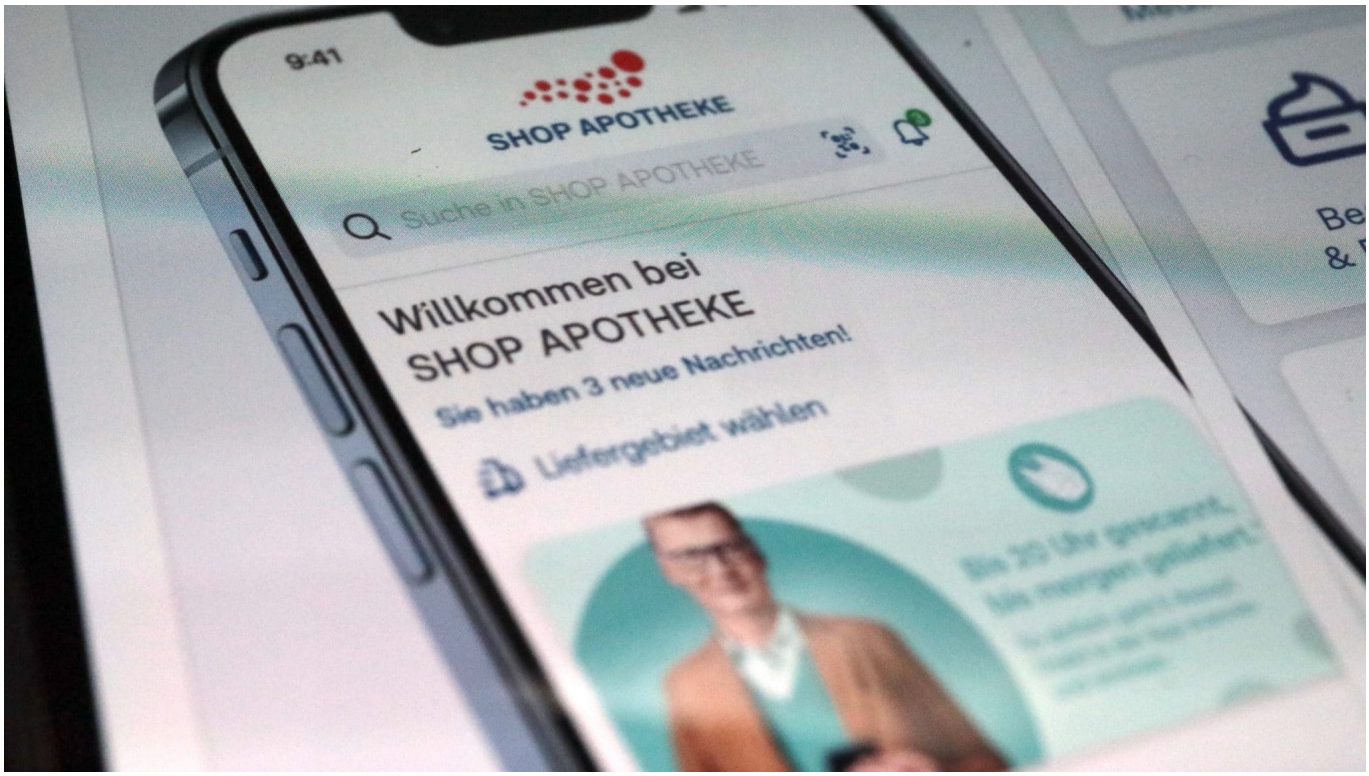
Schieb Report

Ausgabe 2023.24

Online-Apotheken: Günstiger, aber dafür auch langsamer



Viele Apotheken hatten dieser Tage als Zeichen des Protests geschlossen. Welche Rolle spielen Online-Apotheken bei der Versorgung? Online zu bestellen hat Vor- und Nachteile.

Vor rund 23 Jahren hat DocMorris den Anfang gemacht: Damals ist in den Niederlanden die erste virtuelle Apotheke gestartet, die ausschließlich online zu erreichen war. Heute gibt es in ganz Europa eine große Auswahl an Online-Apotheken, die rund um die Uhr Bestellungen entgegennehmen. Online bestellt – per Post oder Kurier gebracht.

Was vor 20 Jahren noch die Ausnahme war, machen heute immer mehr Menschen. Das gefällt vielen: Allein Branchenprimus DocMorris macht in Deutschland 783 Mio. EUR Umsatz pro Jahr. Die Zahl der Apotheken vor Ort nimmt gleichzeitig kontinuierlich ab – auch und vor allem auf dem Land. Eine Bestellung bei der Online-Apotheke des Vertrauens per Mausklick ist bequemer, als in den nächsten Ort zu fahren.

Die großen Online-Apotheken machen in Deutschland enorme Umsätze

Online-Apotheken: Vor allem auf dem Land eine Hilfe

Auf der einen Seite befördert der Trend zu mehr Online-Apotheken das Apothekensterben, auf der anderen Seite können sie aber das Problem gerade auf dem Land verringern, meint Jürgen Wasem, Professor für Medizinmanagement an der Universität Duisburg-Essen. „Online-Apotheken können gerade auf dem Land die Versorgung sichern, wir müssen sie daher stärken“, sagt der Fachmann dem WDR.

Längst können Kunden heute in einer Online-Apotheke nicht nur rezeptfreie Produkte und Waren bestellen (in der Branche „OTC“ genannt, für „Over the counter“), sondern auch gesetzlich besonders geschützte rezeptpflichtige Medikamente (in der Fachsprache „RX“ genannt). Bei rezeptpflichtigen Produkten müssen sich die Kunden in der Regel beim Portal registrieren und das Rezept abfotografieren oder scannen. Es gelten höhere Sicherheitsstandards.

Rezeptpflichtige und rezeptfreie Medikamente

In der Apotheke vor Ort gibt es Medikamente sofort (sofern verfügbar, seit Corona keine Selbstverständlichkeit mehr) – wer online bestellt, muss oft einige Tage

warten.

Doch gerade bei rezeptfreien Medikamenten, die Kunden aus eigener Tasche bezahlen müssen (etwa: Schmerzmittel, Verbandsmaterial, Vitaminpräparate, Pflegeprodukte), ist das Sparpotenzial beim Einkauf in Internet-Apotheken mitunter enorm. Stationäre Apotheken orientieren sich in der Regel an den unverbindlichen Preisempfehlungen der Hersteller (UVP) oder den offiziellen Apothekenverkaufspreisen (AVP), also den Preisen, zu denen sie Arzneimittel mit den gesetzlichen Krankenkassen abrechnen könnten, wenn sie verschrieben werden.

Da Online-Apotheken deutlich geringere Kosten für Personal, Miete oder Bevorratung haben, können sie insbesondere solche Produkte günstiger anbieten. Sie unterbieten die offiziellen Preise oft deutlich. Nicht selten lassen sich 30% und mehr sparen. Zudem werden Neukunden mit Extrarabatten, Treuepunkten und Gutscheinen geködert.

Enorme Preiseinsparungen von bis zu 50%

Das Verbrauchermagazin „IMTEST“ hat kürzlich untersucht, wie hoch das Sparpotenzial bei Internet-Apotheken tatsächlich ausfällt: Die Redakteure haben dazu einen Warenkorb mit 25 beliebten Medikamenten und

Gesundheitsprodukten zusammengestellt und die Preise mit der unverbindlichen Preisempfehlung verglichen. Das Ergebnis: Selbst die teuerste Online-Apotheke (in diesem Fall: Apodiscounter) war im Schnitt 18 Prozent günstiger. Bei einzelnen Produkten sind Rabatte von 50 Prozent und mehr möglich.

Aufgrund der gesetzlichen Preisbindung ist es Online-Apotheken in Deutschland nicht gestattet, für rezeptfreie Medikamente im Zusammenhang mit rezeptpflichtigen Arzneimitteln günstiger anzubieten. Seit Ende 2021 dürfen Versandapotheken gesetzlich Versicherten keine Rabatte mehr auf verschreibungspflichtige Arzneimittel gewähren – selbst, wenn diese Online-Apotheken im europäischen Ausland sitzen. Das sieht das Gesetz zur Stärkung der Präsenzapotheken vor.

Online lohnt sich keineswegs immer

Doch nicht immer lohnt es sich, online Medikamente zu bestellen. Wer sein Medikament dringend benötigt, ist bei der stationären Apotheke besser versorgt – erst recht, wenn es einer Beratung bedarf. Auch kommt es darauf an, wie viele Medikamente benötigt werden und was sie kosten. Viele Online-Apotheken bieten erst ab einem bestimmten Warenwert einen kostenlosen Versand an. Es sollte also vor einer Bestellung genau überprüft werden, ob sich überhaupt ein Spareffekt einstellt.

Außerdem empfiehlt sich ein Preisvergleich – denn bei Online-Apotheken gibt es mitunter enorme Preisunterschiede. Auch tagesaktuell.

