Erledigt 500 Millionen gestohlene Mailadressen

Beitrag von „Altemirabelle“ vom 13. Juli 2017, 21:11

Hab spasshalber meine Mailadresse, wie in dem Artikel von Macwelt beschrieben wurde überprüft, und sehe da: Treffer.
Mein account bei Adobe und das Passwort wurde schon 2013 gehackt.

https://www.macwelt.de/a/bka-5...ter-schnell-check,3447331

Hier Email prüfen:

https://sec.hpi.uni-potsdam.de/leak-checker/search?lang=de

Beitrag von „umax1980“ vom 13. Juli 2017, 21:13

Ich habe fünf Adressen, zwei waren auch 2013 dabei. Ich Wechsel aber monatlich die Kennwörter, von daher alles Safe .

Beitrag von „al6042“ vom 13. Juli 2017, 21:16

2 Mailadressen wurden bei mir auch als geknackt angezeigt...
Die aber schon 2013 und 2016...
In der Zeit wurden die PWs dazu schon mehrfach geändert.

Beitrag von „Altemirabelle“ vom 13. Juli 2017, 21:24

Hab natürlich das Passwort geändert. Schaden hab ich keinen gemerkt.

Beitrag von „macmac512“ vom 13. Juli 2017, 21:40

Schneller mit gleicher Liste geht es übrigens hier: https://haveibeenpwned.com

Keine Ahnung wieso die Uni Potsdam dafür so elend lang braucht.

Ich war auch bei allen obigen dabei, D.r.o.p.b.o.x, Adobe,... 

Das zensieren von D.r.o.p.b.o.x ist irgendwie echt ein bisschen nervig.

Beitrag von „al6042“ vom 13. Juli 2017, 21:50

Dann nutze das Wort nicht... 
Hintergrund sollte aber einleuchten... Links zu D.r.o.p.b.o.x. werden hier nicht unterstützt...

Beitrag von „Nio82“ vom 13. Juli 2017, 21:52

Bei mir ist nur meine Müll eMail Adresse betroffen, bei einem Myspace Account den ich vor ca 10 Jahren mal angelegt aber dann doch nie eingerichtet & genutzt habe.

Meine Haupt eMail Adresse ist glücklicherweise nicht betroffen. Und das PW bei der anderen wurde seit damals auch mehrfach geändert.

Beitrag von „macmac512“ vom 13. Juli 2017, 22:04

@al6042: Weiß ich ja alles.
Im Fließtext selbst ohne .com dahinter, nervt es halt manchmal.

Beitrag von „Patricksworld“ vom 13. Juli 2017, 22:16

Meine sind dankbarer Weise auch nicht betroffen. Und für alles zum Identifizieren gibt es ja ohnehin 2 Phasen Authentifikation.


Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Glückwunsch: Ihre E-Mail-Adresse [redacted]@googlemail.com taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.

Haftungsausschluss: Wir übernehmen keine Haftung für die Vollständigkeit und Korrektheit der bereitgestellten Informationen unseres Dienstes. Die Daten werden automatisch gesammelt und entsprechend für Abfragen aufbereitet. Wir werten für unseren Dienst nur öffentlich im Internet verfügbare Quellen aus und können keine Vollständigkeit garantieren. Wir bereiten nur den Teil der im Internet veröffentlichten Identitätsdatenbanken auf und haben keinen Zugriff auf "analoge Daten", also z.B. Daten, die physikalisch von Betrügern ausgetauscht werden oder Daten die von Dokumenten (Reisepass, Ausweis, Rechnungen, persönliche Briefe) abgeschrieben wurden.

Ihr HPI Identity Leak Checker Team
Impressum

Edit: Was damals auch toll war bei chip.de

Die hatten mal eine Empfehlung für eine Webseite ausgesprochen die die Passwörter auf stärke überprüft hat.
Nur mal andersrum gedacht. Aus den eingegebenen PW's kann man dann auch ne gute DB erstellen. Danke Chip.de
dafür. Mal abgesehen das auch die Nutzerdaten von denen geklaut wurden.

