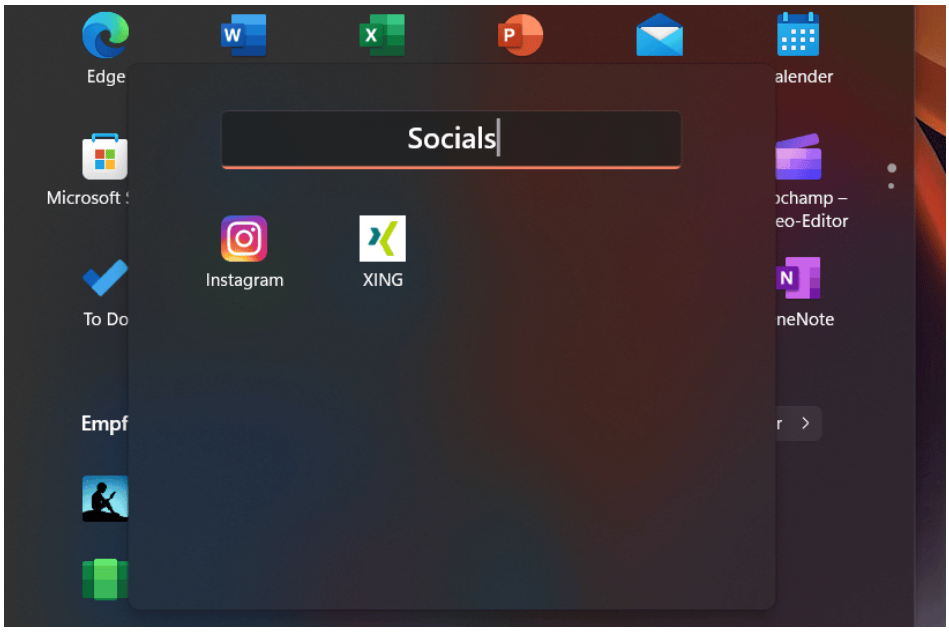
Aktualisieren der Apps/Symbole

Kennt Ihr die Situation? Ihr habt ein Programm/eine App hinzugefügt und findet sie nicht im Startmenü? Im Explorer würdet Ihr dafür **F5** oder **Aktualisieren** drücken. Die Funktion gab es bisher nicht. Mit 22H2 könnt Ihr eine Aktualisierung des Startmenüs erzwingen, indem Ihr mit der **rechten Maustaste** auf die Schaltfläche **Mehr>** oder **Alle Apps**> klicken und dann auf **Aktualisieren**.

Anlegen von Ordnern im Startmenü

Endlich: Von Windows 10 zu Windows 11 ist für viele Benutzer die wichtigste Möglichkeit verloren gegangen, Ordnung im Startmenü zu schaffen: Ordner. Zumindest konnte man das vermuten, so laut, wie die Reklamationen waren. Mit dem 22H2-Update ist diese Funktion wieder zurück - zumindest teilweise:

- Zieht in einem der Bereiche des Startmenüs ein App-Symbol auf ein anderes, dann legt Windows 11 einen Ordner an, in den beide Symbole bereits verschoben sind.
- Klickt auf das Ordnersymbol, dann auf den Namen, und Ihr könnt dem Ordner einen Namen geben.
- Das funktioniert allerdings leider (noch?) nicht in der Liste mit **Allen Apps**.
- Wie gewohnt könnt Ihr Apps aus dem Ordner ins Startmenü ziehen, um sie aus dem Ordner zu entfernen.