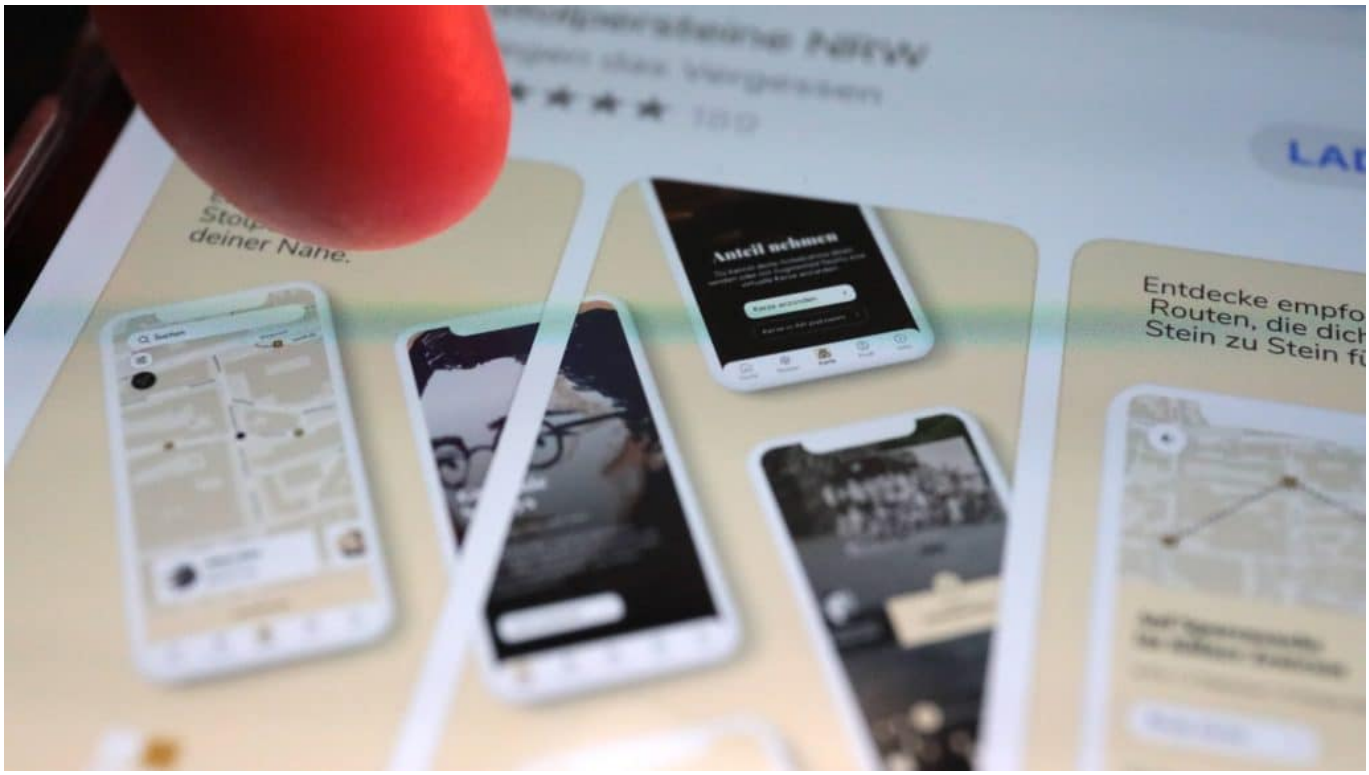
Grimme Online Award 2023: Die besten Onlineangebote des Jahres

Einmal im Jahr vergibt das Grimme-Institut den „Grimme Online Award“ für die besten deutschsprachigen Online-Angebote. Dieses Jahr wurden viele Podcasts nominiert.

Eine Besonderheit beim „Grimme Online Award“ (GOA): Die Preisträger wissen vorher nicht, ob und dass sie gewonnen haben. Das macht die Preisverleihung, die jedes Jahr in der „Flora“ in Köln stattfindet, für alle Nominierten zu einem besonders spannenden Ereignis. Insgesamt 28 Angebote waren nominiert.

Am Ende durften sich acht Angebote über eine Auszeichnung als beste deutschsprachige Online-Angebote des Jahres freuen: Die Jury hat insgesamt drei Preise in der Kategorie „Information“, drei Preise in der Kategorie „Wissen

und Bildung“ sowie zwei Auszeichnungen in der Kategorie „Kultur und Unterhaltung“ vergeben.

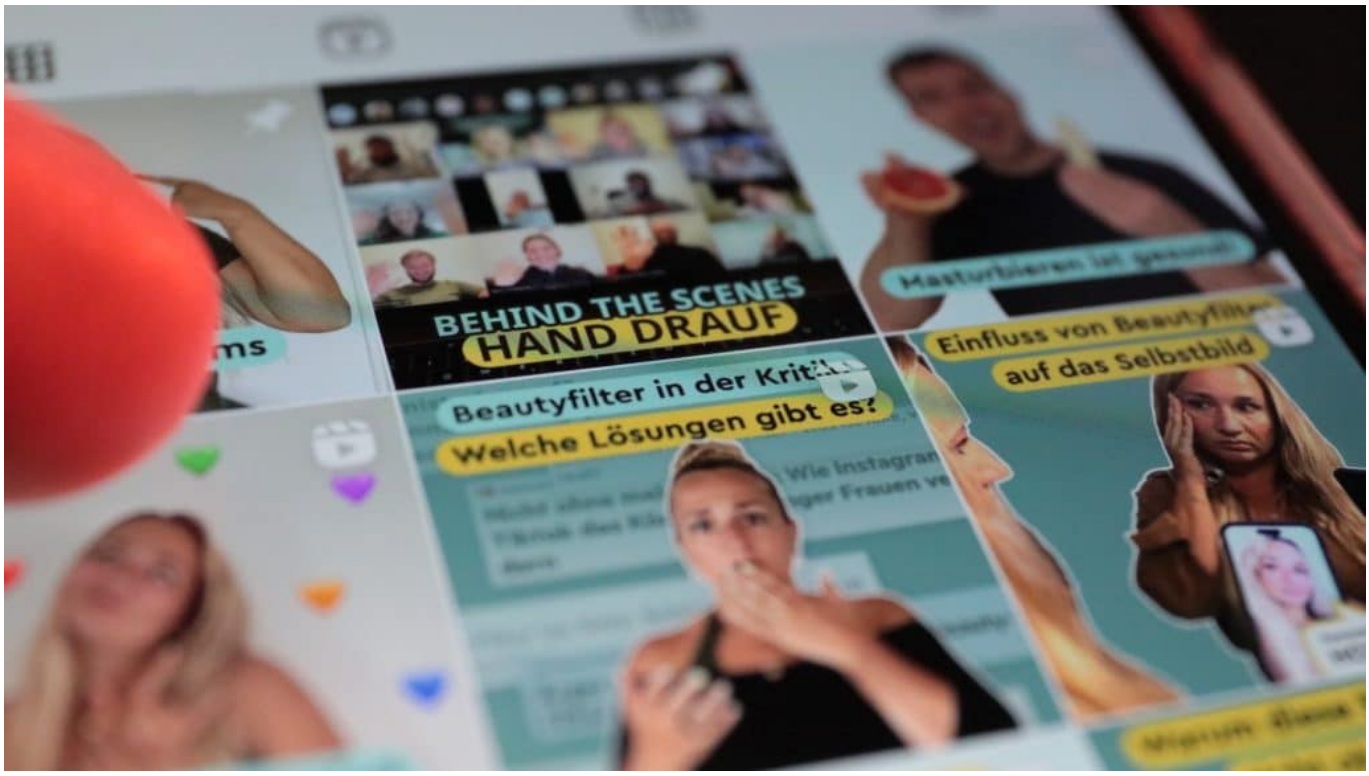


Die Stolpersteine App verwendet Augmented Reality, um Geschichte erfahrbar zu machen

Stolpersteine NRW

Ausgezeichnet in der Kategorie „Wissen und Bildung“ wurde „Stolpersteine NRW: Gegen das Vergessen“: Die Augmented-Reality-App erzählt multimedial die Geschichten von Menschen, die vom nationalsozialistischen Terror-Regime verfolgt wurden. App und Website zeigen auf einer interaktiven Karte alle rund 16.000 Stolpersteine, die vom Künstler Gunter Demnig in NRW verlegt wurden.

Tausende biografische Texte, Illustrationen, Hörspiele und historische Fotos geben Einblicke in die Lebensgeschichten, die sich hinter den Steinen verbergen. Für den Einsatz im Schulunterricht gibt es passende Begleitmaterialien, die Lehrende kostenlos nutzen können.



Gefällt mir: "Hand drauf" entführt in die Welt von Gehörlosen

Instagram-Kanal „Hand drauf“

Ebenfalls ausgezeichnet wurde „Hand drauf“, ein Instagram-Kanal des WDR für „funk“, dem Online-Angebot von ARD und ZDF für junge Menschen in Social-Media-Diensten wie Youtube oder Instagram. Hier werden in gebärdensprachlichen Videos (die ohne Ton auskommen) Themen aus und für die Community behandelt – und im Ergebnis eine Brücke zwischen Hörenden und Nichthörenden gebaut.

In Deutschland leben etwa 83.000 gehörlose Menschen. Der Schwerpunkt liegt dabei auf Themen, die Gehörlose betreffen, aber für alle interessant sind. Untertitel sorgen dafür, dass auch Hörende einbezogen werden – ganz inklusiv eben.

