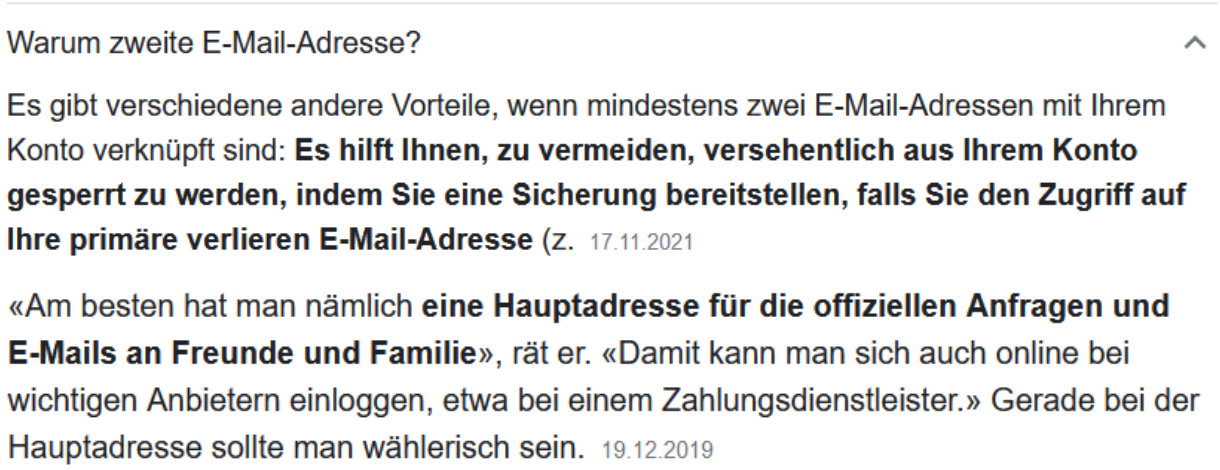
DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Gründe für eine zweite Email-Adresse



Nur eine E-Mail-Adresse zu haben, ist OK für ein persönliches Konto. Aber wenn es um die Arbeit geht, fühlt man sich schnell mal von mehr E-Mails überflutet als man verwalten kann. Du bist Jungunternehmer und fragst dich, ob verschiedene E-Mail-Konten dein Leben erleichtern würden? Die Antwort ist ja!

Unterschiedliche E-Mail-Konten ermöglichen es, verschiedene Geschäftsbereiche und Informationsflüsse in Gruppen zu organisieren. So schaffst du Möglichkeiten für eine bessere Zusammenarbeit mit den Kollegen und schützt dich und dein Unternehmen vor Spam-Praktiken und potenziellen Bedrohungen.

Angenommen du hast eine eigene E-Mail-Domain (falls nicht, kannst du diese schnell bei Gmail für Unternehmen mit der G Suite einrichten und für die gleiche Domain bezahlen, um in dein Google Mail-Konto aufgenommen zu werden). Hier sind 9 Gründe warum du mehrerer E-Mail-Konten für dein Unternehmen benutzen solltest, und einige Ideen für professionelle E-Mail-Adressen.

1. Du willst professionell auftreten

Das Wichtigste zuerst: du solltest eine “professionell” klingende Email haben. Wenn du immer noch eine E-Mail-Adresse aus der Steinzeit des Internets, wie ¨drdracula@funnymail.com¨ hast, wird es Zeit für ein Update. Dabei brauchst du nicht super kreativ zu werden – für den Anfang sind Vor-und Nachname mehr als genug. Wenn du einen komplizierten Nachnamen hast, nimm einfach nur den Vornamen. Um so besser wenn du deine eigene Domain hast – dann wird der Name auch nicht vergeben sein.

Beispiel

- Vorname.Nachname@deinedomain.de
- Vorname@deinedomain.de

2. Du willst anonym bleiben

Während eine ¨Vorname.Nachname¨ E-Mail-Adresse für die tägliche Kommunikation funktioniert, möchtest du dich nicht immer in der Öffentlichkeit identifizieren. Wenn du Teil eines Online-Forums bist, einen Blog Beitrag schreibst oder Artikel kommentierst, würdest du dich vermutlich freier unter Verwendung einer Pseudonym-Adresse ausdrücken können (aber vielleicht trotzdem nicht ¨drdracula¨).

