

Berichte | Kontosicherheit

Um zu dein berichten zu gelangen, melde dich im Web Passwortmanager an:

<https://icrar.jwebbi.de>

Die Berichte vom Passwortmanager sind extrem nützlich, um mögliche Schwachstellen in seinen Logins zu finden. Identifiziere und schließe Sicherheitslücken in deinen Online-Konten, indem du auf die Berichte unten klickst.



Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Berichte

Identifiziere und schließe Sicherheitslücken in deinen Online-Konten, indem du auf die Berichte unten klickst.



Kompromittierte Passwörter

Durch Datendiebstahl aufgedeckte Passwörter sind einfache Ziele für Angreifer. Ändere diese Passwörter, um mögliche Einbrüche zu verhindern.



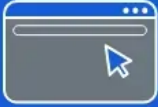
Wiederverwendete Passwörter

Die Wiederverwendung von Passwörtern macht es Angreifern leichter, in mehrere Konten einzubrechen. Ändere diese Passwörter so, dass jedes einzigartig ist.



Schwache Passwörter

Schwache Passwörter können von Angreifern leicht erraten werden. Ändere diese Kennwörter mithilfe des Passwort-Generators in sichere Passwörter.



Ungesicherte Websites

URLs, die mit http:// beginnen, verwenden nicht die bestmögliche Verschlüsselung. Ändere die Anmelde-URLs für diese Konten zu https:// für sicheres Surfen.



Inaktive Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dir bei der Absicherung deiner Konten hilft. Wenn eine Webseite 2FA anbietet, solltest du es immer aktivieren.



Datendiebstahl

Kompromittierte Konten können deine persönlichen Daten preisgeben. Sichere kompromittierte Konten, indem du 2FA aktivierst oder ein sicheres Passwort erstellst.

Hier hast du 6 verschiedenen Check zur Auswahl, wir werden jeden Check durchgehen und genau angucken.

1. Kompromittierte Passwörter

Dieser Bericht überprüft, ob eines deiner gespeicherten Passwörter in bekannten Datenlecks veröffentlicht wurde. Solche Passwörter sind besonders anfällig, da Angreifer sie aus öffentlich zugänglichen Datenbanken entnehmen können. Wenn ein Passwort als kompromittiert markiert wird, solltest du es sofort ändern. Nutze dabei ein starkes, einzigartiges Passwort, das du mit dem integrierten Passwort-Generator erstellen kannst.

Durch Datendiebstahl aufgedeckte Passwörter sind einfache Ziele für Angreifer. Ändere diese Passwörter, um mögliche Einbrüche zu verhindern.

Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Kompromittierte Passwörter

Durch Datendiebstahl aufgedeckte Passwörter sind einfache Ziele für Angreifer. Ändere diese Passwörter, um mögliche Einbrüche zu verhindern.

Auf kompromittierte Passwörter prüfen

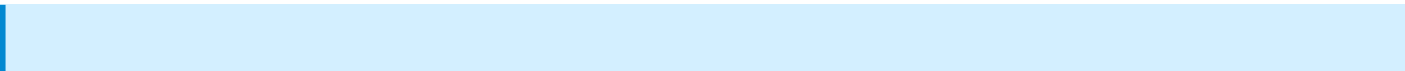
⚠ ES WURDEN KOMPROMITTIERTE PASSWÖRTER GEFUNDEN

Wir haben 10 Einträge in deinem/deinen vault gefunden, die Passwörter enthalten, die in bekannten Passwortdiebstahl-Datenbanken veröffentlicht wurden. Du solltest diese ändern und ein neues Passwort verwenden.

Name	Besitzer	
[Name]	Ich	4.957.283 mal kompro...
[Name]	Ich	4.957.283 mal kompro...
[Name]	Ich	2.701 mal kompromitti...
[Name]	Ich	3.420 mal kompromitti...
[Name]	Ich	2.701 mal kompromitti...
[Name]	Ich	4 mal kompromittiert
[Name]	Ich	8.767 mal kompromitti...
[Name]	Ich	2.406 mal kompromitti...
[Name]	Ich	582 mal kompromittiert
[Name]	Ich	9.065 mal kompromitti...

2. Wiederverwendete Passwörter

Die Wiederverwendung desselben Passworts für mehrere Konten ist riskant. Wenn ein Konto gehackt wird, können Angreifer leicht auf andere Konten zugreifen, die dasselbe Passwort verwenden. Dieser Bericht zeigt dir, welche Passwörter mehrfach verwendet werden. Du solltest für jedes Konto ein individuelles Passwort erstellen, um dieses Risiko zu minimieren.



Die Wiederverwendung von Passwörtern macht es Angreifern leichter, in mehrere Konten einzubrechen. Ändere diese Passwörter so, dass jedes einzigartig ist.

Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Wiederverwendete Passwörter

Die Wiederverwendung von Passwörtern macht es Angreifern leichter, in mehrere Konten einzubrechen. Ändere diese Passwörter so, dass jedes einzigartig ist.

⚠ **WIEDERVERWENDETE PASSWÖRTER GEFUNDEN**

Wir haben 36 Passwörter in deinem/deinen vaults gefunden, die mehrfach verwendet werden. Du solltest diese ändern und einzigartige Passwörter verwenden.