Angebote mit hohem Rechercheaufwand

Ganz gezielt ausgezeichnet hat die Jury dieses Jahr aber auch Angebote mit hohem Rechercheaufwand. Etwa „Teurer Wohnen“ von detector.fm, ein Podcast, der eine Auszeichnung in der Kategorie „Information“ erhalten hat. Sieben Folgen hörenswerter Podcast, das sich dem überregional relevanten Thema „teurer

Wohnraum“ widmet. Mit sehr persönlichen Eindrücken und Erfahrungen – aber auch einem kritischen Blick auf eine fehlgeleitete Politik.

Recherche-intensiv auch das Story-Telling-Angebot „Das Ende vom ewigen Eis“ vom Tagesanzeiger aus der Schweiz. Die Autoren machen in acht Kapiteln die Geschichte eines Gletschers in der Antarktis und die Arbeit der Forscher vor Ort erlebbar. Komplexe Sachverhalte werden anhand von Grafiken, Karten und Bildern erläutert.

Ein verdienter Grimme Online Award in die Kategorie „Wissen und Bildung“.

Afrikanische Geschichte auf TikTok

Über einen Grimme Online Award freuen durfte sich auch der Macher von „Dein Bruder Steve“: Ein TikTok-Format, das sehr persönlich ist und von einer Privatperson ganz allein gemacht wird: Afrikanische Geschichte, Hintergründe und Empowerment, das Ganze mit einer Prise Humor.

„Kompakter kann die Vermittlung aktueller Themen und historischer Zusammenhänge mit Fokus auf den afrikanischen Kontinent nicht sein“, meint die Jury. Stève Hiobi verleiht diesen oft vernachlässigten Themen mehr Sichtbarkeit, trotz des kanalspezifischen Kurzformats. Das Konzept verfängt: Der Macher

bekommt auf TikTok jede Menge Zuspruch in Form von Followern und Views.

Wissenschaft kommt beim Publikum an

Den Publikumspreis hat das Youtube-Format „Doktor Whatson“ erhalten: Auf dem vielseitigen und abwechslungsreichen Wissenschaftskanal präsentiert Decrik Engelt jeden Sonntag Videos, die den 300.000 Abonnenten gut recherchierte Themen aus Physik, Umwelt, Philosophie, Nachhaltigkeit und Technologie verständlich erklären.

Alle Gewinner bekommen eine Trophäe aus Glas mit dem Logo des Preis. Ein Preisgeld gibt’s nicht, der Grimme-Online-Preis ist undotiert. Aber dafür jede Menge Aufmerksamkeit – und die Gewissheit, zu den wirklich herausragenden Online-Angeboten des Jahres zu gehören.

Zum Nachschauen: Grimme Online Award 2023: Nominierungen [Grimme]

https://www.grimme-online-award.de/2023/nominierte

Der erste Hack: Eine Reise zurück in die Geschichte der digitalen Angriffe

Hackangriffe: Heute allgegenwärtig - und zunehmend bedrohlich. Aber wer hätte gedacht, dass der erste "Hack" im Jahr 1903 erfolgt ist?

Gefühlt gibt es das Internet schon immer. In Wirklichkeit natürlich nicht. Deshalb muss es auch einen ersten Hackangriff gegeben haben. Ich muss zugeben: Ich wusste selbst nicht, wann das gewesen sein soll.

Ein Magier war der erste Hacker

Nach allem, was wir wissen, geht in der Welt der Cybersicherheit der erste bekannte Hack auf das Jahr 1903 zurück. Täter war niemand Geringeres als der berühmte Magier und Erfinder Nevil Maskelyne.

Dieser Vorfall, auch bekannt als das **Hacken des Marconi-Systems**, markiert das Aufkommen eines Phänomens, das unsere digitale Welt bis heute prägt. Stellen Sie sich eine Welt ohne Firewalls, ohne Antivirussoftware und ohne

jegliches Bewusstsein für Cybersicherheit vor - genau das war die Szenerie des ersten bekannten Hackangriffs.

Ein Magier war offiziell der erste Hacker der Geschichte

Drahtlose Telegrafie ist auch ein Netz

Um zu verstehen, wie dieser Hack funktionierte, müssen wir uns zuerst mit der Technologie auseinandersetzen, die damals genutzt wurde: der drahtlosen Telegrafie, einem Vorläufer des Radios. Guglielmo Marconi, ein italienischer Erfinder, hatte eine Methode entwickelt, um Morsecode-Nachrichten drahtlos über große Entfernungen zu senden, ein Meilenstein der Kommunikationstechnologie seiner Zeit.

Marconi behauptete stolz, dass sein System völlig sicher und nicht zu knacken sei - eine Herausforderung, die Nevil Maskelyne nicht ablehnen konnte. Maskelyne, der Sohn eines berühmten englischen Zauberers und selbst ein versierter Erfinder, sah in Marconis Prahlerei eine Gelegenheit, seine eigenen Fähigkeiten unter Beweis zu stellen.

Oft stecken auch Hacker hinter einem Breach; Sie versuchen sich Zugang zu sensiblen Daten zu verschaffen

Funkstörer war erster Hack

Maskelynes Plan war einfach, aber genial: Er entwickelte einen "Funkstörer", der in der Lage war, die gleichen Frequenzen wie Marconis System zu verwenden. Er schlich sich in eine öffentliche Demonstration von Marconi ein und verwendete sein Gerät, um eine eigene Nachricht über Marconis System zu senden, bevor Marconi seine Demonstration starten konnte.

Die Nachricht, die er sendete, war nicht nur eine Demonstration seiner technischen Fähigkeiten, sondern auch eine satirische Ode an den griechischen Gott Hermes, den Schutzpatron der Diebe. Als Marconis Gerät diese Nachricht statt der erwarteten Demonstration ausgab, war das Publikum geschockt und Marconi blamiert.

Mit seinem Hack zeigte Maskelyne der Welt zwei wichtige Dinge. Erstens, dass kein System unknackbar ist - eine Lektion, die in der modernen Welt der

Cybersicherheit immer noch zentral ist. Und zweitens, dass Technologie immer auch ein Werkzeug sein kann, das in den falschen Händen Schaden anrichten kann.

Nicht komplex, aber effektiv

Dieser erste Hack war natürlich noch weit entfernt von den komplexen Cyberangriffen, die wir heute kennen. Es gab keine schädliche Software, keine Phishing-Angriffe und keine gestohlenen Kreditkarteninformationen. Aber in seiner Essenz war Maskelynes Hackangriff das Gleiche wie ein moderner Cyberangriff: das Ausnutzen von Schwachstellen in einem System, um unerlaubten Zugang zu erlangen und eine unerwünschte Nachricht zu senden.

Maskelynes Hack ist auch eine Erinnerung daran, dass Technologie nie in einem Vakuum existiert. Sie ist immer ein Spiegelbild der Gesellschaft, die sie hervorbringt, und sie kann sowohl für gute als auch für schlechte Zwecke genutzt werden. Wie wir mit den Herausforderungen umgehen, die sie uns stellt, liegt letztlich an uns.

Cyber-Security wird immer wichtiger

Seit dem Hack von Maskelyne hat sich die Welt der Cybersicherheit rasant weiterentwickelt. Wir haben Firewalls und Antivirenprogramme, Verschlüsselung und Zwei-Faktor-Authentifizierung, und doch finden Hacker immer wieder neue Wege, diese Barrieren zu überwinden.

In einer Welt, die zunehmend digitalisiert und vernetzt ist, ist die Erinnerung an den ersten Hack wichtiger denn je. Sie erinnert uns daran, dass es bei der Cybersicherheit nicht nur darum geht, neue Tools und Technologien zu entwickeln, sondern auch darum, ständig wachsam zu sein und die menschliche Dimension der Technologie nie aus den Augen zu verlieren.

Denn letztlich sind es nicht die Maschinen, die hacken - es sind Menschen. Und so wie Nevil Maskelyne im Jahr 1903 seine Fähigkeiten nutzte, um die Welt zu schockieren und zu erstaunen, so nutzen auch moderne Hacker ihre Fähigkeiten - ob zum Guten oder zum Schlechten hängt immer von der Person hinter dem Computer ab.

Roaming: Wenn die Datenverbindung aussetzt

Ihr seid mir Eurem Smartphone im Ausland unterwegs und wollt natürlich auch online gehen. Wenn dann trotz guter Netzversorgung die Daten nicht fließen wollen, ist guter Rat teuer. Wir zeigen Euch, was Ihr tun könnt.

Der Vertrag als Ursache

Früher war die Nutzung von Mobiltelefonen in einem anderen Land schwierig: Die Netzbetreiber warn nicht miteinander verbunden, jeder wollte seine eigene kleine Insel für sich haben und nicht kooperieren. Das hat sich mit zunehmender Mobilität und vor allem durch die Vorgaben der EU verändert.

Mittlerweile kann so gut wie jeder Vertrag im In- und Ausland mit nahezu gleichem Leistungsumfang eingesetzt werden. "So gut wie jeder", weil es Ausnahmen gibt:

- Manche Prepaid-Verträge sind ausgeschlossen und können nur in Deutschland bzw. dem Land des Anbieters genutzt werden.
- Die SIM-Karten von WLAN Hotspots sind generell nur für das Land des Anbieters zugelassen.