Beispiel:

- community@deinedomain.de

3. Du willst Spam vermeiden

Möchtest du dich für einen Service registrieren, aber auf die Zusendung von nervigen Werbe-Mails verzichten? Dann melde dich mit einer anderen E-Mail-Adresse an als die deines Haupt-Accounts. Deinen ¨Spam-Account¨ kannst du dann in deiner Freizeit durchschauen.

Beispiel:

- inbox@deinedomain.de

4. Du willst E-Mail Kampagnen verschicken

Wenn wir gerade von Spam sprechen, wenn du deinen eigenen Spam (natürlich nur Spaß) in einer E-Mail-Marketing Kampagne mit Hilfe einer Software wie SendinBlue oder ActiveCampaign planst, willst du zum Verschicken vielleicht eine andere E-Mail-Adresse als deine eigene verwenden. Dadurch wird dein Posteingang nicht mit Antworten überflutet. Abhängig von der Art deiner Kampagne (Vertrieb, Marketing, etc.) kannst du eine allgemeine E-Mail-Adresse verwenden.

Beispiel:

- marketing@deinedomain.de

5. Du willst öffentlich kommentieren

Datenschutz wird immer wichtiger und somit auch die Verteilung deiner Daten. Getrennte Accounts für verschiedene Bereiche wie den Online-Einkauf und soziale Webseiten zu haben (welche mehr anfällig für Attacken sind), wird deinen Haupt-Account weniger angreifbar machen. Im gleichen Zug solltest du sicherstellen, dass deine verwendeten Passwörter verschieden und jeweils stark sind.

6. Du nutzt Zugang übers Handy

Wenn du einen E-Mail-Service nutzt, der nur am Desktop zugänglich ist, könntest du weiterhin einen webbasierten Service in Anspruch nehmen, um auch von unterwegs aus Zugang zu Mails zu haben. Du kannst ebenfalls Regeln festlegen, um E-Mails von deinem Desktop-basierten Account auf einen separaten webbasierten Account weiterzuleiten.

7. Du willst mehrere Personen zugleich kontaktieren

Arbeitest du in verschiedenen Teams, Projekten oder Bewerbungen, bekommst du Unmengen von Informationen von unterschiedlichen Quellen zugeschickt. Es macht Sinn, separate E-Mail-Adressen für diese konkreten Workflows zu eröffnen; nicht nur die Verwaltung deiner Kommunikationskanäle wird dadurch erleichtert, du kannst auch die Login-Daten mit anderen Personen teilen, die ebenfalls an dem Projekt beteiligt sind.

Beispiel:

- sales@deinedomain.de
- hr@deinedomain.de

8. Du nutzt gemeinsame Accounts

Gemeinsame E-Mail Accounts können praktisch sein. Besonders wenn du einen Service nutzt, der unter einem Account registriert ist, jedoch von mehr als einer Person genutzt wird. Ein weiterer Vorteil, mehreren Personen Zugang zu dem Account zu geben ist, dass jeder wichtige E-Mail Updates bekommt, ohne dass jemand dafür verantwortlich sein muss, Mails weiterzuleiten.

Beispiel:

- redaktionsteam@deinedomain.de

9. Du brauchst ein Backup

E-Mail Anbieter sichern häufig deinen Account im Fall eines vergessenen Passwortes oder unberechtigtem Zugriff, indem sie eine Sicherungsmail für die Wiederherstellung nutzen. Mindestens zwei Mail-Adressen zu haben stellt sicher, dass du ein Backup hast, wenn du den Zugang zu deinem Haupt-Account verlierst.

Mehrere E-Mail-Adressen sind besser als eine

weil Mail-Accounts leicht zu erstellen sind und es keine Beschränkung gibt, wie viele man besitzen kann. Mehrere E-Mail-Adressen zu nutzen kann die Kommunikation und Prozesse beschleunigen. Wenn du deine E-Mails noch besser organisieren willst, versuche es mit einer professionellen E-Mail-Management Software und hole das Meiste aus deinen verschiedenen Mail-Adressen raus.

