

使用しているパスワードが流出済か確認してみませんか

パスワードを決めるとき、『以前に使用したパスワードを使わない』こととされています。

なぜなら、サイバー犯罪者らは何億個もの流出済みのパスワードのリストを持っており、流出済みのパスワードのリストに、同じく流出済みのメールアドレスを合わせることで、あらゆるサービスに忍び込もうとしているからです。すなわち、以前に使用したパスワードが流出していたら、たとえそれを他人が使用していたとしても、それを新しいアカウントに使用するとアカウントを乗っ取られる恐れがあるからです。

新しく使用する予定のパスワードがすでに流出しているかを確認できるウェブサイトがあります。

名前は『Pwned Password』といい URL は <https://haveibeenpwned.com/Passwords> です。すでに流出されているかどうかの判定は、流出済の 5 億件のパスワードと入力されたパスワードと突き合わせで行われます。

パスワードを入力し『pwned?』ボタンをクリックしすると、突き合わせ結果が、過去に流出がなければ『Good news – pwnage found』、過去に流出があれば『Oh no – pwned』と流出件数が表示されます。

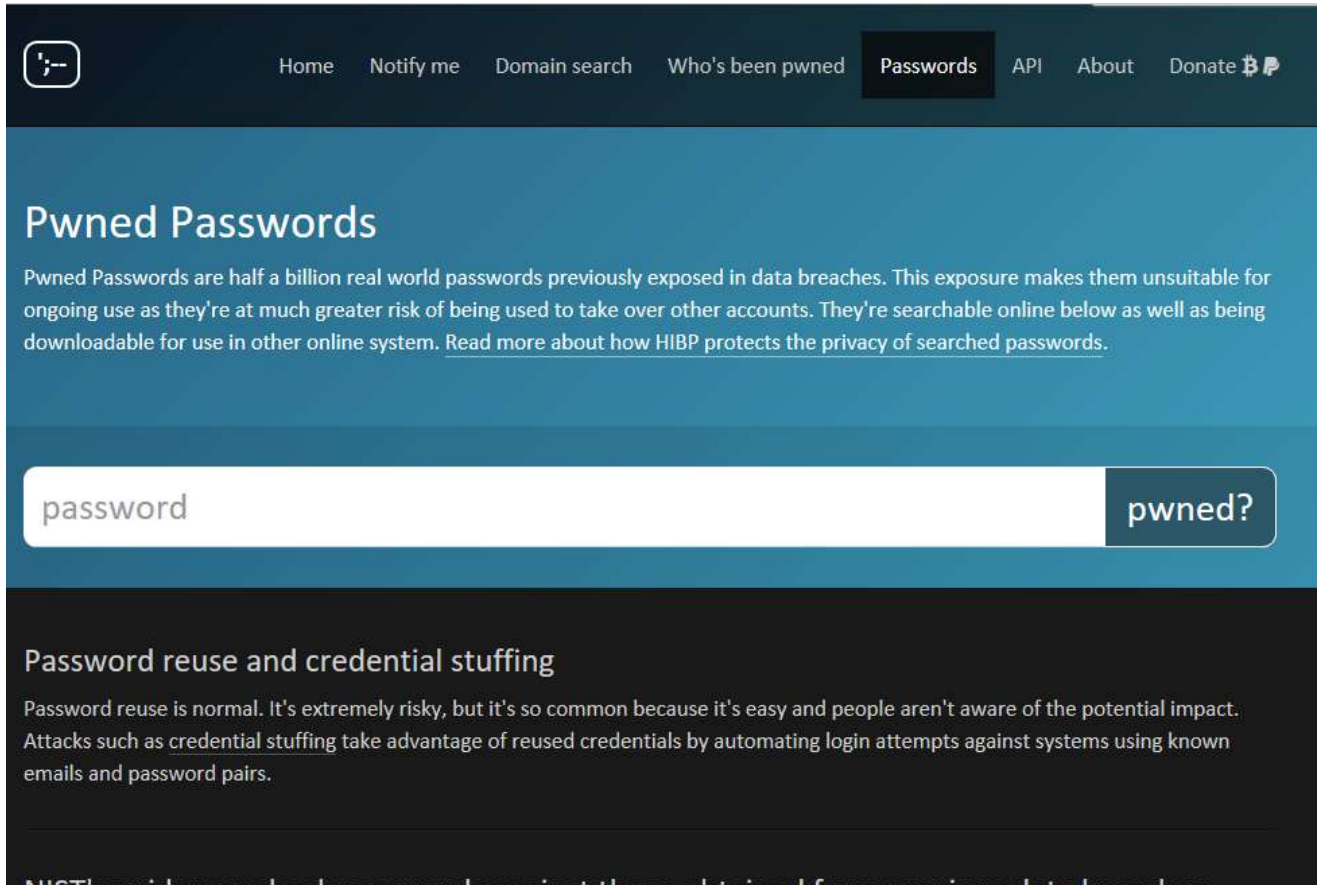
『Oh no – pwned』と表示されたパスワードは避けるほうが良いのではないのでしょうか。