Wenn Ihr eine solche Karte verwendet, dann kontrolliert vorher, ob diese im Ausland aktiviert werden kann.

Das Roaming

Um im Ausland Eure Karte nutzen zu können, müsst Ihr das so genannte Roaming aktivieren. Das ist Eure Zustimmung, dass Ihr für alle eventuellen Kosten aufkommt.

Das könnt Ihr in iOS schnell ändern:

- Tippt in den Einstellungen auf **Mobiles Netz**, dann auf **Datenoptionen**.
- Schaltet dann die Option **Datenroaming** ein.
- Auf Grund der Vorgaben bekommt Ihr beim Einbuchen in ein fremdes Netz eine SMS vom Netzbetreiber. Diese enthält die Kosten für das Surfen, die Telefonie und Kurznachrichten in diesem Netz.

Auch bei Android müsst Ihr das Roaming einschalten, das geht ähnlich.

Das richtige Netz?

Wenn Ihr die beiden Dinge oben geprüft habt und die Datenverbindung trotzdem nicht funktioniert, dann ist das oft ein Problem des Netzes, in das Ihr gerade eingebucht seid. Im Ausland könnt Ihr - im Gegensatz zum Inland - frei zwischen den verfügbaren Netzen wechseln. Probiert hier einfach manuell ein anderes aus:

- Wechselt in die Einstellungen der Mobilfunkverbindung.
- Tippt auf den Netzbetreiber (wenn Ihr nur eine SIM-Karte im Gerät habt, ist das nur einer).
- Deaktiviert den Schalter bei **Automatisch**.
- Es dauert einen Moment, bis die verfügbaren Netzbetreiber angezeigt werden. Tippt auf den, mit dem Ihr Euer Smartphone verbinden wollt.
- Wechselt gegebenenfalls solange den Netzbetreiber, bis die Datenverbindung funktioniert.

Reddit-Blackout: Massiver Protestausfall hat begonnen

Reddit ist in den USA eine der populärsten Social-News-Websites und Foren. In Deutschland spielt Reddit bislang keine so große Rolle - doch es gibt aktuell große Proteste gegen den Anbieter wegen hoher Gebühren.

Eine riesige Protestaktion: Praktisch alle großen deutschsprachigen Subreddits sind alsaus Protest nicht mehr erreichbar. Wachsende Alternativen befinden sich im Fediverse, etwa Feddit.

Nahezu sämtliche großen deutschsprachigen Sub-Reddits sind in einer Protestaktion nun unzugänglich. Währenddessen wachsen Alternativen im Fediverse wie Feddit.

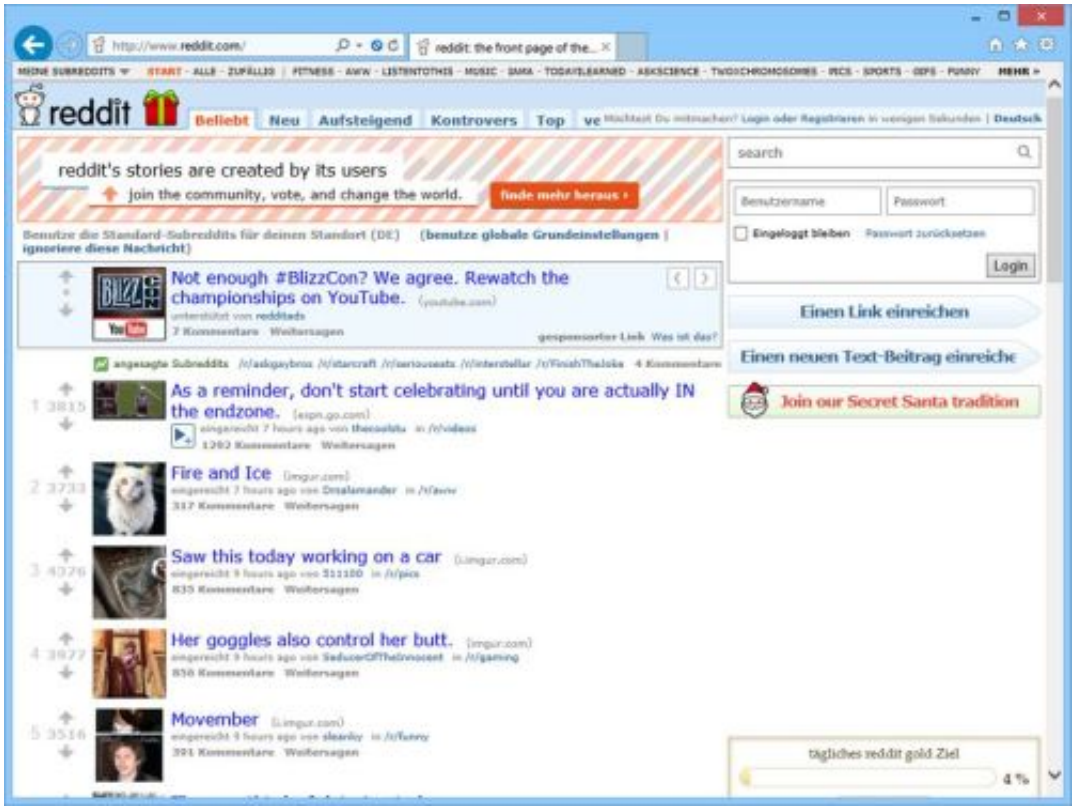
Über 7200 Sub-Reddits protestieren

Am heutigen 12. Juni sind Tausende Subreddits unerreichbar: Über 7200 Subreddits sind Teil einer Protestaktion, die sich gegen die neue API-Bepreisung von Reddit richtet. Diese Bewegung wird als Blackout bezeichnet.

Reddit plant, ab Juli die Kosten für API-Aufrufe so stark zu erhöhen, dass beliebte Third-Party-Apps, darunter Apollo, rif is fun, Sync und Relay, ihren Service einstellen müssen. Die meisten Subreddits haben sich für zwei Tage, also bis zum Ende des 13. Juni, auf den Privatmodus umgestellt, was jegliche Interaktion unmöglich macht.

Zu den beteiligten internationalen Großsubreddits gehören r/funny, r/aww, r/gaming, r/Music, r/Pics, r/science und r/todayilearned, die jeweils mehr als 30 Millionen Abonnenten haben. 00:02 / 00:16 Anzeige. Der redaktionelle Inhalt startet in 14 Sekunden Deutsches Reddit ist vollständig offline In Deutschland sind nahezu alle großen Subreddits Teil der Aktion, darunter r/de, dessen englischsprachige Variante r/German, r/finanzen, r/de_IAmA, r/ich_iel, r/tja, r/mauerstrassenwetten, r/arbeitsleben, r/kochen, r/OkBrudiMongo und r/de_EDV. Auch die Subreddits unserer Nachbarn wie r/austria und r/Switzerland sind dabei.

Einige Subreddits haben bereits angekündigt, im Privatmodus zu bleiben, bis Reddit der Community entgegenkommt – also ohne festgelegtes Ende. Dazu zählt r/videos mit über 20 Millionen Abonnenten.



Feddit&Co als Alternative?

Die Moderatoren der deutschen Subreddits behalten sich vor, den Protest über den 13. Juni hinaus zu verlängern. Je nach weiterem Verlauf der Situation können Reddit-Mitarbeiter die Kontrolle über Subreddits übernehmen und vollständige Moderatorenteams ersetzen. Dies ist jedoch in der Masse schwierig, da viele Subreddits von der Leidenschaft ihrer unbezahlten Moderatoren leben.

Feddit & Co. als Reddit-Alternativen Eine wachsende Alternative zu Reddit, die wie Mastodon auf das Fediverse setzt, ist Lemmy, ein Link-Aggregator, der Reddit ähnelt. Für deutschsprachige Nutzer gibt es die Instanz Feddit und tchncs, auf internationaler Ebene gibt es Lemmy.ml, Beehaw und kbin.social.

Aktuell kann es aufgrund des großen Ansturms zu Leistungsproblemen kommen. Lemmy teilt dabei das Schicksal von Mastodon, als zahlreiche Twitter-Nutzer wechselten: Aufgrund der föderierten Hosting-Struktur der Instanzen können die Serverkapazitäten gelegentlich ausfallen. Die Anzahl der Lemmy-Nutzer hat sich

im Juni bislang auf etwa 100.000 verdoppelt.

Über 10% aller Unternehmen von Hackangriffen betroffen

Eine aktuelle Studie fördert es zutage: Jedes zehnte Unternehmen war jüngst von Hackangriffen betroffen. Die restlichen 90% haben es vielleicht nicht bemerkt.

IT-Sicherheitsexperten machen gerne einen Witz: Es gibt nur zwei Arten von Unternehmen. Die einen, die schon mal gehackt wurden - und die anderen, die es noch nicht bemerkt haben.

Da ist leider etwas dran - und unter diesem Motto muss man wohl auch die jüngsten Erkenntnisse bewerten.