Quelle: https://www.getapp.de/blog/2/10-grunde-warum-du-mehr-als-eine-e-mail-adresse-haben-solltest

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Hast Du mehrere E-Mail Adressen? Evtl. sogar für jedes Deiner Benutzerkonten eine eigene? Oder hast Du schonmal gehört oder angedacht, dass das eine gute Idee wäre?

Dann bist Du bei dieser Episode der Datenwache genau richtig. Denn hier sprechen wir darüber, warum mehrere Email-Adressen ein guter Schutz vor Kriminellen, aber auch Datensammlern sind. Und Du erhältst natürlich auch wieder Tipps, welche Möglichkeiten Du hast, um Dir Deine **private Email**-Adressen zu erzeugen. Zum Schutz Deiner Privatsphäre und für die Sicherheit Deiner Daten.

Denn in dieser Folge schauen wir uns zunächst erstmal an:

- **Warum und wofür sind mehrere E-Mail-Adressen eigentlich sinnvoll?**
  Wir sehen uns an wie typische Kriminelle und Datensammler vorgehen und wie du diese aktiv durch unterschiedliche E-Mail-Adressen ausbremsen kannst.
- **Welche Möglichkeiten für mehr als eine E-Mail gibt es und welche sind sinnvoll, welche kannst du sein lassen?**
  Hier sehen wir uns an wo und wie du neue E-Mail-Adressen anlegen kannst und welche Vor- und Nachteile **Kurzzeit-Emails**, **modifizierte Emails** (z.B. klausi+paypal@…), **eine eigene Domain** und sogenannte **Aliase** haben.
- **Und du kriegst natürlich auch direkt wieder Tipps, mit denen du sofort loslegen kannst.**

Inhaltsverzeichnis

Warum sind mehrere Email-Adressen sinnvoll?

Gucken wir uns zunächst mal an: Warum sind mehrere E-Mail-Adressen überhaupt sinnvoll? Denn klar, im Thema der Datenwache schützen mehrere E-Mail-Adressen sowohl vor Kriminellen als auch vor Datensammlern.

Typisches Vorgehen von Kriminellen bei der Jagd auf Benutzerdaten

Denn wie gehen Kriminelle typischerweise vor? Eine Vorgehensweise ist: Es wird bei irgendwelchen Anbietern eingebrochen und es werden Listen geklaut, **Listen mit E-Mails oder Benutzernamen und Passwörtern.**

Und was der Kriminelle dann halt macht, ist ausprobieren, ob mit der E-Mail und vielleicht sogar dem Passwort er bei anderen Accounts auch reinkommt. Also wenn bei Facebook geklaut wurde, probiert er halt mal aus, geht das auch für PayPal?

Wie kannst du dich vor diesen Kriminellen schützen?

Was natürlich hilft, und du als Datenwache-Hörer weißt das natürlich, ist, verschiedene gute Passwörter für jeden Benutzeraccount, für jedes Benutzerkonto ein eigenes. Also Folge 11 gibt dir da noch mehr Hintergrundinformationen, wenn du magst.

Und natürlich ein zweiter Faktor, zum Beispiel ein Code, den du auf deinem Handy erzeugst, auch das hilft und haben wir in Folge 13 besprochen.

Denn auch, wenn keines dieser Verfahren hundertprozentig sicher ist, damit bist du schon verdammt gut aufgestellt.

Wäre es nicht gut, wenn Kriminelle gar nicht erraten könnten, was Dein Benutzername bei einem Anbieter sein kann?

Aber jetzt wäre es ja vielleicht auch ganz cool, wenn so ein Krimineller gar nicht erraten könnte, ob du einen Account bei irgendeinem anderen Anbieter hast und wie der denn wohl lautet.

Beispiel:
Es werden bei einem Anbieter Daten geklaut und da kommt jetzt deine E-Mail-Adresse klausi@irgendwas als E-Mail drin vor.

Und jetzt denkt sich der Kriminelle: Mensch, das probieren wir doch auch mal bei PayPal aus, wo wir vorher bei Facebook geklaut haben vielleicht und dann kriegst du halt erstmal den Versuch bei PayPal mit klausi@ und deinem Passwort sich anzumelden, das funktioniert nicht.

Aber jetzt ist der Kriminelle vielleicht hochmotiviert und denkt sich: Mensch, bei Klausi, da würde ich aber gerne rein. Und dann kriegst du vielleicht Phishing-Mails an klausi@ jetzt im Namen von PayPal, um deine Kreditkartennummer zu ändern oder ähnlich spannende Sachen.

