1Password is introducing a new phishing prevention feature

When a 1Password user clicks a link and opens a website with a URL that doesn’t match the one they have saved alongside login details, the 1Password browser extension will do two things. It won’t autofill their login credentials, and it will display a pop-up warning explaining that the current website’s URL “isn’t linked to a login in 1Password.”

The feature isn’t a foolproof way to stop phishing attacks from succeeding. Users can still choose to manually copy and paste their credentials into a suspicious website. But it will make them aware that they’re potentially dealing with a phishing scam with the hope that they will think twice and exercise more caution before proceeding.

The new phishing prevention feature is being rolled out to users starting today, but it could take several weeks for it to be available to everyone. For individual and family plan users, 1Password is enabling this feature by default once it’s available. For businesses it will need to be manually enabled by 1Password Admins.

https://www.theverge.com/tech/864980/1password-security-phishing-attack-prevention-password-browser-extension-scammers