Demnach bedrohen Cyberattacken jedes zehnte deutsche Unternehmen. Neueste Daten zeigen, dass im letzten Jahr etwa 11% der deutschen Firmen von Hackern infiltriert wurden. Phishing und Ransomware sind dabei die am häufigsten verwendeten Angriffstechniken.

Oft stecken auch Hacker hinter einem Breach; Sie versuchen sich Zugang zu sensiblen Daten zu verschaffen

Jedes zehnte Unternehmen betroffen

Laut einer aktuellen Ipsos-Studie, die im Auftrag des TÜV-Verbands durchgeführt wurde, hat im letzten Jahr jedes zehnte deutsche Unternehmen einen IT-Sicherheitsvorfall erlebt. Für die Umfrage wurden etwa 500 Firmen mit mehr als zehn Mitarbeitern befragt. Die Ergebnisse zeigten, dass es zu rund 50.000 Cyberattacken, Sabotageaktionen oder Diebstählen von Hardware kam.

Seit Beginn des Konflikts in der Ukraine ist die Anzahl der Angriffe gestiegen. 16% der Firmen melden einen Anstieg von Cyberattacken oder -versuchen, während 58% die Gefahr solcher Angriffe als erhöht einschätzen. Phishing, bei dem

Passwörter durch Emails abgegriffen oder schädliche Software verbreitet wird, war die häufigste Methode, mit der Unternehmen angegriffen wurden.

Bei 62% der Firmen war ein solcher Angriff erfolgreich. Ransomware-Angriffe, bei denen die IT-Systeme gehackt und Firmen danach mit ihren verschlüsselten Daten erpresst werden, waren die zweithäufigste Methode und bei 29% der Firmen erfolgreich. Ebenfalls erfolgreich waren Cyberangriffe durch Manipulation von Mitarbeitern, auch bekannt als Social Engineering. Dabei werden beispielsweise falsche Anrufe vom IT-Support gemacht, um sensible Daten zu erlangen. In 26% der Fälle waren solche Angriffe erfolgreich. 22% der Unternehmen berichten von einem Passwortangriff, bei dem Zugangsdaten gestohlen wurden.

Hackangriffe gehören leider an die Tagesordnung

Finanzielle Verluste durch Hackangriffe

Diese Angriffe hatten gravierende Auswirkungen. Laut der Umfrage erlitten 42% der Firmen finanzielle Verluste, 38% konnten ihre Services für Mitarbeiter oder

Kunden (29%) nicht bereitstellen. In 13% der Fälle kam es zu Produktionsausfällen. Bei weiteren 13% wurden sensible Daten entwendet.

Unternehmen reagieren auf diese Cyberkriminalität mit erhöhten Investitionen. Etwa jedes zweite Unternehmen hat in den letzten zwei Jahren seine Ausgaben für Cybersecurity erhöht. Zudem ziehen 72% externe IT-Experten zu Rate und 51% der Unternehmen setzen auf Mitarbeitertraining.

Digitales Erbe: Wie umgehen mit Onlinekonten nach dem Ableben?

Wer seinen Nachkommen Zugangsdaten zu Onlinekonten hinterlassen möchte, sollte Password Manager verwenden: Sie sind die einfachste und praktische Methode, diese Herausforderung zu meistern.

Irgendwie läuft immer mehr digital. Shoppen. Tickets buchen. Oder das Ferienhaus. Getränke bestellen. Kommunikation. Bankgeschäfte, Konto, Aktiendepot. Alles in der Regel gut abgesichert mit Zugangsdaten, Passwörter, geheimen Schlüsseln. Nur Behördengänge sind noch nicht digital, aber das ist ein anderes Thema. Am Freitag ist „Digitaltag“ in Deutschland. Mit vielen Aktionen, auch vor Ort, um uns alle fit(er) zu machen im Umgang mit Digitalisierung.

Und wir wollen heute mal über das „Dititale Erbe“ sprechen. Damit ist gemeint: Wie schaffe ich es, meinen Verwandten oder Nachfahren nach meinem Ableben die Zugangsdaten zu allen wichtigen Onlinediensten zu übergeben?

Passwörter sollten kontrolliert übergeben werden

Experten empfehlen Papierlisten - wenig praktikabel

Früher war da einfach: Einen Brief in die Schublade oder in den Tresor – zusammen vielleicht noch mit einem Schlüssel. Das war's. Heute ist es aber komplizierter mit all den Accounts und Passwörtern...

Das ist ja schon zu Lebzeiten für einen selbst schwierig, sich alles zu merken. Denn wir wissen ja: Es wird dringend empfohlen, für jedes Onlinekonto ein anderes Passwort zu benutzen. Damit Hacker, wenn ihnen die Zugangsdaten für ein Konto in die Hände fallen, nicht gleich überall rein können, um sich zu bedienen. Wenn man das macht, ist das gut – aber für Nachfahren natürlich schwierig.

Denn man kann ja eben nicht sagen: Mein Passwort lautet „Balinesischer Sonnenuntergang" – und das war's. Nein, man muss die Zugangsdaten zu allen wichtigen Konten notieren und weitergeben. Zu den Bankkonten bekommt man im Zweifel noch auf normalem bürokratischen Weg Zugriff, nicht aber auf Facebook,

Twitter, Bitcoin Konto oder all die anderen Konten, die man heute so hat. Da muss man wohl oder übel eine Aufstellung machen.

Password Manager bieten Komfort

Eine Liste auf Papier, auf der alles notiert wird – ist das denn noch zeitgemäß?

Eine berechtigte Frage. Die Verbraucherzentralen empfehlen diese Vorgehensweise teilweise noch: Benutzername und Passwort aufschreiben, ausdrucken und an einem sicheren Ort verwahren. In Wahrheit ändern wir aber unser Passwort gelegentlich, etwa, wenn wir gewarnt werden, das sei nicht mehr sicher. Dann müsste man streng genommen jedes Mal seine Papierliste auf den neuesten Stand bringen und ersetzen. Wirklich unpraktikabel.

Da ist eine geheime Datei auf der Festplatte oder in einem Online-Laufwerk, natürlich verschlüsselt und mit Passwort gesichert, schon eine bessere Idee. Aber auch diese Übersicht müsste man immer auf dem neuesten Stand halten – das geht und ist einfacher als auf Papier, aber auch mühselig. Viel einfacher ist es, einen Passwort Manager zu benutzen – das hilft einem sowieso, seine Zugangsdaten optimal zu verwalten und zu organisieren.

Zugang zum Passwort Manager

Aber wie kommen Verwandte dann an die Daten im Passwort Manager dran?

Die guten Passwort Manager wie Lastpass, 1Password, Dashlane oder Keepass. Letzteres ist sogar kostenlos. Solche Passwort Manager haben alle ein Master Passwort: Wer das kennt, kann dann auf alle anderen zugreifen, sie einsehen und benutzen. Einige der Passwort Manager bieten sogar die Möglichkeit, gespeicherte Passwörter zu teilen. Entweder einzelne oder alle – etwa mit Verwandten.

Einige wie Dashlane sehen sogar explizit eine Funktion für den digitalen Nachlass vor: Da trägt an einen Verwandten oder eine Vertrauensperson ein, die im Fall der Fälle dann auf alle Daten und Passwörter zugreifen kann. Es reicht, das zu notieren und/oder in der Software einzutragen.

Da sich in solchen Passwort-Managern oft auch noch andere Daten eintragen lassen, zum Beispiel Dokumente oder Bankdaten, kann man auf diese Weise auch darauf bequem Zugriff gewähren. Nach meiner Einschätzung sind Passwort Manager die eleganteste Lösung, damit Hinterbliebene im Todesfall auf die Onlinekonten zugreifen können. Aber das ist eben eine Lösung, die einem immer etwas bringt – auch jetzt schon. Wer Passwort Manager benutzt, hat überall sichere Passwörter und ist generell besser geschützt.

Abmelden bei Facebook, Twitter und Co.

Eine Aufgabe übernehmen Passwort-Manager aber nicht: Eine Abmeldung bei Facebook, Twitter und Co.

Prinzipiell ist es so, dass Erben nicht nur materielle Güter erben, sondern auch digitale. Sie haben also erst mal Zugriff auf die Konten und auch Anspruch auf digitale Güter.

Etwa Guthaben, digitale Kunstwerke etc. Die meisten großen Sozialem Netzwerke wie Facebook, Twitter, Instagram und Co. haben festgelegte Abläufe, wie im Fall eines Todes vorzugehen ist: In der Regel muss die Sterbeurkunde oder ein anderes Dokument vorgelegt werden, dann kann ein Konto geschlossen oder gelöscht werden. Das ist ein manueller Verwaltungsakt, dafür gibt es in der Regel keine Funktionen, die man einfach so online ansteuern kann – und es dauert auch ein wenig. Twitter zum Beispiel erwartet ein notariell beglaubigtes Dokument.

