

## Was ist "Have I been Pwned?"?

Tolleiv Nietsch - 2024-09-08 - Fragen zum Produkt

### Was bedeutet "pwned"?

Das Wort "pwned" (ausgesprochen wie "poned") hat seinen Ursprung in der Hackerkultur und ist eine Abwandlung des englischen Wortes "owned". Die Schreibweise entstand durch einen Tippfehler, bedingt durch die Nähe der Tasten für die Buchstaben "O" und "P" auf der Tastatur. Der Begriff drückt aus, dass jemand kompromittiert oder gehackt wurde. Später wurde das Wort durch die Verwendung in der Videospielszene der breiteren Masse bekannt. Dort drückt es Dominanz über einen Gegner aus, der eine Niederlage erlitten hat ("You just got pwned!"). Ein ausführlicher Artikel über den Ursprung des Wortes findet sich in [diesem Artikel](#).

### Was ist "Have I been Pwned?"?

Die Webseite [haveibeenpwned.com](https://haveibeenpwned.com) stellt eine Datenbank zur Verfügung, die bekannte Datenlecks und Hacks beinhaltet. Wann immer persönliche Informationen und Anmeldedaten im Internet auftauchen, werden diese der Datenbank hinzugefügt. Internetnutzer können die Webseite verwendet, um zu prüfen, ob ihre E-Mail-Adressen und aktuellen Passwörter in einem solchen Datenleck auftauchen und ggf. entsprechende Maßnahmen einleiten.

### Wie nutzt Bare.ID "Have I been Pwned?"?

"Have I been Pwned?" stellt außerdem eine Programmierschnittstelle (API) zur Verfügung, um die Sicherheitsprüfung in eigene Applikationen einzubinden. Bare.ID nutzt diese API, um auf Wunsch zu prüfen, ob Nutzerpasswörter in einem Datenleck aufgetaucht und ggf. zu ersetzen sind. Passwörter, die bei der Verwendung mit anderen Diensten geleakt wurden und auf entsprechenden Listen gelandet sind, können für die Anmeldung an Bare.ID dann nicht mehr verwendet werden. Die Bare.ID-Instanz ist somit gegen Wörterbuch-Attacken, in denen dieselben Passwortlisten verwendet werden, geschützt.

### Werden meine Passwörter bei der Überprüfung zu [haveibeenpwned.com](https://haveibeenpwned.com) übertragen?

Das Klartextpasswort wird niemals übertragen. Das Passwort wird mit einer

kryptographischen Hashfunktion verschlüsselt. Aus diesem Hash (dem Ergebnis dieser Verschlüsselung) lässt sich das Passwort bereits nicht wieder rekonstruieren und nur ein kleiner Teil des Hashes wird zu [haveibeenpwned.com](https://haveibeenpwned.com) übertragen. Details dazu finden sich in der [API-Dokumentation von haveibeenpwned.com](#).

*Detaillierte Anleitungen, wie die "Have I Been Pwned?"-Funktionen in einer Bare.ID-Instanz aktiviert werden können, finden sich im Bare.ID-Handbuch in den Kapiteln [Passwortrichtlinien](#) und [Authentifizierung](#).*