Beitrag von „Dr.Stein“ vom 13. Juli 2017, 22:20

Ich bin auch nicht dabei obwohl ich 3 verschiedene Adresse habe. O.o wundert mich ein wenig.

Beitrag von „Leggalucci“ vom 13. Juli 2017, 22:29

Ich bin auch nicht betroffen. Durch 1Password habe ich auch überall ein anderes PW und meist min 10 Stellen

---

Beitrag von „Patricksworld“ vom 13. Juli 2017, 22:33

Meine Strategie. Nur kryptische unendlich lange Passwörter die in einer Bilddatei gespeichert sind. Und natürlich für jeden acc unterschiedlich. Dann halt in einem Schlüsselbund abspeichern. Fertig ...

Beitrag von „umax1980“ vom 13. Juli 2017, 22:42

Ich nutze 12 Zeichen für alles wichtige, sind ja letztlich nur 8 Accounts.

Für den Rest 8 Zeichen - aber da sind die Passwörter gleich. Sind aber unkritische Zugänge.

Beitrag von „griven“ vom 13. Juli 2017, 22:43

Tut zwar nichts zu Thema aber ich habe Dropbox mal wieder von der Zensurliste genommen denn das hat letztlich nur dazu gedient zu verhindern das in der Zeit nach der Übernahme von Daten aus dem Public Ordner von Dropbox bis zu Abschaltung der Funktion keine neuen Inhalte über diesen Kanal hinzugefügt werden. Da der Public Ordner bzw. dessen allgemeine Freigabe von Dropbox nun schon eine Weile abgeschaltet ist besteht diese Gefahr nicht mehr und es gibt demnach auch keinen Grund mehr das Wort auf der Liste zu behalten 

Beitrag von „al6042“ vom 13. Juli 2017, 23:10

Na dann.... können wir ja wieder kräftig Dropboxen...

Beitrag von „Dr.Stein“ vom 13. Juli 2017, 23:13

DropBox Dropbox Dropbox! Yeiihh

Beitrag von „macmac512“ vom 13. Juli 2017, 23:14

Danke!

Beitrag von „derHackfan“ vom 14. Juli 2017, 00:10

Geht es jetzt um das Passwort der E-Mail Adresse oder um einen Account?

Letzteres habe ich zwei betroffene Kandidaten DropBox und Planet3DNow! und auf beide kann ich verzichten aber einloggen geht auch nicht.

Beitrag von „griven“ vom 14. Juli 2017, 00:18

Nee schon um die Accounts und populär geworden ist das bei dem DropBox Leck wo ein Großteil der Accounts abgegriffen wurde. Das Problem ist das viele Angebote die Email als username nutzen und viele Leute aus reiner Bequemlichkeit überall das selbe Passwort verwenden. Es ist auf die Weise dann ein leichtes per Try and Error weitere Dienste auszuspähen die nach dem Verfahren funktionieren und bei denen der Nutzer angemeldet sein könnte (PayPal zum Beispiel)...

Beitrag von „derHackfan“ vom 14. Juli 2017, 00:25

> Zitat von griven
>
> und viele Leute aus reiner Bequemlichkeit überall das selbe Passwort verwenden.

Aber nicht mit mir Leute, da müsst ihr schon früher aufstehen und fünf Minuten kalte Dusche aushalten können, wer will den Bequemlichkeit im Alltag? 😛

Beitrag von „Altemirabelle“ vom 14. Juli 2017, 09:39

@Patricksworld

Auch wenn es seltsam klingt, habe ich nie die Schlüsselbund-Funktion verwendet und habe davon keine Ahnung. Hab es sogar für unsicher gehalten.
Aber deine Strategie finde ich sehr interessant. Was meinst du mit: Passwörter die in einer Bilddatei gespeichert sind, wo sind die gespeichert?