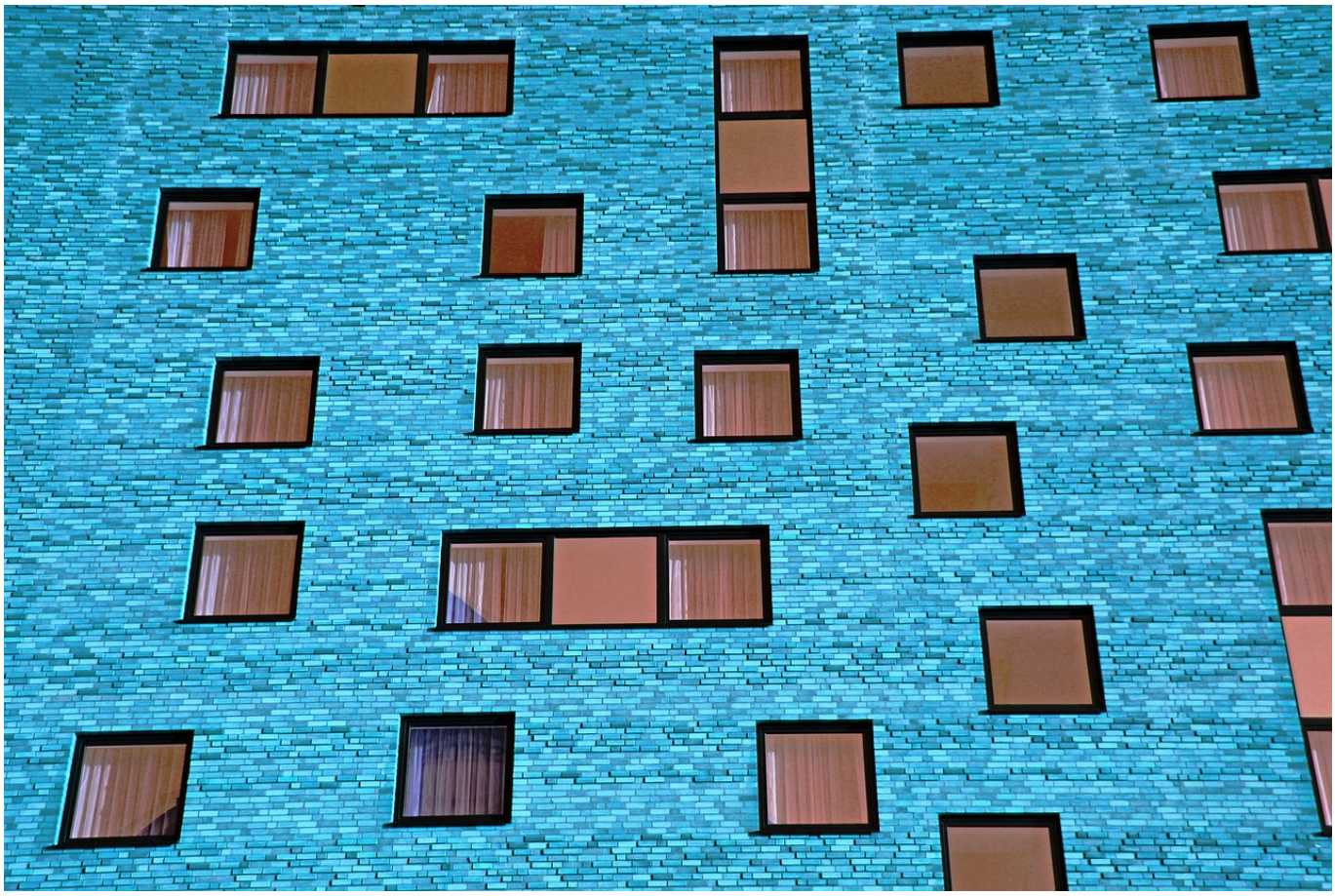
Unterschiedliche App-Dichte im Startmenü

Ihr kennt es vermutlich von Android und iOS: Bei den mobilen Betriebssystemen könnt Ihr die Dichte der Symbole im Startmenü verändern. Das war bisher nicht der Fall. Unter Windows 11 22H1 findet Ihr diese Funktion, indem Ihr mit der **rechten Maustaste** auf die Schaltfläche **Mehr>** oder **Alle Apps**> klickt und dann auf **Starteinstellungen**.

Mehr angeheftete Elemente verdichtet die Darstellung, allerdings nicht im Hinblick auf geringeren Symbolabstand, sondern indem mehr angeheftete Apps

pro Seite (und damit weniger Empfehlungen) angezeigt werden.

