

Wichtig! Datenleck

Beitrag von „svenska“ vom 25. Januar 2019 um 10:44

Hallo Gemeinde,

ich weiß es gehört nicht hierher, aber das sollten so viele wie möglich lesen und der Moderator kann es dann vielleicht in die richtige Abteilung verschieben.

Ich möchte keine Panik machen, es sollte nur jeder Nutzer wissen (evtl. Rundmail an alle TF-Nutzer machen?).

ich habe gestern aus gegebenen Anlasse einen Identity Check beim Hasso Plattner Institut durchgeführt und die Email die ich erhielt war wenig erfreulich.

Dort steht dass mein Passwort von dieser Seite beim großen aktuellen Datenleak mit veröffentlicht wurde. Inwieweit das kritisch ist bezüglich Mailadresse klauen usw. mag ich nicht zu beurteilen aber ich möchte es hier mitteilen damit das jeder selber prüfen kann.

Den Check kann jeder selber auf unterschiedlichen Homepages durchführen.

Meine Mail sah so aus, ich habe nur meine Mail unkenntlich gemacht.

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse t.....@gmx.net taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.

Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

touareg-freunde.de Feb. 2017 ✓ 20.617

Betroffen: Diese Daten wurden in der zum angegebenen Zeitpunkt veröffentlichten Identitätsdatenbank der jeweiligen Quelle gefunden.

–: Es wurden keine solche Daten gefunden.

Bei einem *verifizierten* Leak (dargestellt mit ✓) handelt es sich um ein vom Dienstbetreiber bestätigtes Datenleck bzw. das Vorliegen eines Datenlecks beim Dienst ist hochwahrscheinlich.

Bei einem *nicht verifizierten* Leak (fehlendes ✓) ist die Herkunft der Daten und deren Legitimität ungewiss. Solche unverifizierten Daten könnten z.B. aus Sammlungen von Passwörtern oder Kombinationen mehrerer älterer Leaks stammen oder auch generiert sein. Das Vorkommen in einem solchen Leak ist demnach kein sicherer Indikator für ein Datenleck.

Bitte beachten Sie, dass wir aus Sicherheitsgründen keine Auskunft über die konkret betroffenen Daten in den aufgeführten Kategorien geben können.

Wir empfehlen die folgende Reaktion:

- **Password:** Ändern Sie Ihr Passwort für sämtliche Accounts mit der E-Mail-Adresse t.....@gmx.net, bei denen das Passwort älter oder gleich dem angegebenen Datum ist.

Generell gilt, dass je mehr Identitätsdaten über Sie veröffentlicht werden, desto leichter kann Ihre Identität missbraucht werden.

Es ist auf jeden Fall ratsam eine Anzeige beim Diebstahl von Informationen wie Bankdaten, Kreditkartendaten und Sozialversicherungsnummern zu erstatten.

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

[Webseite](#)

Grüße
svenska

Beitrag von „coala“ vom 25. Januar 2019 um 11:06

Servus Svenska,

das Ganze bezieht sich auf den Februar 2017(!) und geistert (nun wieder mal...) aktuell herum. Die Passwörter sind in der Datenbank nur als Hashwert und nicht im Klartext gespeichert, insofern ist es kaum praktisch möglich, diese zu entschlüsseln. Zudem speichern wir ja - außer der Mailadresse - keine personenbezogenen Daten von irgendwelchem Wert. (Ganz im Gegensatz zu vielen anderen Seiten.)

Grundsätzlich empfehlen wir, wie auch allgemein bekannt & angeraten, ein sicheres Passwort zu verwenden (nicht 1234, Geburtsdatum, den eigenen Namen oder den der Kinder, denn damit werden die meisten Passwörter geleakt) und Passwörter grundsätzlich nicht mehrfach zu verwenden, insbesondere nicht bei sensiblen Sachen. Ebenso empfiehlt es sich, Passwörter nach längerer Zeit mal auszutauschen.

Jeder User kann sein Passwort auch bei uns jederzeit ändern, das geht auch ganz einfach:

- Benutzerkontrollzentrum
- Mein Benutzerkonto
- E-Mail & Kennwort ändern

Grüße
Robert

Beitrag von „darkdiver“ vom 25. Januar 2019 um 14:07

Hallo zusammen,

genau wie immer gilt, ein gutes Passwort, öfter mal wechseln und nicht überall das selbe verwenden. Ist unangenehm und aufwendig aber aus meiner Sicht heute leider sinnvoll. Zudem speichern wir keine Daten ausser Login und Passwort. Sonst nicht. Nicht einmal eine Adresse, oder Telefonnummer oder irgendwelche Bankdaten. Es geht also nur um eure Email und das Passwort.

Sinn macht also immer mal das Passwort ändern so oder so 😊

Viele Grüsse
Eric