Eine Lösung könnte ja jetzt aussehen:
Wenn du für Facebook und für PayPal in diesem Fall ganz unterschiedliche E-Mail-Adressen hast, dann kann natürlich der Kriminelle das zum einen mal mit deiner Facebook E-Mail-Adresse bei PayPal probieren, das funktioniert ja nicht, aber wenn er dir jetzt Phishing auf deine Facebook E-Mail-Adresse für was anderes außer Facebook schickt, dann ist die Sache natürlich auch relativ schnell klar.

Das heißt, du generierst dir **unterschiedliche E-Mail-Adressen für unterschiedliche Konten** und kannst schon anhand der E-Mail-Adresse erkennen, macht das hier eigentlich gerade alles Sinn oder nicht. Ich kann euch versprechen, ihr gewöhnt euch so schnell da dran, bei E-Mails als allererstes zu gucken, **macht es eigentlich Sinn, den Inhalt, den ich da gerade kriege an diese E-Mail-Adresse** und das ist so ein **starker Filter**.

Dann die anderen Details, die wir schon besprochen haben, wie erkennt man **Phishing**, wie kann man damit sinnvoll umgehen, das ist ein anderer Schnack, das kommt dann auch.

Aber überhaupt erstmal zu gucken: Warum schickt mir die Sparkasse jetzt eine Information an mein PayPal-Konto, an meine PayPal E-Mail? Dann ist das Thema direkt durch. Dann wisst ihr sofort: Da kann was nicht stimmen. Also gegen Kriminelle mehrere E-Mail-Adressen, feine Sache.

Datensammler oder die „anderen Kriminellen“ – so kannst du Datensammler blockieren

Was sind Datensammler? Es gibt ja noch mehr Kriminelle, die nennen sich dann halt Datensammler und auch da gibt es durchaus sinnvolle Anwendungsgebiete von mehreren E-Mail-Adressen.

Denn auch Datensammler, die sammeln halt die Daten, indem sie dich zum Beispiel auf Webseiten verfolgen oder mit irgendwelchen Webseiten zusammenarbeiten. Und die können entweder zusammenarbeiten, mehrere Anbieter von mehreren Seiten oder ein Anbieter bekommt halt Daten von mehreren Seiten und führt diese zusammen.

Da gibt es schöne **seitenübergreifende Profile**. Wenn du dir die ersten Folgen der Datenwache nochmal anhören möchtest, also die mit den einziffrigen Nummern, da geht es ja viel um dieses, was ist eigentlich das Problem von Überwachung und Daten sammeln, und dann kannst du dir so Szenarien überlegen, da haben wir lange nicht mehr darüber gesprochen, warum das eigentlich so perfide ist das Ganze.

Aber denke dir solche Profile aus, wo rauskommt, dass du auf Seitensprungseiten unterwegs bist, dass du vielleicht im Online-Shopping aktiv bist und was du dann natürlich auch gerne kaufst, vielleicht auch was für Diätpläne, auf was für Diätseiten du unterwegs bist und nach welchen Gesundheitsthemen du suchst.

Das kann schon richtig Spaß machen. Also vielleicht jetzt weniger für den Betroffenen, aber so für den Datensammler, das gibt ein **knackiges Profil, damit kann man vermutlich irgendwie Geld machen.**

Genau das ist der Grund, warum wir da reingrätschen müssen, weil diese Daten halt spannend sind, auch wenn sie einzeln für sich genommen uns vielleicht jetzt erstmal leidlich belanglos erscheinen.

Wenn du dir Folge 5 speziell nochmal anschaust, dann wirst du hören, was einzelne Firmen nur auf Basis deiner E-Mail-Adressen an Datenmengen über dich vorhalten und auf Basis deiner E-Mail-Adresse dann halt mit anderen Anbietern gegen Geld teilen.

Deshalb ist es wichtig darüber nachzudenken auch deine E-Mail-Adresse als **Verschleierung** zu benutzen. Verschiedene E-Mail-Adressen, damit über die E-Mail nicht zusammengeführt werden kannst. Denn deine E-Mail, die behältst du typischerweise ja wirklich lange. Ich glaube, Leute ändern öfter ihre Telefonnummer als ihre E-Mail-Adresse, zumindest, dass du eine E-Mail-Adresse wirklich löschst. Deshalb ist es ein ganz, ganz starker Identifikator.