Dropbox und Google Drive: Verknüpfungen statt Dateien

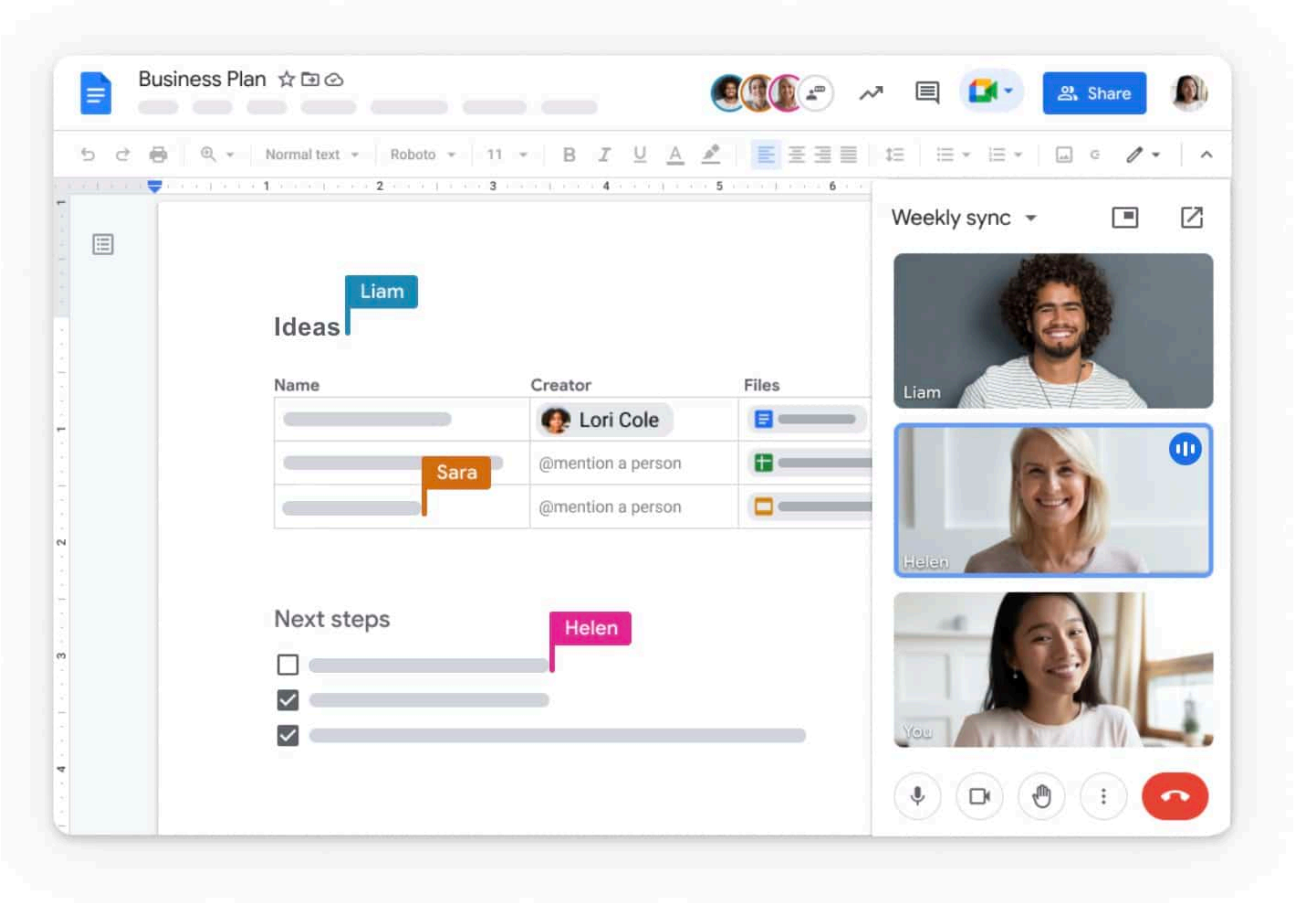
Cloudspeicher sind toll, weil sie Platz auf Euren Geräten frei machen und stattdessen die Speicherkapazitäten der Anbieter nutzen. Das hat allerdings auch seine Grenzen: Auch die Cloudanbieter haben nur limitierte Kapazitäten. Dropbox löst das jetzt elegant.

Google Drive und Dropbox

Cloud-Anbieter nutzen alle ihren eigenen Speicher, aber in manchen Fällen bieten diese auch eigene Office-Pakete an, so beispielsweise Google. Die zugehörigen Dateien sind eindeutig Google zuordenbar, können aber natürlich auch lokal gespeichert werden oder auf einem anderen Cloudspeicher abgelegt werden.

- Eigentlich sollten Google-Dokumente auf dem zugehörigen Google Drive liegen. Schließlich hat jeder, der das Google Office nutzt, logischerweise auch ein Google Konto und damit ein Google Drive als Cloudspeicher.
- Wenn Ihr Dropbox als primären Cloudspeicher nutzt, dann liegen gegebenenfalls viele Google-Dokumente stattdessen in der Dropbox und nehemn dort Speicher weg.
- Effizienter wäre es, diese stattdessen in Google liegen zu haben und nur

eine Verknüpfung in der Dropbox vorzuhalten. Die nimmt kaum Platz weg, Ihr könnt aber trotzdem alles über die Dropbox machen.