Beitrag von „Hunk89“ vom 14. Juli 2017, 16:15

Wie sind die an die Passwörter gekommen? Brute force?

LG
Hunk

Beitrag von „Nio82“ vom 14. Juli 2017, 18:39

@Hunk89

Das ist es was ich dir damals versucht habe klar zu machen als du so ein riesen Ding aus FileVault gemacht hast. Wen dir einer Identitätsdaten klaut, kommt der nicht nach Hause an deinen Rechner, dann geschieht das online. Da haben sich Hacker auf die Server verschiedenster Dienste Anbieter rein gehackt & komplette Datenbanken an Nutzerdaten gestohlen. Was für Methoden sie genutzt haben um auf die Server drauf zu kommen, kann man jetzt nicht so genau sagen.

Ich denke nicht das diejenigen die Brute force methode verwendet haben um sich dann in einen Server Administrator account ein zu hacken, da gibts sicher einfachere Methoden.

Beitrag von „Hunk89“ vom 14. Juli 2017, 18:46

Sind lange und komplizierte Passwörter auch gefährdet?

Beitrag von „umax1980“ vom 14. Juli 2017, 18:50

Es geht hier primär nicht um die Sicherheit deiner Passwörter im Sinne von leicht zu knacken.

Vielmehr wurden hier komplette Datensätze entwendet mit deinem Kennwort ....

Daher immer regelmäßig die Kennwörter ändern.

Beitrag von „Hunk89“ vom 14. Juli 2017, 19:19

danke. was heißt regelmäßig?

Gesendet von iPhone mit Tapatalk

Beitrag von „Nio82“ vom 14. Juli 2017, 19:34

@Hunk89

So ballt ganze Datenbanken mit Nutzerdaten gestohlen wurden ist es egal wie kompliziert das Passwort ist, den die Diebe haben es dann ja schon! Da hilft es nur, sobald du weißt das deine Daten in den Datenbanken enthalten waren, dein Passwort zu ändern.

Bei der Sicherheit des PW kommt es nicht nur auf die Länge an. Wichtig ist, es dürfen keine Worte sein wie sie in einem Duden oder Lexikon zu finden sind & auch keine Eigennamen oder Markennamen oder ähnliches.

Das PW sollte möglichst eine kryptische Zahlen Buchstaben Sonderzeichen Kombination sein von der nur du die Bedeutung kennst.

Ein einfaches Beispiel: Namen & Geburtsdaten deiner Ältern.

Tina Schmitt 20.08.1965

Paul Gärtner 08.06.1958

Das Kombinierst du dann zu **Ts_2o*o8*65+Pg_o8*o6*58**

Da hast du jetzt Großbuchstaben Kleinbuchstaben Sonderzeichen & ein 23 Zeichen langes PW das du dir über die Eselsbrücke deiner Eltern merken kannst.

Was regelmäßig heißt sollte dir schon selber klar sein! Du überlegst dir einen Zeitraum nachdem du deine online Accounts neue Passwörter gibst. Alle 3 Monaten, 6 Monate oder 1 mal Pro Jahr. Das ist dir überlasen wie oft!

Beitrag von „umax1980“ vom 14. Juli 2017, 19:34

Es gibt sicherlich Anwender die wöchentliche Wechsel vornehmen.

Ich wechsel monatlich alle sehr wichtigen Kennwörter - kannst ja mal alles aufschreiben was du zusammen bekommst und da eine Liste erstellen nach Wichtigkeit.

Beitrag von „Ka209“ vom 14. Juli 2017, 20:03

Viele user haben auch das Problem das sie sich auf Seiten Registrieren die nicht so seriös sind und am besten auch mit den allgemeinen Daten und diese sind auch noch auf allen anderen Seiten gleich und liegen somit auf einem Silber tablet....