Schau dir Folge 5 nochmal an, ist glaube ich ganz interessant einfach zu gucken, was es so mit manchen Firmen auf sich hat, welche Daten dahinterstecken und damit auch wie viel Geld.

Natürlich reicht es nicht, um deine Daten zu verschleiern, wenn du nur deine E-Mail-Adressen jetzt irgendwie durchrotierst oder verschiedene verwendest. Auch deine Kreditkarte, Cookies, Browser Fingerprinting, all so Sachen spielen da mit rein.

In Folge 38 habe ich einen Überblick über dieses Thema Privatsphäre gegeben und gebe dir da Hintergrundinformationen und Verweise auf alle Details. Aber eine E-Mail-Adresse oder verschiedene E-Mail-Adressen ist ein Superschritt halt auch, um Datensammler auszubremsen.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Woher bekomme ich verschiedene Email-Adressen?

Jetzt haben wir gesehen, verschiedene E-Mail-Adressen helfen gegen alle Arten von Kriminellen, den typischen Kriminellen und den Datensammlern. Jetzt wäre es ja vielleicht ganz interessant: Wie kommst du jetzt zu einer guten weiteren E-Mail-Adresse beziehungsweise gleich zu vielen davon? Da gibt es natürlich verschiedene Wege, die wir jetzt mal kurz durchgehen.

Jedes Mal neue Email-Adresse anlegen

Das eine ist natürlich, du kannst jedes Mal einen neuen Account anlegen. Du meldest dich bei dem einen Anbieter an, gehst zu Googlemail, Mailbox, Posteo.de und legst einen neuen Account an. Beim nächsten Anbieter dasselbe in Grün, beim nächsten Anbieter dasselbe in Grün.

Wenn du wenige Benutzerkonten hast, aber wenige sind dann im einziffrigen Bereich, ist das vielleicht ein gangbarer Weg, weil es halt einfach **aufwendig** ist. Dafür aber auch eine **gute Verschleierung**, weil damit kannst du natürlich komplett in der Masse untergehen.

Kurzzeit (10 min) oder Wegwerf-Email

Was viel zu wenig gemacht wird und was ich sehr empfehlen kann, sind Kurzzeit E-Mails oder auch Wegwerf E-Mails, 10-Minuten-Mails, Einmal-Emails oder Trash-Emails genannt. In Folge 5 gibt es auch darüber noch ein bisschen Informationen. **Ganz wichtig da, nutzt das nur für Belangloses**.

Aber dann hast du da wirklich eine schnelle, anonyme und temporäre E-Mail-Adresse, die funktioniert vielleicht einmal oder 10 Minuten lang, die kannst du prima verwenden, wenn du zum Beispiel mal irgendein Benutzerforum ausprobieren möchtest und nicht weißt, ob du da bleibst.

Oder wenn du bei der Tageszeitung irgendwas kommentieren möchtest, aber dafür keinen eigenen Account anlegen oder jedes Mal zum Beispiel einen eigenen Account anlegen, da kannst du sowas nehmen. Der **Chaos Computer Club** hat mit der **anonbox** einen Generator, mit dem du dir bei jedem Neuladen der Seite kostenlos eine neue Kurzzeit Email erstellen lassen kannst.

Email-Adresse modifizieren („+“-Zeichen)

Was halt auch oft vorkommt, ist das Modifizieren von E-Mails mit dem Pluszeichen. Also dass du nicht mehr Klausi@ verwendest, sondern klausi+paypal@ für PayPal und klausi+facebook@ für Facebook.

Ist **super zum Sortieren deiner E-Mails**, hilft auch manchmal ein bisschen, um **Spam und Phishing zu erkennen**, aber da natürlich jedes Mal Klausi+ und dann irgendwas da drinsteht, erkennt natürlich auch ein Blinder mit Krückstock, dass klausi eure wahre E-Mail-Adresse ist.

Also ein **wahrer Schutz ist das nicht**, aber ganz praktisch, um zumindest mal anzufangen mit dem Thema.