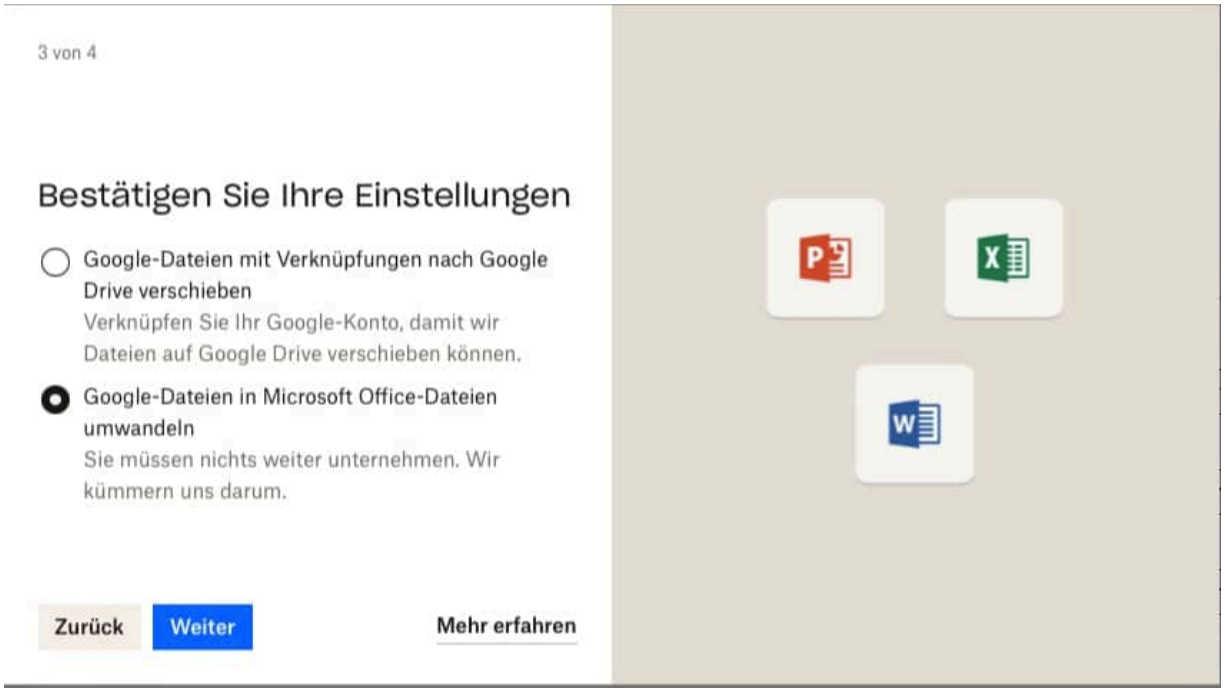


Migration von Google-Dokumenten zurück

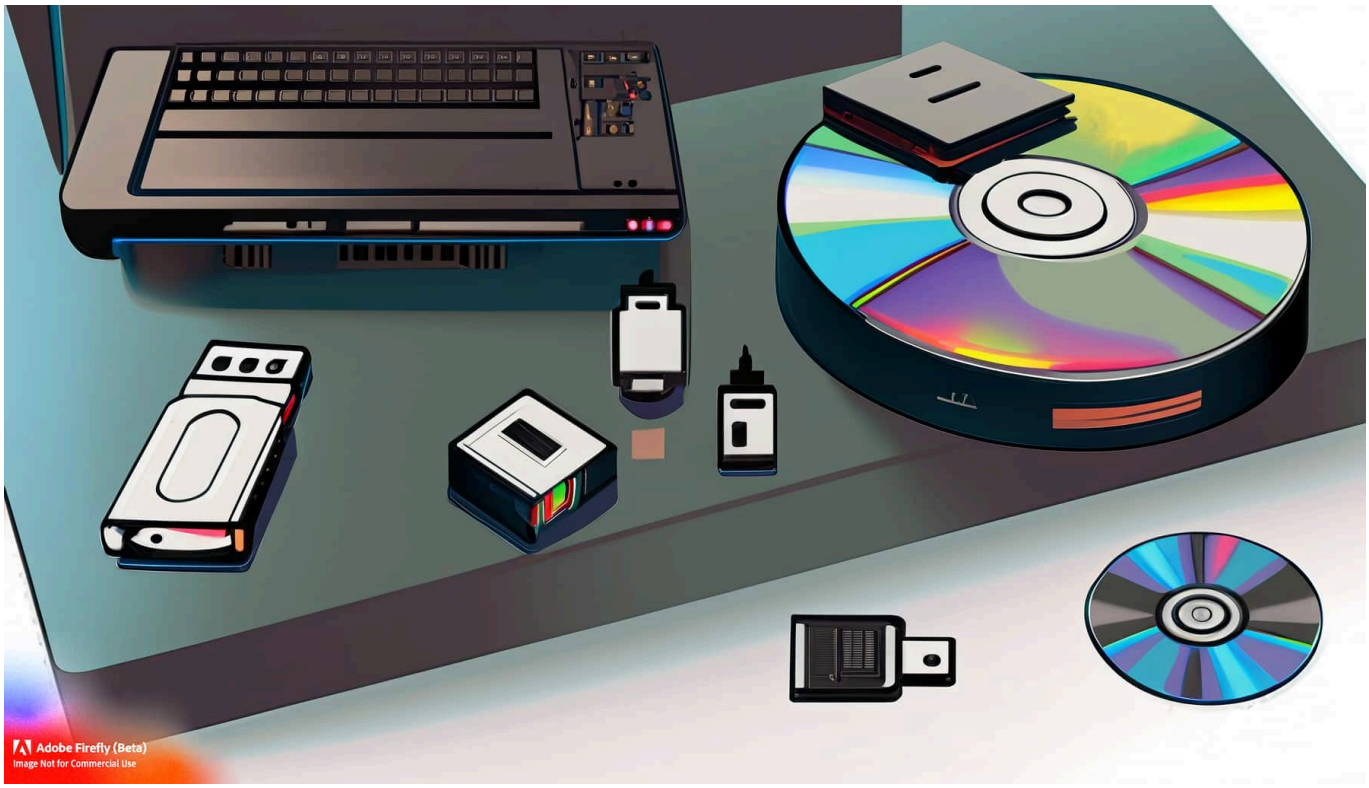
Dropbox informiert seine Benutzer proaktiv, dass eine Migration ihrer Google-Dateien aus der Dropbox nach Google möglich ist. Wenn Ihr die nicht bekommt, dann klickt auf diesen Link.

- Bestätigt die Meldungen von Dropbox, die Euch über das Verfahren informieren.
- Wählt aus, ob Ihr eine Verknüpfung mit Eurem Google Drive erzeigen wollt oder die Dateien in MS Office-Dateien umwandeln wollt (die dann auf der Dropbox gespeichert bleiben).
- Wenn Ihr das Verschieben auf das Google Drive auswählt, dann müsst Ihr Euch im nächsten Schritt mit Eurem Google-Konto anmelden und den Zugriff erlauben.
- Dropbox verschiebt die Dateien dann automatisch nach Google und legt

an der Stelle der Originaldatei in Dropbox eine Verknüpfung dazu an.
- Die Verknüpfung könnt Ihr anklicken und die Datei damit öffnen, als wäre sie noch auf der Dropbox gespeichert.



Datenspeichereinheiten: Byte, Kilobyte, Megabyte, Gigabyte, Terabyte und mehr!



Es gibt viele Abkürzungen für Speichermengen. Aber was genau sind eigentlich KB, MB und GB? Ein Überblick.

Willkommen, liebe Technik-Enthusiasten und alle, die an der digitalen Welt Interesse haben. Heute tauchen wir in das weite Meer der Speichereinheiten ein. Sie denken vielleicht, dass "Byte" und seine Ableitungen trockene Begriffe sind, die ausschließlich für Programmierer und IT-Fachleute bestimmt sind, aber lassen Sie sich von mir erzählen, es gibt viel mehr zu entdecken.

Das Byte: Die kleinste Einheit

Wir beginnen mit dem Byte, der grundlegenden Einheit des digitalen Speichers. Aber warum heißt es "Byte"? Der Begriff Byte leitet sich vom englischen "bite" (Biss) ab, jedoch wurde das "i" zu "y" geändert, um eine Verwechslung mit "bit" zu vermeiden. Ein Byte besteht aus acht Bits. Und was ist ein Bit? Es ist die grundlegendste Einheit in der Informatik und kann einen von zwei Zuständen

repräsentieren - 0 oder 1.

Ein einzelnes Byte kann 256 unterschiedliche Werte (von 0 bis 255) darstellen, was ausreicht, um ein einzelnes Zeichen in einem Text, wie einen Buchstaben oder eine Zahl, zu speichern. Ja, genau, dieses kleine "a" auf Ihrem Bildschirm benötigt nur ein Byte!

Das Kilobyte: Der nächste Schritt

Wenn Sie dachten, ein Byte wäre klein, dann lassen Sie uns zum Kilobyte (KB) aufsteigen. Ein Kilobyte entspricht 1.024 Bytes. Aber warten Sie, warum 1.024 und nicht 1.000? Das liegt daran, dass Computer in der Binärsprache funktionieren, die auf Potenzen von 2 basiert, und 1.024 ist eine Potenz von 2 (genau gesagt 2^10).

Ein Kilobyte ist in etwa so viel Speicher, wie Sie für einen kurzen Absatz an Text benötigen. Wenn Sie also das nächste Mal einen Text in Ihre Notizen-App eingeben, denken Sie daran, dass jeder dieser Absätze etwa ein Kilobyte Ihres Speichers belegt.

Das Megabyte: Wo wir ins Große kommen

Ein Megabyte (MB) entspricht 1.024 Kilobytes. In dieser Größenordnung beginnen wir, Dinge wie Bilder und Musikdateien zu speichern. Ein durchschnittliches Foto, das mit einem Smartphone aufgenommen wird, kann etwa 2-5 MB groß sein, während ein einminütiges MP3-Lied etwa 1 MB Speicherplatz benötigt.

Das Gigabyte: Der digitale Spielplatz

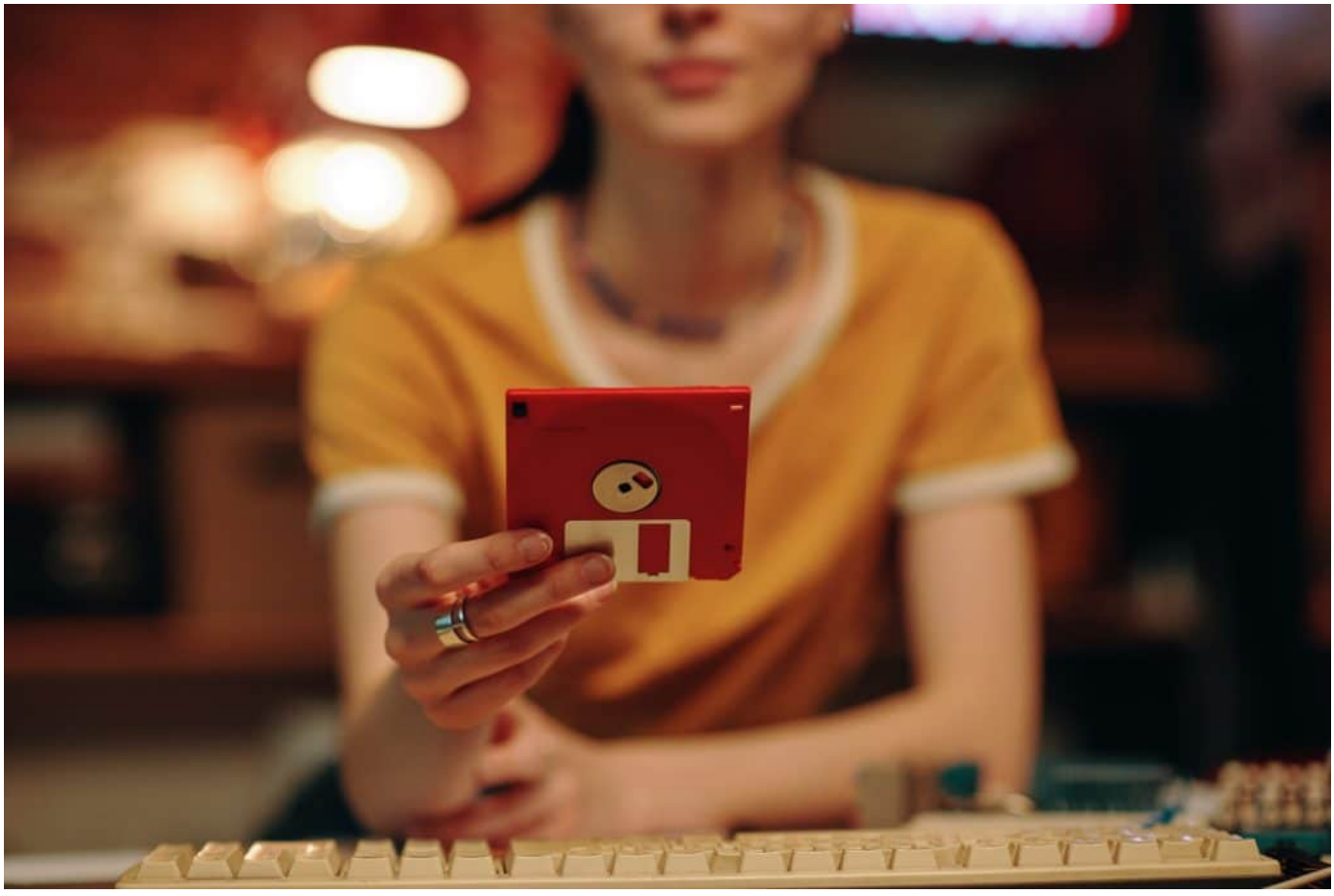
Ein Gigabyte (GB) entspricht 1.024 Megabytes und ist eine sehr gängige Einheit

für den Speicher in unseren Geräten heute. Ihr Smartphone könnte einen Speicher von 64 GB oder 128 GB haben, und ein typischer Laptop könnte einen Speicher von 256 GB oder 512 GB haben.