Beitrag von „Nio82“ vom 14. Juli 2017, 20:11

Stimmt^^daher nicht überall wo man sich Registriert die selben Daten oder eMail Adresse verwenden. Dafür hab ich schon immer zwei eMail Konten, eins für Seiten die ich wirklich nutze, YouTube eBay Facebook unser Forum & eins für Seiten wo ich für DLs meine eMail angeben musste oder ähnliches.

Es gibt dann auch noch die Möglichkeit von Wegwerf eMail Konten, die man einmal benutzt & die dann nach 24, 48 Stunden oder so automatisch wieder gelöscht werden.

Beitrag von „Ka209“ vom 14. Juli 2017, 20:21

Ja ich bin auch böse und nutze auf manchen Seiten die selbigen Passwort und Mail.

generel werden jedoch bestimmte Forums oder Seiten wie Facebook oder so eine Standart mail Adresse von mir bekommen die man gerne hacken darf die auch dafür gedacht ist nur Registrierungen machen zu können und dort auch bestimmt keine wichtigen Daten drauf kommen und der Inhaber der Mail Adresse fiktiv ist...

Beitrag von „umax1980“ vom 14. Juli 2017, 20:44

Genauso mache ich das - ein Kennwort für alle Foren. Mit dahinter liegender unwichtiger email Adresse.

Beitrag von „Schorse“ vom 15. Juli 2017, 08:40

Moin.
In der Vergabe von Passwörtern kommt macOS mit Safari einem doch sehr entgegen,

bequemer geht es doch nun wirklich nicht. Bei der Registration schlägt es ein Passwort vor welches dann bequem im Schlüsselbund abgelegt wird.

Diesen Weg nutze ich:
- Erstellung von erst Passwort im Schlüsselbund von macOS/Safari.
- Übergabe der Passwort/Benutzerdaten in 1 Passwort.
- Passwort löschen im Schlüsselbund.
- Jährliches wechseln des Passwort mit 1 Passwort durch eine Erinnerung.
- Nutzen einer VPN und Wegwerfemail bei registrierten legalen Downloads.
- Dropbox und andere Boxen nur für unwichtiges Datenkram.

Beitrag von „Altemirabelle“ vom 15. Juli 2017, 09:33

Muss mich ernst mit Schlüsselbund beschäftigen.
Meine Strategie war: immer wenn es geht nicht echte Daten eingeben. So existiere ich im Netz fast gar nicht. Nur eine fiktive Person.
Deswegen auch über ein Einbruch bei Adobe mach ich mir wenig Gedanken, aus dem Grund, weil mein account ebenfalls mit einer fiktiven Identität angelegt wurde, haha 

Beitrag von „Schorse“ vom 15. Juli 2017, 10:05

Softwarelizenzen oder Onlinedienste können nur nicht mit fiktiven Personen betrieben werden, da liegt das hauptsächliche Problem. Wie löst du das?

Beitrag von „Altemirabelle“ vom 15. Juli 2017, 10:30

Das hast du übersehen: "immer wenn es geht".

Bei Adobe zB wenn du deine Adobe-ID erstellst bist du doch nicht gezwungen deine echten

Daten einzugeben. Habe also mehrere IDs.

Beitrag von „blackcat“ vom 15. Juli 2017, 10:32

Bei mir ist nur eine Adresse betroffen.
Und natürlich ausgerechnet die bei eBay registrierte. Da vermutete ich schon seit längerem ein Leck, denn ich erhalte seit ca. 1 Jahr gelegentlich Phishingattacken darauf, in denen auch eine uralte Handynummer und mein eBayname drinstehen. Vermutlich wurde der Datensatz bei eBay schon vor etwa 7 oder 8 Jahren gestohlen.

War aber zuviel Arbeit für die Staatsanwaltschaft Potsdam.
Vermutlich kennt man sich da mit Ladendiebstahl oder Falschparken besser aus.