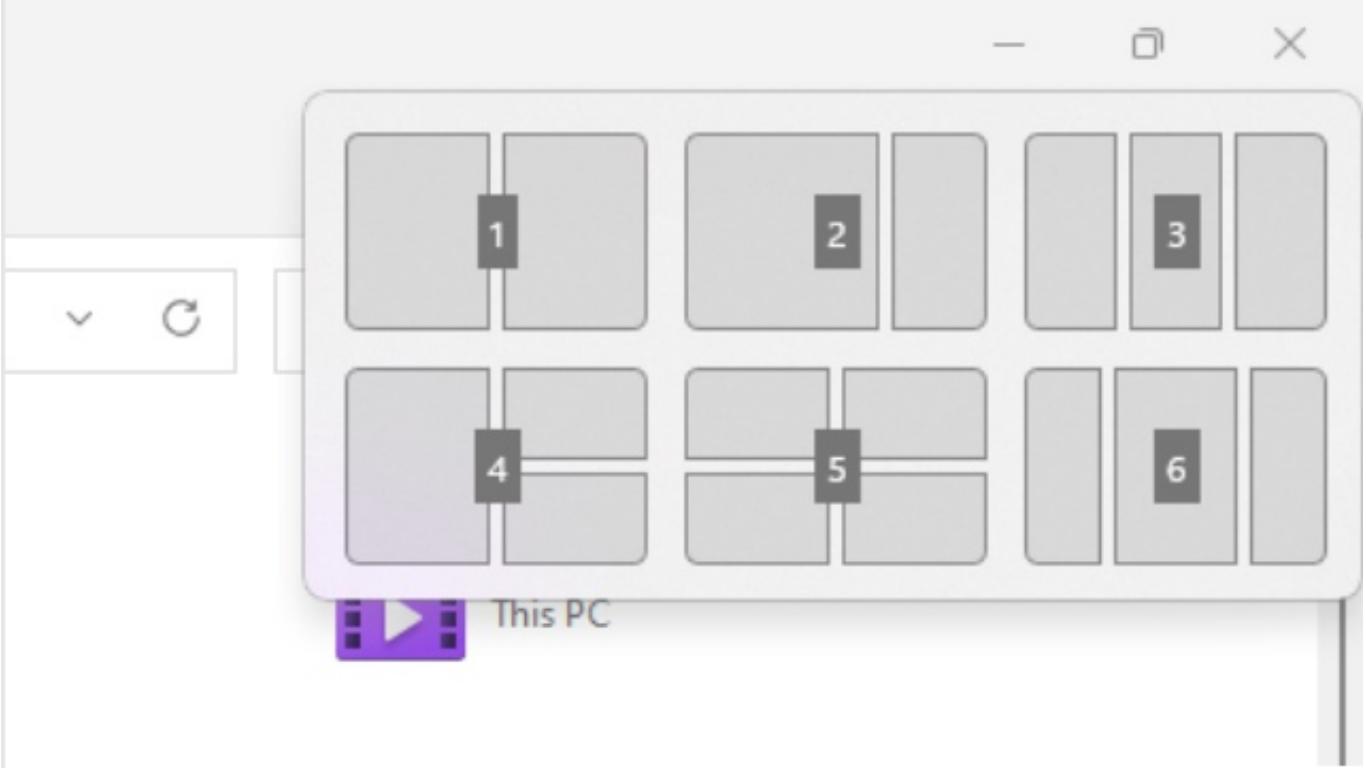
Neue Snap-Layouts in Windows 11 22H2



Je mehr Programme offen sind, desto mehr Fenster wollen verwaltet werden. Die Snap-Layouts von Windows 11 helfen dabei. Mit dem Funktionsupdate 22H2 ist die Funktionalität nochmal erweitert worden.

Auf dem stationären PC habt Ihr meistens mehr als einen Monitor, aber auch der reicht nicht, um alle Fenster sichtbar zu haben

Diese müsst Ihr einmal aktivieren, indem Ihr unter Einstellungen auf **System** > **Multitasking** > **Fenster andocken** die beiden Optionen mit **Snap-Layouts** im Text aktiviert.



- Um ein Fenster in ein solches Layout einzuordnen, bewegt den Mauszeiger im betroffenen Fenster auf die **Maximieren-Schaltfläche**.
- Windows 11 zeigt jetzt verschiedene Schablonen an, in die die Fenster eingeordnet werden können. Für jedes Element der Schablone zeigt das System eine Übersicht der offenen Fenster an. Klickt darin jeweils das Fenster an, das an diese Position und Größe geschoben werden soll.
- Nach Installation des 22H2-Updates könnt Ihr die Snap-Layouts deutlich komfortabler per Tastenkombination nutzen: Drückt dazu einfach **Windows** + **Z**, dann könnt Ihr über die Zifferntasten das gewünschte Layout aussuchen. Das geht schneller als der Weg über die Maximieren-Schaltfläche, wenn Ihr die Maus nicht gerade sowieso in der Hand habt.
- Alternativ könnt Ihr das Fenster auch in die Mitte des oberen Bildschirmrandes ziehen, dann zeigt Windows 11 Euch die Snap-Layouts an. Ihr könnt das Fenster/die aktuelle App in dem gewünschten Snap-Layout in die entsprechende Position ablegen.