Alle 36

Ich 33

Name	Besitzer	
	Ich	2 Mal wiederverwendet
	Ich	2 Mal wiederverwendet
	Ich	2 Mal wiederverwendet
	Ich	7 Mal wiederverwendet
	Ich	7 Mal wiederverwendet
	Ich	7 Mal wiederverwendet
	Ich	2 Mal wiederverwendet

3. Schwache Passwörter

Schwache Passwörter sind leicht zu erraten, insbesondere wenn sie einfache Muster, Wörter oder Zahlenfolgen enthalten. Der Bericht identifiziert solche Passwörter und hilft dir, sie durch sicherere Alternativen zu ersetzen. Ein starkes Passwort sollte mindestens 14 Zeichen lang sein und eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

Schwache Passwörter können von Angreifern leicht erraten werden. Ändere diese Kennwörter mithilfe des Passwort-Generators in sichere Passwörter.

Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Schwache Passwörter

Schwache Passwörter können von Angreifern leicht erraten werden. Ändere diese Kennwörter mithilfe des Passwort-Generators in sichere Passwörter.

SCHWACHE PASSWÖRTER GEFUNDEN
Wir haben 17 Einträge in deinem/deinen vaults mit unsicheren Passwörtern gefunden. Du solltest diese ändern und sicherere Passwörter verwenden.

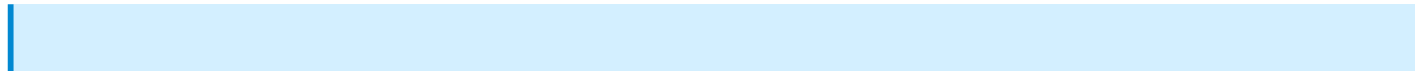
Alle 17

Ich 15

Name	Besitzer	
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
		Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Sehr schwach
	Ich	Schwach
	Ich	Schwach

4. Ungesicherte Websites

Websites, die mit "http://" beginnen, verwenden keine verschlüsselte Verbindung. Das bedeutet, dass Daten, die du auf diesen Seiten eingibst, wie Passwörter oder persönliche Informationen, von Dritten abgefangen werden können. Der Bericht zeigt dir, welche URLs in deinem Tresor unsicher sind. Du solltest diese auf "https://" aktualisieren oder die Website meiden, falls keine sichere Verbindung verfügbar ist.



URLs, die mit http:// beginnen, verwenden nicht die bestmögliche Verschlüsselung. Ändere die Anmelde-URIs für diese Konten zu https:// für sicheres Surfen.



Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Ungesicherte Websites

URLs, die mit http:// beginnen, verwenden nicht die bestmögliche Verschlüsselung. Ändere die Anmelde-URIs für diese Konten zu https:// für sicheres Surfen.

UNGESICHETERTE WEBSITES GEFUNDEN

Wir haben 28 Einträge in deinem/deinen vaults mit ungeschützten URIs gefunden. Du solltest deren URI-Präfix in https:// ändern, wenn die Webseite dies zulässt.

Alle 28

Ich 26

Name	Besitzer
	Ich
	Ich
	Ich
	Ich

5. Inaktive Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu, indem sie neben dem Passwort einen zweiten Faktor wie einen Code oder eine biometrische Bestätigung erfordert. Der Bericht zeigt dir, bei welchen deiner gespeicherten Konten 2FA nicht aktiviert ist. Wenn verfügbar, solltest du 2FA aktivieren, um deine Konten besser zu schützen.

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dir bei der Absicherung deiner Konten hilft. Wenn eine Webseite 2FA anbietet, solltest du es immer aktivieren.

Tresore
Send
Werkzeuge
Generator
Daten importieren
Tresor exportieren
Berichte
Einstellungen

Inaktive Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dir bei der Absicherung deiner Konten hilft. Wenn eine Webseite 2FA anbietet, solltest du es immer aktivieren.

ZUGANGSDATEN OHNE 2FA GEFUNDEN

Wir haben 40 Website(s) in deinem/deinen vaults gefunden, die eine Zwei-Faktor-Authentifizierung anbieten (laut 2fa.directory), aber bei denen diese Funktion möglicherweise nicht aktiviert ist. Um diese Konten weiter abzusichern, solltest du die Zwei-Faktor-Authentifizierung aktivieren.

Alle 40Ich 37

Name	Besitzer	
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
	Ich	Anleitung
		Anleitung
	Ich	Anleitung

6. Datendiebstahl

Dieser Bericht überprüft, ob eines deiner Konten in einem Datenleck kompromittiert wurde. Wenn ein Konto betroffen ist, solltest du sofort das Passwort ändern und, falls noch nicht geschehen, 2FA aktivieren. Dies hilft, den Schaden zu begrenzen und zukünftige Angriffe zu verhindern.

Kompromittierte Konten können deine persönlichen Daten preisgeben. Sichere kompromittierte Konten, indem du 2FA aktivierst oder ein sicheres Passwort erstellst.

**Vaultwarden**
Password Manager

Tresore

Send

Werkzeuge

Generator

Daten importieren

Tresor exportieren

Berichte

Einstellungen

Datendiebstahl

Kompromittierte Konten können deine persönlichen Daten preisgeben. Sichere kompromittierte Konten, indem du 2FA aktivierst oder ein sicheres Passwort erstellst.

Benutzername

Prüfen Sie alle Benutzernamen und E-Mail-Adressen, die Sie verwenden.

Auf Datendiebstähle prüfen

GUTE NEUIGKEITEN

wurde in keinem der bekannten Datendiebstahlvorfällen gefunden.

Zurück zu den Berichten

Version #1

Erstellt: 20 Oktober 2025 07:31:24 von craftman96

Zuletzt aktualisiert: 20 Oktober 2025 07:33:13 von craftman96