

# **Password Monitor is available in Microsoft Edge**

Password Monitor is the latest feature Microsoft has added to its browser to help Edge users protect their online privacy and security. Each year, hundreds of millions of personal credentials are exposed online in third-party data breaches and end up for sale on the online black market, often referred to as the Dark Web. Leaked usernames and passwords can be used to gain access to your online accounts via “credential stuffing” attacks. In these attacks, automated scripts are used to try different username and password combinations with the goal of hijacking accounts.

Though users are warned not to reuse the same pair of credentials for more than one account, it’s a common practice. This leaves them vulnerable on multiple sites when breaches occur.

While it’s impossible to prevent leaks from ever happening, you can now browse with more peace of mind, knowing Microsoft Edge has your back with Password Monitor, designed to help you keep your online accounts secure.

## **How Password Monitor works**

After you save your username and password credentials to the browser, Microsoft Edge will begin proactively monitoring them for matches against credentials leaked to the Dark Web.

It checks the credentials you’ve saved in Microsoft Edge against an ever-growing database of usernames and passwords that are known to have been breached, collected by a network of researchers, law enforcement agencies, security teams at Microsoft and other trusted sources. The check is done using enterprise-grade encryption and privacy-preserving techniques. When a match has been found, the unsafe passwords will be displayed on the Password Monitor page.

Password Monitor is turned off by default and a few steps are required to turn it on.

Open Edge > Go to Settings > Profiles> Passwords and turn on the toggle next to Show alerts when passwords are found in an online leak.