注

『pwned』とは、『大失敗』または『ボロ負けした』というスラングです。

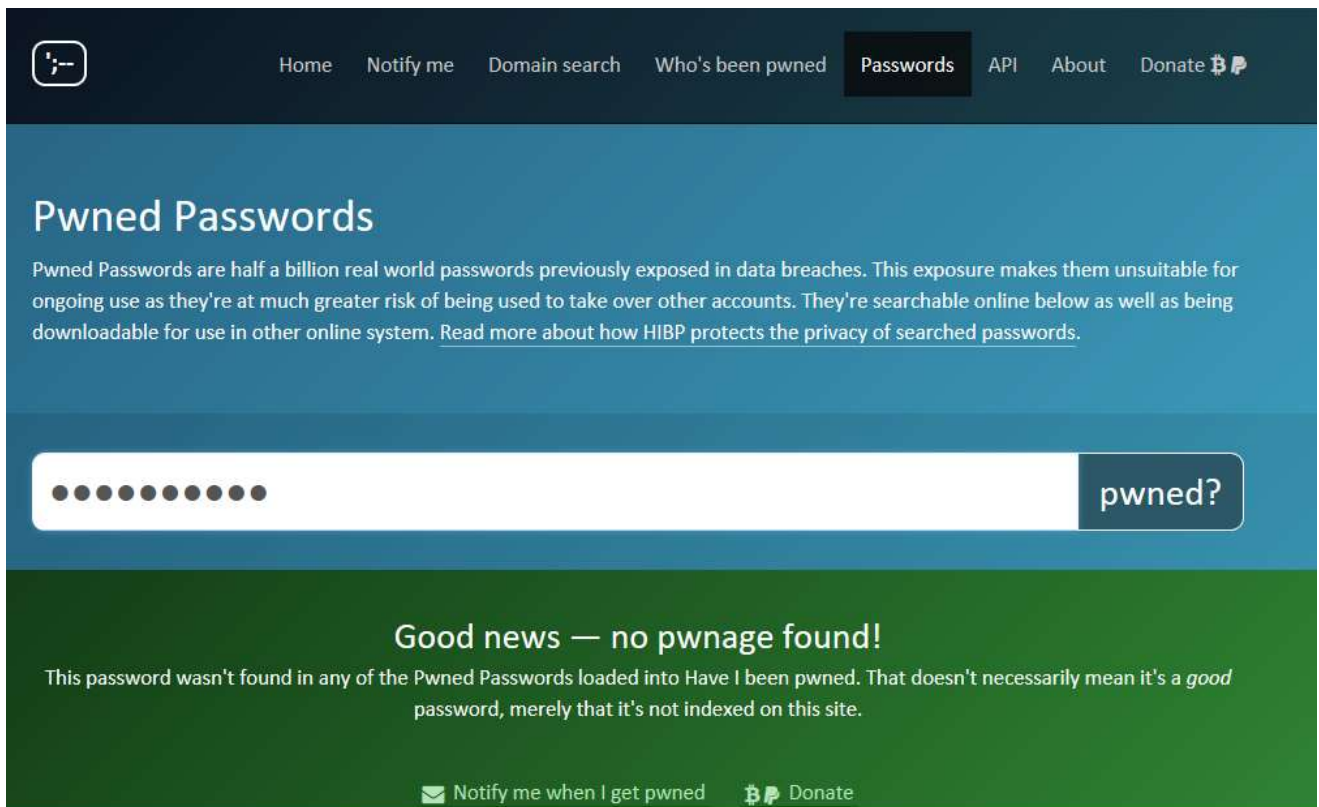
『pwnage』とは、『圧勝』というスラングです。

パスワード入力画面



The screenshot shows the top navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords (highlighted), API, About, and Donate. Below the navigation is a blue header with the title "Pwned Passwords" and a paragraph explaining that pwned passwords are half a billion real-world passwords previously exposed in data breaches. A search input field contains the text "password" and a "pwned?" button. Below the search field is a section titled "Password reuse and credential stuffing" with a paragraph explaining that password reuse is normal but risky, and attacks like credential stuffing take advantage of reused credentials.

過去に流出がない場合の画面



The screenshot shows the same top navigation bar. Below the navigation is a blue header with the title "Pwned Passwords" and a paragraph explaining that pwned passwords are half a billion real-world passwords previously exposed in data breaches. A search input field contains ten black dots, indicating a password was entered but not found. A "pwned?" button is visible. Below the search field is a green section with the title "Good news — no pwnage found!" and a paragraph explaining that the password wasn't found in any of the pwned passwords loaded into Have I been pwned. At the bottom, there are links for "Notify me when I get pwned" and "Donate".

過去に流出があった場合の画面

The screenshot shows the 'Pwned Passwords' search interface. At the top, there is a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords (highlighted), API, About, and Donate. Below the navigation bar, the main heading is 'Pwned Passwords'. A paragraph explains that pwned passwords are half a billion real-world passwords previously exposed in data breaches, making them unsuitable for ongoing use. Below this text is a search input field with a password mask (represented by dots) and a 'pwned?' button. The search results area has a dark red background and displays the message: 'Oh no — pwned! This password has been seen 7,016,669 times before'. A warning message states: 'This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!'. At the bottom, there are links for 'Notify me when I get pwned' and 'Donate'.