Domain Mail

Eine spannende Sache, die auch viele andere Vorteile hat, ist eine eigene Domain. Das heißt du registrierst dir klausiseigenedomain.de und kannst das dann für jede E-Mail verwenden, indem du klaus@klausiseigenedomain.de verwendest oder was dir gerade einfällt. Das Hosting deiner Domain Mail(s) ist dann dasselbe wie das deiner Domain.

Anstatt bestimmte Domain Mails einzurichten, gibt es auch die Möglichkeit ein sogenanntes Catch-All einzurichten. Dann bekommst du alle Nachrichten an alle Email-Adressen die mit @klausiseigenedomain.de enden, egal was vor dem @ steht. Dazu kannst du einfache die Email „*@klausiseigenedomain.de“ bei deinem Webhosting einrichten und das Sternchen ist ein Platzhalter für alles mögliche was vor dem @ stehen kann.

Also egal an welche E-Mail-Adresse, ob es die E-Mail-Adresse schon gab vor zwei Sekunden oder nicht, vollkommen egal, gehen dann an diese Catch-All E-Mail-Adresse und werden an dein Postfach weitergeleitet. Ein kurze Anleitung zur Einrichtung findest du hier.

Nachteil, vielleicht einigermaßen offensichtlich, das ist natürlich **genau dir zugeordnet** diese Domain. Das heißt, wenn jetzt Daten wegkommen, dann findet der Kriminelle in jedem Benutzerkonto, das geknackt wurde, genau eine E-Mail von klausiseigenedomain.de und die Wahrscheinlichkeit, dass das immer dieselbe Person ist, auch wenn der Name davor anders ist, ist vermutlich relativ offensichtlich.

Also ist das nur ein Teilschutz, aber nichtsdestotrotz eine spannende Sache, weil du damit wirklich sehr gut natürlich erkennen kannst, wofür du welche E-Mail verwendet hast. Aber um zu verschleiern, wer du bist, ist es leider nicht so richtig gut.

Aliase Email

Dafür ist aber richtig gut, wenn du anonyme Aliase verwendest. Und das bietet dir fast jeder E-Mail-Anbieter an, nämlich dass du unterschiedliche E-Mail-Adressen dir erzeugst, die alle auf deine wahre E-Mail-Adresse zeigen, die du also einfach verwenden kannst wie deine wahre E-Mail-Adresse, also primär jetzt mal zum Empfang, seltener zum Senden.

Wobei es auch da bei manchen Anbietern Möglichkeiten gibt von dem Alias aus Mails zu senden. Aber das Coole ist halt wirklich, da generierst du dir komplett zufällige E-Mail-Adressen, die verweisen auf deine Originale und **das einzige Traurige ist, dass fast alle Anbieter da sehr knauserig mit sind.**

Außer Runbox kenne ich jetzt aktuell keinen, wo du richtig große Mengen von Aliasen für wenig Geld kriegst. Bei Runbox sind es glaube ich aktuell 100 frei wählbare.

Und das ist super, das ist wie eigene E-Mail-Adressen, dafür aber ohne den großen Aufwand und das große Geschiss, dass du da jedes Mal einen kompletten Account einrichten musst, sondern du generierst dir halt diesen Alias. Also eine gute Sache.

Tipps

Und damit kommen wir auch schon zu den Tipps.

Tipp 1: Vermeide Perfektionismus

Ganz wichtig ist wie immer bei der Datenwache, es geht hier nicht um die hundertprozentig perfekte Lösung, weil die wird vermutlich entweder kompliziert oder unmöglich und macht vermutlich auch keinen Spaß, es geht um den guten ersten Schritt.

Tipp 2: Nutze verschiedene Email-Adressen für verschiedene Benutzerkonten

Das Wichtigste, denke ich, ist erstmal zu akzeptieren, verschiedene E-Mail-Adressen für verschiedene Benutzerkonten. Dann kannst du variieren, **nimmst du komplett zufällige Aliase, spielst du erstmal mit dem Pluszeichen oder benutzt du mal ein paar Gruppen von E-Mails?**

Richtest du zum Beispiel ein für deine Newsletter, für dein Online-Shopping und gehst so damit dann halt eins nach dem anderen immer weiter vor. Dann kommst du da irgendwie zumindest mal in dieses Mindset, eigene E-Mail-Adressen für eigene Benutzerkonten rein.

