# OIDC vs SAML

SAML and OIDC are two identity protocols that authenticate users, transmit data, and provide access control information and a communication method for a user's ID. SAML is most commonly utilized by businesses to allow customers to access paid services, whereas OIDC is best suited for mobile and single-page web applications

Enterprises that adopt SAML must use a SAML-based IdP to authenticate users. When a user requests access, the SP asks the IdP to authenticate the user, and the IdP returns an assertion to the SP. If authentication is successful, the IdP grants the user access to multiple web applications based on a single set of login credentials.

OIDC uses a public, third-party IdP to authenticate users. Examples of IdPs that support OIDC include Google, Microsoft, and Amazon. With OIDC, a user can gain access to an application by signing on with a trusted, OIDC-compatible account.

# Real scenario

A phishing attack is a way for hackers to steal user data, including login credentials, encryption details, and even credit card numbers

OIDC

Because OIDC allows users to sign on to an application through a trusted third party such as Google, users can skip the step of signing up for an account on that application. If no account exists for that user, there are no login credentials for a hacker to exploi

SAML

SAML protects against phishing attacks by storing the user’s identity, location data, timestamps, and validity conditions within an encrypted SAML assertion. The IdP can then return the SAML assertion to the service provider, granting the user access to the requested applications.

Idp for identity provider

Open ID connect