Beitrag von „Ka209“ vom 15. Juli 2017, 11:20

Ja gut aber das muss nicht von ebay herühren

in meiner sebständigkeit war ich mit meinen daten bei mehreren lieferanten registriert. Nach konkurz eines bzw. Kurz vor fing es an mit spam und der gleichen.
dir besagte firma hatte meine daten verkauft und dieser datensatz existiert immernoch da auf diese mails regelmässig neue angeboten von firmen kommen weltweit mit den ich noch nie zusammen gearbeitet habe und ich angeblich einen konto bei denen hätte.

Beitrag von „Hunk89“ vom 15. Juli 2017, 11:27

2013 wurde adobe geknackt. ich hab PW geändert.

Gesendet von iPhone mit Tapatalk

Beitrag von „Wolfe“ vom 15. Juli 2017, 14:19

Meine Adresse war auch dabei und betroffen war last.fm
An einen Brute-Force-Angriff glaube ich aber irgendwie nicht, da das Passwort mit "#o]I,^*2b[c5|R5TUYVu" relativ stark war.

Beitrag von „Hunk89“ vom 15. Juli 2017, 14:21

ja brute forcen kann man glaub ich auch keines meiner Passwörter .

Gesendet von iPhone mit Tapatalk

Beitrag von „blackcat“ vom 15. Juli 2017, 14:58

> Zitat von Ka209
>
> Ja gut aber das muss nicht von ebay herühren

Die betreffenden Daten (Lieferadresse, HandyNr. und Username) waren aber ausschließlich bei eBay so angegeben und nirgendwo anders - erst recht nicht in dieser Kombination ....

Beitrag von „macmac512“ vom 15. Juli 2017, 15:15

Dort sind doch auch gar keine Passwörter aufgelistet, die einzeln geklaut wurden - bspw. durch Brute Force.

Wenn ich das Passwort von einem User hier errate und mich mit seiner eMail hier anmelde, wird er das nicht komisch finden, aber niemals in der Liste sehen. 

Es sind nur die Fälle aufgelistet, wo ganze Datensätze quasi im Klartext geklaut wurden und andere Leute somit darauf zugreifen können. Mit der Sicherheit von dem individuellen PW hat das 0,0 zu tun - egal ob "12345" oder 200 stellig mit Sonderzeichen.

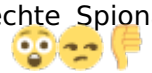
Beitrag von „Hunk89“ vom 15. Juli 2017, 15:16

ist klar

Gesendet von iPhone mit Tapatalk

Beitrag von „Nio82“ vom 15. Juli 2017, 15:51

Ich weiß echt nicht wie hier einige immer wieder noch darauf kommen, dass sich Hacker wirklich die Mühe machen & sich in einzelne Accounts bei eBay, Amazon, Facebook Google & was weiß ich noch hacken!?

Zu viele schlechte Spionage Hacking Filme geschaut? Achtung! Ich hack mich jetzt in den "Mainframe"!!! 

Was Hacker machen ist, sich in die Server von Webseiten Diensteanbietern, Online Shops zu hacken & dort komplette Daten Sätze/Packete stehlen bestehend aus 10,000den von Nutzerdaten. Diese werden dann im sogenannten "Darknet" zum verkauf angeboten. So was wurde in den letzten 10 Jahren immer wieder bekannt. Der letzte große Hack an den ich mich erinnere war der Sony Konzern wo neben Sony - Columbia Pictures auch das PlayStation Netzwerk gehackt wurde.

