|  |
| --- |
| Using Edge Password Manager |

# Using Edge Password Manager

## Background and benefit

Microsoft Edge has advanced password protection features built into it.

It securely stores your passwords and syncs them across devices. It also uses strong encryption and two-factor authentication to protect your data. This is done locally on your device, to protect sensitive data like passwords, credit card numbers and cookies.

It also auto-fills log-in details for websites, making it easier to access your accounts. Because you don’t need to remember all your passwords, you can create unique and complex passwords for each site. You can enable the in-built password generator and ask it to suggest a strong, randomly generated password. This reduces the risk of password reuse and enhances security.

Edge Password Manager only auto-fills passwords on legitimate sites. This helps prevent phishing attacks from fake websites.

The browser also scans your password to determine if it has been compromised in any data breaches, which keeps you informed about the security of your accounts.

## What your staff will need to do

If staff are using the latest version of Windows and are logging in using their Microsoft 365 account, Microsoft Edge Password Manager will automatically be enabled and will sync their passwords across all their devices.

## More resources

For more information, see [How to keep your passwords safe with Microsoft Edge](https://www.youtube.com/watch?v=G6zGupsRwNQ&list=PL4z1-7pjJU6yD5Ljecgo1vPUZwzCQ7OIM&index=6).

For help troubleshooting Edge sync, see [Diagnose and fix Microsoft Edge sync issues](https://learn.microsoft.com/en-us/deployedge/microsoft-edge-troubleshoot-enterprise-sync).