Ein GB ist genug, um einen HD-Film oder mehrere hundert Musikstücke zu speichern. Wenn Sie beispielsweise einen Film bei Netflix streamen, verbrauchen Sie je nach Qualität zwischen 1 und 3 GB pro Stunde.

Das Terabyte: Die Speicherriesen

Ein Terabyte (TB) entspricht 1.024 Gigabytes. Jetzt sprechen wir von ernsthaften Speichermengen! Viele Desktop-PCs und einige High-End-Laptops verfügen heute über Terabyte-Festplatten. Ein TB könnte ungefähr 250.000 MP3-Dateien oder etwa 300 Stunden HD-Video aufnehmen.



Floppy Disk

Und darüber hinaus

Aber warum aufhören bei Terabyte? Es gibt noch Petabyte (1.024 TB), Exabyte (1.024 PB), Zettabyte (1.024 EB) und Yottabyte (1.024 ZB), die in der Regel für die Speicherung von großen Datenmengen in Cloud-Netzwerken oder für das Verständnis der Big Data-Welt verwendet werden.

Um ein Gefühl dafür zu bekommen, wie groß diese Einheiten sind: Wenn Sie jeden Tag 1 Terabyte Daten speichern würden, würden Sie 1 Petabyte in etwa 1.000 Jahren erreichen und 1 Exabyte in etwa 1.000.000 Jahren!

Fazit

Wir leben in einer Ära, in der die Menge an generierten Daten exponentiell wächst. Es ist faszinierend zu sehen, wie wir ständig neue Wege finden, diese Daten effizient zu speichern und zu nutzen. Bei all den rasanten technologischen Fortschritten gibt es eines, das sicher ist: Unser Bedarf an immer größeren Speichereinheiten wird nicht so schnell abnehmen. Also, bis wir uns wiedersehen, behalten Sie Ihren Speicher im Auge und vergessen Sie nicht, ab und zu ein Byte zu nehmen!

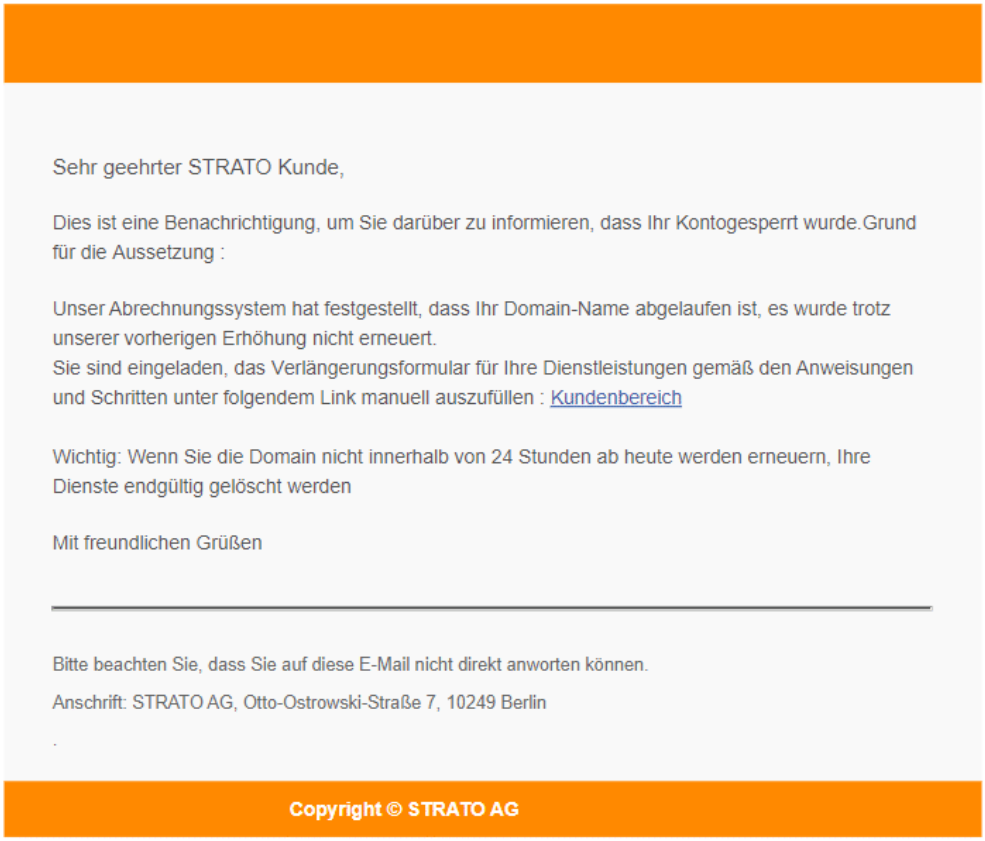
Phishing: Wenn der Hoster (angeblich) Domains sperrt

Ihr habt eine Internetseite? Dann wollt Ihr der Welt vermutlich Inhalte zur Verfügung stellen. Wenn die Webseite gesperrt wurde, dann geht das nicht mehr. Da ist Eile geboten. Aber auch Vorsicht!

Domains als Wegweiser im Internet

Die Domain (oder Internetadresse) ist die Verknüpfung zwischen der Welt und Euren Inhalten. Wenn ein Besucher diese in seinen Browser eingibt, dann wird dieser an Euren Hoster, also den Anbieter eures Webspaces.

Der Hoster leitet die Anfrage dann auf Eure Inhalte weiter. Und genau das ist ein Flaschenhals: Wenn der Hoster diese Weiterleitung sperrt, dann bekommt der Besucher statt Eurer Inhalte nur eine Fehlermeldung. Je nach der Wichtigkeit Eurer Inhalte schafft das schnell Panik: Geschäft geht verloren, Kunden und Besucher wandern ab, das wollt ihr nicht und lasst euch zu einer schnellen Reaktion verleiten. Das machen sich Phishing-Angreifer zu Nutze:



Sehr geehrter STRATO Kunde,

Dies ist eine Benachrichtigung, um Sie darüber zu informieren, dass Ihr Kontogesperrt wurde.Grund für die Aussetzung :

Unser Abrechnungssystem hat festgestellt, dass Ihr Domain-Name abgelaufen ist, es wurde trotz unserer vorherigen Erhöhung nicht erneuert.
Sie sind eingeladen, das Verlängerungsformular für Ihre Dienstleistungen gemäß den Anweisungen und Schritten unter folgendem Link manuell auszufüllen : Kundenbereich

Wichtig: Wenn Sie die Domain nicht innerhalb von 24 Stunden ab heute werden erneuern, Ihre Dienste endgültig gelöscht werden

Mit freundlichen Grüßen

Bitte beachten Sie, dass Sie auf diese E-Mail nicht direkt anworten können.

Anschrift: STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin

.

Copyright © STRATO AG

Die Phishing-Masche

Ihr bekommt eine E-Mail, in Ihr mitgeteilt bekommt, dass Eure Internetseite gesperrt ist. Weil es Unregelmäßigkeiten mit der Zahlung gab, weil eine notwendige Verifizierung nicht durchgeführt wurde, die Gründe sind vielfältig. Die E-Mail sieht erst einmal legitim aus, weil die Phisher die Domain verwenden, die auch zu Eurer E-Mail-Adresse gehört. Folgt Ihr dem Link, dann landet Ihr auf einem Fake-Portal, in dem Ihr Eure Zugangsdaten zur Konfigurationsoberfläche eingeben sollt. Die dann natürlich kompromittiert sind und eine Übernahme Eurer Webseite erlauben. Um das zu vermeiden, solltet Ihr folgende Schritte durchführen, statt auf die Links in der E-Mail zu klicken:

- Der erste Schritt ist eine Prüfung: Ist der angebliche Absender tatsächlich der Hoster Eurer Webseite?
- Wenn das der Fall ist, dann ruft als erstes Eure Webseite auf. Wenn die normal erreichbar ist, dann ist das ein Hinweis darauf, dass es sich um eine Phishing-Aktion handelt.
- Um sicher zu sein, geht manuell (NICHT über den Link in der E-Mail!) auf die Konfigurationsoberfläche Eurer Webseite. Sollte tatsächlich eine Sperrung oder ein anderes Problem bestehen, dann bekommt Ihr das da

angezeigt.