"Brute Force" ist wahrscheinlich die einzige Methode mit der man jedes PW knacken kann, genügend Zeit & Rechnerleistung vorausgesetzt. Da helfen auch Sonderzeichen & ein sehr langes PW nicht. Was aber nicht heißt das man wieder zu dem allseits beliebten PW 123456 zurückkehrten soll! Ein besonders langes & kryptisches PW ist dazu da, den Aufwand um das PW zu knacken so weit zu erhöhen das es sich nicht mehr lohnt! Und keine "echten" Worte zu nutzen, dabei geht es darum, einen Datenbank Angrief ins lehre laufen zu lassen. Datenbank Angriff, so bezeichnet man eine Methode des PW Hackings, bei der eine Datei/Datenbank mit Millionen von Wörtern als PW durchprobiert wird. Wer dann ein Wort als PW verwendet wie "Hausstaubmilbe" wird dieses mit großer Wahrscheinlichkeit in der Datenbank enthalten sein. Diese Datenbanken, das sind meist .txt oder .doc Dateien die bis zu mehre GB groß sind wegen der Milionen enthaltenen Wörtern.

Beitrag von „Hunk89“ vom 15. Juli 2017, 15:55

wie hoch ist die Wahrscheinlichkeit, dass dann irgendjemand, der die Passwörter gekauft hat zB Großeinkauf macht?

Gesendet von iPhone mit Tapatalk

Beitrag von „Nio82“ vom 15. Juli 2017, 16:06

@Hunk89

Ich merk wie dir bei dieser Frage schon wieder innerlich die Knieehe zittern! 

Kommt drauf an was für Daten der der betreffende kauft. Bei Kreditkarten Daten oder von eBay Amazon dürfte es ja eindeutig sein. 

Wenn jemand so ein Datenpacket kauft sind da ja nicht nur 2 5 12 40 100 drinne sonndern 1000de & da wird dann eben durchprobiert. Welcher Account funktioniert noch welcher nicht. Deswegen sollte man eben regelmäßig sein PW erneuern damit, für den Fall das dein Account dabei ist, wenigstens das PW nicht mehr stimmt & der jenige nicht in deinen Account rein kommt.

Beitrag von „Hunk89“ vom 15. Juli 2017, 16:09

ok, das leuchtet mir ein... gut, dass es besprochen wurde. Danke.

Gesendet von iPhone mit Tapatalk

Beitrag von „Ka209“ vom 15. Juli 2017, 22:50

@blackcat ja genau deswegen ja bei jedem kauf den du bei ebay tätigst gibst du deine Daten einer dritten Person weiter damit er oder sie dir was zukommen lassen kann und diese ganzen Personen sind potenziell angreifbar oder auch Daten Verkäufer.

wir wollen alles so billig wie möglich wenn jemand dir etwas zum einkaufspreis verkauft muss er auch irgendwo gewinn machen.

z.B. unsere letzte ebay gemeinschaftlicher PC Maus Einkauf hier im Forum bei eBay wo alle die 1 € maus gekauft haben mich eingeschlossen....

Beitrag von „Schorse“ vom 15. Juli 2017, 23:46

Ich hatte einmal ein paar sehr interessante Gespräche mit Banken. Eine davon schilderte mir die 90% Methode und die ist nicht von Hackern ausgegangen sondern es ist der Postbote oder der Postverteiler 
Und Paypal geht einem Hack nur grob nach und meldet es der Staatsanwaltschaft so wie sie es gesetzlich müssen da fast alle Bemühungen ins leere führen.

Beitrag von „Patricksworld“ vom 16. Juli 2017, 15:30

@Altemirabelle

> Zitat von Altemirabelle
>
> Was meinst du mit: Passwörter die in einer Bilddatei gespeichert sind, wo sind die gespeichert?

Schau dir mal die Videos von Sempervideo an. Ist zwar schon was älter. Aber funktioniert trotzdem reibungslos. Und du kannst dann halt mit jedem beliebigen Texteditor auch auf dem handy drauf zugreifen.

MFG Patrick

Beitrag von „Hunk89“ vom 19. Juli 2017, 18:04

Hallo Hackintosher,

kann man mit dem Apple Wiederherstellungsschlüssel das Passwort und die zweistufige Bestätigung umgehen?

Muss ich auch die Antworten auf Sicherheitsfragen ändern? Wie geht das überhaupt?