Tipp 3: Nutze Kurzzeit/Wegwerf-E-Mail-Adressen

Unterschätzt, aber definitiv eine gute Sache, **Kurzzeit- und Wegwerf E-Mails** wie die anonbox vom Chaos Computer Club. Solltest du auf jeden Fall dir mal angucken, für belangloses Zeug spitze.

Tipp 4: Nimm einen sicheren E-Mail-Anbieter

Und nimm einen **guten E-Mail-Anbieter**, ich rede ja immer von posteo, mailbox.org und runbox.com, dazu kannst du Folge 10 dir noch mal anhören. Aber das ist natürlich ganz essenziell, wenn es um E-Mails geht, dass du auch einen E-Mail-Anbieter hast, dem du vertrauen kannst.

Wenn du Kommentare zu diesem Thema hast, mich würde sehr interessieren, wie gehst du mit deinen E-Mails um? Schreibe gerne Kommentare. Ich freue mich darauf und ich antworte darauf.

Quelle: https://www.datenwache.de/private-email/

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Internet inkognito: warum mehrere E-Mail-Adressen sinnvoll sind

Die E-Mail ist Schaltzentrale des digitalen Lebens: Ob zur Anmeldung bei Online-Shopping-Diensten, auf einer Dating-Plattform oder bei Online-Bezahlservices, fast überall wird die Angabe einer E-Mail-Adresse gefordert. Auch das Zurücksetzen vieler Passwörter ist nur über den E-Mail-Account möglich. Doch wer unbedacht seine Mail-Adresse preisgibt, kann schnell zum Opfer von Cyberkriminellen werden. Es ist also durchaus sinnvoll, mehr als nur eine E-Mail-Adresse zu verwenden.

23. Februar 2023 von Alessandra Hamsch

Manchmal ist es sinnvoll, mehr als nur eine E-Mail-Adresse zu verwenden, denn wer unbedacht seine Mail-Adresse preisgibt, kann schnell zum Opfer von Cyberkriminellen werden. (c) Shutterstock

Klarname kann riskant sein

Bei seriösen E-Mail-Adressen ist es üblich, den Vor- und Nachnamen zu benutzen. Was für die Kommunikation hilfreich ist, kann für die Anmeldung auf Social-Media-Plattformen, bei Mailinglisten, auf Auktionsplattformen und Kleinanzeigenbörsen oder in Internetforen zum Risiko werden. E-Mail-Adressen mit Klarnamen von seriösen E-Mail-Anbietern haben unter Spammern eine besonders gute Reputation, weil sich dahinter ein echter Mensch verbirgt. Tauchen solche „validen“ E-Mail-Adressen also gehäuft bei unterschiedlichen Online-Plattformen auf, werden sie mit höherer Wahrscheinlichkeit zum Ziel von Spam-Mails. Deshalb sollte man bei diversen Online-Diensten lieber auf Alias-Adressen ohne Klarnamen setzen. Alias-Adressen sind im Postfach der Haupt-Adresse untergeordnet, dabei bleiben Nutzername und Kennwort gleich.

Schutz durch Anonymität und mehrere E-Mail-Adressen

Wer mehrere E-Mail-Adressen verwendet, um seine Haupt-Adresse zu schützen, tut sich auch leichter mit einem Wechsel: Bekommt zum Beispiel eine der Alias-Adressen besonders viel Spam zugeschickt, legt man einfach eine weitere an. Diese neue Adresse ist bei den Spamversendern unbekannt und die Haupt-Adresse bleibt weiter geschützt. Übrigens kann man in den Einstellungen bei GMX jederzeit neu festlegen, welche der dem Konto zugeordneten E-Mail-Adressen die Absendeadresse sein soll.

Bei GMX haben FreeMailer zum Beispiel die Möglichkeit, sich eine weitere kostenlose E-Mail-Adresse in ihrem Account anzulegen. Diese zusätzliche Mail-Adresse kann bei Bedarf auch wieder gelöscht und durch eine neue ersetzt werden.

Quelle: https://newsroom.gmx.net/2023/02/23/internet-inkognito-warum-mehrere-e-mail-adressen-sinnvoll-sind/