LG
Hunk

Beitrag von „Nio82“ vom 19. Juli 2017, 18:16

@Hunk89

Mach ein @ vor seinen Namen so wie ich bei dir^^ dann bekommt er die Frage schneller mit.


Beitrag von „al6042“ vom 19. Juli 2017, 18:20

Der Recovery Key wird meines Erachtens nur abgefragt, wenn deine AppleID gesperrt wurde.
Zu keinem anderen Zeitpunkt wird dieser Key abgefragt... somit kann der auch nicht zur umgehung des Passworts oder der Multi-Faktor-Authentifizierung genutzt werden.
Der Key erlaubt dir nur die Änderung deines Passworts, sollte Apple dies beim Freischalten deines gesperrten Accounts verlangen.

Beitrag von „Hunk89“ vom 19. Juli 2017, 18:29

> Zitat von Nio82
>
> @Hunk89
>
> Mach ein @ vor seinen Namen so wie ich bei dir^^ dann bekommt er die Frage schneller mit.

Das war Plural für Alle;)

> Zitat von al6042
>
> Der Recovery Key wird meines Erachtens nur abgefragt, wenn deine AppleID gesperrt wurde.
> Zu keinem anderen Zeitpunkt wird dieser Key abgefragt... somit kann der auch nicht zur umgehung des Passworts oder der Multi-Faktor-Authentifizierung genutzt werden.
> Der Key erlaubt dir nur die Änderung deines Passworts, sollte Apple dies beim Freischalten deines gesperrten Accounts verlangen.

Bei iforgot wird auch der Wiederherstellungsschlüssel gefragt.

Beitrag von „al6042“ vom 19. Juli 2017, 18:48

iforgot ist ja das gleiche wie oben erklärt, nur dass du keinen Hinweis von Apple beim fehlgeschlagenen Anmeldeversuch erhältst, sondern damit proaktiv ein vergessenes Passwort auf ein neues Passwort ändern kannst.
Dann ist mir natürlich klar, dass Apple das nur zulässt, wenn du einen Recovery Key vorweisen kannst...
Sonst würde ja jeder einfach so das Kennwort eines anderen Apple-Users ändern können...

Beitrag von „Hunk89“ vom 19. Juli 2017, 19:20

ok. Ich habe zumindest mal das Kennwort von Dropbox und Apple ID geändert.

Gesendet von iPhone mit Tapatalk

Beitrag von „griven“ vom 23. Juli 2017, 02:12

Naja zumindest Apple macht es einem im Moment ja leicht das Kennwort zu ändern man wird ja bei jedem Update oder jeder neuen Installation im Moment zwangserinnert daran

---

Beitrag von „the_viking90“ vom 23. Juli 2017, 07:42

Und eine meiner Mailadressen war dabei.

Beitrag von „vviolano“ vom 23. Juli 2017, 12:33

Ups...


Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Naja. Die Dienste nutze ich eh nicht mehr.

Beitrag von „Hunk89“ vom 4. August 2017, 12:41

Hi liebe Hackintosher,

müssen auch die App Kennwörter erneuert werden?

LG
Hunk

Beitrag von „the_viking90“ vom 4. August 2017, 14:10

Bei dieser Überprüfung wird dir angezeigt von welchen Seiten die IDs gehackt wurden

---

Beitrag von „Nio82“ vom 4. August 2017, 15:01

@Hunk89

App Kennwörter? Meinst du Kennwörter damit die Apps gestartet werden können oder Kennwörter mit denen sich die Apps bei den Online Diensten anmelden?

Wenn du das Passwort deines eMail postfachs geändert hast muss dein eMail Client natürlich auch das neue Passwort kennen um sich einloggen & die eMails abrufen zu können.

Beitrag von „Hunk89“ vom 4. August 2017, 16:43

Die "in App Kennwörter" meine ich 

Gesendet von iPhone mit Tapatalk